U N I V E R Z I T E T U B E O G R A D U

Dr ĐURO KUREPA
profesor Univerziteta u Beogradu

VIŠA ALGEBRA

KNJIGA PRVA

DRUGO IZDANJE, ISPRAVLJENO I DOPUNJENO

ZAVOD ZA IZDAVANJE UDŽBENIKA
SOCIJALISTIČKE REPUBLIKE SRBIJE
B E O G R A D

Ovaj udžbenik, kao stalni univerzitetski udžbenik, odobrila je za upotrebu Komisija za udžbenike Univerziteta u Beogradu svojim rešenjem broj 06-2013/1
od 2. jula 1969. godine

U SPOMEN
MOJIM RODITELJIMA

PREDGOVOR DRUGOM IZDANJU

Prvo izdanje Više algebre I, II rasprodano je u vremenu od dve godine. Potreba za novim izdanjem je stvarna. Pristupamo novom izdanju. Ono se od prvog razlikuje što su ispravljene uočene greške.

Kao odraz mojega mišljenja o jedinstvu srpskohrvatskog jezika[1)]*, terminologija i tekst su ostali skoro nepromenjeni, iako su pojedini termini više u upotrebi u jednim krajevima Jugoslavije a drugi u drugim krajevima Jugoslavije. Tipičan primer u tom pogledu pružaju reči jednadžba i jednačina. One danas znače jedno te isto. Obe se mnogo upotrebljavaju, iako lično mislim da bi ispravnije bilo govoriti o jednačidbama ili jednáčnjama kao sinonimima. Vrlo bi dobro došla i reč jednačenje.*

Srdačno se zahvaljujem stručnjacima i studentima koji su mi skrenuli pažnju na pojedine greške u 1. izdanju. Posebnu zahvalnost dugujem kolegama dr Veselinu Periću (Univerzitet u Sarajevu) i dr Slaviši Prešiću (Beograd): oni su pažljivo čitali 1. izdanje i ukazali na brojne ispravke; srdačno zahvaljujem drugu Petroniju Milojeviću (Skoplje), kolegi Miodragu Trifunoviću (Beograd) te studentu Gojku Kalajdžiću.

Bit ću zahvalan svakom onom koji mi i ubuduće pruži bilo kakav prilog, ukaže na grešku, predloži kakvu izmenu, itd.

Beograd, 27. jun 1969. *Đuro Kurepa*

[1)] Kad bi se po nekoj osnovi proglasilo da su srpski jezik i hrvatski jezik dva različna jezika, moglo bi se na sličnoj osnovi proglasiti da se npr. nemački jezik raspada na desetak različitih nemačkih jezika pa bi se spisi, knjige, ... trebali prevoditi sa jedne inačice (varijante) nemačkog jezika na desetak drugih inačica toga jezika! Slično bi vredilo za francuski jezik, engleski jezik, itd.

U V O D

Ovo djelo, Viša algebra, nastalo je kao plod višegodišnjih predavanja na Prirodoslovno-matematičkom fakultetu u Zagrebu, i to na II i III stupnju; o pojedinim dijelovima, posebno o matricama i algebarskim strukturama, predavao sam i na Prirodno-matematičkom fakultetu u Beogradu ljetnog semestra školske godine 1951/52.

Djelo je namijenjeno studentima matematike, mehanike i fizike na prirodoslovno-matematičkim fakultetima. Kao pomoćno djelo korisno će poslužiti studentima i stručnjacima iz raznih struka i institucija, specijalno onima sa elektrotehničkih, strojarskih, geodetskih fakulteta te viših pedagoških škola. Detaljan stvarni sadržaj kao i abecedni sadržaj olakšat će korisniku da u knjizi brzo nađe ono što mu treba.

Cilj je djela da se studentu i drugim korisnicima pruži osnovni algebarski materijal kako bi se s njim mogao služiti u raznim drugim oblastima unutar matematike i van matematike.

Naime, razvitak nauke i tehnike u vezi je sa sve većom potrebom matematičkog aparata uopće, a algebarskog napose pa su spregovi između nauke i tehnike s jedne strane i matematike s druge strane u međusobnom vrlo plodotvornom i korisnom djelovanju. Pri tom, algebra i algebarske metode imaju vanredno važnu ulogu pa smo svjedoci na kako se sve novim oblastima ljudske djelatnosti očitava povezanost s matematičkim rasuđivanjima i metodama. Od prirodnih, ekonomskih, socijalnih i humanih nauka pa do teorije igara, strategije, strojeva, teorije jezika, informacije, nastave i kibernetike, svuda su nikle ili su u začetku matematičke metode uopće i algebarske strukture posebno.

Posebno, svako odvijanje u prirodi i u mislima nosi pojedine matematičke i algebarske pravilnosti; odatle i potreba da se razrade pojedine matematičke, odnosno algebarske strukture. Broj tih struktura naravno neprestano raste, no u tom nastajanju neke su tekovine (npr. broj, vektor, tenzor, grupoid, grupa, prsten, vektorski prostor, tijelo, linearni operator, uređenost, relacije) dobro zacrtane.

Nastojao sam da ti pojmovi budu jasno obrađeni. Grupama i matricama posvećena je osobita pažnja. Također sam nastojao da numeričkim izračunavanjima i konkretnim situacijama bude dana odgovarajuća važnost.

Djelo je podijeljeno u dvije knjige. Prva knjiga obuhvata poglavlja 1—22.

Druga knjiga obuhvata preostalih 13 poglavlja, tj. poglavlja 23—35.

Nadalje druga knjiga obuhvata Treći dio djela: Dodaci, ispravke, rješenja i upute za rješavanje zadataka.

Zasad su dana rješenja samo nekih zadataka.

Pojedine dijelove rukopisa, odnosno korektura pročitali su: dr Vladimir Devidé, dr Svetozar Kurepa, magistar Mirko Mihaljinec, viši predavači Veselin Perić, Milenko Vučkić; na svim primjedbama ja im srdačno zahvaljujem; posebno se zahvaljujem drugu M. Mihaljincu na uloženu trudu pri redigiranju rješenja zadataka i abecednog sadržaja.

Zahvaljujem slagarima, drugovima Velebitu Biseru i Vladimiru Tončiću što su pridonijeli da djelo grafički bude što bolje opremljeno.

Zahvaljujem Komisiji za izdavanje udžbenika i skripata na Sveučilištu u Zagrebu jer je ona novčanom dotacijom omogućila da djelo bude financijski dostupnije.

Svjesni smo poteškoća u sastavljanju i pisanju tako obimnog djela koje bi obuhvatilo čitavu algebru. Znamo da djelo ima nedostataka i grešaka; neke su i naznačene, odnosno ispravljene; bit ćemo zahvalni svakom onom tko nam skrene pažnju na bilo koji nedostatak, grešku, odnosno na koristan prijedlog koji bi se mogao uzeti u obzir pri eventualnom drugom izdanju djela.

Zagreb, mjeseca maja 1965. *ĐURO KUREPA*

SADRŽAJ PO DIJELOVIMA I POGLAVLJIMA

KNJIGA PRVA

P r v i d i o

KNJIGA DRUGA

D r u g i d i o

Dalja izgradnja matričnog računa i nekih drugih dijelova algebre

Treći dio

SADRŽAJ

PRVI DIO

(poglavlja 1—22)

Poglavlje 1.

Algebra logike (3—16)

Poglavlje 2.

Skup i elementi skupova. Algebra skupova (17—38)

Poglavlje 3.

Algebra funkcija (39—82)

Poglavlje 4.

Vrste brojeva (83—108)

Poglavlje 5.

Algebarske jednadžbe stupnja 1, 2, 3, 4 s jednom nepoznanicom (109—150)

Poglavlje 6.

Kolo ili prsten cijelih racionalnih brojeva (151—252)

Poglavlje 7.

Kolo ili prsten algebarskih polinoma (253—284)

Poglavlje 8.

Uvod u sisteme linearnih jednadžbi. Pojam rješenja (285—296)

Poglavlje 9.

Sistem linearnih jednadžbi s općim koeficijentima. Pojava determinante (297—320)

Poglavlje 10.

Prvi uvod u račun matrica (321—359)

Poglavlje 17.

Teorija grupa (567—672)

Poglavlje 18.

Korijeni jedinice. Dijeljenje kruga. Pravilni n-vrhovi (673—688)

Poglavlje 19.

Simetrične funkcije (689—706)

KONAC I DIJELA

PRVI DIO

POGLAVLJE 1.

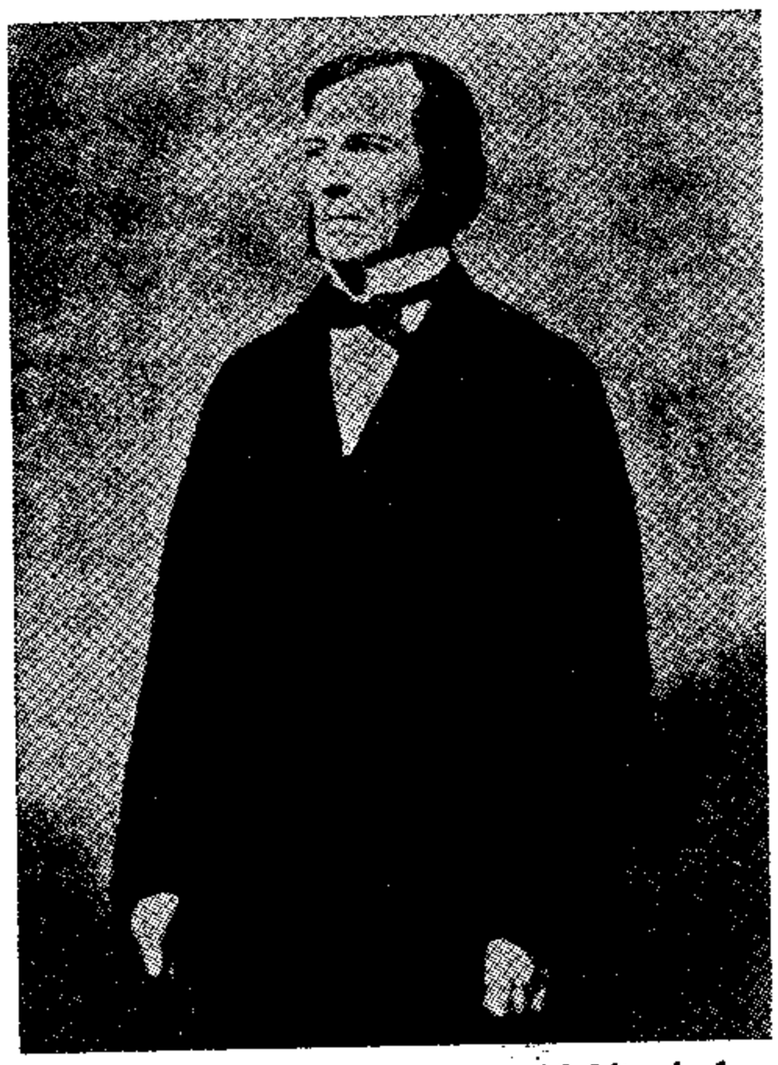
ALGEBRA LOGIKE[1)]

0. PREGLED

Relativno se kasno primijetilo kako se često u matematici pojavljuju riječi: „ne“, „i“, „ili“, „uključuje“, „onda i samo onda“ te neodređene zamjenice: svako(je), neko(je), niko(je). Danas je to svjesno izučeno pa to saznanje mnogo olakšava i pojednostavnjuje studij matematike.

S *logičkim sudovima* ili *rečenicama* »*računamo*« kao i s raznim drugim matematičkim predmetima: iz zadanih sudova proizvodimo druge sudove služeći se „logičkim operacijama“ kao što su: negacija, konjunkcija, disjunkcija. Tako dolazimo do osnovnih logičkih funkcija, koje se zovu: *negacija*, *konjunkcija*, *disjunkcija*, *implikacija* i za koje upotrebljavamo oznake $\neg$ (čitaj „nije“), $\wedge$ (č. i), $\vee$ (č. ili), $\Rightarrow$ (ili $\supset$) (č. uključuje).

Zanimljivo je da negacija konjunkcije ili sastava (rastava) daje disjunkciju, rastav (konjunkciju, sastav), a da negacija pojma „svako“ (neko) daje „neko“ (svako).



G. Boole (č. Bul; 1815—1864), jedan od osnivača matem. logike

1. PRVA LOGIČKA FUNKCIJA. NEGACIJA. ZNAK $\neg$ ZA NEGIRANJE

Svakom logičkom sudu (izreci, rečenici, iskazu, ...) x pridružujemo negaciju $\neg x$ suda x. Znak $\neg$ stoji za negiranje „ne“, „nije istina“ i sl.; znak $\neg$ podsjeća na — (minus).

1.1. Za $x =$ „Kiša pada“ imamo: $\neg x = \neg$ „Kiša pada“ = „Nije istina da kiša pada“, tj. „Kiša ne pada“, Tu bi $\neg(\neg x)$ značilo: „Nije istina da nije istina da kiša pada“, dakle „kiša pada“; tj. $\neg(\neg x) = x$.

1.2. $\neg(1>2) =$ nije $1>2$.

[1)] Na ovo poglavlje neka se čitalac navrati s vremena na vrijeme.

1.3. Ako znak x stoji za rečenicu: „$\triangle$ *ima* 2 *jednaka kuta*“, onda $\neg x$ znači negaciju te rečenice, dakle znači: $\triangle$ *nema dva jednaka kuta.*

Prema tome, svakom skupu S logičkih sudova pridružujemo skup $\neg S$ negacijâ $\neg x$ sudova x iz S. Naravno, ako je x sud iz S, ne mora $\neg x$ biti član u S.

1.4. Zadaci o negaciji. Navedi nekoliko rečenica; napiši negaciju tih rečenica.

2. ARITMETIČKA VRIJEDNOST SUDA; v-FUNKCIJA

Engleski matematičar George Boole [Džordž Bul] (1815—1864) otkrio je da je *vrlo korisno svakom istinitom sudu pridružiti broj* 1 *kao njegovu vrijednost, a svakom lažnom sudu pridružiti broj* 0 *kao* (*aritmetičku*) *vrijednost*. Na taj način, za neku izreku a simbolička jednakost $va = 1$ označuje rečenicu: »*a je istinito*«; slično, $va = 0$ stoji umjesto rečenice: »*a je lažno*«.

G. W. Leibnitz (č. Lajbnic; 1646—1716) jedan od preteča u razvitku matematičke logike

Odmah se vidi ovo: ako je $va = 0$, onda je $v(\neg a) = 1$; ako je $va = 1$, onda je $v(\neg a) = 0$. Kraće: $v(\neg a) = 1 - va$, tj,

$$va + v(\neg a) = 1.$$

Ili još kraće: $\neg 0 = 1$, $\neg 1 = 0$.

2.1. Zadaci o v-funkciji.

1. Odredi vx ako x označuje ovaj sud: 1) $3 < 7$; 2) $-3 > -7$; 3) 0 je pozitivan broj; 4) 0 nije ni pozitivan ni negativan broj; 5) Svaki kvadrat je pravokutnik; 6) Svaki pravokutnik je trapez; 7) SSSR je najprostranija i najnapučenija država; 8) Posjetio sam planetu Veneru; 9) Kvadratura kruga je moguća pomoću ravnala i šestara.
2. Iskaži $\neg x$ za sudove 1—9. iz prethodnog zadatka; nađi $v\neg x$.

3. PRVA LOGIČKA FUNKCIJA S DVIJE PROMJENLJIVE: KONJUNKCIJA ILI SASTAVLJANJE ILI LOGIČKO MNOŽENJE (SJEČENJE, PRESJEK, IOVANJE). OPERATOR $\wedge$

Ako je a neka rečenica isto kao i b, onda je također

a i b

određena rečenica. Ako npr. a znači »*Idem u šetnju*«; ako b stoji umjesto izreke: »*Uživam u prirodi* onda

a i b, simbolički $a \wedge b$

stoji umjesto izreke:

$$\underbrace{\textit{Idem u šetnju}}_{a} \quad \text{i} \quad \underbrace{\textit{uživam u prirodi}}_{b}.$$

3.1. *Definicija konjunkcije. Konjunkcija dvaju ili više zadanih sudova nastaje tako da te sudove spojimo veznikom »i«, a formalno tako da među oznake zadanih sudova stavimo znak* $\wedge$ *(izvrnuto* V*) ili* & (lat. *et* = *i*).

Konjunkcija zadanih sudova istinita je onda i samo onda ako je istinit ***svaki*** *od tih sudova.*

Ta se definicija može kraće izreći ovako:

$$v(a \wedge b) = \inf \{v\,a,\ v\,b\}.$$

3.2. Uopće, *za svaku obitelj O sudova definiramo konjunkciju ili sastav* $\wedge O$ *kao sud za koji je* $v(\wedge O) = \inf\limits_{x} vx$, *pri čemu x prolazi kroz O.*

Za sudove *a*, *b* možemo to označiti pomoću tablice ovako:

a	0	0	1	1
b	0	1	0	1
$a \wedge b$	0	0	0	1

ili ovako

$x \wedge y$	$\rightarrow$ 0	1
$\downarrow$		
0	0	0
1	0	1

ili još kraće ovako:

$\wedge$	0	1
0	0	0
1	0	1.

Tako npr. za sudove *a*, *b*, *c* pripadna konjunkcija glasi:

$$a \wedge b \wedge c \text{ (č. } i \text{ a } i \text{ b } i \text{ c)}.$$

3.3. Zadaci o konjunkciji

1. Odredi aritmetičku vrijednost ovih sudova:
   1) $(1<2) \wedge (2<5)$; 2) $(1<3) \wedge (-3<-2)$; 3) $(0<-1) \wedge (\pi$ je broj);
   4) (Descartes [Dekart] je bio veliki filozof) $\wedge$ (Demosten je bio odličan govornik); 5) $\neg(1<2) \wedge (\pi<9)$; 6) $\bigwedge\limits_{n} (n<n+1)$.
2. Izračunaj: 1) $1 \wedge 0 \wedge 1$; 2) $1 \wedge \neg 0$; 3) $1 \wedge 1 \wedge 1 \wedge 1$; 4) $0 \wedge 0 \wedge 0$; 5) $(0 \wedge 0) \wedge \neg 0$.

4. DISJUNKCIJA ILI RASTAVLJANJE DVAJU SUDOVA. OPERATORI $\vee$, $\underline{\vee}$

4.1. Definicija. *Ako je* (*a*, *b*) *uređen par logičkih sudova, onda disjunkcija* ili *rastavljanje tih sudova a, b jest sud: a ili b*, simbolički: *»a* $\vee$ *b«; on je istinit onda i samo onda ako je istinit* ***najmanje jedan*** *od zadanih sudova a, b. Disjunkcija sudova a, b čita se a ili b* (latinski: *a* vel *b*) i označuje sa $a \vee b$ (znak $\vee$ je malo $\vee$, početno slovo latinske riječi vel = ili).

Prema tome, imamo ove operacije rastavljanja:

$$0 \vee 0 = 0 \qquad 1 \vee 0 = 1$$
$$0 \vee 1 = 1 \qquad 1 \vee 1 = 1.$$

Dakle $x \vee y = \sup \{x, y\}$ ako x i y znače 0, 1.

Preglednije se ta operacija prikazuje ovom *tablicom rastavljanja*:

$\vee$	0	1
0	0	1
1	1	1.

4.2. Ekskluzivna disjunkcija. Operator $\underline{\vee}$ (ili · · · ili).

Definicija: $x \underline{\vee} y$ znači ili x ili y, a ne oboje.

Npr. $a=2 \underline{\vee} a=3$ znači da je a ili 2 ili 3, ali ako je 2, onda ne može biti ujedno 3.

4.3. Zadaci o disjunkciji. 1. Odrediti vrijednost ovih iskaza:

1) $(3<5)\vee(4<2)$; 2) $(3<5)\underline{\vee}(4<2)$; 3) $(3<5)\underline{\vee}(1<4)$;

4) $(10^2=100)\underline{\vee}(2^{\frac{1}{2}}$ je iracionalan broj); 5) (X je krug) $\underline{\vee}$ (X je tačka);
6) $\neg(2>1)\underline{\vee}((a+b)^2=a^2+2ab+b^2)$; 7) $\neg(a^2-b^2)=(a-b)\cdot(a+b)\vee 3^2=3$.

2. Izračunaj: 1) $0\vee 0\vee 1$; 2) $0\underline{\vee}0$, $0\underline{\vee}1$, $1\underline{\vee}0$, $1\underline{\vee}1$; 3) $(0\vee 1)\wedge 0$; 4) $(1\underline{\vee}0)\wedge(1\wedge 1)$; 5) $\neg(1\vee 1)\vee\neg(0\wedge 0)$.

3. Za $x, y, z\in I2=\{0, 1\}$; dokaži: $(x\vee y)\wedge z=(x\wedge z)\vee(y\wedge z)$ i dualno: $(x\wedge y)\vee z=(x\vee z)\wedge(y\vee z)$.

4. Dokaži: 1) $v(\neg x)=1-vx$; 2) $v(x\wedge y)=vx\cdot vy$; 3) $v(x\vee y)=vx+vy-vx\cdot vy$; 4) $v(x\underline{\vee}y)=|vx-vy|$.

5. VEZA IZMEĐU SASTAVA I RASTAVA DVAJU SUDOVA. DE MORGANOVI OBRASCI

5.1. Neka su a, b dvije rečenice; npr. a . . . »*Kiša pada*«, b . . . »*Danas je četvrtak*«; negirajmo $a\wedge b$; dobijemo izreku: »*Nije istina da i kiša pada i da je danas četvrtak*«; to znači da bar jedna od zadanih rečenica a, b ne stoji; znači da ili kiša ne pada ili da danas nije četvrtak, ili da nije ni jedno ni drugo. Drugim riječima, služeći se uvedenom simbolikom, dobili smo ovo:

$$\neg(a\wedge b)=\neg a\vee\neg b. \tag{1}$$

Zaključak je općenit: *negacija sastava zadanih sudova je rastav negacijâ tih sudova.*

5.2. Na isti način zaključujemo da je

$$\neg(a\vee b)=\neg a\wedge\neg b. \tag{2}$$

Na taj smo način dokazali:

5.3. ***Teorem (De Morgan)***[1] ***Negacija sastava (rastava) niza zadanih logičkih sudova je rastav negacija tih sudova; simbolički:***

$$\neg(a\wedge b)=\neg a\vee\neg b;\ \neg(a\vee b)=\neg a\wedge\neg b;\ \textit{općenito:}$$

$$\neg\bigvee_x x=\bigwedge_x\neg x;\ \textit{pri tom } x \textit{ prolazi skupom ili nizom sudova.}$$

---

[1] *A. de Morgan* (1806—1871), engleski matematičar.

5.4. Zadaci.

1. Odredi aritmetičku vrijednost ovih sudova: 1) A ... Aristotel je bio veliki *filozof*; 2) B ... Aleksandar Makedonski je Napoleonov savremenik; 3) $A \vee B$; 4) $A \wedge B$; 5) $\neg A \wedge \neg B$; 6) $A \wedge \neg B$; 7) $A \vee \neg B$; 8) $\neg A \vee \neg B$.
2. Promatraj ova tri suda: 1) A = *Broj 5 je neparan*; B = *Svaki paralelogram ima bar dvije jednake stranice*; C = *površina kruga je* πr. Odredi aritmetičku vrijednost sudova A, B, C kao i ovih sudova: 2) $A \vee B \vee C$; 3) $(A \vee B) \wedge C$; 4) $(A \wedge B) \wedge \neg C$; 5) $\neg A \wedge \neg B \wedge \neg C$; 6) $\neg A \vee \neg A \vee \neg C$; 7) $B \wedge \neg C$.
3. Nađi negaciju i aritmetičku vrijednost svakog suda iz zadatka 1. pa na njima objasni De Morganove obrasce.
4. Isto pitanje za sudove iz zadatka 2.
5. Nađi negaciju suda: 1) $\neg(x \vee \neg y)$; 2) $(\neg x \vee \neg y) \wedge (\neg x \vee \neg x)$; 3) $(\neg x \wedge \neg y) \vee (\neg x \wedge \neg z)$.

6. IMPLIKACIJA ILI ZAKLJUČIVANJE ILI ZAKLJUČNA FUNKCIJA. ZNAK ⇒

Najizrazitija logička funkcija je implikacija ili zaključivanje; specijalno je ta funkcija česta u matematici.

6.1. Definicija (*znak usmjerene jednakosti*). *Kaže se da sud x implicira (daje, obuhvaća, uključuje, upleće, ima za posljedicu) sud y i piše:*

(1) $$x \Rightarrow y \text{ ili } x \supset y$$

ako nije moguće da stoji x, a da ne stoji y; simbolički:

(2) $$x \Rightarrow y \quad \text{znači} \quad \neg(x \wedge \neg y), \text{ tj.}$$

$$x \Rightarrow y \overset{\text{def}}{=} \neg(x \wedge \neg y).$$

Primjer: $x>0 \wedge y>0 \Rightarrow xy>0$ (izreci to riječima!).

Vrlo važna veza* (1) *čita se također i na ove načine:

Ako x, onda y.

Da bude x, mora biti y.

Da bude x, nužno je da bude y.

Da bude y, dovoljno je da bude x.

Nuždan uslov za sud x jest sud y.

Dovoljan uslov za sud y jest sud x.

Simbolički i slikovito:

(3) $$\textit{dovoljan uslov} \Rightarrow \textit{nuždan uslov}.$$

To je vanredno čest način matematičkog izražavanja.

Ta raznolikost u izgovaranju veze (1) ujedno je dokaz kako je veza (1) važna, općenita i raznovrsna. Specijalno ukazujemo na vanredno veliku olakšicu u poimanju matematičkih rasuđivanja, ako imamo na umu način izražavanja (3); imamo ovaj „kalup“:

Ako ....., onda .....

Često se kaže: u (1) *x je hipoteza*, a *y teza*, pa imamo:

hipoteza (pretpostavka) $\Rightarrow$ *teza (tvrdnja).*

6.2. Tablica istinitosti zaključne funkcije $\Rightarrow$. U definiciji (2) može sud x biti istinit ili lažan; sud y također.

Na taj način dobivamo ove četiri mogućnosti:

prvi slučaj $vx = 1$, $vy = 1$, tj. $1 \Rightarrow 1$;

drugi slučaj $vx = 1$, $vy = 0$, tj. $1 \Rightarrow 0$;

treći slučaj $vx = 0$, $vy = 1$, tj. $0 \Rightarrow 1$;

četvrti slučaj $vx = 0$, $vy = 0$, tj. $0 \Rightarrow 0$.

Odredimo vrijednost tih „zaključaka“, i to prema definiciji (2).

6.2.1. *Za x istinito i y istinito,* prirodno je da smatramo istinitim i sud:

Ako x, onda y.

To je jasno ako y „izvire“ iz x kao logična posljedica; no nije nam strano da sud $x \Rightarrow y$ smatramo istinitim i u slučaju kad y nije logička posljedica od x, kao recimo u ovom primjeru:

$(1 < 3) \Rightarrow$ (Azija je najveći kontinent).

Pogotovu nam se čini jasno da ne možemo prihvatiti kao istinu da bi „istinito uključilo neistinito“, tj. da bi bilo $(1 \Rightarrow 0) = 1$.

Druga je stvar ako polazimo od 0, tj. od lažnog suda x: ako je x lažno, a y istinito, istina od y stoji bez obzira na x, pa bilo x i lažno: laž neće srušiti istinu.

Ostaje slučaj: *x lažno* i *y lažno.* Npr. sud $2 = 10$ i sud $3 = 8$ te sud

(4) $$(2 = 10) \Rightarrow (3 = 8).$$

Ako za nekoga „vrijedi“ $2 = 10$, onda se ne čudimo da za njega može vrijediti i $3 = 8$, tako da bi sud (4) imao vrijednost 1, tj. $(0 \Rightarrow 0) = 1$.

Na taj način dolazimo do toga da je istinit i sud $0 \Rightarrow 1$ i sud $0 \Rightarrow 0$.

Dakle: *laž upleće i istinu i laž*; u srednjem vijeku su na latinskom govorili: Ex falso quodlibet (iz laži sve!).

Ukratko, dolazimo do ove *tablice za* $\Rightarrow$:

$x \Rightarrow y$	y: 0	y: 1
x: 0	1	1
x: 1	0	1.

Odredimo na primjer formalno, na osnovu definicije (2), vrijednost $1 \Rightarrow 1$. Imamo $(1 \Rightarrow 1) =$ (po (2)) $= \neg(1 \wedge \neg 1) =$ (jer je $\neg 1 = 0$) $= \neg(1 \wedge 0) =$ (jer je $1 \wedge 0 = 0$) $= \neg 0 = 1$; dakle je $(1 \Rightarrow 1) = 1$.

Na sličan se način provjere i preostala tri slučaja: $(1 \Rightarrow 0) = 0$, $(0 \Rightarrow 1) = 1$ i $(0 \Rightarrow 0) = 1$.

7. OBRAT ZAKLJUČKA

Zaključak $y \Rightarrow x$ *zove se obrat ili reciprok zaključka* $x \Rightarrow y$.

Tako npr. obrat od zaključka:

Ako $\triangle$ *ima dva kuta jednaka, onda taj* $\triangle$ *ima dvije stranice jednake* glasi:

Ako $\triangle$ ima dvije stranice jednake, onda on ima dva kuta jednaka; *taj je obrat ispravan.*

Za brojeve x, y vrijedi:

Sud: $x>0 \wedge y>0 \Rightarrow xy>0$; obrat bi glasio:

Za brojeve x, y vrijedi:

$$xy>0 \Rightarrow x>0 \text{ i } y>0.$$

Taj obrat nije ispravan jer je npr. $(-2)(-3)>0$, premda je $-2<0$ i $-3<0$.

Vrlo je korisno za svaki zaključak $x \Rightarrow y$ *odrediti da li stoji njegov obrat.*

8. IZRAZ „AKO I SAMO AKO". LOGIČKA RAVNOPRAVNOST SUDOVA. DVOSTRUKO USMJERENA JEDNAKOST $\Leftrightarrow$

Definicija. Ako je istinit *i sud* $x \Rightarrow y$ *i njegov obrat* $y \Rightarrow x$, kaže se da je sud x *ravnopravan (ekvivalentan) sa sudom* y i piše:

$x \Leftrightarrow y$; govori se i ovako:

x je istinito ***ako i samo ako*** *je istinito y; ili ovako:*

x stoji (vrijedi) ako i samo ako stoji (vrijedi) y.

Npr. sud:

1) Kvadratna jednadžba $ax^2+bx+c=0$ ima realna rješenja
   i sud:
2) *Diskriminanta* $b^2-4ac \geq 0$
   međusobno su ravnopravni (pritom pretpostavljamo da radimo s jednadžbama s realnim koeficijentima).

9. KONTRARNI ILI SUPROTNI ZAKLJUČAK

Svakom zaključnom sudu $x \Rightarrow y$ pridružen je i ovaj sud:

$$\neg x \Rightarrow \neg y, \tag{1}$$

koji je *kontraran* ili *suprotan* sudu $x \Rightarrow y$. Sud (1) može, no ne mora biti istinit. Obrat kontrarnog suda zove se *recipročno-kontrarni zaključak*; glasi:

$$\neg y \Rightarrow \neg x.$$

Na taj način dolazimo do ovakve *četvorke zaključaka*:

$$x \Rightarrow y, \quad y \Rightarrow x, \quad \neg x \Rightarrow \neg y, \quad \neg y \Rightarrow \neg x$$

(*zaključak*; *obrat*; *suprotni*; *obratno-suprotni zaključak*).

Svaki put treba ispitati koji su od tih sudova istiniti a koji lažni.

9.1. Primjer o brojevima. Promatrajmo ispravan zaključak:

$$a = b \Rightarrow a + c = b + c;$$

obrat: $a + c = b + c \Rightarrow a = b$;

suprotan: $a \neq b \Rightarrow a + c \neq b + c$;

obratno-suprotan: $a + c \neq b + c \Rightarrow a \neq b$.

Sva četiri suda su ispravna.

10. Zadaci u zaključnoj funkciji

1. Za ove uređene parove sudova x, y odredi aritmetičku vrijednost suda $x \Rightarrow y$:

1) $3 = 2 + 1$; $\quad -3 = -1 - 3$;

2) $3 < 4$; $\quad -3 < -4$;

3) $2 < 1$; $\quad 1 = 3 - 2$;

4) $2 < 1$; Evropa je najveći kontinent;

5) u $\triangle ABC$ je $AB < BC$; u $\triangle ABC$ je $\sphericalangle C < \sphericalangle A$;

6) u $\triangle ABC$ je $AB < BC$; u $\triangle ABC$ je $\sphericalangle A < \sphericalangle C$;

7) u $\triangle ABC$ je $\sphericalangle C = 90^0$; u $\triangle ABC$ je $AB^2 = AC^2 + CB^2$;

8) $(a < b) \wedge (b < c)$; $\quad a < c$;

9) $(a = b) \wedge (b = c)$; $\quad a = c$;

10) (a, b, c su ravnine) $a \parallel b$, $b \parallel c$; $\quad a \parallel c$;

11) (a, b su brojevi) $a > 3$, $b > 3$ i $ab > 9$;

12) $\left(\sum_{n=j}^{\infty} |a_n| \right.$ konvergira; $\sum_{n=j}^{\infty} a_n$ konvergira i $\left| \sum_{n=1}^{\infty} a_n \right| \leq \sum_{n=1}^{\infty} |a_n|$ (pri tom su a_n brojevi).

2. U zadacima 1.1.—1.10. promatraj obratne zaključke i odredi im vrijednost.

3. U zadacima 1.1.—1.11. promatraj suprotne zaključke i odredi im vrijednost.

4. Isto za obratno-suprotne zaključke.

5. U kojim su zadacima 1.1.—1.10. ispravna sva četiri zaključka: direktni, obratni, suprotni, obratno-suprotni?

6. Riješi $x \Leftrightarrow y$ za zadatak 1.

6′. Neka su a, b realni brojevi; izrazi na ravnopravan način sud:
1) $ab > 0$; 2) $ab \geqq 0$; $ab \leq 0$; $ab < 0$.

7. **(Modus ponens)**. Ako je x i $x \Rightarrow y$, onda je i y. Dokaži!

8. Dokaži ispravnost ovih *Fregeovih »aksioma sudovnog računa«*[1], pri čemu su x, y, z bilo kakvi logički sudovi s vrijednostima 0, 1:

F_1 $\quad x \Rightarrow (y \Rightarrow x)$

F_2 $\quad ((x \Rightarrow (y \Rightarrow z)) \Rightarrow ((x \Rightarrow y) \Rightarrow (x \Rightarrow z))$

F_3 $\quad (x \Rightarrow (y \Rightarrow z)) \Rightarrow (y \Rightarrow (x \Rightarrow z))$

F_4 $\quad (x \Rightarrow y) \Rightarrow (\neg y \Rightarrow \neg x)$

F_5 $\neg\neg$ $\quad x \Rightarrow x$

F_6 $\quad x \Rightarrow \neg\neg x$.

9. Dokaži ispravnost ovih *Lukasiewiczevih aksioma*[2]:

L_1 isto kao F_1

L_2 isto kao F_2

L_3 $(\neg x \Rightarrow \neg y) \Rightarrow (y \Rightarrow x)$.

10. *Shefferova*[3] *funkcija* glasi: $\neg(x \wedge y)$; označuje se sa $|$ ili S; ona iskazuje da je *bar jedno od* x i y *lažno*.

1) Dokaži da vrijedi ova tablica:

S	0	1
0	1	1
1	1	0.

2. Izrazi $\neg x$, $x \vee y$, $x \wedge y$, $x \Rightarrow y$ pomoću Shefferove funkcije.

---

[1] F. L. G. Frege (1848—1925), njemački matematičar i logičar.
[2] J. Lukasiewicz [Lukasjevič] (19/20. st.), poljski matematičar i logičar.
[3] M. H. Sheffer [Šefer] (*1883), američki logičar.

11. Isto pitanje za Lukasiewiczevu funkciju $L(x, y) = \neg x \wedge \neg y$; njena tablica glasi:

L	0	1
0	1	0
1	0	0.

12. Dokaži da je disjunkcija razdjelna ili distributivna prema konjunkciji, tj. da vrijedi $x \vee (y \wedge z) \Leftrightarrow (x \vee y) \wedge (x \vee z)$.

13. Dokaži dual od prethodnog iskaza: konjunkcija je razdjelna prema disjunkciji: $x \wedge (y \vee z) \Leftrightarrow (x \wedge y) \vee (x \wedge z)$.

14. $((x \Rightarrow y) \wedge (x' \Rightarrow y)) \Rightarrow ((x \vee x') \Rightarrow y)$.

15. Dokaz istinitosti suda x pomoću svođenja na proturječje (reductio ad absurdum): pretpostavi $\neg x$ pa izvedi i y i $\neg y$.

16. Dokaz istinitosti suda $\neg x$ pomođu svođenja na proturječje: pretpostavi x i izvedi y i $\neg y$.

17. Dokaz istinitosti suda $x \Rightarrow y$ pomcću svođenja na proturječje: pretpostavi x i $\neg y$ pa izvedi z i $\neg z$ (npr. z može biti x pa y).

18. Promatraj ova 4 suda.

    1) $x \Rightarrow x$ (identitet);

    2) $x \vee \neg x$ (zakon o isključenom trećem);

    3) $\neg(x \wedge \neg x)$ (zakon proturječnosti ili kontradikcije);

    4) $(x \wedge y) \Rightarrow x$.

19. Promatraj ove sudove (a, x, y su sudovi):

    1) $(x \Rightarrow y) \Rightarrow ((a \wedge x) \Rightarrow (a \wedge y))$;

    2) $(x \Rightarrow y) \Rightarrow ((a \vee x) \Rightarrow (a \vee y))$;

    3) $(x \Rightarrow y) \wedge (x' \Rightarrow y') \Rightarrow ((x \wedge x') \Rightarrow (y \wedge y'))$;

    4) $(x \Rightarrow y) \Rightarrow ((a \wedge x) \Rightarrow y)$;

    5) $(x \Rightarrow y) \Rightarrow (x \Rightarrow (a \vee y))$.

20. Ako u zadacima 19.1.—19.5. slova znače brojeve, a oznake $\Rightarrow$, $\wedge$, $\vee$ znače $=, \cdot, +$, da li se dobiju ispravni zaključci?

21. Isto pitanje za slučaj da $\Rightarrow$ znači $<$.

22. *Indirektan dokaz* jest onaj kod kojeg se pretpostavlja istinitost negacije; evo nekoliko takvih obrazaca:

    1) $(\neg x \Rightarrow x) \Rightarrow x$; drugim riječima: pretpostavka da negirano x uključuje x dokazuje ispravnost od x;

    2) $\neg x \Rightarrow (y \wedge \neg y) \Rightarrow x$;

    3) $[(\neg x \Rightarrow y) \wedge \neg y] \Rightarrow x$;

    4) $[(x \wedge \neg y) \Rightarrow (z \wedge \neg z)] \Rightarrow (x \Rightarrow y)$;

    5) $[(x \wedge \neg y) \Rightarrow (\neg x \vee y)] \Rightarrow (x \Rightarrow y)$.

11. SUDOVNA ILI PROPOZICIJSKA FUNKCIJA. KVANTORI

11.1. Primjer. Promatrajmo izreku ili sud:

(1) „3 x *je pozitivan broj*".

U toj se izreci pojavljuje slovo x; zato izreku (1) možemo označiti i sa $P(x)$. Tako imamo posebne sudove, npr.:

$P(2)$ ... „3 · 2 je pozitivan broj" (ovaj sud je istinit).

$P(-5)$... „3 · −5 je pozitivan broj" (ovaj sud je lažan).

$P(0)$ ... „3 · 0 je pozitivan broj" (ovaj sud je lažan).

Je li sud Px lažan ili istinit? *Odgovor zavisi od značenja veličine* x koja se pojavljuje u rečenici $P(x)$: ako je $x>0$, onda je $P(x)$ istinito; ako je $x=0$ ili $x<0$, onda je $P(x)$ neistinito. Kaže se da je $P(x)$ sudovna funkcija.

11.2. Definicija sudovne funkcije. Ako u nekoj izreci ili rečenici $I(x)$ dolazi proizvoljan član x nekog skupa S, kaže se da je $I(x)$ *sudovna funkcija nad* S *ili u* S; to *znači da svakom članu* x *iz* S *odgovara jedna ili više rečenica* $I(x)$.

Tako npr. ako x znači proizvoljnog državljanina Jugoslavije na dan $01 \cdot 01 \cdot 1960$, tada rečenica:

Osoba x *je rođena* 1892. *godine*

predstavlja određenu sudovnu funkciju $I(x)$.

Za svako dopušteno x sud $I(x)$ je ili lažan ili istinit: npr. rečenica „*I* (*Nikola Tesla*, *izumilac*)" je lažna; no za neko x sud $I(x)$ je sigurno istinit, npr. „*I* (*Ivo Andrić*, *književnik*)".

11.3. Kvantori. Oznaka $\wedge$ za svako i $\vee$ za neko. Primjetilo se da sudovne funkcije dolaze vrlo često; također se vrlo često pojavljuju „*neodređene zamjenice*": *svaki*, *svi* te *neki*, *najmanje jedan*. Te riječi u matematici i logici nose posebno ime: zovu se *kvantori* ili *kvantifikatori* ili *kolikotnici*.

Veliki ili dugi kvantor ili univerzalni kvantor jesu riječi: svaki, svi; oznaka: A ili $\forall$ (izvrnuto A) ili $\wedge$.

Mali ili **kratki** ili **egzistencijalni kvantor** jesu riječi: *neki*, *najmanje jedan*; označuje se sa E, $\exists$ (izvrnuto E), $\vee$; čita se još: „*egzistira* ili *postoji*".

Tako npr. ako n označuje prirodan broj, onda imamo istinite sudove:

$\bigwedge_n (3n>1)$; riječima: „Za svaki prirodni broj n vrijedi $3n>1$";

$\bigvee_n (3n<10)$; riječima: Za neki prirodni broj n vrijedi $3n<10$, kao npr. za $n=2$.

$\bigwedge_n (1+3+5+\cdots+(2n-1))=n^2$.

Za sudovnu funkciju $F(x)$ oznaka

$\bigwedge_x F(x)$ čita se: „*za svako* x *vrijedi* $F(x)$".

$\bigvee_x F(x)$ čita se: „*za nekoje x vrijedi* $F(x)$ ili postoji x *za koje vrijedi* $F(x)$ *ili za bar jedno* x stoji $F(x)$“.

$\underset{x}{\text{V!}}$ čita se: „*jedno jedino*“ x ili *jedincato* x.

Npr. ako je x broj, tada $\underset{x}{\text{V!}}\ (3x=6)$; naime za $x=2$.

11.4. Negacija kvantora. Formule $\neg\wedge = \vee\neg$, $\neg\vee = \wedge\neg$.

11.4.1. P r i m j e r. Negirajmo izreku:

(1) *Svaka je osoba visoka* 160 *cm.*

Dobijemo rečenicu:

(2) „Nije istina da je svaka osoba visoka 160 cm“, jer neka osoba ima visinu $\neq$ 160 cm.

U polaznoj rečenici pojavljivao se *dugi* kvantor „*svaka*“, a u dobivenoj rečenici dolazi *kratki* kvantor „*neka*“ u vezi s *negacijom* polaznog suda.

Označimo sa $O(x)$ rečenicu: „*Osoba x je visoka* 160 *cm*“. Tada sud (1) glasi: $\bigwedge_x O(x)$; negacija toga suda: $\neg\bigwedge_x O(x)$ glasi: $\bigvee_x \neg O(x)$ (tj. „nekoja osoba x nije visoka 160 cm“). Na taj način dolazimo do jednakosti:

(3) $$\neg\bigwedge_x O(x) = \bigvee_x \neg O(x).$$

11.4.2. ***T e o r e m. Formula*** **(3)** ***vrijedi ne samo za gornju posebnu sudovnu funkciju*** $O(x)$ ***nego i za svaku drugu sudovnu funkciju*** $O(x)$ ***kojom svakom promatranom predmetu x pridružujemo određen sud*** $O(x)$***, koji je istinit ili lažan.***

11.4.3. Ako u (3) pišemo

$F(x) = \neg O(x)$, dakle

$\neg F(x) = O(x)$, tada relacija (3) postaje:

$\neg\bigwedge_x \neg F(x) = \bigvee_x F(x)$; odatle negiranjem:

(4) $$\neg\neg\bigwedge_x \neg F(x) = \neg\bigvee_x F(x);$$ no $\neg\neg$ možemo ispustiti;

ako još u (4) obrnemo strane, izlazi:

(5) $$\neg\bigvee F(x) = \bigwedge\neg F(x);$$

tu $F(x)$ znači svaku sudovnu ili propozicionu funkciju.

11.4.4. Specijalno, pišući u (5) slovo O umjesto F, dobije se „dual“ relacije (3):

(3)* $$\neg\bigvee_x O(x) = \bigwedge_x \neg O(x).$$

Vidi se da (3)* nastaje iz (3) zamjenjujući međusobno veliki i mali kvantor: umjesto $\wedge$ dolazi V, a umjesto V dolazi $\wedge$. Tako nastaje:

11.4.5. Teorem. *Za svaku sudovnu funkciju* $F(x)$ *vrijedi*

$$\neg \bigwedge_x F(x) = \bigvee_x \neg F(x) \text{ } \textit{i dualno}$$

$$\neg \bigvee_x F(x) = \bigwedge_x \neg F(x);$$ ***kraće se to izražava:***

$\neg \wedge = \vee \neg$ ***(negacija velikog kvantora daje mali kvantor negacije);***

$\neg \vee = \wedge \neg$ ***(negacija malog kvantora daje veliki kvantor negacije).***

11.4.6. Primjer o konvergenciji i divergenciji niza. Znamo da niz brojeva a_n *konvergira* ako ***postoji neki*** broj a sa svojstvom da za ***svaki broj*** $\varepsilon > 0$ ***postoji*** neki indeks $n_0(\varepsilon)$ za koji iz $n > n_0(\varepsilon)$ izlazi $|a - a_n| < \varepsilon$.

To je dosta teška definicija; ona je vanredno teška ako svjesno ne baratamo s kvantorima. Izrazimo istu definiciju u jeziku matematičke i logičke simbolike:

(6) (Niz brojeva a_n je konvergentan) $\Leftrightarrow \bigvee_{a_0} \bigwedge_{\varepsilon>0} \bigvee_{n_0(\varepsilon)} \bigwedge_{n>n_0(\varepsilon)} |a_0 - a_n| < \varepsilon;$

a_0, ε, $n_0(\varepsilon)$, n su brojevi; $n_0(\varepsilon)$, n su prirodni brojevi.

Vidimo kako se naizmjenice nižu veliki i mali kvantori.

Negacija ekvivalencije (6) daje na lijevoj strani izreku:

Niz brojeva a_n *je divergentan.*

Negacija desne strane u (6) daje:

$\neg \bigvee_{a_0} \bigwedge_{\varepsilon>0} \bigvee_{n_0(\varepsilon)} \bigwedge_n$; ovo je prema teoremu dalje $= \bigwedge_{a_0} \neg \bigwedge_{\varepsilon>0} \bigvee_{n_0(\varepsilon)} \bigwedge_n$; iz istog razloga je to dalje $= \bigwedge_{a_0} \bigvee_{\varepsilon>0} \neg \bigvee_{n_0(\varepsilon)} \bigwedge_n$, pa $\bigwedge_{a_0} \bigvee_{\varepsilon>0} \bigwedge_{n_0(\varepsilon)} \neg \bigwedge_n$ te najzad $\bigwedge_{a_0} \bigvee_{\varepsilon>0} \bigwedge_{n_0(\varepsilon)} \bigvee_n \neg$, tako da negiranjem u (6) dobijemo:

(7) (*Niz brojeva* a_n *je divergentan*) $\Leftrightarrow \bigwedge_{a_0} \bigvee_{\varepsilon>0} \bigwedge_{n_0(\varepsilon)} \bigvee_{n>n_0(\varepsilon)} \neg |a_0 - a_n| < \varepsilon.$

Međutim, $\neg |a_0 - a_n| < \varepsilon$ znači $|a_0 - a_n| \geq \varepsilon$. Na taj način (7) iskazuje da izvan *neke* okoline *svakog* broja leži beskonačno mnogo članova promatranog niza brojeva a_n.

11.5. Istovremena pojava više kvantora. Može se desiti da se u jednoj te istoj rečenici pojave 2, 3 pa i *više kvantora*, i to iste vrste ili raznih vrsta. Npr. za *svaki* broj m i *svaki* broj s postoji *jedan jedini* d sa svojstvom $m - s = d$; simbolički se to iskazuje ovako: $\bigwedge_m \bigwedge_s \bigvee_d ! \; m - s = d$; slova m, s, d su uzeta kao početna slova riječi: *minuend, suptrahend, diferencija.*

11.6. Zadaci o sudovnim funkcijama i kvantorima.

1. Neka $x, y, \ldots$ znače brojeve; koji je od ovih sudova istinit:

1) $\bigwedge_x x + x = 2x$; 2) $\bigwedge_x 2x = 6$; 3) $\bigvee_x 2x = 6$; 4) $\neg \bigwedge_x (2x = 6)$;

5) $\neg \bigvee_x (2x = 6)$; 6) $\bigwedge_x (x = -x)$; 7) $\bigvee_x (x = -x)$; 8) $\bigwedge_x (x = x + 3)$;

9) $\underset{x,\,y}{\wedge}(x^2=y^2) \Leftrightarrow (x=y)\,\mathrm{v}\,(x=-y)$; 10) $\underset{x}{\vee}\neg(x^2=x)$;

11) $\underset{x}{\wedge}(x-2)\cdot(x-3)=0$; 12) $\underset{x}{\wedge}\underset{y}{\wedge}(x+y=y+x)$;

13) $(\underset{x}{\vee}\underset{y}{\vee}\underset{z}{\vee})(x<y)\wedge(y<z) \Rightarrow (x<z)$; 14) $\underset{x}{\wedge}\underset{y}{\vee}!\,(x+y=x)$;

15) $\underset{x}{\wedge}(x\neq 0) \Rightarrow \underset{y}{\vee}(xy=1)$; 16) $\underset{x}{\wedge}\underset{y}{\vee}!\,(x+y=0)$?

2. Izreci riječima zadatke 1.1.—1.16.

3. Negiraj relacije 1.1.—1.16.

4. U kojim zadacima 1.1.—1.16. možemo umjesto V ili umjesto $\wedge$ pisati V!?

5. Neka $f=f(x, y)$ znači: „x je otac od y“, pri čemu x, y označuje ljudska bića; izreci riječima i odredi aritmetičku vrijednost ovih sudova:

   1) $\underset{x}{\wedge}\underset{y}{\wedge}f$; 2) $\underset{x}{\wedge}\underset{y}{\mathrm{V}}f$; 3) $\underset{x}{\mathrm{V}}\underset{y}{\mathrm{V}}f$; 4) $\underset{x}{\mathrm{V}}\underset{y}{\wedge}f$; 5) $\underset{x}{\mathrm{V}}\underset{x}{\mathrm{V}}f$;

   6) $\underset{x}{\wedge}\underset{x}{\wedge}f$; 7) $\underset{y}{\wedge}\underset{x}{\wedge}f(x, y)$; 8) $\underset{y}{\wedge}\underset{x}{\mathrm{V}}$; 9) $\underset{y}{\mathrm{V}}\underset{x}{\mathrm{V}}$; 10) $\underset{y}{\mathrm{V}}\underset{x}{\wedge}$.

6. U zadatku 5. piši umjesto V znak V!; koji se ispravni sudovi dobiju?

7. Svaki prirodni broj je suma od 4 kvadratna cijela broja (npr. $16=4^2+0^2+0^2+0^2$); napiši to simbolički.

8. $\underset{n}{\wedge}\underset{h}{\wedge}(1+h)>0 \Rightarrow (1+h)^n\geq 1+nh$; pri tom su n, h brojevi te $n=1,\ 2,\ 3,\ \ldots$

9) Nađi $xfxfyfy$, ako f označuje: 1) Shefferovu, 2) Lukasiewiczevu funkciju; pri tom je $x, y\in\{0,\ 1\}$.

10) Promatraj sudove: 1) $(x_1\Rightarrow x_2)\vee(x_2\Rightarrow x_1)$; 2) $(x_1\Rightarrow x_2)\vee(x_2\Rightarrow x_3)\vee\vee(x_3\Rightarrow x_1)$; 3) $\underset{i=1,\,\ldots\,,\,n-1}{\vee}(x_i\Rightarrow x_{i+1})\vee(x_n\Rightarrow x_1)$. Ima li koji od tih sudova vrijednost 1 za svaki izbor promjenljivih $x_i\in\{0,\ 1\}$?

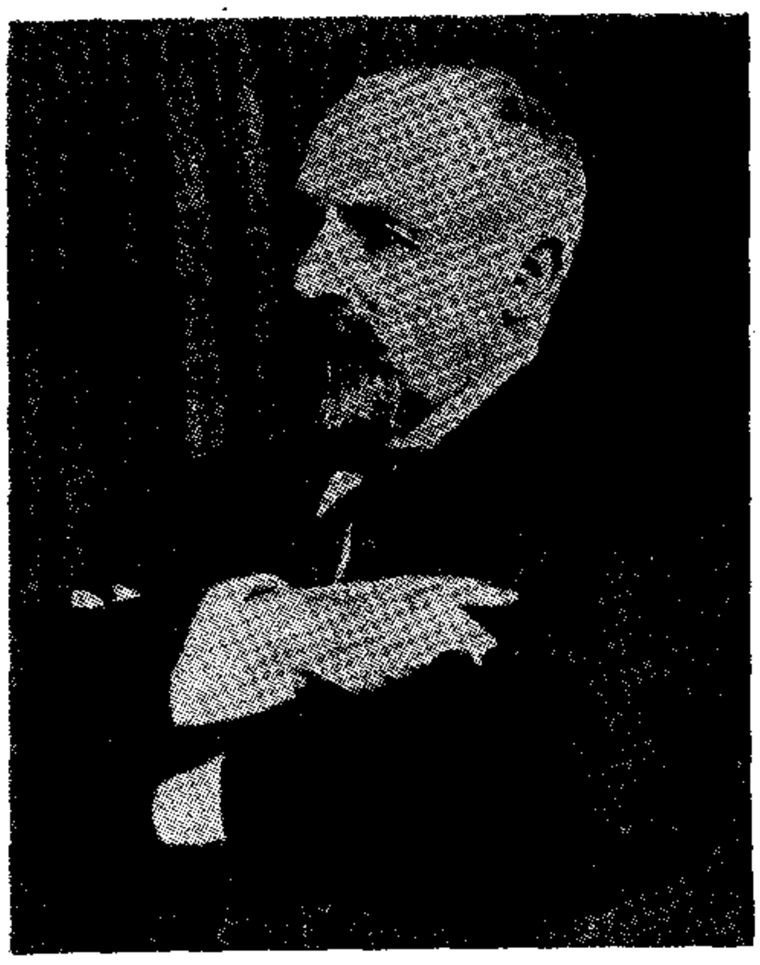
Literatura

Curry H. B [1], Devidé Vl [1], Hilbert D. — Ackermann W [1], Mendelson E [1], Mostowski A. [1], Prešič Sl. [1], Prijatelj N. [1], Shoenfield J.R. [1], Stoljar A.A. [1].

POGLAVLJE 2.

SKUP I ELEMENTI SKUPOVA. ALGEBRA SKUPOVA

Skup, skupnost, mnogost ili množina [1] i funkcija (pridruživanje, operacija, preslikavanje) [2] jesu osnovni pojmovi. S tim u vezi upoznat ćemo se s nekim pojmovima koji se neprestano pojavljuju. U ovom poglavlju upoznat ćemo se specijalno s nekim pojmovima o skupovima (relacija članstva, relacija dijela ili djelitelja) te o osnovnim operacijama sa skupovima (ujedinjenje i presjek, odstranjivanje skupova).



Georg Cantor (č. Kantor; 1845 — 1918), osnivač teorije skupova.

1. NEŠTO O SKUPOVIMA

1.1. Skupovi i članovi skupova. [3]

Govori se o skupu gradova neke države, o skupu ili množini cifara dekadskog sistema, o skupu prvih 100 parnih prirodnih brojeva, o skupu krugova u ravnini, itd. Ne upuštamo se u to da li se pojam mnogosti može svesti na nešto još jednostavnije i da se kaže šta je zapravo skup ili mnogost. Treba znati da se kod mnogosti radi u prvom redu o tom da se odrede članovi (jedinke, jedinice, atomi, elementi, tačke, brojevi ...) od kojih je pojedina mnogost sastavljena.

1.2. Shematsko prikazivanje skupova i njihovih članova. Elemente i skupove možemo prikazivati na razne načine, npr. krugovima, modelima ili kakvim drugim predmetima. Tako se npr. shematski može skup označiti sa stanovitim

---

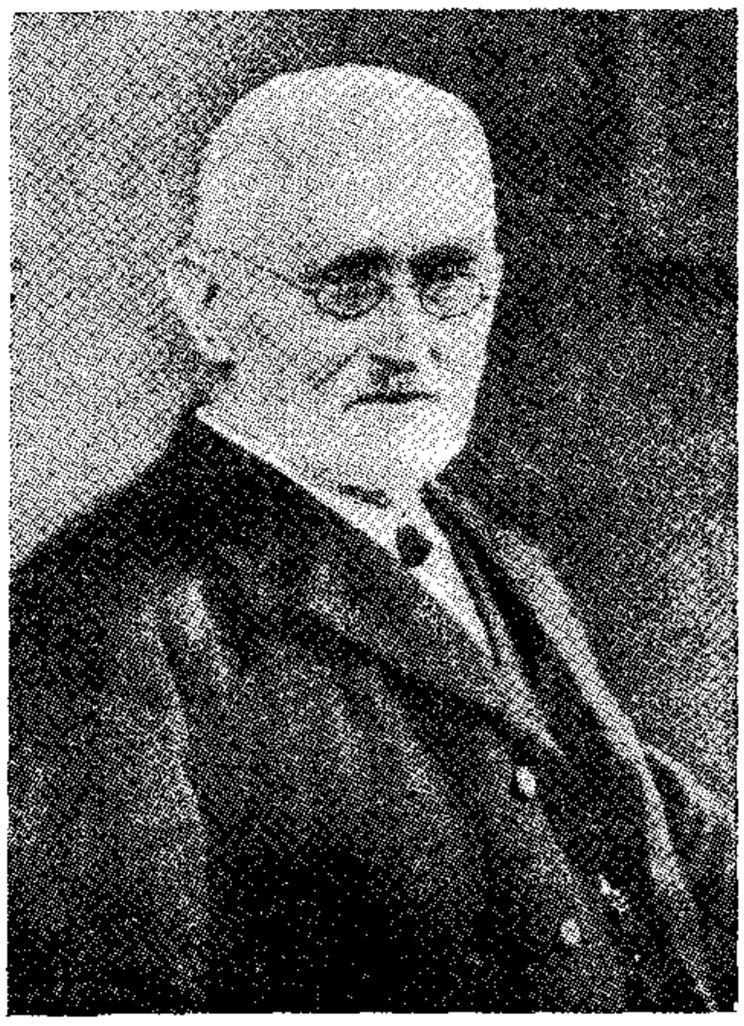
[1] Rus.: совокупность ili множество; engl.: set; fr.: ensemble; njem.: Menge.

[2] Rus.: соотвествие; engl.: mapping; fr.: fonction, correspondance: njem.: Abbildung.

[3] *Skup, mnogost i množina* znače jedno te isto (i riječi: sustav, sistem, zbirka, kolekcija, obitelj, cjelina itd. mogu poslužiti kao i riječi: skup, množina). Ako je u jednom slučaju određenije i zgodnije da se služimo jednom umjesto drugom od te tri riječi, onda ćemo se njome i služiti. Tako npr. lakše je govoriti: podskup, nadskup nego: podmnožina, nadmnožina. Isto tako, naziv mnogost upotrijebit će se uvijek kad bi bilo sumnje da skup, skupa znači nešto drugo a ne množinu.

brojem načrčkanih tačaka ili drugih stvari. Glavno je da pri rasuđivanju imamo kakav konkretniji oslonac, da gledamo kakav konkretan skup i da na njemu rasuđujemo kao na kakvom predstavniku općeg skupa. Tako npr. skupom ovih 5 tačaka:

možemo predstaviti shematski bilo koji skup od 5 članova, npr. skup od pet kontinenata: Azija, Afrika, Amerika, Evropa, Australija.



J. W. R. Dedekind (1831 — 1916), njemački matematičar, preteča i izgrađivač teorije skupova.

1.3. Označavanje skupova. *Skupove označujemo raznim znakovima, slovima, figurama.* Tako npr. skup svih prirodnih brojeva 1, 2, 3, 4, . . . označujemo sa $\{1, 2, 3, 4, \ldots\}$ i sa N. U prvoj oznaci odmah se vide i članovi mnogosti. Općenito, *ako neke predmete shvatimo kao cjelinu, npr. tako da ih stavimo formalno u vitičastu zagradu, dobijemo skup sastavljen od tih predmeta kao svojih članova.* Tako npr. $\{1, 2\}$ je skup sastavljen od 1 i 2 kao svojih članova. Isto tako $\{p\}$ je skup sastavljen od p kao svojeg jedinog člana; pri čemu p može biti kakav predmet, misao, odnos, skup, neskup, ništa, itd. Tako je npr.

$$\{\{1, 2, 3\}\}$$

skup kojemu je $\{1, 2, 3\}$ jedini član; a taj član $\{1, 2, 3\}$ je sa svoje strane skup sastavljen od 1, 2 i 3 kao svojih članova.

Skup svih cijelih racionalnih brojeva

$$\ldots, -2, -1, 0, 1, 2, 3, \ldots$$

označuje se sa D; skup neodřečnih cijelih brojeva

$$0, 1, 2, 3, \ldots$$

ili skup rednih brojeva označuje se sa N_0 ili I_ω. Znajmo da je 0 prvi redni broj, pa se i čita: *prvi*. Za svaki prirodnï broj n stavljamo:

$$I\,n = \{0, 1, 2, \ldots n-1\},\quad 1\,(n) = \underbrace{\{1, 2, 3, \ldots\}}_{n};$$

pri čemu je I početno slovo riječi interval. To je tzv. cifarski skup; on počinje sa 0. Također se promatra I 0 kao skup bez ikojeg člana; to je prazan skup. Stavljat ćemo: $0\,[1, n] = \{1\ 2, 3, \ldots, n\}$.

1.4. *Jednočlani skupovi ili unioni* jesu oni koji su sastavljeni od jednog jedinog člana; oni su oblika $\{p\}$. *Dvočlani skupovi ili ambe* sastavljeni su od 2 člana ili dvije tačke; ambe su oblika $\{a, b\}$, pri čemu je a različito od b. *Tročlani skupovi* zovu se *terne*. *Kvaterne* su skupovi od po 4 člana.

1.5. *Nulion* ili *prazni skup* se uvodi kao skup koji nema nijednog člana. Označit ćemo ga sa v (početno slovo lat. riječi vacuum = praznina) ili sa $\varnothing$ ili sa $\{\ \}$.

Pokazalo se vanredno korisno uvesti pojam prazna skupa. Uz njega su vezane mnoge matematičke i filozofske teškoće. Zanimljivo je npr. da je $\{\varnothing\}$ jednočlan skup! Element od $\{\varnothing\}$ jest prazni skup $\varnothing$.

Primijetimo da »*sveskup*« kao nešto što bi obuhvatalo kao svoje članove svaki predmet i misao nije nikakva *mnogost ili skup.*

1.6. Relacija $\in$. Ako je M mnogost, a p njen član, onda se to simbolički naznačuje sa

$$p \in M$$

i čita: p je član (jedinka, jedinica, tačka, element, broj, ...) množine M.

Odnos $p \in M$ ispisuje se i ovako;

$$M \ni p$$

i čita: *M sadrži p kao svoj član* (jedinku; jedinicu itd.).

Kod praznog skupa $\varnothing$ ne može biti $p \in \varnothing$ ni za koje p.

1.7. *Kardinalni* ili *glavni broj skupnosti* S kazuje koliko ta skupnost ima članova. Kardinalni broj skupnosti S označuje se sa kS ili $k(S)$. Tako npr.

$$k\varnothing = 0,\ k\{0,\ 1,\ 2\} = 3,\quad \text{tj.}\quad k(I3) = 3;\ k\,In = n$$

za svaki prirodni broj n, tj. $k\,In = n$ za svako $n \in N$.

1.8. Dio ili djelitelj mnogosti. Relacija $\subset$. Kombinacije.

1.8.1. Često se u vezi sa zadanim skupom, npr. odborom, promatra pojedini njegov pododbor (komisija, podskup ili dio). Tako ćemo vidjeti *da je jedno od osnovnih pitanja odrediti koliko zadani odbor može imati raznih pododbora po r članova.*

Da stvar postane određena, uvedimo neke važne definicije i oznake.

1.8.2. Definicija. Ako je svaki član skupnosti A član skupnosti B, kaže se *da je A podskup* (dio, djelitelj, divizor, predstavništvo, kombinacija, podmnožina) *množine B i piše*:

$$A \subset B;$$

znak $\subset$ čita se »*je dio od*« ili »*je sadržano u*« ili »*leži u*«, »*je uključeno u*«, itd. Govori se o *relaciji (odnosu) inkluzije.*

Umjesto $A \subset B$ piše se i *dualno* $B \supset A$ i govori da je B *nadskup ili kratnik* (multiplum) od A ili da B sadržava A kao svoj dio, itd.

1.8.3. Definicija. *Ako je i* $A \subset B$ *i* $B \subset A$, *piše se* $A = B$ *i govori da je A jednako B.* Ako nije $A = B$, piše se $A \neq B$ i govori da je A *nejednako B.* Drugim riječima, za skupove A, B jednakost $A = B$ znači upravo ove dvije stvari: $A \subset B$ i $A \supset B$. To je vanredno važno imati na umu **(zlatno pravilo o jednakosti skupova).**

1.8.3.1. *Napomena.* Upamtimo da pri $A \subset B$ može biti $A = B$; posebno je $A \subset A$ za svaki skup A (u ovom izdanju znak $\subset$ stoji umjesto znaka $\subseteq$ u prvom izdanju).

1.8.4. Definicija. Ako je $A \subset B$ i $A \neq B$, piše se $A \subsetneq B$ i kaže da je *A pravi podskup* (dio) od *B*. Umjesto $A \subsetneq B$ piše se dualno $B \supsetneq A$ i govori da je *B pravi nadskup* od *A*.

1.8.5. Smatra se da je $\varnothing \subset M$ za svaki skup *M* ($\varnothing$ je prazni skup ili nulion). Ako je *M* neprazno, onda je $\varnothing \subsetneq M$.

1.8.6. Skup svih dijelova skupnosti *M* označuje se sa *PM* i zove *partitivni* ili *diobeni skup skupnosti M*.

1.8.7. r-člane kombinacije mnogosti *M* (isp. pogl. 2, § 3.10).

Definicija. Ako je *r* kardinalan broj, a *M* mnogost, tada se sa

$$\binom{M}{r} \quad \text{(čitaj: } M \text{ iznad } r\text{)}$$

označuje skup svih dijelova mnogosti *M* po *r* članova, tj. ako je $x \subset M$ i $kx = r$, tada je

$$x \in \binom{M}{r}, \qquad \text{i obrnuto.}$$

Tako npr. $\binom{I4}{2} = \big\{\{0, 1\}, \{0, 2\}, \{0, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\big\}$; sjetimo se da je $I4 = \{0, 1, 2, 3\}$. Isto je tako

$$\binom{I4}{1} = \big\{\{0\}, \{1\}, \{2\}, \{3\}\big\}, \quad \left\{\binom{I4}{4}\right\} = \big\{\{0, 1\ 2, 3\}\big\},$$

$$\binom{I4}{n} = \varnothing \text{ (prazno) za } n > 4.$$

1.8.8. Zadaci o skupovima.

1. Što su članovi mnogosti: $\{1, 2, 3\}$, $\big\{\{1, 2\}, 3\big\}$ $\big\{\{1, 2, 3\}\big\}$? Koji od ta tri skupa ima najviše članova?
2. Je li relacija $3 \in A$ ispravna ili nije ispravna u svakom od ovih slučajeva: $A = \{3, 4, 5\}$, $\{3\}$, $\big[\{3, 5\}, 8\big]$, $\big[2, \{3\}, \{5\}, \{2, 3, 5\}\big]$?
3. Što je $I5$, a što je $1(5)$? Je li $I5 \subset 1(5)$? A $1(5) \subset I5$?
4. 1) Odredi $PI4$. Koliko ta mnogost ima članova? Odredi joj sve dvočlane članove. 2) Isto pitanje za $PI6$, $PI10$, $P\{a, b, c, d\}$.
5. Navedi nekoliko skupova i nekoliko predmeta koji: a) pripadaju; b) ne pripadaju tim skupovima.
6. Odredi nekoliko predmeta i njihov skup.
7. Navedi nekoliko slučajeva u kojima se pojavljuje prazan skup.
8. Odredi $\binom{I4}{r}$ za $r = 1, 2, 3, 4, 5, 100, 0, 10^5$.

9. Ako su A, B, C skupovi pa ako je (1) $A \subset B$, $B \subset C$, onda je $A \subset C$; pri tom posljednje $\subset$ *znači* $\subsetneq$ *ako u* (1) znak $\subset$ stoji za $\subsetneq$ najmanje jedanput. Dokaz!

10. Zašto ne može biti $A \subsetneq B$ i $B \subsetneq A$ istovremeno?

11. Je li $\{1, 2\ 3\} = \{1, 1, 2, 2, 3\}$? Zašto je $\{5, 5, 5\} = \{5\}$?

12. Neka je $G(10^6)$ *skup gradova, od kojih svaki ima najmanje* 10^6 stanovnika; navedi nekoliko članova toga skupa. Je li u godini 1961. koji grad Jugoslavije član toga skupa? A u 1970. godini?

13. Navedi primjer množine koja se sastoji od: 1) 5 jednadžbi; 2) 5 konkretnih *predmeta:* 3) 5 trokuta; 4) 5 funkcija; 5) 5 zvijezda.

14. Navedi *sve članove* OUN u godini 1969; je li OUN jedan skup?

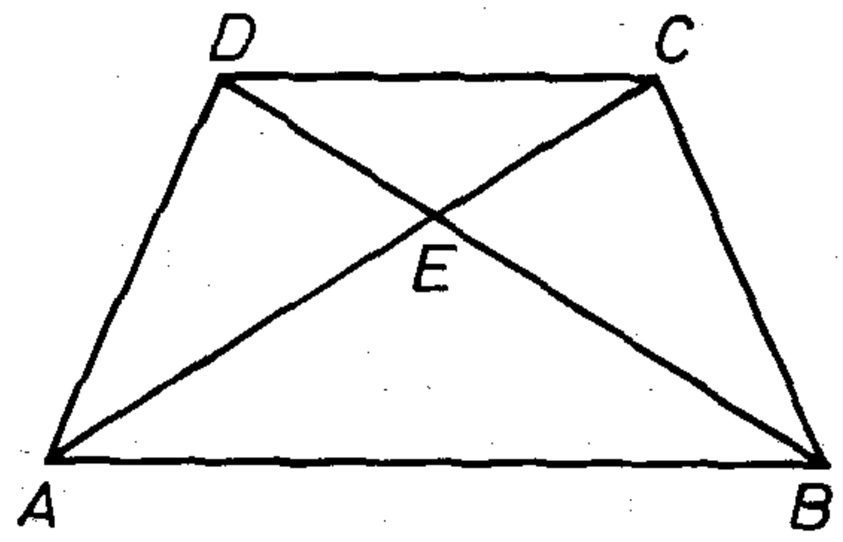
15. Navedi *po jedan skup iz* oblasti: 1) strojeva; 2) alata; 3) tkanina; 4) ljudi; 5) lijekova; 6) zvijezda; 7) vještačkih satelita; 8) velikih otkrića, 9) neriješenih matematičkih problema, itd.

2. ALGEBRA SKUPOVA ILI MNOGOSTI

Radi se o tome da se zadanoj množini skupova pridruže drugi skupovi, kao što je zajednički dio (presjek), unija itd.

2.1. *Zajednički* dio ili presjek skupova ($\cap$-operator).

2.1.1. P r i m j e r i. 1. Neka je $ABCD$ trapez i $AB \parallel CD$; tada dijagonale AC, BD imaju jednu zajedničku tačku, nazovimo je E, a trokut ΔABC i ΔBCD imaju čitav ΔABE kao svoj *zajednički dio.* U zavisnosti od skupova ABC, BCD piše se: $\Delta ABC \cap \Delta ABD = \Delta ABE$; također se piše: $AC \cap BD = \{E\}$. Svi dijametri kugle imaju središte O kugle, odnosno skup $\{O\}$ kao svoj zajednički dio.



Sl. 2.2.1.1.

2.1.2. D e f i n i c i j a. *Pod presjekom ili zajedničkim dijelom zadanih skupova razumijevamo* ***najobuhvatniji*** *zajednički dio svih tih skupova,* tj. presjek zadanih skupova je *skup* sastavljen od svih onih predmeta koji su elementi u *svakom* od tih zadanih skupova.

Presjek skupova A, B označuje se sa $A \cap B$; presjek skupova A_0, A_1, A_2, označuje se sa $A_0 \cap A_1 \cap A_2$ ili $\cap A_i$ $(i = 0, 1, 2)$. Presjek skupova A_0, A_1, $A_2 \ldots$ označuje se sa $A_0 \cap A_1 \cap A_2 \ldots$ ili $\cap A_k$; *pritom* k *prima vrijednosti* 0, 1, 2, ...

Ako je S *skup množinâ,* tada se presjek tih množinâ označuje sa $\cap S$ ili potpunije:

$$\bigcap_{X \in S} X. \tag{1}$$

Imajmo na umu ovo:

ako je $a \in \bigcap X$, *onda je* $a \in X$ *za svako* $X \in S$; *i obrnuto.*

Specijalno, $A \cap B$ je sastavljeno od svih x-ova za koje je $x \in A$ i $x \in B$.

P r i m j e d b a. Naravno da se u oznaci (1) umjesto znaka X može uzeti kakav god drugi znak.

2.1.3. D e f i n i c i j a. *Kaže se da su dva skupa* ***disjunktna****, razdvojena ili mimoležna ili strana jedan drugom ako im je presjek prazan*, tj. $A \cap B = \varnothing \Leftrightarrow A$ i B su disjunktni. Tako su npr. dvije pravulje u ravnini paralelne ako im je presjek prazan skup.

2.1.4. D e f i n i c i j a. Skup množina je *disjunktan* ili *disjunktivan* ako su mu dva po dva člana disjunktna. Tako npr. skup sastavljen od $\{0\}$, skupnosti svih pozitivnih brojeva i skupnosti svih negativnih brojeva je tročlan i disjunktan.

2.1.5. N a p o m e n a. Imaj na umu da je presjek skupova opet skup (prazan, jednočlan ili višečlan); presjek zadanih skupova je određen dio ***svakog*** od tih skupova („faktora“).

Specijalno je $A \cap A = A$ za svaki skup A; $A \cap \varnothing = \varnothing$.

2.2. Unija, zbir ili udruženje skupova ($\cup$-operator). P r i m j e r. Krug je unija svojih dijametara u tom smislu da je krug sastavljen od svih tačaka koje su članovi *bar jednog* od dijametara kruga. Kaže se da je krug unija i svojih tačaka.

2.2.1. Definicija unije. Neka je S zadan skup skupova; pod *unijom, udruženjem ili zbirom* članova skupa S razumijevamo *najmanji skup* u kojem se svaki član skupa S pojavljuje kao dio. Unija se označuje sa $\cup S$ ili ispisanije:

(1) $$\bigcup_{X \in S} X, \quad \text{odnosno} \quad \bigcup_{X \in S} X.$$

Prema tome, *svaki član svakog člana iz* S ulazi kao član i u zbir; obrnuto, time se dobije svaki član zbira skupova.

Drugim riječima: ako je $x \in X \in S$, tada je $x \in (1)$; i obrnuto: ako je x član unije (1), tada je najmanje za jedno $X \in S$ ispunjeno $x \in X$. Naravno da pojedini član unije može biti član u više „sastojaka“. Međutim, treba definirati i uniju množine zadanih skupova i elemenata koji nisu skupovi.

2.2.2. D e f i n i c i j a. Neka je S zadani skup; neka je S_0 skup svih onih članova iz S koji nisu skupovi; pod unijom elemenata skupa S razumijevamo uniju množine S_0 i svih skupova — članova iz S. Ta se unija označuje kao i u definiciji 1.

Tako je npr. svaki kvadrat unija svojih tačaka. Svaki skup brojeva je unija svojih članova.

Unija ili zbir od A, B označuje se sa $A \cup B$; unija od A_0, A_1, A_2 označuje se sa $A_0 \cup A_1 \cup A_2$ ili $\bigcup_{k=0,1,2} A_k$; unija od A_0, A_1, A_2 ... označuje se sa $A_0 \cup A_1 \cup A_2 \cup \ldots$

Specijalno se vidi da je

$$A \cup A = A \text{ za svaki skup } A$$

$$A \cup \varnothing = A.$$

2.3. Rastavljanje zadane množine. Kad je skup M unija skupova $A, B, \ldots,$ govori se također da je skup M *rastavljen* na $A, B, \ldots$; to rastavljanje mnogosti M je *disjunktno* (*mimoležno*) ako su dva po dva dobivena sastojka $A, B, \ldots$ disjunktna (mimoležna).

Specijalno, za svaki skup M i svaki njegov dio X imamo rastav od M na X i ostatak $M \setminus X$.

Tako npr. ako za neki skup S realnih brojeva i realne brojeve a i b za koje je $a<b$ označimo sa $S(a, b)$ skupnost svih onih brojeva iz S koji su položeni između a i b, tada za svaki broj $x \neq 0$ možemo promatrati intervale:

$$S(0, x), \quad S(x, 2x), \quad S(2x, 3x), \ldots$$

Dva po dva takva intervala su disjunktna.

Očigledno je S unija od skupova $S[nx, (n+2)x]$, kad n prolazi skupom D svih cijelih brojeva.

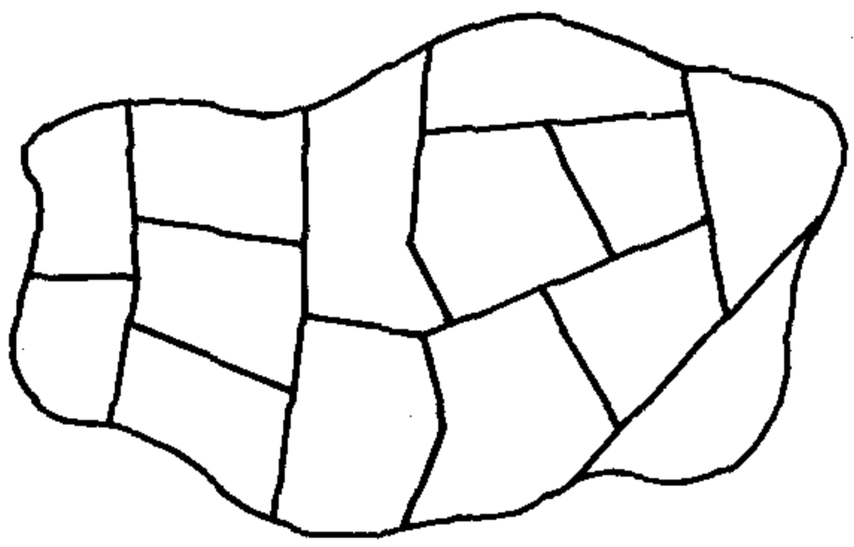
Mnogost K svih kugala može se rastaviti u razrede kugala s istim središtem. Tako se dobije određen skup S razreda kugala.

Unija svih tih razreda je, naravno, polazni skup K kugala. Simbolički $\cup S = K$ ili potpunije

$$\bigcup_{x \in S} x = K.$$

Rastavljanje skupova i sastavljanje skupova su operacije od vanredno velike važnosti. Naročito ističemo vanrednu važnost procesa da se zadani skup rastavi i onda promatra sistem (skup) dobivenih parcela (dijelova) — parcele mogu, ali ne moraju biti disjunktne.

Tu na slici imamo zadan skup, zadanu parcelaciju i skup parcela ili čestica.



Sl. 2.2.3.

2.4. Oduzimanje *ili* odstranjivanje skupova. Primjer. Promatrajmo $\{0, 1, 2, 3, 4, 5, 6\}$; odstranimo li odatle sve parne brojeve, ostaje $\{1, 3, 5\}$.

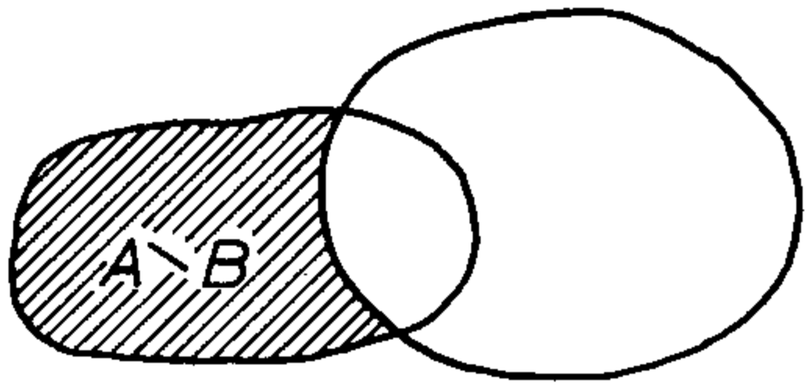
2.4.1. Definicija. Ako iz skupnosti A odstranimo sve one članove koji su i članovi skupnosti B, preostala se skupnost zove *preostatak* ili *diferencija skupova* A, B i označuje sa

$$A \setminus B, \text{ (čitaj: } A \text{ bez } B)$$

Skup $A \setminus B$ zove se i *komplement* skupa B u odnosu na skup A pa se označuje sa $C_A B$.

Specijalno vidimo ovo: ako je $A \cap B = \varnothing$, tj. ako A i B nemaju nijednog zajedničkog elementa, tada je $A \setminus B = A$.

Ako je $A \supset B$, onda je



Sl. 2.2.4.1.

$$(A \setminus B) \cup B = A.$$

Ako nije $A \supset B$, onda je $(A \setminus B) \cup B \supsetneq A$.

Odmah se vidi da je

$$A \setminus B = A \setminus (A \cap B).$$

Prema tome, $A \setminus B$ daje ono što je u A, a nije u B.

2.4.2. Simetrična diferencija. *Simetrična diferencija* $A \dot{-} B$ skupova A i B je unija od $A \setminus B$ i $B \setminus A$, tj.

$$A \dot{-} B = (A \setminus B) \cup (B \setminus A).$$

Ta diferencija sadrži ono što je u A ili B, ali nije u obojem, tj.

$$A \dot{-} B = (A \cup B) \setminus (A \cap B).$$

To se odmah vidi.

2.5. Polje ili tijelo skupova.

2.5.1. Definicija. Za neki skup S skupova kaže se da je *polje* ili *tijelo skupova* ako iz $A \in S$ i $B \in S$ izlazi $A \cup B \in S$ i $A \setminus B \in S$, tj. ako je ispunjen ovaj uslov:

$$\{A, B\} \subset S \Rightarrow \{A \cup B, A \setminus B\} \subset S,$$

odnosno

$$(A \in S) \wedge (B \in S) \Rightarrow (A \cup B \in S) \wedge (A \setminus B \in S).$$

Izrazito polje skupova čine rješenja X relacije $X \subset A$.

2.6. Nekoliko pravila o operacijama sa skupovima.

2.6.1. Za *sječenje* skupova lako se dokazuju ova pravila:

$$A \cap B = B \cap A \quad \text{(komutacija)}$$

$$(A \cap B) \cap C = A \cap (B \cap C) \quad \text{(asocijacija)}$$

$$A \cap A = A \quad \text{(idempotencija)}.$$

Ako je $A \subset B$, onda je $A \cap B = A$; i obrnuto (zakon apsorpcije).

2.6.2. Za *udruživanje* skupova važe dualna pravila: u gornjim obrascima dopušteno je svuda pisati $\cup$ umjesto $\cap$, te istodobno $\supset$ umjesto $\subset$.

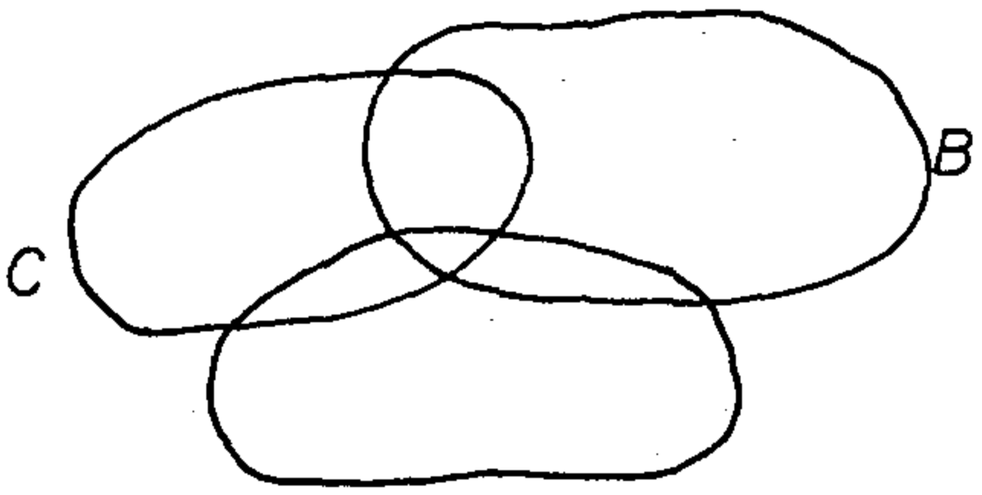
Tako npr. zakon apsorpcije postaje: ako je $A \supset B$, onda je $A \cup B = A$; i obrnuto.

2.6.3. *Zakoni distribucije* (*raspodjele*). Sa slike se odmah vidi da je sječenje distributivno svojstvo prema udruživanju,

tj. $(A\cup B)\cap C=(A\cap C)\cup(B\cap C)$

i »*dualno*«:

$(A\cap B)\cup C=(A\cup C)\cap(B\cup C)$.



Sl. 2.2.6.3.

Dokaz. Dokažimo (1). To znači da treba dokazati ovo:

$$x\in(1)_1 \Leftrightarrow x\in(1)_2.$$

No, to izlazi iz ovoga lanca ravnovaljanih vezâ:

$$x\in(1)_1 \Leftrightarrow x\in(A\cup B)\cap C \Leftrightarrow$$

$$(x\in A\cup B)\wedge(x\in C) \Leftrightarrow ([x\in A]\vee[x\in B])\wedge(x\in C)$$

$$\Leftrightarrow([x\in A]\wedge(x\in C))\vee([x\in B]\wedge(x\in C)) \Leftrightarrow$$

$$x\in(A\cap C)\vee(x\in B\cap C) \Leftrightarrow x\in[(A\cap C)\cup(B\cap C)] \Leftrightarrow x\in(1)_2.$$

2.7. Operator okupljanja { }. Primjer. Promatrajmo skup $S(30)$ svih prirodnih brojeva kojima je kvadrat <30; taj skup možemo opisno označiti sa $\{x;\ x\in N,\ x^2<30\}$ ili potpunije: $\{x;\ x\in N\wedge x^2<30\}$.

Definicija. Skup svih članova mnogosti M koji zadovoljavaju stanovitim pogodbama $A, B, \ldots$ označuje se sa $\{x;\ x\in M, A, B, \ldots\}$; tu se znak $\{x;$ čita „skup svih x za koje vrijede ovi uslovi“. Tu je specijalno važno da imamo: *početak i svršetak skupovne vitičaste zagrade* { } u koju se stavi proizvoljni član x iz M za koji član vrijede propisani uslovi.

Npr. za skup R realnih brojeva definiramo $R(0, 1)=\{x;\ x\in R\wedge x>0\wedge x<1\}$ umjesto logičkog znaka $\wedge$ stavlja se i , (zarez).

Još jedan primjer: vidi se da je za skupove A, B ispunjeno $A\cap B=$ $=\{x;\ x\in A\wedge x\in B\}$.

2.8. Zadaci o skupovima

1. Nađi presjek $A\cap B$ ovih skupova A i B: 1) $\{1, 2, 3, 4\}$, $\{3, 5, 4, 8, 9\}$; 2) A je skup velikih latinskih slova, B je skup velikih ćirilskih slova; 3) A je trokut, B je duž.
2. Navedi nekoliko X-ova za koje je $\{2, 3, 4\}\subset X$; nađi presjek svih takvih skupova.
3. Kakav sve može biti presjek dvaju trokuta?
4. A presjek trokuta i kruga?
5. Razmatraj *Paschov* [Paš] *aksiom*: zadan je $\triangle$ i takva pravulja 1 u njegovoj ravnini koja ne sadrži ni jednog vrha trokuta; tad je presjek pravulje i trokuta ili prazan skup ili duž.

6. Kako izgleda presjek dvaju elementarnih geometrijskih skupova uzetih iz skupa duži, trokuta, poligona, krugova, kugala, piramida itd? Navedi npr. što sve može biti presjek dviju kocaka.

7. Kako izgleda unija od 2, 3, 4, 5 duži? Crtaj.

8. Isto pitanje za: 1) zrake; 2) pravulje.

9. Zadaj tačku, duž, zraku i pravulju; kako im izgleda unija u najopćenitijem, a kako u najspecijalnijem slučaju?

10. Označimo sa $S(x, y)$ skup svih članova iz S koji su smješteni između x i y; stavimo $S[x, y) = \{x\} \cup S(x, y)$, $S(x, y] = S(x, y) \cup \{y\}$, $S[x, y] = \{x\} \cup S(x, y) \cup \{y\}$. Neka je $N = \{1, 2, 3, \ldots\}$; nađi $N(1, 10)$, $N[1, 10)$, $N(2, 8) \cup N(3, 15)$, $N[8, 3) \cup N(1, 1]$.
Nađi $N[1, 5) \cup N[5, 20)$, $N(1, 3) \cup N(2, 4) \cup N(3, 5) \cup \ldots$

11. Dokaži da je $N = \bigcup_{k \in N} N[5k, 5(k+1)) \cup N[1, 5)$.

12. Promatraj duž $\overline{AB}$; neka je $X \in \overline{AB}$; što je onda $\overline{AB} \setminus \{X\}$? Kad će i to biti duž?

13. Ako je S pravulja i $T \in S$, od čega se sastoji $S \setminus \{T\}$?

14. Isto pitanje ako je S zraka, krug, ravnina, trokut, prostor.

16. Neka je k zadani krug, a Rk njegova ravnina. Što je $Rk \setminus k$?

17. S pravulje odstrani jednu, dvije, tri tačke. Što još preostaje?

18. Nađi $N \setminus 2N$, $N \setminus \{-2, -1, 0, 1, 2, 3\}$, $\{0, 1, 2, 3\} \setminus N$,
$\{1, 2, 3, 4, 5, 6\} \setminus \{1\}$, $\{1, 2, 3, 4, 5, 6\} \setminus \{\{1\}\}$.
$\{1, 2, 3, 4\ 5, 6\} \setminus \{\{1\}, \{2\}, \{3\}\}$.

19. Promatraj skup $\{1, 2, 3, 4, 5\} = 1(5)$ i sve njegove disjunktne ili d-razdiobe tj. takve razdiobe u kojima su članovi bez zajedničkih članova. Koliko ima d-razdioba skupnosti $1(5)$?

20. Razvrstajmo skup D cijelih brojeva tako da u istu skupinu stavljamo one i samo one brojeve koji pri dijeljenju brojem: 1) 2; 2) 3; 3) 7 daju jedan te isti ostatak. Koliko se skupina dobije? Radi li se u svakom slučaju o d-podjeli skupa D?

21. Zašto podjela četverokuta u kvadrate i trapeze nije potpuna?

22. Je li podjela kutova u konveksne, konkavne, oštre i tupe jedna d-podjela?

23. Izrazi u cm visinu učenika; podijeli učenike u skupine tako da u istu skupinu dođu oni kojima visina leži u $R[150, 155)$, $R[155, 160)$ itd.

24. Nađi $(A \cup B) \cap C$ za ove skupove A, B, C: 1) $\{a, b, 1\}$, $\{b, 1, c\}$, $\{a, 1\}$; 2) pozitivni brojevi, negativni brojevi, racionalni brojevi: 3) baza kocke, baza kocke, površina kocke.

25. Nađi uniju svih pravulja $\perp p$ i njen presjek s pravuljom p.

26. Nađi presjek unije težišnicâ trokuta i oboda i s t o g trokuta.

27. Dokaži ovo: 1) $S_1 \cup S_2 = (S_1 \setminus S_2) \cup (S_2 \setminus S_1) \cup (S_1 \cap S_2)$;
2) $S_1 \cup S_2 \cup S_3 = (S_1 \setminus S_2) \cup (S_2 \setminus S_3) \cup (S_3 \setminus S_1) \cup (S_1 \cap S_2 \cap S_3)$;
3) $S_1 \cup S_2 \cup S_3 \cup S_4 = (S_1 \setminus S_2) \cup (S_2 \setminus S_3) \cup (S_3 \setminus S_4) \cup (S_4 \setminus S_1) \cup$
$\cup (S_1 \cap S_2 \cap S_3 \cap S_4)$. Kako bi glasio sličan obrazac za 5 skupova $S_1, S_2, \ldots S_5$? A za n skupova?

28. Zadan je skup $S = \{1, 2, 3\}$. Nađi rastav i sve najobuhvatnije dijelove X iz tog rastava sa svojstvom da iz $a \in X$, $b \in X$ izlazi: 1) $a \cap b = \varnothing$; ili $a \subsetneq b$, ili $a \supsetneq b$. Nađi uniju članova iz svakog takvog X.

29. Odredi najmanje tijelo skupova kojemu su skupovi $\{1, 2, 3\}$, $\{2, 3, 5\}$ dva člana.

30. Isto pitanje za skupove $R(x, x+2)$, pri čemu x prolazi skupom D svih cijelih brojeva.

31. Kako izgleda najmanje tijelo skupova kojemu pripadaju svi intervali realnih brojeva?

32. Dokaži da za simetričnu diferenciju (isp. § 2.4.2.) vrijede ovi obrasci:

ako je $A = B$, onda je $A \dot{-} B = \varnothing$; i obratno

$$A \dot{-} B = B \dot{-} A$$

$$(A \dot{-} B) \dot{-} C = A \dot{-} (B \dot{-} C)$$

$$A \cap (B \dot{-} C) = A \cap B \dot{-} A \cap C$$

$$A \dot{-} \varnothing = A$$

$$A \dot{-} (A \dot{-} C) = C.$$

33. Što bi značilo $A_1 \dot{-} A_2 \dot{-} A_3$? Poopći i dokaži da se za svaki konačan niz skupova $A_1, A_2, \ldots, A_n$ skup $A_1 \dot{-} A_2 \dot{-} \ldots \dot{-} A_n$ sastoji upravo od onih elemenata koji su članovi u neparnom broju skupova $A_1, \ldots, A_n$.

34. Dokaži ispravnost ovih definicionih relacija služeći se logičkim simbolima $\vee$ (ili), $\wedge$ (i), $\neg$ (nije); (isp. § 2.7):
1) $A \cup B = \{x;\ x \in A \vee x \in B\}$; 2) $A \setminus B = \{x;\ x \in A,\ \neg x \in B\}$;
3) $\cup F = \{x;\ \vee_A,\ x \in A \in F\}$; 4) $\cap F = \{x;\ \underset{A \in F}{\wedge} x \in A\}$.

35. Neka je α zadana ravnina i $O \in \alpha$; neka je r broj > 0; šta znači skup:
1) $\{x;\ x \in \alpha \wedge Ox = r$; 2) $\{y;\ y \in \alpha \wedge Oy < r\}$; 3) $\{y;\ y \in \alpha \wedge Oy > r\}$?

3. O KOMBINACIJAMA

3.0. Problem. Ako je M zadan skup, a r nekakav kardinalan (glavni) broj, odredi broj

$$k\binom{M}{r}$$

svih dijelova (predstavništava) X od M od kojih *svako* X ima r članova.

3.1. Jedno je jasno: jednočlanih predstavnika skupa M ima koliko i članova u M jer svako $x \in M$ može biti proglašeno za predstavnika od M; simbolički:

$$k\binom{M}{1} = k\,M.$$

3.2. Također se uzima po definiciji da je

$$k\binom{M}{0} = 1 \text{ za svaki skup } M.$$

3.3. Jasno je da je

$$k\binom{M}{r} = 0 \text{ za svako } r > k\,M, \text{ jer je tada } \binom{M}{r} = \varnothing.$$

3.4. K o n k r e t a n z a d a t a k. Zadan je odbor O od 10 članova; koliko se može sastaviti raznih pododbora od po 3 člana (naravno, svaki član iz O može biti član raznih pododbora?

Radi preglednosti možemo članove odbora O označiti brojevima 0, 1, 2, 3, 4, 5, 6, 7, 8 9, tako da umjesto skupa O možemo promatrati skup $I\,10 = \{0, 1, \ldots, 9\}$ i njegove članove. Svi traženi pododbori tvore skup $\binom{O}{3}$, odnosno $\binom{I\,10}{3}$.

Tako npr. $\{0, 1, 2\} \in \binom{I\,10}{3}$. Zasad ne znamo koliko članova ima skup $\binom{I\,10}{3}$ kao ni skup $\binom{I\,10}{2}$ svih dvočlanih dijelova iz $I\,10$, no važno je uočiti vezu između članova ta dva skupa $\binom{I\,10}{2}$ i $\binom{I\,10}{3}$.

Tako npr. $\{0, 1\} \in \binom{I\,10}{2}$; $\{0, 1, y\}$ za $y = 2, 3, 4, 5, 6, 7, 8, 9$, tj. za svako $y \in I\,10 \setminus \{0, 1\}$ jesu svi oni članovi $Y \in \binom{I\,10}{3}$ za koje je $\{0, 1\} \subsetneq Y$. Isto tako za svako zadano Y iz $\binom{I\,10}{3}$ imamo upravo 3 člana X iz $\binom{I\,10}{2}$ za koje je $X \subsetneq Y$, a dobiju se tako da se iz Y ukloni po jedan vlastiti član.

Koliko dakle relacije:

$$X \subsetneq Y$$

(1) $$X \in \binom{I\,10}{2}$$

$$Y \in \binom{I\,10}{3}$$ imaju rješenja?

Rješenja ima $k\binom{I\,10}{2} \cdot 8$, odnosno $k\binom{I\,10}{3} \cdot 3$; zato je

(2) $$k\binom{I\,10}{2} \cdot 8 = k\binom{I\,10}{3} \cdot 3.$$

Na sasvim sličan način imamo jednakost:

$$k\binom{I\,10}{1}\cdot 9 = k\binom{I\,10}{2}\cdot 2,$$

što — *s* obzirom na $k\binom{I\,10}{1} = 10$ — daje:

$$10\cdot 9 = k\binom{I\,10}{2}\cdot 2, \text{ odnosno:}$$

$$k\binom{I\,10}{2} = \frac{10\cdot 9}{2}. \tag{3}$$

Zbog veze (3) daje (2) traženi broj:

$$k\binom{I\,10}{3} = \frac{10\cdot 9\cdot 8}{2\cdot 3},$$

dakle:

$$k\binom{I\,10}{3} = 120.$$

3.5. Osnovna formula. Na posve sličan način kao što smo došli do obrasca (2) dokazuje se ova osnovna formula:

Za prirodne brojeve n i *r vrijedi*:

$$k\binom{In}{r-1}\cdot\binom{n-r+1}{} = k\binom{In}{r}r. \tag{4}$$

Naime, broj rješenjâ (X, Y) relacijâ $X \subsetneq Y$, $X\in\binom{In}{r-1}$, $Y\in\binom{In}{r}$ iznosi $(4)_1$, odnosno $(4)_2$, pa odatle tražena jednakost (4).

3.6. Stavimo li u (4) za *r* po redu: 1, 2, 3, 4, . . . , izlazi po redu:

$$k\binom{In}{0}\cdot n = k\binom{In}{1}\cdot 1, \text{ tj. } k\binom{In}{1} = n, \text{ jer je } k\binom{In}{0} = 1$$

$$k\binom{In}{1}\cdot\binom{n-1}{} = k\binom{In}{2}\cdot 2, \text{ tj. } k\binom{In}{2} = \frac{n(n-1)}{2}$$

$$k\binom{In}{2}\binom{n-2}{} = k\binom{In}{3}\cdot 3, \text{ tj. } k\binom{In}{3} = \frac{n(n-1)(n-2)}{2\cdot 3}$$

$$k\binom{In}{3}\binom{n-3}{} = k\binom{In}{4}\cdot 4, \text{ tj. } k\binom{In}{4} = \frac{n(n-1)(n-2)(n-3)}{2\cdot 3\cdot 4}.$$

3.7. Definicija faktorijala: Za svaki prirodni broj *r* stavlja se:

$r! = 1\cdot 2\cdot 3 \ldots (r-1)\cdot r$; $r!$ se čita *faktorijal broja r*.

Stavlja se $0! = 1$.

3.8. Definicija. Za svako $r\in\{0, 1, 2, \ldots\}$ i svaki broj x ili izraz x stavlja se: $\binom{x}{r}=\frac{x(x-1)(x-2)\ldots(x-r+1)}{r!}$. Specijalno: $\binom{0}{0}=1$.

Oznaka $\binom{x}{r}$ čita se x iznad r.

Primjedba. U definiciji izraza $\binom{x}{r}$, x ne mora biti cio broj, pa ni broj; x može biti npr. funkcija, itd.

Npr. $\binom{1/2}{4}=\frac{(1/2)\cdot(1/2-1)\cdot(1/2-2)\cdot(1/2-3)}{1\cdot2\cdot3\cdot4}=\frac{1\cdot-1\cdot-3\cdot-5}{2^4\cdot1\cdot2\cdot3\cdot4}=$

$$=\frac{-5}{2^7}=-2^{-7}\cdot5.$$

3.9. Uz te oznake prethodni obrasci za $k\binom{In}{r}$ postaju

$$k\binom{In}{r}=\binom{n}{r}$$ za svaki prirodni broj n i

svako $r\in\{0, 1, 2, 3, \ldots\}$ (isp. 3. § 9.1).

⟶ **3.10. Teorem.** ***Svih r-članih dijelova skupnosti od n članova ima upravo***

$$\binom{n}{r}=\frac{n(n-1)(n-2)\ldots(n-r+1)}{1\cdot2\cdot3\ldots r}.$$

To je traženi osnovni teorem o kombinacijama.

3.11. Zadaci o kombinacijama.

1. Izračunaj: 1) $\frac{10!}{5!}$; 2) $\frac{15!}{14!}$; 3) $\frac{0!}{0!}$; 4) $\sum_{k=0}^{5}k!$; 5) $\sum_{k=3}^{8}k!$;

   6) $\frac{(n+1)!}{n!}$; 7) $\frac{(n+r)!}{n!}$; 8) $\frac{(n+1)!}{(n-1)!}$; 9) $5!^2-5^2$.

2. Koji je broj veći: 1) $5!^2$ ili $5^2!$; 2) $n!^r$ ili $n^r!$: pri tom razmatranju su n, r prirodni brojevi.

3. Odredi $\binom{x}{2}$ za $x=3, 5, 100, -3, -5, -100; 3^{-1}, 3^{1/2}, u^2+v^2$.

4. Dokaži: 1) $\binom{2r}{r}=2\binom{2r-1}{r-1}$; 2) $\binom{-1}{r}=\left(-1\right)^r$;

   3) $\binom{-2}{r}=\left(-1\right)^r\left(1+r\right)$; 4) $\binom{-n}{r}=\left(-1\right)^r\binom{n+r-1}{r}$;

   5) $\binom{2n}{n}2^{-2n}=\left(-1\right)^n\binom{-1/2}{n}$.

5. Nađi n iz: $\binom{n}{2} =$ 1) 351; 2) 5000; 3) -2^{-3}; 4) -3^{-2};
5) $2^{-n-1}(2^{-n}-1)$.

6) Odredi sve odbore po 3 člana iz danog skupa od 7 osoba. Koliko tih odbora ima?

7. Koliko ima raznih trokuta kojima su vrhovi u zadanom skupu S od 7 tačaka (pretpostavljamo da nikoje tri tačke iz S ne leže na istoj pravulji).

8. Na koliko se načina od 7 olovaka mogu izabrati 3 olovke?

9. Na koliko se načina može k knjiga podijeliti na u učenika tako da svaki učenik dobije po m knjiga? Za k, u, m promatraj npr. ove slučajeve: 1) 8, 2, 4; 2) 8, 4, 2; 3) 12, 3, 4; 4) 12, 4, 3; 5) 12, 8, 4; 6) $u\,m$, u, m; 7) $m\,u$, m, u.

10. U odboru je 7 muških i 5 ženskih; koliko ima pododbora po 4 muška i 2 ženska člana? Poopći problem.

11. Iz posude s $n=10$ kuglica izaberi 6 kuglica i to 2 crvene, 2 žute i 2 bijele, ako u posudi ima po 3 kuglice crvene, žute i bijele te jedna crna kuglica. Na koliko se načina to može učiniti?

12. Na koliko se načina u našoj abecedi mogu izabrati 4 suglasnika i 2 samoglasnika?

13. Zadan je skup S od 9 tačaka; koliko ima: 1) pravulja; 2) ravnina; 3) kuglinih površina; 4) trokuta; 5) tetraedara koji su određeni jednoznačno s elementima iz S.

14. Koliko ima traženih skupova u prethodnom zadatku koji sadrže jednu od zadanih tačaka? Kojih od 5 traženih vrsta skupova ima najviše?

15. Iz skupa $I\,10=\{0, 1, \ldots, 9\}$ odaberi: 1) 3; 2) 7; 3) 5 članova među kojima se mora nalaziti: a) član 8; b) članovi 3, 5. Na koliko je to načina moguće učiniti?

16. Obitelj se sastoji od djeda d, bake b, oca o, majke m, njihove ženske djece $ž_1$, $ž_2$ i muške djece m_1, m_2, m_3. Na koliko se načina predstavništvo od n članova te obitelji može pojaviti na predstavi ako majka m svakako ide na predstavu te sa sobom uzima najmanje jedno od djece i najmanje jedno od d i b? Promatraj slučajeve: $n=1, 2, 3, 4, \ldots, 9$.

17. Odredi broj dijagonala u konveksnom: a) poligonu; b) poliedru od n vrhova ako je poliedar omeđen trokutima.

18. Predstavništvo sveučilišta od k fakulteta $f_1, f_2, \ldots, f_k$ sa po $n_1, n_2, \ldots, n_k$ delegatâ predstavnikâ treba da izabere komisiju u koju predstavnikâ fakulteta f_i ulazi e_i $(i=1, 2, \ldots, k)$ delegata. Na koliko se načina može izabrati tražena komisija? Konkretiziraj.

19. Formuliraj sličan zadatak ako se radi o predstavnicima kakve škole i njenih razreda ili odjeljenja.

20. Iz običnog skupa od 32 karte treba izvući 7 karata, i to: 3 pika, 2 kare, 1 srce i 1 djetelinu. Na koliko se načina to može učiniti?

21. Isti zadatak uz dodatni zahtjev da među izvučenim kartama: 1) ne smije; 2) mora biti karta srce-as.

22. Ako se na ravan pod baci 6 komada dvodinarki, na koliko se načina može desiti da dvodinarke tako padnu da im gornje strane budu: 1) 3; 2) 4 grba?

4. PRIMJENA TEOREMA O KOMBINACIJAMA. BINOMNI I POLINOMNI TEOREM

4.1. Znamo da je $(a+b)^2 = a^2 + 2ab + b^2$

$$(a+b)^3 = a^3 + 3a^2 b + 3ab^2 + b^3;$$

kako da nađemo $(a+b)^n$ za svaki prirodni broj n?

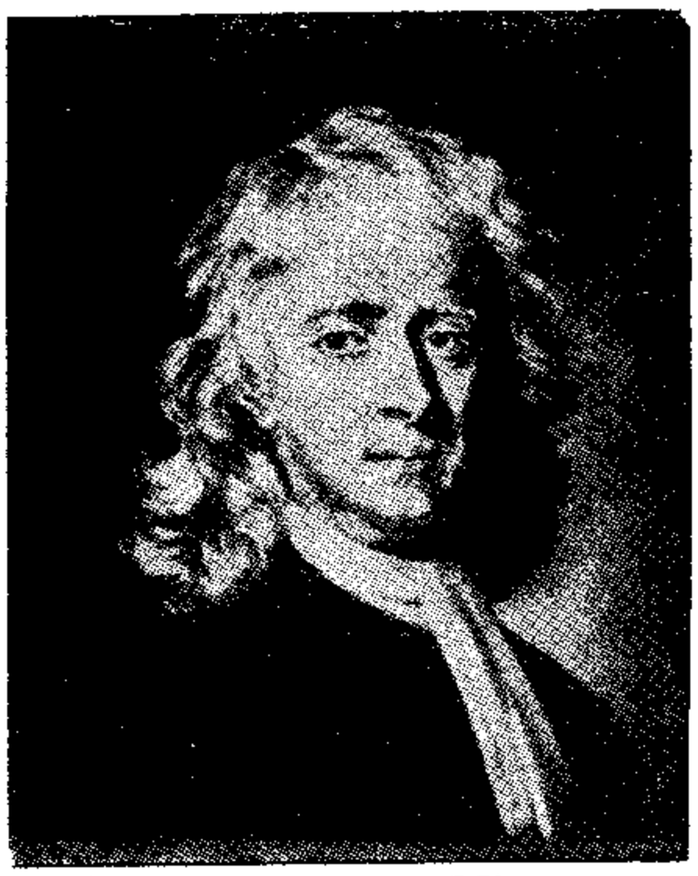
Da se izračuna

$$(1) \qquad (a+b)^n = \underbrace{(a+b)\cdot(a+b)\cdot\cdots\cdot(a+b)}_{n},$$

treba od svakog od tih n faktora uzeti po jedan član, pomnožiti ih i sve sabrati. Ako uzmemo upravo r a-ova, onda smo time obvezani da uzmemo $n-r$ b-ova; no r a-ova se može uzeti na $\binom{n}{r}$ načina; zato u izmnoženom produktu $(1)_2$ imamo i član

$$\binom{n}{r} a^r b^{n-r}.$$

Saberemo li sve te članove za $r = 0, 1, 2, \ldots, n$, dobit ćemo traženi



Isaac Newton (Njutn, 1642 — 1727), veliki engleski matematičar.

4.2. Teorem. **Binomni obrazac**. (Newton)[1)]

$$(2) \qquad (a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}.$$

Brojevi

$$\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{r}, \ldots, \binom{n}{n}$$

zovu se *binomni koeficijenti reda n* ili *poretka n*.

4.3. Napišimo *binomni obrazac u simetričnijem obliku*. Proširimo li razlomak $\dfrac{n(n-1)\cdot\cdots\cdot(n-r+1)}{r!}$ sa $(n-r)!$ dobijemo $\dfrac{n!}{r!\,(n-r)!}$ pa je zato

$$(3) \qquad \binom{n}{r} = \frac{n!}{r!\,(n-r)!} \text{ za svako } r = 0, 1, 2, \ldots, n.$$

[1)] Newton [Njutn] (1642—1727], veliki engleski matematičar.

Na taj način dobijemo obrazac:

$$(4)\qquad (a_1+a_2)^n=\sum_{r_1,\,r_2}\frac{n!}{r_1!\,r_2!}\,a_1^{r_1}a_2^{r_2},\ \text{uz uslov:}$$

$$r_1+r_2=n,$$

$$(5)\qquad r_1,\,r_2\in\{0,\,1,\,\ldots,\,n\}.$$

Dokažimo da sličan obrazac vrijedi za svaki polinom.

4.4. Teorem. **Za svaki prirodni broj k i svako $n\in N$ vrijedi:**

$$(6)\qquad (a_1+a_2+\cdots+a_k)^n=\sum_{r_1\cdots r_k}\frac{n!}{r_1!\,r_2!\cdots r_k!}\,a_1^{r_1}a_2^{r_2}\cdots a_k^{r_k};$$

tu je

$$r_1,\,r_2,\,\ldots,\,r_k\in\{0,\,1,\,\ldots,\,n\},\ r_1+r_2+\cdots+r_k=n.$$

4.5. Dokaz. Obrazac (6) vrijedi za $k=2$ i za svako n. Pokažimo da iz pretpostavke da on vrijedi za $k=s$ i svako n izlazi da on vrijedi i za $k=s+1$ i za svako n.

No

$$(a_1+a_2+\cdots+a_s+a_{s+1})^n=([a_1+\cdots+a_s]+a_{s+1})^n=\text{prema (4)}=$$

$$=\sum_{r_{s+1}=0}^{n}\frac{n!}{(n-r_{s+1})!\,r_{s+1}!}[a_1+\cdots+a_s]^{n-r_{s+1}}a_{s+1}^{r_{s+1}}=$$

(prema (6) su k i n jednako s, odnosno $n-r_{s+1}$) =

$$=\sum_{r_{s+1}=0}^{n}\frac{n!}{(n-r_{s+1})!\,r_{s+1}!}\left[\sum_{r_1\cdots r_s}\frac{(n-r_{s+1})!}{r_1!\cdots r_s!}\,a_1^{r_1}a_2^{r_2}\cdots a_s^{r_s}\right]a_{s+1}^{r_{s+1}}.$$

Tu je $r_1,\ldots,r_s\in\{0,\,1,\,\ldots,\,n-r_{s+1}\}$ i $r_1+\cdots+r_s=n-r_{s+1}$; taj se uslov može nadomjestiti ovim: $r_1,\ldots,r_s\in\{0,\,1,\,\ldots,\,n\}$, $r_1+r_2+\cdots+r_s=n-r_{s+1}$. Kako se nadalje oba znaka Σ u (*) mogu zamijeniti jednim Σ, to (*) postaje

$$=\sum_{r_1\,r_2\cdots r_s\,r_{s+1}}\frac{n!}{(n-r_{s+1})!\,r_{s+1}!}\cdot\frac{(n-r_{s+1})!}{r_1!\,r_2!\cdots r_s!}\,a_1^{r_1}\cdots a_s^{r_s}\,a_{s+1}^{r_{s+1}}.$$

A to je upravo obrazac (6) za $k=s+1$.

Iz činjenice da (6) vrijedi za $k=1$ te da vrijedi za $k=s+1$ čim vrijedi za $k=s$, zaključujemo da (6) vrijedi za *svaki prirodni broj* k.

4.6. Trokutna tablica binomnih koeficijenata.

4.6.1. Za binomne koeficijente

$$(1)\qquad \binom{n}{r}=\frac{n(n-1)(n-2)\cdots(n-r+1)}{r!},\quad r=0,\,1,\,\ldots,\,n$$

lako se vidi da vrijedi obrazac:

$$\binom{n+1}{s}=\binom{n}{s-1}+\binom{n}{s},\ (s=1,\ 2,\ \ldots,\ n+1). \tag{2}$$

Obrazac (2) dokazuje se formalno pomoću (1), a vidi se da on iskazuje kako se s-člani dijelovi iz $I(n+1)$ grade iz s-članih dijelova množine $In=\{0,\ 1,\ \ldots,\ n-1\}$.

4.6.2. Stavljamo li po redu $n=0,\ 1,\ 2,\ 3,\ 4,\ \ldots$, tada brojevi (1), ako ih ispisujemo za svako n u posebnom retku, daju ovu tablicu:

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
. . . .

Tu svaki član koji nije krajnji izlazi kao suma od neposredno gornjeg člana i onoga koji je lijevo do ovoga. To je smisao *rekurzione formule* (2). Na taj način vidimo da nam (2) omogućuje sastaviti gornju tablicu — jer krajnji članovi tablice svakako su 1; naime:

$$\binom{n}{0}=\binom{n}{n}=1 \qquad \text{za } n=0,\ 1,\ 2,\ \ldots \tag{3}$$

Drugim riječima, iz (2) i (3) nužno proizlazi (1). Formalan dokaz te činjenice nije baš tako jednostavan.

4.6.3. Iz tablice binomnih koeficijenata očitavamo da je svaki redić te tablice simetričan u tom smislu da su članovi koji su jednako udaljeni od početka i od svršetka redića međusodno jednaki. Formalno, to znači da je

$$\binom{n}{r}=\binom{n}{n-r} \quad \text{za } r=0,\ 1,\ 2,\ \ldots,\ n. \tag{4}$$

Dokaz te jednakosti vrlo je jednostavan. Naime, neka je X kakav r-člani dio množine In; preostatak $In\setminus X$ ima $n-r$ članova; različitim X-ovima odgovaraju različiti skupovi $In\setminus X$; a to upravo znači da različitih X-ova i različitih skupova oblika $In\setminus X$ ima jednako mnogo; no to se i hoće izreći jednakošću (4).

4.6.4. Primjedba. Gornja trokutna tablica obično se zove Pascalov [Paskal] trokut, no pojavljuje se već 1303. god. u knjizi kineskog matematičara Ču-Ši-Keja „Dragocjeno ogledalo četiriju elemenata".

4.7. Zadaci o binomnom razvoju.

1. Nađi: a) $(x+y)^2$; b) $(x+y)^3$; c) $(x+y)^4$ ako $x+y$ znači:
   1) $2x-3y$; 2) $3a^2b+4ab^2$; 3) $a^{-1}+b^{-2}$; 4) $0,\ 32+3,\ 25$;
   5) $2ab^{-1}+3ba^{-1}$.

2. Nađi 5. član u razvoju za $(3x^2y-5{,}8xy^{-2})^n$ za $n=5, 6, 7, 8$.
3. Nađi 8. član u razvoju za $\left(\frac{x^{1/2}}{4}-\frac{2y}{x^{5/2}}\right)^{12}$.
4. Nađi središnji član u razvojima iz zadatka 2.
5. Nađi najveći koeficijent u razvoju $(x+y)^8$.
6. Isto za: 1) $(3x^2+5y^3)^8$; 2) $(a^x+a^{-x})^5$.
7. Nađi koeficijent od x^2 u razvoju za: 1) $(1+3x)^5$; 2) $(x^2+2x^{-1})^6$; 3) $(3x^{-1}+x+1)^2$; 4) $(x+x^{-2}+x^{-3}+1)^3$.
8. Nađi konstantni član u razvoju iz zadatka 7.
9. $(x+y-z)^n=?$ za $n=2, 3, 4, 5$.
10. Nađi koeficijent od x^2 u razvoju za $(1+x+x^{-1}+x^2)^3$.
11. U razvoju za $(1+0{,}02)^8$ nađi članove koji su $>10^{-5}$. Na osnovu toga odredi $1{,}02^8$ na 4 dec.
12. Broj $1{,}02^{10}$ odredi na 4 dec.
13. Isto pitanje za broj $0{,}98^{10}$.
14. Dokaži: 1) $\sum_{r=0}^{n}\binom{n}{r}=2^n$; 2) $\sum_{r=0}^{n}(-1)^r\binom{n}{r}=0$.
15. Dokaži: 1) $\sum_{r=0}^{s}\frac{(n+r)!}{r!}=\frac{(n+s+1)!}{(n+1)\,s!}$; 2)[1] $\binom{n+r+1}{n+1}+\sum_{\nu=r+1}^{s}\binom{n+\nu}{\nu}=\binom{n+k+1}{n+1}+\sum_{\nu=k+1}^{s}\binom{n+\nu}{\nu}$ pri $0\leq r,\ k\leq s\wedge r,\ k\in N$.
16. Ako je n prirodan broj, onda to vrijedi i za brojeve: 1) $(2n)!/(n!\,2^n)$; 2) $(2n-2)!\ n!/(n-1)!$.

5. PRINCIP TOTALNE INDUKCIJE

5.1. Prirodne brojeve 1, 2, 3, ..., *nižemo po redu* tako da poslije svakog prirodnog broja n dolazi *naredni prirodni broj* $n+1$; na taj način i dolazimo do *niza svih prirodnih brojeva*: $1,\ 1+1=2,\ 2+1=3,\ 3+1=4, \ldots, n, n+1, \ldots$

5.2. Množinu svih prirodnih brojeva označujemo sa N; dakle je po definiciji $N=\{1, 2, 3, 4, 5, \ldots, n, n+1, \ldots\}$.

U tome načinu pisanja — da poslije n stavljamo i zamišljamo $n+1$ — sastoji se *princip totalne* (*potpune*) *indukcije* za skup prirodnih brojeva. Glasi ovako:

5.3. Princip potpune indukcije ili princip prelaženja od n na $n+1$. *Neka skup S ima ova dva svojstva:*

S_1 (*prvo svojstvo*): $1\in S$;

S_2 (*drugo svojstvo*): iz $n\in N\cap S$ izlazi $n+1\in S$ (tj. ako je neki prirodni broj n u S, onda je i naredni prirodni broj $n+1$ u S).

Zaključak. *Onda $N\subset S$, tj. svaki prirodni broj nalazi se u S.*

[1] Dostavio 1970. god. student Kalajdžić Gojko.

5.4. Primjer. Označimo za S skup svih prirodnih brojeva n za koje vrijedi obrazac u teoremu 4.4. Očigledno je $1 \in S$; nadalje smo u § 4.5. dokazali da za svaki prirodni broj k iz $k \in S$ izlazi $k+1 \in S$. Znači da su za skup S ispunjena oba gornja induktivna uslova; prema principu totalne indukcije zaključujemo da je $N \subset S$; to znači da je obrazac (6) u § 4.4 istinit za svaki prirodni broj k. A u tome se i sastoji iskaz teorema 4.4.

5.5. Napomena. Kod principa potpune indukcije treba razlikovati dvije indukcione pretpostavke i glavni zaključak. Treba razlikovati glavni zaključak $N \subset S$ od druge indukcione pretpostavke, u kojoj se pojavljuje beskonačno mnogo zaključaka u obliku: ako je $n \in S$, onda je također $n+1 \in S$ (relacija $n+1 \in S$ je *unutarnje svojstvo* od S; relacija $N \subset S$ je *svojstvo od N prema S*). *Početnik često brka indukcione pretpostavke S_2 i glavni zaključak.*

5.6. Princip totalne indukcije ima vrlo veliku ulogu u matematici. Na osnovu toga principa možemo dokazati ovaj *princip indukcije*:

Neka je a bilo koji cio broj. Ako za neki skup S znamo da je $a \in S$ te da iz $x \in S \cap D$ izlazi $x+1 \in S$, onda je $D[a_1 \cdot) \subset S$, tj. svaki cio broj koji je $\geq a$ član je u S.

Primjer za primjenu potpune indukcije. **Dokažimo da binomni obrazac**

$(1)^n \quad (a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}$ **vrijedi** za sve redne brojeve $n = 0, 1, 2, \ldots$

Neka je S skup svih rednih brojeva n za koje vrijedi obrazac $(1)^n$. Po dogovoru, obrazac $(1)^0$ vrijedi za $n=0$, jer je i $(1)^0_1$ i $(1)^0_2$ jednako 1. Dakle je $0 \in S$; dokažimo da za svaki redni broj m relacija $m \in S$ ima za posljedicu $m+1 \in S$.

Relacija $m \in S$ znači ispravnost formule $(1)^m$. Idemo da dokažemo da zaista vrijedi i $(1)^{m+1}$, tj. da je lijeva strana $(1)_1{}^{m+1}$ jednaka desnoj strani $(1)_2{}^{m+1}$ u relaciji $(1)^{m+1}$. No,

$$(1)_1{}^{m+1} = (a+b)^{m+1} = (a+b)^m (a+b) = (\text{po pretpostavci da vrijedi } (1)^m) =$$

$$= \left(\sum_{r=0}^{n} \binom{m}{r} a^r b^{m-r} \right) (a+b) = (\text{po pravilu o množenju}) =$$

$$= \sum_{r=0}^{n} \binom{m}{r} a^{r+1} b^{m-r} + \sum_{r=0}^{m} \binom{m}{r} a^r b^{m+1-r} = (\text{sređeno po uzlaznim potencijama}$$

$a^0, a^1, a^2, \ldots) = a^0 b^{m+1} + \left(\binom{m}{0} + \binom{m}{1} \right) a^1 b^m + \left(\binom{m}{1} + \binom{m}{2} \right) a^2 b^{m-1} + \cdots = (\text{po ob-}$

rascu (2) iz § 4.6.1.) $= a^0 b^{m+1} + \binom{m+1}{1} a^1 b^m + \binom{m+1}{2} a^2 b^{m-1} + \cdots +$

$$+ \binom{m+1}{r} a^r b^{m+1-r} + \cdots + \binom{m+1}{m+1} a^{m+1}.$$ No ovo je upravo $(1)_2{}^{m+1}$.

Dakle je zaista $(1)_1{}^{m+1} = (1)_2{}^{m+1}$, tj. obrazac $(1)^{m+1}$ vrijedi, tj. $m+1 \in S$.

Dakle smo dokazali da iz $m \in S$ izlazi $m+1 \in S$. No $0 \in S$, dakle $0+1 \in S$, pa dakle $1+1 \in S$, pa dakle $2+1 \in S$, itd., svaki prirodni broj $n \in S$, tj. obrazac $(1)^n$ vrijedi za svaki redni broj $n = 0, 1, 2, \ldots$ *Q. E. D.*

5.7. Zadaci o potpunoj indukciji.

1. Dokaži: 1) $\sum_{k=1}^{n} k = \frac{1}{2} n(n+1)$; 2) $\sum_{k=1}^{n} k^2 = \frac{1}{6} n(n+1)(2n+1)$;

3) $\sum_{k=1}^{n} k^3 = \frac{1}{4} n^2 (n+1)^2 = \left(\sum_{k=1}^{n} k \right)^2$;

4) $\sum_{k=1}^{n} k^4 = \frac{1}{30} n(n+1)(2n+1)(3n^2+3n-1)$.

2. Dokaži: 1) $1+3+5+\cdots+(2n-1) = n^2$;

2) $1^2+3^2+5^2+\cdots+(2n-1)^2 = \frac{1}{3} n(4n^2-1)$.

3. Bernoulijeva [Bernuli] nejednakost:
Ako je $1+h > 0$, onda je $(1+h)^n > 1+nh$ za svaki prirodni broj >1 (Jacob Bernoulli, 1689).

B. Pascal (čitaj Paskal, 1623—1662), francuski matematičar, jedan od začetnika principa *potpune* indukcije.

4. Vandermondeova [Vandermonde č. Vandermond] jednakost:
Ako $(x)_n = x(x-1)(x-2)\cdots(x-n+1)$, onda je

$$(a+b)_n = (a)_n + \binom{n}{1}(a)_{n-1}(b)_1 + \binom{n}{2}(a)_{n-2}(b)_2 + \cdots +$$

$$+ \binom{n}{n-1}(a)_1 (b)_{n-1} + (b)_n .$$

5. Ako je $a_0 = 1$, $a_{n+1} = a_n(n+1)$, onda je $a_n = n!$

6. $(n!)^{\frac{1}{n}} \geqq n^{\frac{1}{2}}$. Dokaži.

7. Za bilo koje prirodne brojeve a, b, n vrijedi:

$$\binom{a+b}{n}=\sum_{\nu=0}^{n}\binom{a}{\nu}\binom{b}{n-\nu};\ \text{specijalno}\ \binom{2n}{n}=\sum_{\nu=0}^{n}\binom{n}{\nu}^2.$$

Pokaži indukcijom da formula vrijedi za $a=1$, svako b i svako n; onda dokaži da vrijedi i za svako a.

8. Za svaki prirodni broj n broj $\frac{1}{4\sqrt{2}}[(3+2\sqrt{2})^n-(3-2\sqrt{2})^n]$ je prirodan. Dokaži.

9. Ako je $k,\ n\in N,\ x_1,\ldots,x_n\geq 0$ te $\sum_{\nu=1}^{n}x_\nu=n\,a$, onda je

$$\sum_{r_1,\ldots,r_n=0}^{k}\frac{x_1^{r_1}\cdots x_n^{r_n}}{r_1!\ldots r_n!}\leq n\,(n^k-1)\,\frac{a^{k+1}}{(k+1)!}$$

(dostavio Kalajdžić Gojko).

Literatura

Kurepa Đ. [1], [2].

POGLAVLJE 3.

ALGEBRA FUNKCIJA

POJAM FUNKCIJE ILI PRIDRUŽIVANJA[1)]

Taj je pojam od osnovne važnosti. On je odraz činjenice da se u prirodi sve mijenja, da se prirodne i društvene pojave zbivaju u međusobnoj zavisnosti i povezanosti. Tako npr. određenom predmetu pripada određen naziv (ime), određenom fizičkom predmetu pripada određena težina, određeno težište, itd. Određenoj količini jednog oblika energije pridružena je određena količina druge energije; u izrazu $2x$ svakom broju x pridružen je broj $2x$, itd. Kad se govori o nizu kuća, predmeta, događaja ..., onda znamo šta je tu *prvi* član šta *drugi*, itd. tako da se opet radi o „*pridruživanju*" tih predmeta i rednih brojeva: *prvi*, *drugi*, *treći*, ..., pa možemo govoriti o stvari 1, o stvari 2, stvari 3, itd.

Sve nas to upućuje da postavimo ovu opću definiciju:

• **1.0.** Definicija. *Ako svakom članu neke mnogosti M pridružimo jedan ili više članova skupa S, onda se govori o preslikavanju, funkciji, transformaciji mnogosti M u skup S ili o funkciji od M prema S.*

1.0.1. Primjer. *Numeriranje i šifriranje kao primjeri funkcija.* Ako se radi o pojedinoj mnogosti M, onda je vrlo korisno njene elemente označiti pojedinim šiframa, znakovima (obično pomoću brojeva 1, 2, ...,). Time se dobije mnogo *bolji pregled mnogosti M*, pogotovu ako se raspored unutar M često mijenja. Imajmo na umu npr. slučaj da je M jedna sportska momčad iz neke strane zemlje s imenima koje teško izgovaramo i pamtimo! Ako operaciju numeriranja označimo sa n, onda za svako $x \in M$ oznaka $n(x)$ kazuje broj ili šifru od n; tu preslikavamo M u skup rednih brojeva 1, 2, ...

1.1. Označivanje funkcije. Funkcije se označuju slovima i drugim *simbolima* i *prikratama*. Ako je npr. f naziv za neku funkciju od M prema S, onda se za *svaki* član x iz M zna što je funkcijom f u S pridruženo tome članu x.

1.2.1. Vrijednost funkcije u $x \in M$. *Onaj* element iz S, odnosno *svaki* onaj element iz S, što je pridružen članu x pomoću f označuje se sa fx ili $f(x)$, f_x i sl. i zove se *vrijednost* ili *član funkcije f u x*. Simbolički se to može i ovako prikazati: $x \to fx$ (polazimo od x i dolazimo na fx) ili također $f: M \to S$, $f \mid M \to S$ ili naprosto $f \mid M$.

[1)] Ruski: соотвествие; engl.: mapping; franc.: correspondance; njem.: Abbildung; drugi nazivi: transformacija, operacija, proces, preslikavanje, itd.

1.2.2. Ništište funkcije; b — ište funkcije. Neka je $f: M \to S$ zadana funkcija te $b \in S$; svako $x \in M$ za koje je $fx = b$ zove se *rješenje jednadžbe* $fx = b$ ili *b -ište funkcije f.* Drugim riječima, *b* -ište funkcije *f* je **svaka** vrijednost argumenta u *M* za koju *f* uzima *b* kao svoju vrijednost.

Najčešći je slučaj $b = 0$, pa se umjesto 0-ište piše i govori: *nulište, ništište, nula, nultačka, ništica, ništična tačka...* funkcije fx (v. dopunu 5 § 4.2.2).

Napr. desetište odnosno stotište kvadriranja su brojevi $\pm 10^{1/2}$, odnosno ± 10.

1.3. Funkcija i pripadna skupovna funkcija. Ako je *f* preslikavanje od *M* prema *S*, onda za svako $x \in M$ možemo sa $f\{x\}$ označiti *skup svih vrijednosti* fx što ih *f* prima u *x*; preslikavanje $x \to f\{x\}$ je određena *skupovna funkcija u M.*

1.4. Oblast (domen) i protuoblast (antidomen) funkcije.

1.4.1. Ako je za svako $x \in M$ definirano $fx \in S$, onda se *M* zove *oblast* ili *domen funkcije f*, pa se može označiti i sa *Domf*, *Dof*, ili čak *Df* (čitaj: *domen od f*). Svaki element oblasti funkcije *f* zove se i vrijednost varijable ili promjenljive ili argumenta funkcije *f.*

1.4.2. Unija svih skupova $\bigcup f(x)$ kad *x* prolazi domenom *Domf*, zove se *protuoblast* ili *antidomen funkcije f*; označuje se sa $^{-}Domf$, ^{-}Dof ili čak ^{-}Df (podignut znak $^{-}$ čita se „*protiv*“ ili „*anti*“) ili *Antidom f.* Dakle $Antidom\, f = \bigcup_{x \in Dom\, f} f\{x\}$.

1.5. Poznavanje domena i antidomena od osnovne je važnosti za pojedinu funkciju.

1.5.1. Definicija. **Preslikavanje u skup i preslikavanje na skup.** Ako je *f* funkcija s oblasti *A* i protivoblasti *B*, kaže se da je *f* preslikavanje (transformacija) mnogosti *A* **na** *B* (dakle: preslikavanje ***na*** *B*, a ne samo ***u*** *B*).

1.5.2. Ako je protuoblast funkcije *f* dio od *B*, govori se o preslikavanju *f* od *A* u skup *B* ili u klasu *B.*

Prema tome, preslikavanja **na skup** *B* su specijalan slučaj preslikavanja **u skup** *B.* Tako je npr. kvadriranje određeno preslikavanje skupa *R* u sama sebe, ali nije preslikavanje od *R* na sama sebe.

1.6. Pojam potfunkcije i natfunkcije. Neka je *f* funkcija, a *Dom f* njen domen; neka je $A \subset Domf$; tada se funkcija kojoj je oblast *A*, a u njoj se podudara sa *f*, označuje sa $f|A$ i zove se *potfunkcija funkcije f* ili *restrikcija od f*; kaže se također da je *f natfunkcija* ili *proširenje funkcije* $f|A$. Prema tome, za svako $x \in A$ imamo $(f|A)(x) = fx$. Tako npr. ako je *D* skup svih cijelih brojeva, tada je $\sin \pi x | D$ konstanta 0.

1.7. Jednakost i nejednakost funkcija. Definicija. *Ako je* (f, g) *uređena dvojka funkcijâ, tada je f jednako g, simbolički* $f = g$, *ako je* $Dom\, f = Dom\, g$, i $f\{x\} = g\{x\}$ za svako $x \in Dom\, f$. Ako nije $f = g$, piše se $f \neq g$ i kaže da su *f, g različite* funkcije.

To je vrlo važna definicija. Specijalno se vidi da ne može biti $f = g$ ako je $Dom\, f \neq Dom\, g$.

Zato je jasno, npr., da ima toliko različitih funkcija $2 + x$ za $x \in S$ koliko ima različitih skupova *S* realnih, odnosno kompleksnih brojeva.

1.8. Jednolisne (univalentne) funkcije. To su funkcije f koje u *različitim* tačkama svoje *oblasti imaju različite vrijednosti*, tj. za koje iz $x \in Dom f$, $x' \in Dom f$, $x \neq x'$ izlazi $f\{x\} \neq f\{x'\}$. *One čuvaju relaciju nejednakosti.*

Tako je npr. kvadriranje u skupu pozitivnih brojeva jednolisno, ali već u skupu svih realnih brojeva *nije jednolisno; uistinu je npr.* $-3 \neq 3$, a ipak je $(-3)^2 = 3^2$.

1.9. Jednoznačne ili uniformne funkcije. Neka je f funkcija od M prema S. To znači da za svako $x \in M$, fx znači jedan ili više elemenata iz S; ako, za dano x iz S, fx označuje jedan jedini član iz S, kaže se da je f u tački x *jednoznačno* (*uniformno*). *Funkcija f je jednoznačna ako je jednoznačna u svakoj tački svoje oblasti.*

Ako *f nije uniformno* u x, kaže se da je *f nejednoznačno* ili *neuniformno* u x.

Ako je f jednoznačno za *svako* $x \in A$, kaže se da je *f jednoznačno u A*; ako f nije jednoznačno u A, kaže se da je *f višeznačno* ili *nejednoznačno* ili *multiformno* u A.

Tako je npr. *antikvadriranje*, tj. funkcija $x \to x^{1/2}$, jednoznačno jedino u 0; a za svako $x \neq 0$ ta je funkcija nejednoznačna — upravo *dvoznačna*.

1.10. Tolikovanja.[1] Definicija. *Jednolisno-jednoznačne funkcije zovu se tolikovanja ili bijekcije.*

Definicija. *Tolikovati A* **u** *B, odnosno* **na** *B, znači jednolisno-jednoznačno ili obostrano jednoznačno preslikati A u B, odnosno na B.*[1] (isp. 1.5.1).

Tolikovanja ili bijekcije su važna preslikavanja.

1.11. Identično preslikavanje. Preslikavanje $x \to x$ za svako $x \in A$ zove se *identično* ili *kanonsko preslikavanje* množine A. Obično se označuje sa 1 ili I, odnosno $I \mid A$.

I je posebno tolikovanje.

1.12. Konstantna preslikavanja ili konstante. *To su preslikavanja koja u* svakoj tački svoje oblasti uzimaju *jednu te istu vrijednost.*

Tako npr. konstanta 0 u A jest preslikavanje f za koje je $fx = 0$ za svako $x \in A$.

Ako su A, A^I dva različita skupa, znajmo da npr. konstanta $O \mid A$ nije isto što i konstanta $O \mid A^I$ (isp. t. 1.7.).

1.13. Permutacija ili automorfizam zadanog skupa M zove se svako obostrano-jednoznačno *preslikavanje od M na samog sebe. Skup* svih automorfizama množine M označuje se sa $M!$ (čitaj: *M faktorijal*). Prema tome, iz $f \in M!$ izlazi da je $Dom f = {}^{-}Dom f = M$.

1.14. Zadaci o preslikavanjima.

1. *Odredi nekoliko jednoznačnih funkcija od skupa* $\{1, 2, 3, 4\}$ na skup $\{a, b, c\}$.
2. *Funkcija signum ili znak.* Za svaki broj $x \neq 0$ definira se

$$sgn\ x \equiv \frac{x}{|x|};$$

stavlja se $sgn\ 0 = 0$ (isp. § 2. 1. 1.). Nacrtaj graf funkcije: a) $\operatorname{sgn} x$; b) $\operatorname{sgn} x^2$; c) $\operatorname{sgn}(x^2 - x)$. Odredi protuoblasti tih funkcija.

[1] Te smo nazive uveli u knjižici *Što su skupovi i kakva im je uloga?* Zagreb, 1960, *XII + 191.*

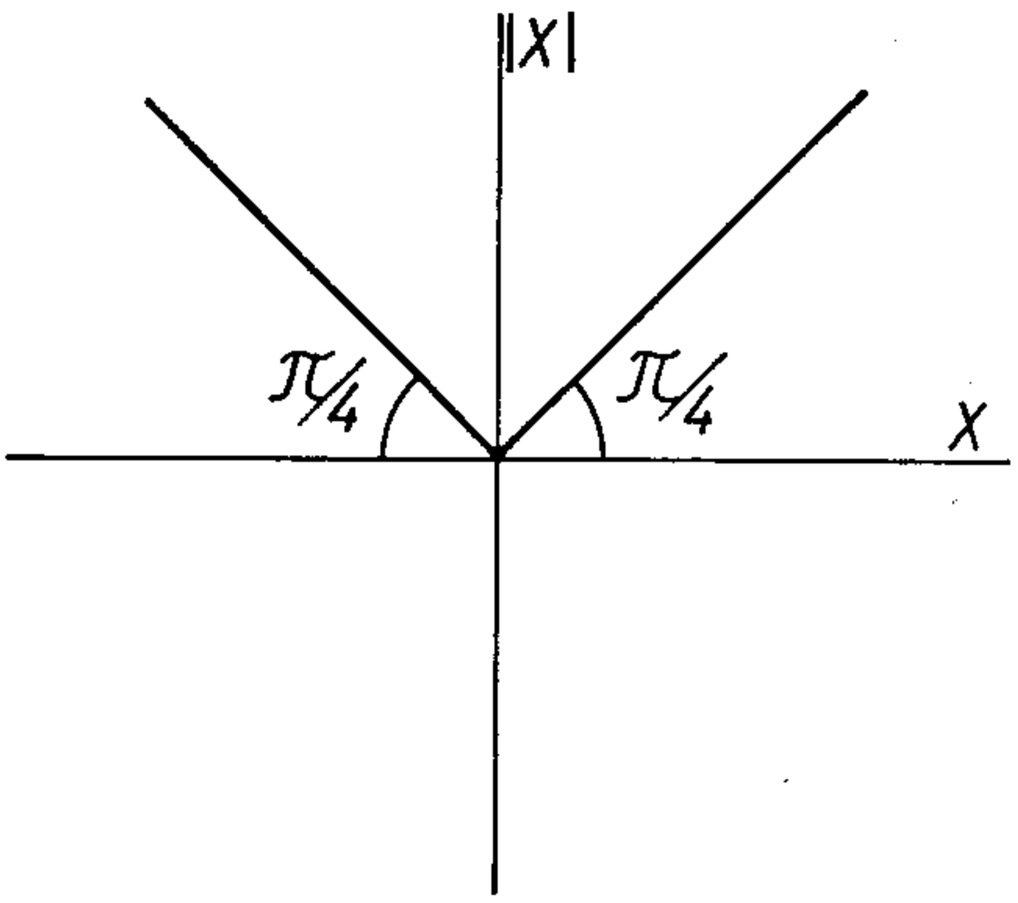
3. Odredi sve permutacije skupnosti {1, 2, 3, 4}; koliko ih ima koje svršavaju sa 4?

4. Prikaži grafički identičnu funkciju $y = 1x$ tj. pridruživanje $x \to x$ za x iz: 1) $I10$; 2) N; 3) D; 4) R; 5) $R(i)$.

2. DVIJE OSNOVNE OPERACIJE S FUNKCIJAMA: OBRTANJE I KOMPONIRANJE

2.1. Funkcija f i pripadna protufunkcija ili antifunkcija ^{-}f.

2.1.1. Primjer: Funkcije *modul* i *antimodul*. Promatrajmo funkciju $y = |x|$ za realne x-ove. Oblast joj je R, a protuoblast skup $R[0, \cdot]$ neodrečnih realnih brojeva. Za svako $y > 0$ postoje u R dva broja $+y$ i $-y$ za koje je $|\pm y| = y$; npr., $|\pm 3| = 3$; ta ista jednakost ispisuje se i ovako:



Sl. 3.2.1.1.

$$\pm 3 = {}^{-}|3|, \text{ odnosno}$$

$$3 = {}^{-}|3|, \; -3 = {}^{-}|3|;$$

kaže se da je ± 3 antimodul od 3. Graf funkcije $y = {}^{-}|x|$ dobije se iz grafa funkcije $y = |x|$ tako da se ovaj zrcali na pravulji $y = x$.

Zaključak je općenit: *ako je E bilo kakav skup koordinatne ravnine, tada je E graf određene funkcije f; ako se E zrcali na pravulji* $y = x$, *izlazi iz E skup* ^{-}E, *koji je graf određene funkcije koja se zove antifunkcija od f i označuje sa* ^{-}f *ili* f^{-1}.

2.1.2. Funkcija f i protufunkcija ^{-}f. Neka je f određena funkcija iz M u S; to znači da za svako x iz M izlazi $fx \in S$; neka je $fx = y$. Tada se jednakost $fx = y$ piše također i ovako: $x = {}^{-}fy$ ili $x = f^{-1}y$. Prema tome, ^{-}f se definira u protuoblasti $^{-}Dom\,f$ funkcije f, pa za svako y iz $^{-}Dom\,f$ označujemo sa ^{-}fy ili f^{-1} y ***svako*** x iz $Dom\,f$ za koje $fx = y$; ^{-}f je određeno preslikavanje protuoblasti od f na oblast od f i zove se *protupreslikavanje*, *protufunkcija*, *antifunkcija*, *inverzna funkcija* u odnosu na f. Tako npr. „*anticosinus*“ simbolički ^{-}cos, pridjeljuje broju 0 sve brojeve $x = {}^{-}\cos 0$ za koje je $\cos x = 0$; dakle je

$$^{-}\cos 0 = \pm\frac{\pi}{2}, \quad \pm\frac{3\pi}{2}, \ldots, \pm(2k+1)\cdot\frac{\pi}{2}, \ldots,$$ pri čemu je $k \in D$.

2.1.3. Ako f preslikava skup M na S, tad ^{-}f preslikava natrag S na M, pa je, dakle, protuoblast (oblast) od ^{-}f isto što i oblast (protuoblast) od f, tj.

$$Dom\,{}^{-}f = {}^{-}Dom\,f$$

$$^{-}Dom\,{}^{-}f = Dom\,f.$$

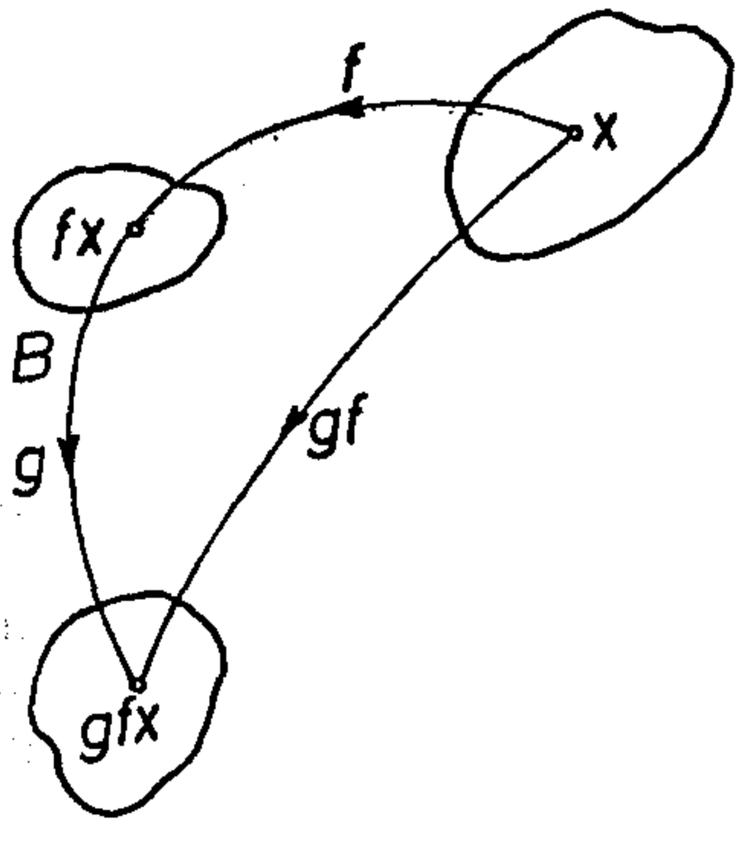
2.1.4. Lako se dokazuje da je $^{-}{-}f=f$.

Pridruživanje $f\to{}^{-}f$ u skupu funkcija vrlo je prirodno i vrlo važno.

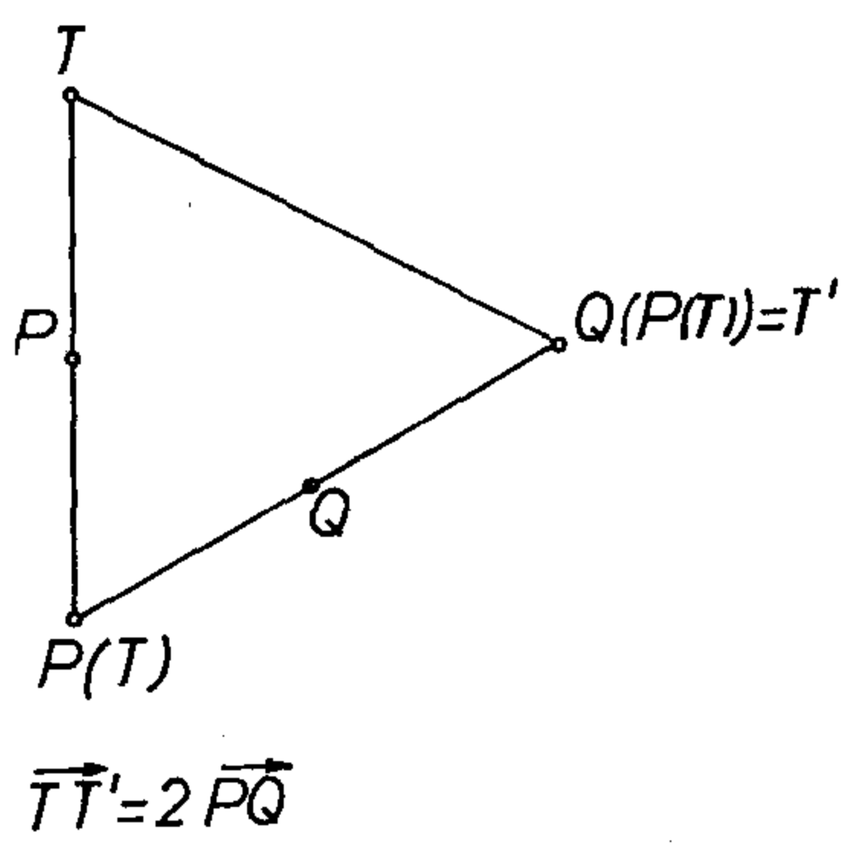
2.1.5. Tako je npr. kvadriranju $x\to x^2$ pridruženo antikvadriranje $x\to x^{1/2}$, kubiranju $x\to x^3$ pridruženo je antikubiranje $x\to x^{1/3}$, itd.

2.2. Slaganje (komponiranje) funkcija.

2.2.1. Definicija: Neka je f funkcija od A u B, a g od B u C; tada svakom $x\in A$ pripada fx iz B, a ovom elementu fx iz B pripada određen element gfx iz C; kaže se da pomoću funkcije gf dolazimo *direktno* od x na $(gf)x$. *Kaže se da funkcija gf nastaje komponiranjem ili slaganjem funkcije f i funkcije g*[1].



Sl. 3.2.2.1.



Sl. 3.2.2.1.

Tako npr. ako su P, Q dvije tačke u prostoru ili ravnini, pa ako sa $T\to P(T)$, odnosno $T\to Q(T)$, označimo centralnu simetriju s obzirom na P, odnosno Q, kao središte simetrije, tada je prelaz $T\to Q[P(T)]$ potpuno određeno preslikavanje QP i vidi se da je to preslikavanje jednako *translaciji* za vektor $2\vec{PQ}$ tj. $QP=2\vec{PQ}$.

Komponiranje funkcija je jedna od najvažnijih i najdalekosežnijih matematičkih operacija.

Specijalno ako funkcija f uzima vrijednosti odande gdje su joj i argumenti, tj. ako je $^{-}Dom\,f\subset Dom\,f$, tada je određena i funkcija ff (simbolički f^2) te $ff^2=f^3$, itd. Tako npr. za svaku simetriju s vrijedi $s^2=1$, jer je $ss(T)=T$ za svaku tačku T.

2.2.2. Teorem. *Za slaganje funkcija vrijedi zakon asocijacije (združivanja):*

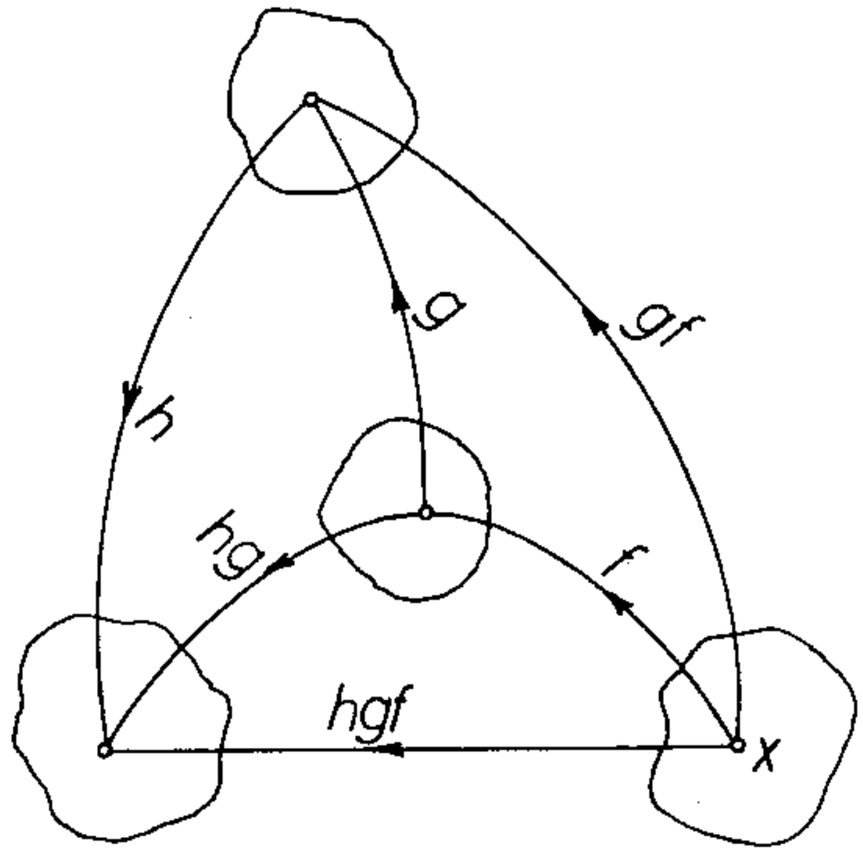
$$h(gf)=(hg)f;$$

naravno da su f, g, h, funkcije za koje je $Dom\,g\subset{}^{-}Dom\,f$, $Dom\,h\subset{}^{-}Dom\,g$.

---

[1]) Pazi na *redoslijed izgovaranja* f i g i *obrnut* redoslijed *pisanja* gf. To dolazi otuda što se *argument funkcije* piše *desno* od *funkcionalnog znaka! Jedan razlog više da se pređe na drukčiji način pisanja: da f „vuče“ x umjesto da ga „gura“*, tj. *da se piše xf umjesto fx* (to je u vezi s našim *načinom pisanja* od *lijeve strane* prema *desnoj strani)*.

Dokaz te osnovne jednakosti vanredno je jednostavan. Ona je upravo očigledna ako su f, g, h jednoznačne funkcije. A i slučaj kad nisu sve jednoznačne neposredno se dokazuje (gledaj sliku!).



Sl. 3.2.2.2.

2.2.3. *Za slaganje funkcija ne mora vrijediti zakon komutacije: općenito je* $gf \neq fg$.

Tako npr. ako f znači rotaciju u ravnini, a g translaciju u istoj ravnini, tada ne mora biti $gf = fg$; ako se najprije izvede rotacija pa translacija, ne mora se dobiti isti rezultat kao kad se izvede najprije zadana translacija pa onda zadana rotacija.

2.2.4. Ako je f tolikovanje, tj. ako je f obostrano jednoznačno preslikavanje, tada je ^{-}ff identično preslikavanje; također je $f\,^{-}f$ identično preslikavanje, dakle je $f\,^{-}f = {}^{-}ff = 1$, ako je f tolikovanje od $Dom\,f$ na $Dom\,f$.

2.2.5. P r i m j e d b a. Komponiranje i obrtanje funkcija (prelaz od f na ^{-}f) vanredno često dolaze u matematici i u drugim oblastima.

2.3. Zadaci o oblasti i protuoblasti funkcija.

1. Promatraj ovih 6 izraza: $d_0 = x$, $d_1 = x^{-1}$, $d_2 = 1 - x$, $d_3 = (1-x)^{-1}$, $d_4 = x(1-x)^{-1}$, $d_5 = (1-x)x^{-1}$. 1) Ako se x kreće u skupu R realnih brojeva, odredi oblast, protuoblast i sliku gornjih 6 funkcija d_i; 2) Nađi protufunkcije $^{-}d_i$. 3) složi svako d_i sa svakim d_j; dobije li se opet jedna od funkcija $d_0, d_1, \ldots, d_5$?
2. Nađi sve jednoznačne funkcije od $\{1, 2, 3, 4\}$ prema a) $\{0, 1\}$, b) $\{0, 1, 2\}$. Koliko ih ima?
3. Promatraj inverznu funkciju od signuma, tj. $^{-}\mathrm{sgn}\,x$. Crtaj.
4. Promatraj složene funkcije: $\mathrm{sgn}\,3^x$, $\mathrm{sgn}\cos x$, $\mathrm{sgn}\sin x$, $\mathrm{sgn}\,\mathrm{tg}\,x$, $\mathrm{sgn}\log x$, $\mathrm{sgn}\,(x^2 - 5x + 6)$. Crtaj.
5. Zadan je paralelogram $ABCD$; promatraj preslikavanja (gl. § 2.2.1 primjer) 1) A tj. $x \to A(x)$; 2) BA; 3) CBA; 4) $DCBA$.
6. Navedi još drugih primjera o funkcijama i njihovim slaganjima.

FUNKCIONALNI SKUPOVI. NIZOVI

Prava građa za pravljenje sve novih i novih skupova jesu funkcije. Razmatranja u ovom § od bitne su važnosti. Specijalno je važno, prvo, shvatiti nizove kao posebne funkcije, i drugo, sve promatrane nizove shvatiti kao elemente jedne cjeline višeg reda. *Time dolazimo do veze između funkcija s jednom varijablom i funkcija s više varijabla.*

3.1. Funkcionalni skup B^A ili funkcionalno potenciranje.

Definicija. *Skup svih* ***jednoznačnih*** *preslikavanja iz A u B označit* ćemo sa B^A; ovdje su A i B skupovi, odnosno klase.

B^A se zove *skup funkcija* ili *funkcionalni skup*; argumenti tih funkcija su elementi u A, a vrijednosti su elementi u B.

Prema tome, ako je $g \in B^A$, onda to znači da svako $x \in A$ uslovljava vezu $gx \in B$, i obrnuto: ako veza $x \in A$ uslovljava vezu $gx \in B$, tada je $g \in B^A$, ukoliko je g jednoznačna funkcija.

Primjer. Jednoznačna konstantna preslikavanja mnogosti A u mnogost B jesu određeni članovi u B^A.

Tako je npr. kvadriranje jedan član mnogosti $R(i)^{R(i)}$, gde je $R(i)$ skup svih kompleksnih brojeva. A to znači upravo činjenicu da je kvadrat svakog kompleksnog broja opet kompleksan broj. Također je kvadriranje $\in N_0{}^D$; N_0 je skup cijelih brojeva $\geqq 0$, a D je skup svih cijelih brojeva.

Među najjednostavnije, a vrlo važne funkcionalne skupove spadaju B^{I2} i uopće B^{Ir}; pri tome je $I2 = \{0, 1\}$, $Ir = \{0, 1, 2 \ldots\}_{<r}$ = skup svih rednih brojeva $<r$ (r je redni broj).

3.2. Niz ili slijed kao funkcija.

3.2.1. Priprema. Govori se o *nizu* događajâ, predmetâ, kućâ, rečenicâ, tonova, itd. Tako je npr. svaka rečenica određen niz riječî. Taj svagdašnji pojam precizno ćemo definirati, jer je on u matematici od osnovne važnosti.

Tako je npr. rečenica „*Matematika je nauka*“ tročlan niz riječi, odnosno niz od 17 glasova. Inače, u matematici tipičnim nizom od 3, odnosno nizom od 17 članova smatramo niz 1, 2, 3, odnosno 1, 2, 3, 4, 5, . . . , 17 ili, još bolje, niz 0, 1, 2, odnosno niz ili povorku 0, 1, 2, 3, . . . , 16.[1)]

3.2.2. Dvočlan niz ili uređena dvojka.

3.2.2.1. Kod *dvočlana niza* ili *uređene dvojke* znamo šta je *prvi član* ili *početni član*, a šta *drugi član*, odnosno član poslije početnog. Ako je početni član p, a drugi q, onda se ta uređena dvojka prikazuje sa $(p; q)$ ili (p, q) ili — u slučaju nedoumice — naprosto pq.

Tako je npr. $+-$ dvočlan niz, $(N; +)$ također $((3, 4); (5, 8, 9, 10))$ je dvočlan niz; drugi mu je član $(5, 8, 9, 10)$.

[1)] Naime, članove ovog niza možemo upotrijebiti kao *cifre brojevnog pozicionog sistema* baze 3, odnosno 17; ima i drugih razloga zašto je za svaki redni broj r zgodnije raditi sa skupom $Ir = \{0, 1, 2, \ldots\}_{<r} = \{0\} \cup \{1, 2, \ldots, r\} \setminus \{r\}$, umjesto sa skupom $\{1, 2, \ldots, r\}$. Od interesa je spomenuti da r može biti i beskonačno; npr. stavlja se $I_\omega = \{0, 1, 2, \ldots n, n+1 \ldots\}$ = skup svih cijelih racionalnih brojeva $\geqq 0$.

Opći oblik uređene dvojke izgleda ovako:

prvi član	*drugi član*
ili: član a_1	član a_2
ili (a_1, a_2).	

Na taj način prvi član pridružujemo prvom rednom broju ili prvoj cifri 0, a drugi član pridružujemo drugom rednom broju, odnosno drugoj cifri 1, pa se i strogo definira:

3.2.2.2. Definicija. *Uređena dvojka* ili *uređen par* ili *dvočlan niz* je svako jednoznačno preslikavanje cifarskog intervala $I2 = \{0, 1\}$, odnosno skupnosti $\{1, 2\}$ prva dva prirodna broja.

Opći je oblik uređene dvojke: $(a_0; a_1)$ ili $(a(0), a(1))$ ili naprosto $a_0 a_1$.

Tako npr. (a_{100}, a_{35}) je dvočlan niz; prvi je član a_{100} a drugi a_{35}; također je (b_{51}, b_3) uređena dvojka.

Dva uređena para jednaka su ako i samo ako imaju jednake prve i jednake druge članove. To je u skladu s onim što smo rekli o jednakosti funkcija (§ 1.7.).

Treba razlikovati uređeni par (a, b) od njegova *protupara* ili *antipara* (b, a), koji se označuju i sa $^{-}(a, b)$ ili $(a, b)^{-1}$.

3.2.3. Što je niz ili povorka? — 3.2.3.1. Definicija. Za svaki redni broj $r > 0$ neka Ir označuje skup svih rednih brojeva koji su $< r$. Stavlja se $1(r) = \{\underbrace{1, 2, \ldots}_{r}\}$. Zapamtimo da u $1(r)$ imamo član 1. Npr. $1(\omega) = \{1, 2, 3, \ldots\}$.

$$I10 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\},\ [1, 10] = \{1, 2, \ldots, 10\} = 1(10).$$

3.2.3.2. Definicija. Ako je r redni broj > 0, tada se pod *nizom*, *slijedom* ili *povorkom* od r članova skupnosti S razumijeva svako jednoznačno preslikavanje, f, skupnosti Ir, odnosno skupnosti $\{1, \ldots, r\}$ u skupnost S.

r-član niz f ima oznaku

$$(1) \qquad f|Ir = (\underbrace{f_0, f_1, f_2, \ldots,}_{r \text{ članova}})$$

odnosno

$$(2) \qquad f|1(r) = (f_1, f_2, \ldots, f_r)$$

već prema tome da li se za domen niza f uzima Ir ili $1(r)$; *oznake* (1), (2) *predstavljaju, po dogovoru, jedan te isti niz.* Inače, uvijek će se razabrati da li npr. f_2 znači po redu treći ili drugi član niza (već prema tome da li postoji ili ne postoji oznaka f_0 za početni član niza f).

3.2.3.3. Tako je npr. prvi ili početni član u nizu rednih brojeva broj 0; prvi ili početni član niza a označuje se sa a_0 kao i sa a_1. *Svaki put treba imati na umu da li smo početni član označili sa a_0 ili sa a_1.* Dublja je i dalekosežnija oznaka ona u kojoj se pojavljuje cifarski skup a ne početni komad množine N prirodnih brojeva. Mi ćemo se služiti jednom i drugom oznakom.

3.2.3.4. Jednočlani nizovi. Primjetimo da svaki predmet p možemo smatrati jednočlanim nizom. Nizovi od ω članova, tj. preslikavanja mnogosti

$$I\omega = \{0, 1, \ldots, n, n+1, \ldots\},\ \text{zovu se } \textit{beskonačni nizovi.}^{1)}$$

---

[1]) U današnjoj matematici promatraju se još duži nizovi, tj. preslikavanje $I\alpha$ i za redne brojeve $\alpha > \omega$.

3.2.4. O jednakosti nizova. Za shvaćanje funkcijâ od više varijabli i rješenjâ jednadžbi s više nepoznanicâ pojam niza je od neophodne važnosti. Vrlo je važno imati na umu da su dva niza jednaka onda i samo onda ako su iste „*dužine*“, tj. ako imaju jednak broj članova te ako su im po redu članovi jednaki. Tako npr. niz (1, 2, 5) nije jednak nizu (1, 2, 5, 5), jer prvi niz ima 3, a drug 4 člana; također nije (1, 2, 5) = (5, 2, 1), jer npr. nije prvi član u prvom nizu jednak odgovarajućem, tj. prvom članu drugog niza.

3.2.5. Uzlazni i silazni nizovi. Niz realnih brojeva $x_1, x_2 \ldots$ je uzlazan ako je $x_1 \leq x_2 \leq \ldots$; on je *strogo uzlazan* ako je $x_1 < x_2 < x_3 < \ldots$

Slično se definiraju silazni i strogo silazni nizovi.

3.2.6. Uzlazni nizovi brojeva iz zadana skupa brojeva zovu se još i *kombinacije s ponavljanjem* i to *kombinacije razreda r* ako je *r* broj članova niza. Strogo uzlazni nizovi zovu se *kombinacije bez ponavljanja.*

Tako je npr. niz 1 1 2 3 3 kombinacija s ponavljanjem razreda 5 brojeva 1, 2, 3 i svakog opsežnijeg skupa brojeva (isp. 2, § 1.8.7.).

3.3. Zadaci o nizovima.

1. Ispiši sve: 1) dijadske; 2) trijadske nizove po 4 člana); 3) uredi ih alfabetski (kako glasi 5. član?); 4) prikaži grafički te nizove.
2. Nađi sve: 1) strogo uzlazne; 2) uzlazne peteročlane nizove slova *a*, *b*.
3. Koliko najviše riječi može biti od: 1) 3; 2) 5; 3) 6 slova u: a) latinskoj; b) ćirilskoj abecedi?
4. Odredi skup B^A, ako (A, B) znači: 1) $(I2, I2)$, 2) $(I10, I3)$, 3) $(I5, \{a, b, c, d\})$.
5. Fibonaccijev niz[1]: Odredi niz $f_0, f_1, f_2, \ldots$ ako je $f_0 = 0$, $f_1 = 1$ i $f_{n+1} = f_{n-1} + f_n$ za svako $n > 1$. Dokaži ove relacije:

   1) $f_n = 5^{-1/2}\left[\left(\frac{1+5^{1/2}}{2}\right)^n - \left(\frac{1-5^{1/2}}{2}\right)^n\right]$;

   2) $f_0 + f_1 + f_2 + \ldots + f_{n+1} = f_{n+2} - 1$; 3) $f_1 + f_3 + f_5 + \ldots + f_{2n+1} = f_{2n+2}$;

   5) $f_0 + f_2 + f_4 + \ldots + f_{2n} = f_{2n+1} - 1$; 5) $f_1^2 + f_2^2 + \ldots + f_n^2 = f_n f_{n+1}$;

   6) $f_1 - f_2 + f_3 - f_4 + \ldots - f_{2n} + f_{2n-1} = 1$; 7) $f_1 - f_2 + f_3 - f_4 + \ldots (-1)^{n-1} f_n = 1 + (-1)^{n-1} f_{n-1}$;

   8) $f_1 f_2 + f_2 f_3 + \ldots + f_{2n-1} f_{2n} = f_{2n}^2$; 9) $f_{n+1} f_{n+2} - f_n f_{n+3} = (-1)^n$;

   10) $f_n^2 - f_{n+1} f_{n-1} = (-1)^{n+1}$; 11) $f_n^4 - f_{n-2} f_{n-1} f_{n+1} f_{n+2} = 1$.

4. FUNKCIJE SA 2 I VIŠE VARIJABLA U MNOŽINI *M*. KARTEZIJEVO MNOŽENJE SKUPOVA

4.1. Primjer: Volumen V kružnog uspravnog valjka, kojemu baza ima polupr̆ečnik r, a kojemu je visina v, iznosi:

$$V = \pi r^2 v.$$

[1] Fibonacci [Fibonači] ≡ Leonardo iz Pize (oko 1170—1250?), talijanski matematičar; taj se niz primjenjuje u biologiji.

Tu V zavisi od dva broja: r i v; to se naznačuje sa $V=V(r, v)$; ovdje su r i v bilo koji brojevi >0. Naravno, nije isto $V(r, v)$ i $V(v, r)$. Tako vidimo da uređenom paru (r, v) brojeva >0 pridružujemo broj $V(r, v)$. Kaže se da V zavisi od 2 varijable koje se nezavisno kreću u skupu pozitivnih brojeva.

4.2. Ako svakom tročlanom nizu (x_1, x_2, x_3) članova množine M pridružimo jedan ili više članova $f(x_1, x_2, x_3)$ množine S, kaže se da je f funkcija od 3 *varijable* koje se ***nezavisno kreću u M***.

Slično se definira funkcija od r varijabla ili r *argumenata* u skupu M, za svaki redni broj $r>0$.

4.3. Definicija. *Ako svakom nizu $(x_0, x_1, x_2, \ldots)$ od r članova koji se kreću u M pridružimo jedan ili više članova $b(x_0, x_1, \ldots)$ množine S, govori se o određenoj funkciji od r varijabla (promjenljivicâ) u M s vrijednostima u S.* Tako npr. pustimo li za svaki prirodni broj $k\leq 100$ da x_k bude realan broj, tada je

$$x_1-x_2+x_3-+\ldots+x_{99}-x_{100}$$

određena funkcija od 100 varijabla u skupu R realnih brojeva.

4.3.1. *Suma (zbroj, zbir) i umnožak zadana niza brojeva.*

Svakom konačnom nizu brojeva (1) $a_1, a_2, \ldots, a_n$ pridijeljujemo *zbroj (zbir, sumu)*

$$(2) \qquad a_1+a_2+\ldots+a_n, \text{ kraće } \sum_{\nu=1}^{n} a_\nu$$

brojeva (1)

te *umnoženik ili produkt*

$$(3) \qquad a_1\, a_2 \ldots a_n \text{ kraće } \prod_{\nu=1}^{n} a_\nu$$

brojeva (1).

Definira se postupno:

$$(3) \qquad \sum_{\nu=1}^{k+1} a_\nu = \left(\sum_{\nu=1}^{k} a_\nu\right) + a_{k+1}$$

$$(5) \qquad \prod_{\nu=1}^{k+1} a_\nu = \left(\prod_{\nu=1}^{k} a_\nu\right) \cdot a_{k+1}.$$

Važno je gledati šta sve indeks može biti u obrascima (1)—(5). Posebno se umjesto jednog slova (znaka) za indeks može upotrijebiti bilo koje drugo slovo ili znak. Npr.

$$\sum_{k=0}^{n} 2^k = \sum_{j=0}^{n} 2^j = 1+2+2^2+\ldots+2^n; \quad \sum_{k=5}^{10} 2^k = 2^5+2^6+\ldots+2^{10}.$$

4.4. Homogena linearna funkcija od r numeričkih varijabla $x_1, x_2, \ldots, x_r$ je oblika:

$$(*) \qquad a_1 x_1 + a_2 x_2 + \ldots + a_r x_r$$

$$\text{ili kraće: } \sum_{n=1}^{r} a_n x_n;$$

tu a-ovi ne smiju zavisiti od x-ova.

Funkcije oblika (*) odista su od velike važnosti.

Nas će specijalno zanimati funkcije od *dvije varijable* od kojih je jedna u Ir, a druga u Is; pri tom su r, s redni brojevi.

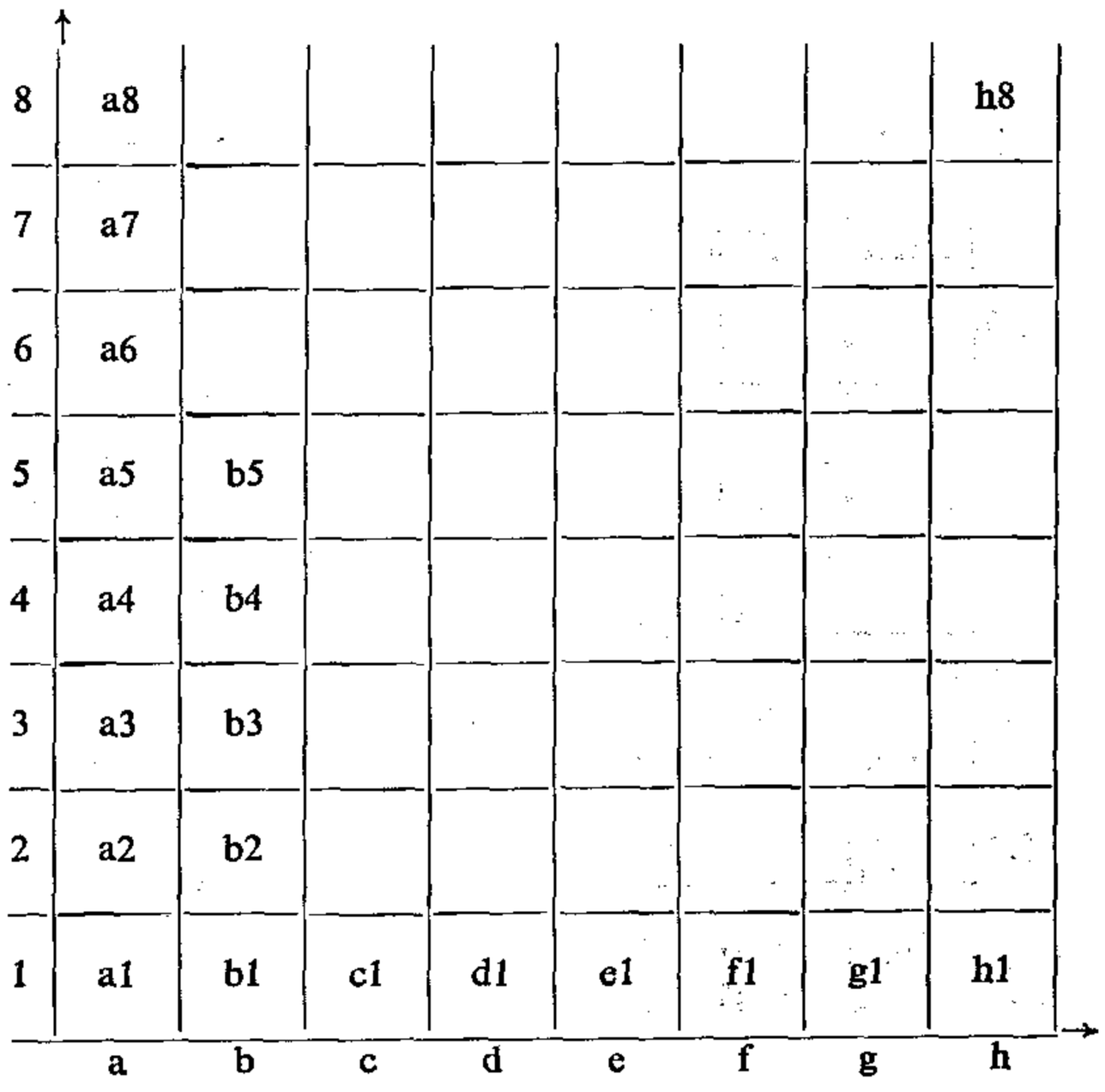
No, prije toga uvedimo pojam *Kartezijeva množenja skupova.*

4.5. Zadaci o vrstama funkcijâ.

1. Imenuj koju homogenu linearnu funkciju od: 1) jedne; 2) tri; 3) 5; 4) 100 varijabla.
2. Za svaku od ovih funkcija odredi da li je linearna i homogena:
   1) $3x$; 2) $5x-3y+1$; 3) $x_1+2x_2+3x_3$; 4) $x_1x_2+x_3x_4$;
   5) $(x_1-x_2)(x_1-x_3)+1$; 6) $a_1x_1+a_2x_2+\ldots+a_nx_n$.
3. Je li: 1) $x^2-2xy+y^2$; 2) $x^3+3x^2y+3xy^2+y^3$; 3) x^3-y^3 određena funkcija izraza $x-y$?
4. Je li x linearna homogena funkcija od:
   1) $x-y$, $x+y$; 2) $3x-2y-1$, $5x+y+4$?

5. KARTEZIJEVO MNOŽENJE SKUPOVA. KARTEZIJEV KVADRAT I KUB ZADANE MNOŽINE[1)]

5.1. Oznake svih šahovskih polja kao tipičan primjer Kartezijeva množenja. Pogledajmo šahovsku ploču i oznake njenih $8\cdot 8=64$ polja:



[1)] Naziv prema imenu velikog francuskog mislioca Kartezija ili Descartesa [Dekart] (latinski: Cartesius [Kartezijus]; na srpskohrvatskom jeziku: Kartezij).

Svakom polju pripada uređen par. Prvi član para je jedno od prvih 8 slova a, b, c, d, e, f, g, h, latinske abecede; drugi član para je jedan od prvih 8 prirodnih brojeva 1, 2, 3, 4, 5, 6, 7, 8. Na taj način imamo polje $a1$ (misli se na uređen par $(a, 1)$), polje $a2$-prikrata za par $(a, 2)$, itd.

Imamo a-liniju kao niz polja kojima oznaka počinje sa a; imamo b-liniju od 8 polja, pa c-liniju, itd., sve do h-linije, koja počinje poljem $h1$, a završava poljem $h8$. Nadalje imamo drugi skup linija koje su okomite na prethodne: *linija* 1, kao niz polja kojima oznaka završava sa 1. Svaka oznaka je oblika x, y pri čemu je $x \in \{a, b, c, d, e, f, g, h\}$, $y \in \{1, 2, 3, 4, 5, 6, 7, 8\}$. Skup svih tih oznaka zove se Kartezijev produkt množine $\{a, b, c, d, e, f, g, h\}$ i množine $\{1, 2, 3, 4, \ldots, 8\}$ i označuje se sa

$$(*) \qquad \{a, b, c, d, e, f, g, h\} \times \{1, 2, 3, 4, 5, 6, 7, 8\}.$$

Smisao znaka $\times$ jest taj da se *svaki* element x množine ispred $\times$ spari sa svakim elementom množine iza znaka $\times$ sačinjavajući uređeni par koji možemo označiti $xy, (x, y)$ i sl. i da se onda *promatra skup svih* tako dobivenih uređenih parova. Prema tome Kartezijev produkt (*) je upravo skup oznaka za polja šahovske table.

5.2. Primjer. $\{0, 1, 2\} \times \{0, 1, 2, 3\} = \{00, 01, 02, 03$
$10, 11, 12, 13$
$20, 21, 22, 23\}.$

Shematski:

	0	1	2	3	→
0	00	01	02	03	
1	10	11	12	13	
2	20	21	22	23.	

↓

Primjedba. Kao što se 02 čita nula, dva, tako npr. 22 treba ovdje čitati: *dva, dva*, a ne dvadeset i dva.

René Descartes (č. Dekart, lat. Kartesius, 1596—1650), veliki francuski matematičar i filozof.

5.3. Definicija. *Kartezijev produkt ili kvadar uređene dvojke (A_1, A_2) skupova A_1, A_2 jest skup svih uređenih parova (x_1, x_2), pri čemu prvi član x_1 prolazi prvim članom A_1, a drugi član x_2 prolazi drugim članom A_2.* Kvadar skupova A_1, A_2 označuje se sa $A_1 \times A_2$ (kružić ili krstić između skupova označuje Kartezijevo množenje).

5.4. Descartesov (ili Kartezijev) kvadrat zadana skupa. Za svaki skup A zove se $A \times A$ još i *Descartesov kvadrat nad A* i označuje A^2, A^{I_2} ili $A^{\{1, 2\}}$.

Tipičan primjer Descartesova kvadrata je veza ravnine s kvadratom pravulje, odnosno s kvadratom R^2 množine R svih realnih brojeva.

Naime, u koordinatnoj ravnini, tj. u ravnini sa dva izabrana nezavisna radijus-vektora (obično iste dužine i međusobno $\perp$) svaka tačka T ravnine dobiva numeričku, odnosno

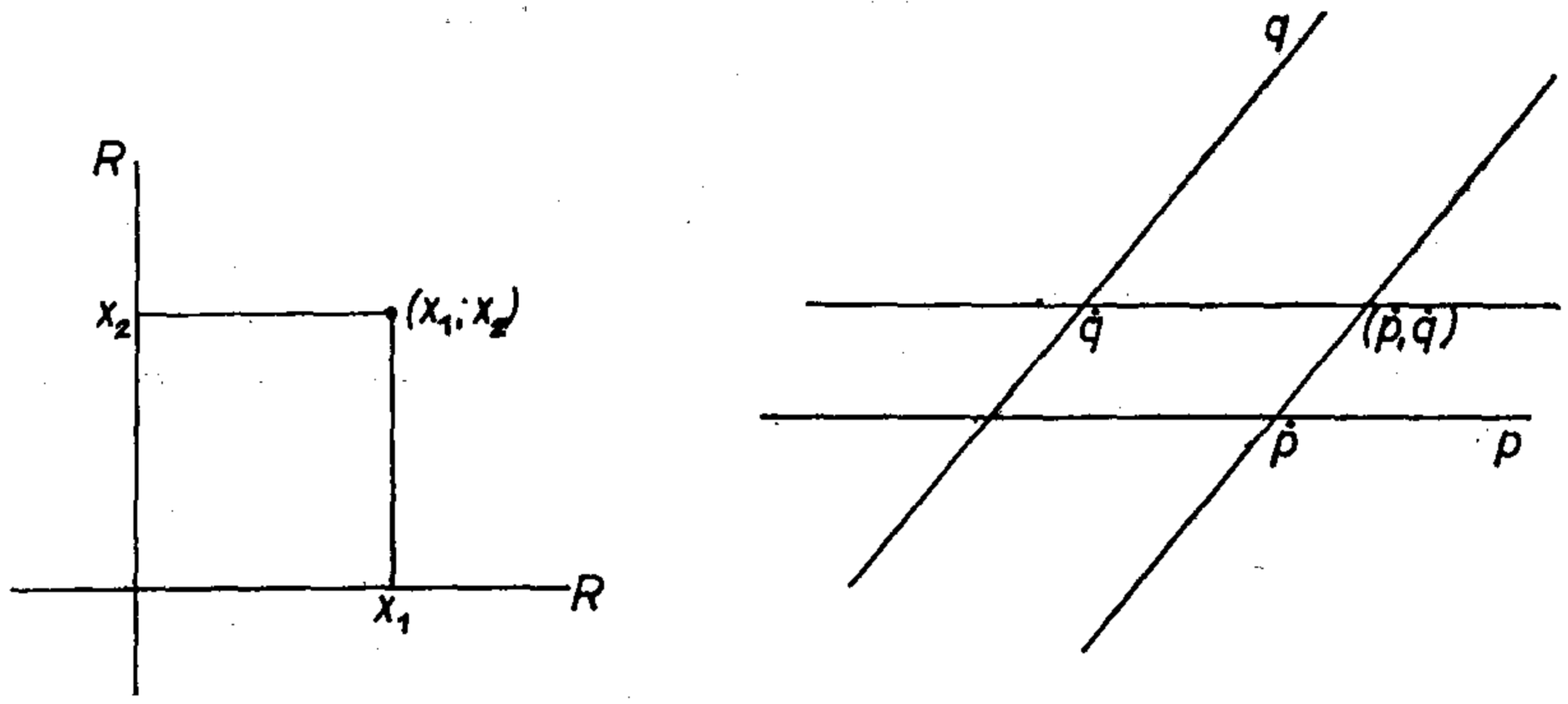
funkcionalnu oznaku oblika (x_0, x_1). Isto tako sa dvije pravulje p, q koje se sijeku svaka tačka P sa p zajedno sa svakom tačkom $Q \in q$ određuje tačku imena (P, Q) ravnine imena $p \times q$. Na taj se način može govoriti o Descartesovu produktu R^2, odnosno $p \times q$, kao o određenoj ravnini kojoj su tačke oblika (x_0, x_1), pri čemu je $x_0, x_1 \in R$, odnosno $x_0 \in p$, $x_1 \in q$.

5.5. Dijagonala Descartesova kvadrata M^2 množine M je skup svih dvojki oblika (x, x), pri čemu je $x \in M$. Npr. dijagonala Descartesove ravnine R^2 je os simetrije prvog i trećeg kvadranta te ravnine.

5.6. Dijagonala Descartesova kvadrata $A_0 \times A_1$ sastavljena je od svih parova oblika (x, x); pri tom je x i u A_0 i u A_1, tj. $x \in A_0 \cap A_1$.

Npr. dijagonala kvadrata $I3 \times I4$ sastavljena je od ove tri tačke:

$$(0, 0),\ (1, 1),\ (2, 2).$$



Sl. 3.5.4.

5.7. Projiciranje skupova iz Kartezijeva produkta. Uređen par (A_1, A_2) skupova određuje jednoznačno svoj Kartezijev produkt $C = A_1 \times A_2$. I obrnuto: Kartezijev produkt $C = A_1 \times A_2$ određuje potpuno svoju *prvu projekciju* »$Pr_1 C = A_1$« i svoju »*drugu*« projekciju $Pr_2 C = A_2$; svaki podskup $M \subset A_1 \times A_2$ određuje svoju prvu projekciju $Pr_1 M$ (drugu projekciju $Pr_2 M$), kao skup svih prvih (drugih) članova od $\dot{M}$, pri čemu $\dot{M}$ prolazi skupom M.

Npr. ako se M sastoji od parova

$$(0, 1),\ (4, 2),\ (3, 5),\ (4, 1)\ (4, 2),$$

onda je po redu:

$$\dot{M} = (0, 1),\ (4, 2),\ (3, 5),\ (4, 1),\ (4, 2);$$

odgovarajući prvi članovi su po redu:

$$0, \qquad 4, \qquad 3, \qquad 4, \qquad 4.$$

Njihov skup je:

$$\{0, 4, 3, 4, 4\} = \{0, 4, 3\},\ \text{tj.}\ \{0, 3, 4\}.$$

Dakle je prva projekcija:

$$Pr_1 M = Pr_1 \{(0, 1), (4, 2), (3, 5), (4, 1), (4, 2)\} = \{0, 3, 4\}.$$

Analogno za drugu projekciju dobijamo $Pr_2 M = \{1, 2, 5, 1, 2\} = \{1, 2, 5\}$.

Prelaz od proizvoljna podskupa M, koji leži u $A_1 \times A_2$, na njegove projekcije $Pr_1 M \subset A_1$, $Pr_2 M \subset A_2$ vrlo je važan i svagdašnji.

Npr. projekcije „parabole $y = x^2$“ su R i $R[0, \infty)$; pri čemu se pod „*parabolom* $y = x^2$“ misli na skup svih parova (x, y) za koje je $y = x^2$ te $x \in R$, tj. na skup svih $(\dot{R}, \dot{R}^2)$; radi kratkoće $\dot{R}$ stoji za svaki element iz R (= tijelo svih realnih brojeva).

5.8. Kvadar od *r* dimenzija.

5.8.1. Definicija. Neka je $(A_0, A_1, A_2 \ldots)_{<r}$ zadan r-član niz skupova; *kombinirani produkt ili kvadar skupova niza* $(A_0, A_1, \ldots)$ *zove se skup svih r-članih nizova* $(a_0, a_1, \ldots)$ *za koje je* $a_x \in A_x$ za svako $x \in Ir$; taj se produkt označuje sa $A_0 \times A_1 \times A_2 \times \ldots$ ili sa $P_{x \in Ir} A_x$.

5.8.2. Kub dimenzije n mnogosti A zove se produkt:

$$\underbrace{A \times A \times \ldots}_{n}$$ i označuje sa A^n ili sa A^{In} ili $A^{\{1, 2, \ldots, n\}}$.

Tako npr. sa R^3 odnosno R^n označujemo obični ili euklidski prostor od 3 dimenzije, odnosno od n dimenzija; specijalno, R^3 je skup svih tročlanih nizova realnih brojeva.

5.8.3. Skup svih konstantnih nizova $(a, a, \ldots)_{<r}$ zove se »*dijagonala kocke* A^r«.

6. FUNKCIJE S VIŠE VARIJABLA I KARTEZIJEVO MNOŽENJE SKUPOVA

6.1. Ako je $f(x_1, x_2)$ funkcija sa 2 varijable x_1, x_2, od kojih prva x_1 prolazi skupom A_1, a druga x_2 skupom A_2, onda to zapravo znači da je f preslikavanje Kartezijeva produkta $A_1 \times A_2$. Uistinu, svaki član iz $A_1 \times A_2$ oblika je $(x_1, x_2,)$, a tome članu (x_1, x_2) pomoću f odgovara upravo $f(x_1, x_2)$. Specijalno, svaka funkcija od 2 nezavisne varijable koje se kreću u nekoj množini M zapravo je jedno preslikavanje Kartezijeva kvadrata M^2, i obrnuto.

Zaključak je općenit. Tako npr. preslikavanje f Kartezijeva kuba M^3 znači isto što i funkcija $f(x_0, x_1, x_2)$ od 3 nezavisne varijable koje se kreću u množini M. *Funkcija* $f(x_0, x_1, \ldots x_{r-1})$ *od r varijabla koje se nezavisno kreću u M je određena funkcija od jedne jedine varijable koja se kreće u r-dimenzionalnoj kocki* M^{Ir} *množine M.*

Na taj način vidimo kako se funkcije od 2 *ili više varijabla* mogu shvatiti kao funkcije od *jedne jedine varijable*, no kojoj je struktura zamršenija.

6.2. Definicija oblasti funkcija od 2 i više varijabla. Ako je f funkcija od dvije varijable koje se kreću: prva u A_0, druga u A_1, onda se Kartezijev produkt $A_0 \times A_1$ zove se *oblast* (područje, domen) *funkcije f i piše* $Domf = A_0 \times A_1$ (umjesto *Dom* može se kraće pisati *Do* ili *D*).

Treba razlikovati oblast svake varijable i oblast funkcije. Tako je npr. A_0 oblast prve varijable x_0, a A_1 je oblast druge varijable x_1.

Slično je kod funkcije s više promjenljivicâ. Tako je npr. oblast sumiranja $a_0+a_1+a_2$ realnih brojeva trodimenzionalni prostor R^3; protuoblast je R. Oblast zbrajanja po 100 realnih brojeva je „prostor R^{100} od 100 dimenzija“; tako npr. tački

$$\underbrace{(5, -5, 5, -5, \ldots, 5, -5)}_{100}$$

iz toga prostora R^{100} od 100 dimenzija pridružujemo element

$$5+(-5)+5+(-5)+(\ldots)+5+(-5), \text{ tj. } 0 \text{ iz } R.$$

Na taj način *vidimo kako u algebri radimo i s prostorima od* 10, 100, 400, . . . n dimenzijâ.

6.3. Slikovito prikazivanje funkcije i Kartezijevo množenje. Ako je f određeno preslikavanje mnogosti A u mnogost B, onda to znači da za svako $x\in A$ vrijedi $fx\in B$.

Definirajmo

$$y=fx \quad (x\in A) \tag{1}$$

kao skup svih uređenih parova $(x;fx)$, pri čemu x prolazi kroz A.

U slučaju da je npr. $fx=x^{1/2}$ i $x\geq 0$, relacijom (1) prikazana je parabola kojoj je x-os ujedno os simetrije. Zato se i u općem slučaju kaže da je pomoću (1) funkcija f *prikazana* u Kartezijevu produktu $A\times B$ kao određen *podskup*. Vrijedi i obrat: *svakom podskupu* E iz $A\times B$ odgovara određeno preslikavanje f od A u B kojemu E služi kao »*slika*«. Specijalno, oblast toga f jest projekcija množine E na „prvu os“ A.[1)]

6.4. Preslikavanje $x\to fx$ skupnosti A u B i pripadno skupovno preslikavanje $x\to\{f_x\}$. Zanimljivo je da oba ta preslikavanja imaju u produktu $A\times B$ istu »*sliku*«. Tako npr. $y=x^{1/2}$ $(x\in R)$, $x\geq 0)$ prikazuje parabolu, a u vezi je i s funkcijom $x\to x^{1/2}$ kao i pripadnom skupovnom funkcijom $x\to\{x\}^{1/2}$.

6.5. Zadaci

1. Dovedi u vezu Kartezijev produkt $\{a, b, c, d, e, f, g\}\times\{1, 2\ 3, 4, 5, 6, 7, 8\}$ i uobičajenu oznaku poljâ na šahovskoj ploči.
2. Prikaži u obliku rešetke Kartezijev: 1) kradrat; 2) kub; 3) bikvadrat skupnosti $I2$. Koliko ima članova?
3. U nekom gradu „telefonski brojevi“ su od 5 znamenaka iz mnogosti $I10=\{0, 1, \ldots, 9\}$. Da li telefonski brojevi (npr. u Zagrebu) iscrpljuju Kartezijev prostor $(I10)^{I5}$ od 5 dimenzija? Ako Z označuje skup svih stanovnika Zagreba u godini 1961, da li se u vezi $\dot{Z}\to t\dot{Z}$ radi

---

[1)] Ako je $E\subset A\times B$, tada se *projekcija* na A mnogosti E zove skup svih x, pri $x\in A$ sa svojstvom da postoji bar jedno y za koje je $y\in B$, $(x, y)\in E$.
Analogno se definira projekcija od E na B.

o određenom preslikavanju, ako $t\dot{Z}$ označuje telefonski broj stanovnika $\dot{Z}\in Z$? Što je oblast, a što protuoblast toga preslikavanja?

4. Kad se radi npr. o zbrajanju po 4 broja, da li vam je jasno da se tu radi o preslikavanju četverodimenzionalnog prostora R^4 na R? Slično npr. jednakost $1+1+1+1+1+1+1=7$ iziskuje da tački $(1, 1, 1, 1, 1, 1, 1)$ iz R^7 pridružujemo broj 7.

5. Nađi S^2 ako je $S\in\{I3, N, I\omega, D, Q, R\}$.

6. Ako $h(m, v)$ označuje koliko je časova u trenutku kad mala kazaljka čini kut od m stupnjeva, a velika kazaljka čini kut od v stupnjeva prema smjeru od središta časovnika do oznake 12, obrazloži da se pri preslikavanju $(m, v)\to h(m, v)$ radi o preslikavanju kvadrata $[0, 360]^{I2}$ na $[0, 12)$. Je li to preslikavanje obostrano jednoznačno? Odredi dijagonalu oblasti i vrijednosti funkcije h na dijagonali.

7. Neka su (A_0, B_0), (A_1, B_1) uređene dvojke nepraznih skupova, tj. skupovi A_0, B_0 te A_1, B_1, su neprazni. Dokaži da vrijedi $(A_0\cup A_1)\times\times(B_0\cup B_1)\supset(A_0\times B_0)\cup(A_1\times B_1)$. Kako glasi sličan zaključak ako se radi o 3, 4, ... uređenih dvojki nepraznih skupova?

8. Ako je M neprazna mnogost pa za svako $m\in M$ neka (A_m, B_m) bude uređen par nepraznih skupova; dokaži relaciju

$$\bigcup_m A_m\times\bigcup_m B_m\supset\bigcup_m(A_m\times B_m).$$

9. Odredi skup B^A za $A=\{0, 1\}^2$, $B=\{0, 1\}$.

7. VARIJACIJE

Koliko u zadanom skupu ima nizova po r članova?

7.1. Umjesto da se govori o nizu od r članova uzetih u nekom skupu M, govori se i o *»varijaciji r-og razreda«* elemenata skupnosti M. Taj se način izražavanja nalazi posebno u starijoj literaturi. Dakle vrijedi:

Definicija. *Varijacija r-og razreda od zadanih elemenata je svaki r-član niz kojemu su članovi među tim zadanim elementima.*

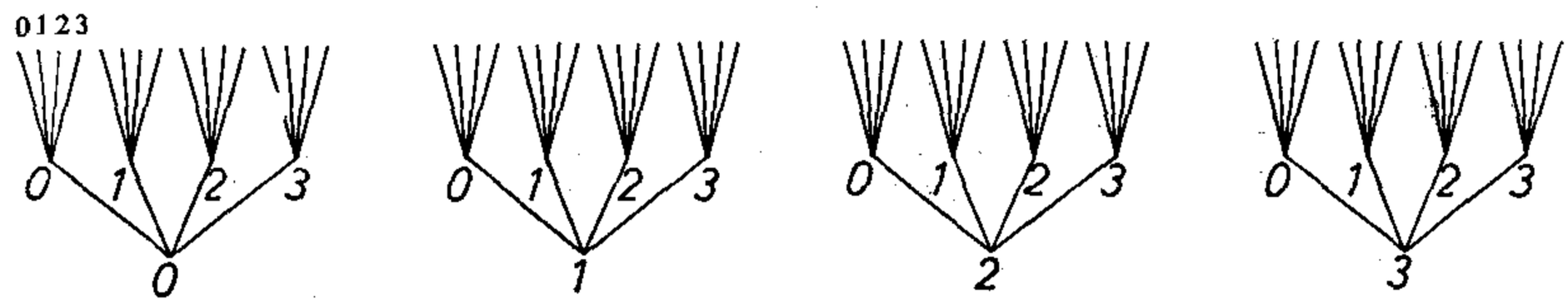
Kaže se da je *varijacija bez ponavljanja (s ponavljanjem)* ako u njoj nema (ima) jednakih članova. Tako npr. niz 5 4 3, odnosno niz 5 4 4 jesu dvije varijacije trećeg razreda; prva je varijacija bez ponavljanja, a druga s ponavljanjem.

7.2. Primjer. Koliko ima 3-članih nizova sagrađenih od članova skupnosti $I4=\{0, 1, 2, 3\}$?

Jedan takav niz ili „šifra“ je npr. 000, a druga je npr. 3 2 1. Opći oblik traženog niza je a_0, a_1, a_2, pri čemu svako od ta tri napisana slova može biti svaki broj 0, 1, 2, 3 u skupu $I4$. Prvi je korak da odredimo a_0; tu su moguća 4 izbora, i to;

0 1 2 3.

Poslije svakog tog izbora biramo a_1, i to opet na 4 načina: 0, 1, 2, 3, itd. Te mogućnosti biranja možemo shematski prikazati u obliku *grananja* ovako (idući odozdo prema gore, kao što raste drvo):



Sl. 3.7.2.

Traženih nizova ima onoliko koliko ima putova od donjeg sloja do posljednjeg sloja, odnosno koliko ima *završetaka putova*. Vidi se da traženih nizova ima $4 \cdot 4 \cdot 4$, tj. $4^3 = 64$.

7.3. Alfabetsko uređivanje nizova. Sve tražene nizove ili „šifre", „riječi" možemo urediti (srediti) alfabetski, tj. onako kako se sređuju riječi u rječnicima, imajući na umu da je 0 ispred 1, a 1 ispred 2, a 2 ispred 3. Na taj način, tročlani nizovi iz § 7.2. nizali bi se ovako:

000, 001, 002, 003, 010, 011, 012, 013,

020, 021, 022, 023, 030, 031, 032, 033.

Sad bi došli po redu slični nizovi koji počinju s 1, pa oni koji počinju s 2 i, najzad koji počinju s 3. Posljednji niz je 333.

Zaključak je općenit:

7.4. Teorem. *Za svaki prirodni broj n može se formirati upravo n^r različitih r-članih nizova u skupu od n elemenata. Broj jednolisnih r-članih nizova, tj. nizova bez jednakih članova, iznosi:*

$$(1) \qquad (n)_r = n(n-1)(n-2)\cdots(n-r+1).$$

Drugim riječima: broj varijacija bez ponavljanja (s ponavljanjem) razreda r od n elemenata iznosi $(n)_r$ (odnosno n^r). Dokažimo posljednju formulu.

Naime, opći traženi niz je oblika $a_0, a_1, \ldots, a_{r-1}$; pri biranju člana a_0 treba uzeti svaki od n članova zadane mnogosti S; pri biranju člana a_1 treba birati svaki od $n-1$ članova preostatka, bez a_0 jer je $a_0 \neq a_1$; a pri biranju a_2 treba isključiti 2 člana: a_0 i a_1, itd.; uopće, pri biranju člana a_i imamo na izbor $n-i$ članova, jer se i članova $a_0, a_1, \ldots a_{i-1}$ isključuje, itd.

7.5. Uzmemo li u gornjem obrascu za $(n)_r$ slučaj $r = n$, dobije se:

$$(2) \qquad (n)_n = n(n-1)(n-2)\ldots 2 \cdot 1,$$

$$(3) \qquad \text{tj. } (n)_n = n!,$$

stavljajući $n! = 1 \cdot 2 \cdot 3 \ldots (n-1) \cdot n$.

Što zapravo znači jednakost (2)? Ona kazuje da za svaki prirodni broj n možemo formirati upravo $n!$ jednolisnih nizova po n članova uzetih u skupu In od n članova.

Svaki takav niz zove se *jednolisna permutacija* ili *automorfizam skupnosti In.*

7.6. Definicija alfabetskog (leksikografskog) uređivanja. Ako je skup M uređen u tom smislu da za svaki par njegovih članova znamo koji je ispred koga, onda se i svaki skup jednoznačnih nizova s članovima iz M može urediti alfabetski, tj. držeći se ovih dvaju pravila:

Prvo pravilo. Ako niz *b produžuje niz a*, onda *b* dolazi poslije *a* (npr. niz 8 1 2 3 4 dolazi poslije niza 8 1 2; tako u rječnicima riječ *podstaknuti* dolazi poslije riječi *pod*).

Drugo pravilo. O tome koji će od dva različita niza *a*, *b* doći ranije, a koji kasnije, odlučuje *prvi* član u kojem se nizovi *a* i *b* razlikuju (*princip prvih diferencija*): *poredak tih članova prenosi se na poredak samih nizova.* Npr. koja od riječi

Prekomjerno, *Predstava*

dolazi prije u rječniku? Odgovor: Predstava, jer *prva* slova u kojem se zadana dva niza razlikuju jesu *k*, *d*; no u alfabetu *d* je ispred *k*.

7.7. Zadaci o varijacijama.

1. Odredi sve varijacije 3. razreda brojeva 1, 2, 3, 4, . . . 9. 1) Sredi ih alfabetski. 2) Jesu li odgovarajući trocifreni brojevi sređeni po veličini? 3) Koja je po redu varijacija 3 5 9? 4) Nađi stotu varijaciju.
2. 1) Jesu li nizovi: BEOGRAD, ZAGREB, ZADAR određene varijacije slova? 2) Koga razreda? 3) S ponavljanjem ili bez ponavljanja? 4) Kako glase odgovarajuće varijacije koje su prve u abecednom uređenju? 5) A posljednje? 6) A tridesete?
3. Isto pitanje za riječi: ARARAT, HIMALAJA.

8. PERMUTACIJE ILI AUTOMORFIZMI ZADANE MNOŽINE

8.1. Definicija. *Permutacija ili automorfizam zadanog skupa S zove se svako obostrano jednoznačno preslikavanje p tog skupa na samog sebe.*

To specijalno znači da *svaki* element iz S služi kao jedna vrijednost preslikavanja p. Specijalno, kod identičkog automorfizma radi se o preslikavanju $x \in S \rightarrow x$.

8.2. Skup svih jednolisnih permutacija ili automorfizama skupnosti S označuje se sa $S!$ (čitaj *S faktorijal*).

Odatle izlazi ovo:

Ako je $a \in S!$, tada je za svako $x \in S$ ujedno i $a(x) \in S$, a k tome postoji jedno jedino $x' \in S$ za koje je $a(x') = x$. Možemo reći da umjesto x dolazi $a(x)$, pa se zato govori o *preuređenju* ili *prerazmještavanju a* skupnosti S.

Obrazac (3), tj. $(n)_n = n!$ iz § 7.5. možemo sada izreći kao ovaj teorem:

—→ **8.3.** Teorem. *Za svako $n \in N$ broj jednolisnih permutacija ili automorfizama od n predmeta iznosi* $n! = 1 \cdot 2 \cdot \cdots (n-1) \cdot n$.

Specijalno, cifarski interval *In* dopušta upravo $n!$ automorfizama, tj. $k(In!) = n!$ (znak k čitaj: *»kardinalni ili glavni broj od«*).

8.3.1. Napomena. Imajmo na umu da je *svaki* automorfizam određena *funkcija*; specijalno, kod identičkog automorfizma radi se o preslikavanju $x \to x$; npr. identički automorfizam mnogosti R svih realnih brojeva predočen je pravuljom $y = x$ u ravnini R^2.

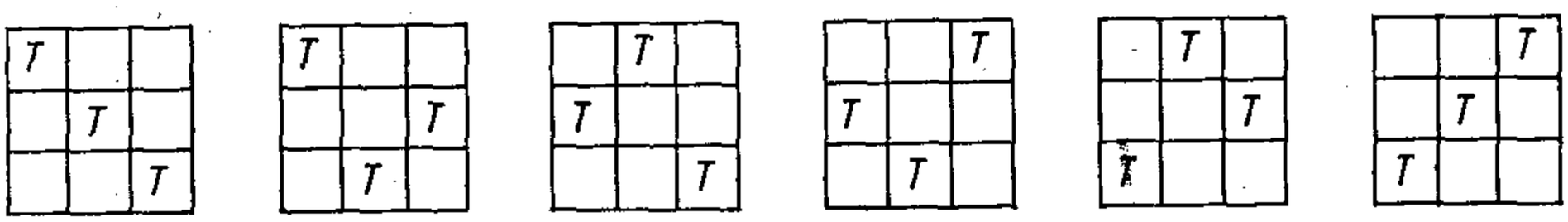
8.3.2. Primjer. $\{0, 1, 2\}! = \{0\,1\,2,\ 0\,2\,1,\ 1\,0\,2,\ 1\,2\,0,\ 2\,0\,1,\ 2\,1\,0\}$. To znači da je npr. 1 2 0 jedna permutacija skupnosti $\{0, 1, 2\}$. Kod te permutacije p došlo je 1 na prvo mjesto 0, tj. $p_0 = 1$, 2 na mjesto 1, tj. $p_1 = 2$, a 0 na mjesto 2, tj. $p_2 = 0$.

Permutacija 1 2 0 može se predočiti i ovako:

$$\begin{matrix} 0\,1\,2 \\ \downarrow\downarrow\downarrow \\ 1\,2\,0 \end{matrix}, \quad \text{ili kraće:} \quad \begin{pmatrix} 0\,1\,2 \\ 1\,2\,0 \end{pmatrix}.$$

8.3.3. *Karakterističan primjer o permutacijama.* Promatraj *»šahovsku ploču«* tipa 3×3 (umjesto uobičajenog tipa 8×8, da stvar bolje razumijemo i da je možemo poopćiti). Tu imamo $3 \cdot 3$ polja. Na koliko se načina mogu na tu ploču smjestiti 3 topa, pa da jedan drugom ne smeta? (Svaki top treba da zauzme jedno polje).

Evo svih mogućih *»pozicija«* ili *položaja*:



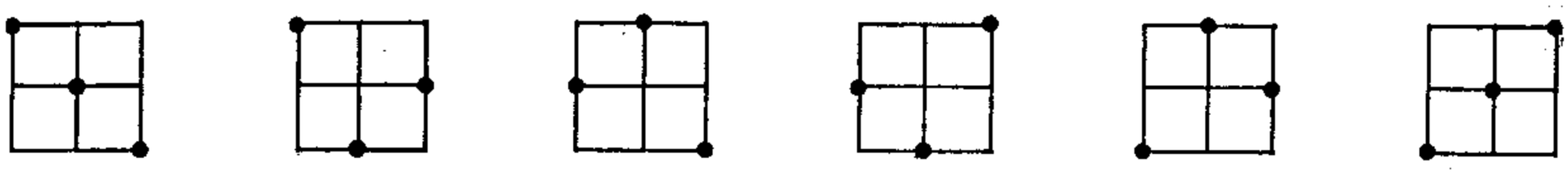
Ima ih $6 = 3!$

Prvi top T_1 može doći u koje god od tri polja prvog stupca; drugi top T_2 u koja god 2 slobodna netučena polja drugog stupca; trećem topu T_3 je položaj već određen.

Generalizacija je očigledna! Tako se na običnoj šahovskoj ploči (tip joj je 8×8) može 8 topova smjestiti na 8! načina, tako da jedan ne tuče drugi, a svako je polje tučeno bar od jednog topa!

Zaključak je općenit. Umjesto 3, odnosno 8, može se uzeti svaki redni broj 1, 2, 3, ... (pa i beskonačni redni broj).

To je osnovno *rasuđivanje za teoriju algebarskih linearnih* jednadžaba i determinanata. Tamo ćemo umjesto „polja“ upotrebljavati čvorišta i na njih postaviti topove. Gornja slika s mrežom čvorišta i pripadnim topovima (ili tvrđavama) izgledala bi ovako:



Slika 3.8.3.3.

8.3.4. Teorem o permutacijama i invarijantnim dijelovima. *Neka je M zadana mnogost i $A \subset M$; tada broj svih permutacija p množine M za koje je $pA = A$ iznosi $(k\,A)!\ (k\,M - k\,A)!$ Općenito, ako su $M_1, M_2, \ldots, M_d$ disjunktni dijelovi mnogosti M i $\bigcup_i M_i = M$, tada ima upravo*

$$(k\,M_1)!\ (k\,M_2)! \ldots$$

permutacija $p \in M!$ za koje $pM_i = M_i$; ako je $p_i \in M_i!$ proizvoljno, tada, definirajući $p \in M!$ jednakostima $p \mid M_i = p_i$, dobivamo svaku permutaciju p za koju vrijedi $pM_i = M_i$ $(i = 1, \ldots, d)$.

Kaže se da je M_i *invarijantno ili postojano* prema permutaciji p.

Dokaz gornjeg teorema prepuštamo čitaocu.

8.4. Permutacije, preuređenja i razmještanja. U vezi s permutacijama mnogosti M govori se i o *preuređenjima* i *razmještanjima* te mnogosti, pogotovu kad je M konačna mnogost. Naime, ako M ima m članova (m je prirodan broj), onda mnogost M možemo zamisliti raspoređenu tako da znamo njen prvi član e_1, pa drugi član, e_2, itd. Ako tada imamo posla s nekom jednolisnom permutacijom p mnogosti M, doći će p_{e_1} na mjesto e_1 (dakle će sad p_{e_1} biti prvi član); na mjesto e_2 dolazi p_{e_2} (pa je sada p_{e_2} drugi član), itd.; dobivenu permutaciju možemo kraće pisati p_1, p_2, itd.

Naravno, za svaku drugu jednolisnu permutaciju q imat ćemo i drugi poredak $q_1, q_2, q_3, \ldots$ Vrijedi i obrat: *svaki raspored mnogosti M od m članova ($m \in N$) određen je jednom permutacijom te mnogosti.* Npr. raspored 5, 4, 13 mnogosti $\{4, 5, 13\}$ određen je permutacijom

$$p = \begin{pmatrix} 4 & 5 & 13 \\ 5 & 4 & 13 \end{pmatrix},$$

za koju je $p_4 = 5$, $p_5 = 4$, $p_{13} = 13$.

8.5. Pojam inverzije ili poremećaja pri permutiranju. Promatrajmo permutaciju 1 2 0 brojeva 0, 1, 2. Vidimo da u permutaciji 1 2 0 dolazi *veći član* 1 *ispred manjeg* 0 kao i 2 ispred 0. Kaže se da u permutaciji 1 2 0 imamo dvije *inverzije* ili dva *poremećaja reda.*

Definicija. *Poremećaj ili inverzija permutacije p je svaki slučaj kad u toj permutaciji veći element dolazi prije manjeg. Skladnost od p je svaki slučaj kad u p manji element dolazi prije većeg.*

Broj inverzija permutacije p, označit ćemo sa ip ili $i(p)$.

Npr. $i(120)=2$; $i(\text{e f a bhg})=2+2+1=5$.

8.6. Pojam transpozicije dvaju članova permutacije.

8.6.1. Definicija. *Transponirati* (premjestiti) dva člana x, y zadane permutacije p znači formirati novu permutaciju koja iz p izlazi tako da članovi x, y zamijene svoja mjesta. Ta nova permutacija može se funkcionalno označiti sa $(x, y)\,p$.

Npr. (3, 4) 5 3 2 0 4 1 = 5 4 2 0 3 1.

8.6.2. Teorem. *Svakom transpozicijom u permutaciji skupnosti* $I\omega = \{0, 1, 2, \ldots, n, n+1, \ldots\}$ *ili njezina dijela mijenja se broj inverzija za neparan broj.*

Dokaz. Neka su x, y dva člana neke permutacije p skupa $I\omega$ ili kojeg njegova dijela.

Promatrajmo $p' = (x, y)\,p$.

Prvi slučaj. Ako su x, y susjedni članovi u p, pa ako je $x<y$, onda će u p' biti y ispred x pa će ta inverzija biti *jedina* promjena u inverzijama prilikom prelaza $p \to p'$. Znači: $ip' = ip + 1$. Ako je $x>y$, onda je $ip' = ip - 1$. U svakom slučaju, dakle: transpozicijom susjednih članova u permutaciji broj inverzija se mijenja za 1.

Drugi slučaj: x i y nisu susjedni članovi, nego se između njih nalazi drugih n članova, recimo $a_1, a_2, \ldots, a_n$. No traženi cilj — transpoziciju (x, y) — možemo dobiti ovim nizom transpozicija *susjednih* članova: (x, a_1) pa $(x, a_2), \ldots$ pa (x, a_n) pa (x, y), (a_n, y), $(a_{n-1}, y), \ldots (a_2, y)$, (a_1, y); dakle svega u $n+1+n$ koraka. To je neparan broj koraka. Kako je pri svakom koraku promjena neparna (i to $+1$ ili -1), bit će i sveukupna promjena inverzija neparna. Dakle je

$$ip - i(x, y)\,p = \text{neparno}.$$

8.6.3. Teorem. *Svaka permutacija p množine In može se izvesti iz svake permutacije q množine In pomoću transpozicija.*

Pogledajmo npr. kako ćemo dobiti $p = 4\,1\,3\,0\,2$ iz $3\,2\,4\,1\,0 = q$. Najprije, transpozicijom (4, 3) u q, izlazi permutacija (4, 3) $q = 4\,2\,3\,1\,0$; u njoj je već element 4 na traženom mjestu kao u p; naredni element 1 iz p još nije pravo smješten; izvedimo zato transpoziciju (1, 2) u 4 2 3 1 0; izlazi 4 1 3 2 0; treća transpozija (2, 0) dovodi do p; dakle je

$$(2, 0)\ (1, 2)\ (3, 4)\,q = p$$

ili slikovito (podebljani elementi se međusobno smjenjuju):

$$q = \mathbf{3}\ 2\ \mathbf{4}\ 1\ 0$$
$$\mathbf{4}\ \mathbf{2}\ 3\ \mathbf{1}\ 0$$
$$4\ 1\ 3\ \mathbf{2}\ \mathbf{0}$$
$$4\ 1\ 3\ 0\ 2 = p.$$

To znači da se permutacija q pomoću 3 transpozicije (3, 4), (1, 2), (2, 0) prevodi u p. Naravno da se upotrebom još dodatnih transpozicija, npr. (4, 2), (4, 2), (0, 3), (0, 3), također dolazi do p. Drugim riječima, broj transpozicija kojima se q prevodi u p nije jednoznačno određen. No, on ne može biti jedanput paran, a drugi put neparan: za zadano p i q broj transpozicija pomoću kojih se q prevodi u p nije, doduše, jednoznačno određen, ali su ti brojevi ili svi parni ili svi neparni.

To izlazi iz činjenice što se svakom transpozicijom u svakoj permutaciji x broj ix inverzija u x mijenja za neparan broj. Tako npr. ako je ip parno kao i iq, tada se p iz q ne može izvesti neparnim brojem, nego jedino parnim brojem transpozicija.

8.7. Parne i neparne permutacije. Definicija. Ako je broj inverzija u permutaciji paran (neparan), kaže se da je permutacija parna (neparna).

Npr. permutacija 1 2 0 je parna; permutacija 1 0 3 2 5 4 ... skupa $I\omega$ brojeva prikazuje ovaj beskonačan niz inverzija:

$$1\,0,\quad 3\,2,\quad 5\,4, \ldots$$

Smatramo je parnom.

Ako p označuje permutaciju množine R svih realnih brojeva koja iz identične permutacije izlazi permutacijom brojeva 0 i 1, tada u p ima beskonačno mnogo inverzija; one su oblika 1, 0 zatim 1, x, x, 0, gdje je x bilo koji pozitivan broj <1. Permutacija p nije ni parna ni neparna.[1)]

8.7.1. Teorem. *Neka je S skup $I\omega = \{0, 1 \ldots\}$ neodrečnih cijelih brojeva ili njegov dio od najmanje 2 člana; tada je svaka permutacija skupa S parna ili neparna. Ima jednako mnogo parnih i neparnih permutacija skupa S. Svaka parna permutacija može se izvesti iz svake parne (neparne) permutacije pomoću parnog (neparnog) broja transpozicija.*

Dokaz. Neka je

$$p_0, p_1, \ldots \tag{1}$$

proizvoljna permutacija skupa S. Za svako p_k možemo reći da li u (1) dolazi prije kojeg manjeg broja iz S ili ne dolazi; ako dolazi, sigurno je jedno: tih manjih članova ima *konačno mnogo*. Zato, idući u permutaciji p po redu od

---

[1)] Slično je kod funkcija: »*većina*« funkcija nije ni parna ni neparna; takva je npr. funkcija $y = x + 1$.

člana do člana, možemo formirati niz (i) poremećajâ; taj se niz sastoji od parova (p_k, p_l), gdje je $p_k > p_l$, $k < l$; sve te parove nižemo po rastućim k-ovima.

Neka je E_k skup svih članova permutacije p koji su $< p_k$, a u p dolaze poslije p_k. Skup E_k je prazan ili konačan. Za svako x iz E_k par (p_k, x) je jedan poremećaj poretka u p. Neka je N_k niz tih poremećaja za dano k. Tada se, nadopisujući na članove niza N_0 članove niza N_1, pa niza $N_2, \ldots$, dobije niz P svih poremećaja koji su u permutaciji p. Taj je niz P ili prazan ili konačan ili beskonačan niz; u prvom i posljednjem slučaju kažemo da je broj inverzija paran. A ako je P konačan niz i ima npr. n članova, onda je n ili parno ili neparno. Time je prvi dio teorema dokazan.

Dokažimo još da $S!$ sadrži jednako mnogo parnih i neparnih članova. Pa neka su r, s dva različita elementa iz S; za svaku permutaciju $p \in S!$ neka je $(r, s)\, p = p'$ rezultat transpozicije članova r, s u p. Tad je $p \to p'$ jedna permutacija samog skupa $S!$, pri čemu parno (neparno) p prelazi u neparno (parno) p'. Najprije, preslikavanje $p \to p'$ je jednolisno. Naime, ako su p, q dva različita člana iz $S!$, postoji bar jedno $n \in S$ za koje je $p_n \neq q_n$. Promatrajmo skup

$$\{p_n, q_n\} \cap \{r, s\}. \tag{2}$$

Ako je taj skup prazan, tada je očigledno $p'_n = p_n$, $q'_n = q_n$ jer prelaz $p \to p'$, odnosno $q \to q'$, mijenja jedino r, s; dakle je $p' \neq q'$. Ako je skup (2) jednočlan, recimo $\{r\}$, tada je ili $p_n = r$ ili $q_n = r$. Ako je $p_n = r$, tada je $(p')_n = s$, $q_n \neq s$, $(q')_n = q_n$, dakle opet $p' \neq q'$. Slično je za slučaj $q_n = r$. Ostaje, najzad, treći slučaj: da je skup (2) dvočlan, tj. $\{p_n, q_n\} = \{r, s\}$, dakle ili $p_n = r$, $q_n = s$ ili $p_n = s$ i $q_n = r$. U prvom slučaju je $p'_n = s$, $q'_n = r$, a u drugom $p'_n = r$, $q'_n = r$; opet je $p' \neq q'$.

Time je jednolisnost preslikavanja $p \to (r, s)\, p$ dokazana.

Da je protuoblast tog preslikavanja upravo skup $S!$, vidi se iz činjenice da je $(p')' = p$, tj.

$$(r, s)\, p' = p.$$

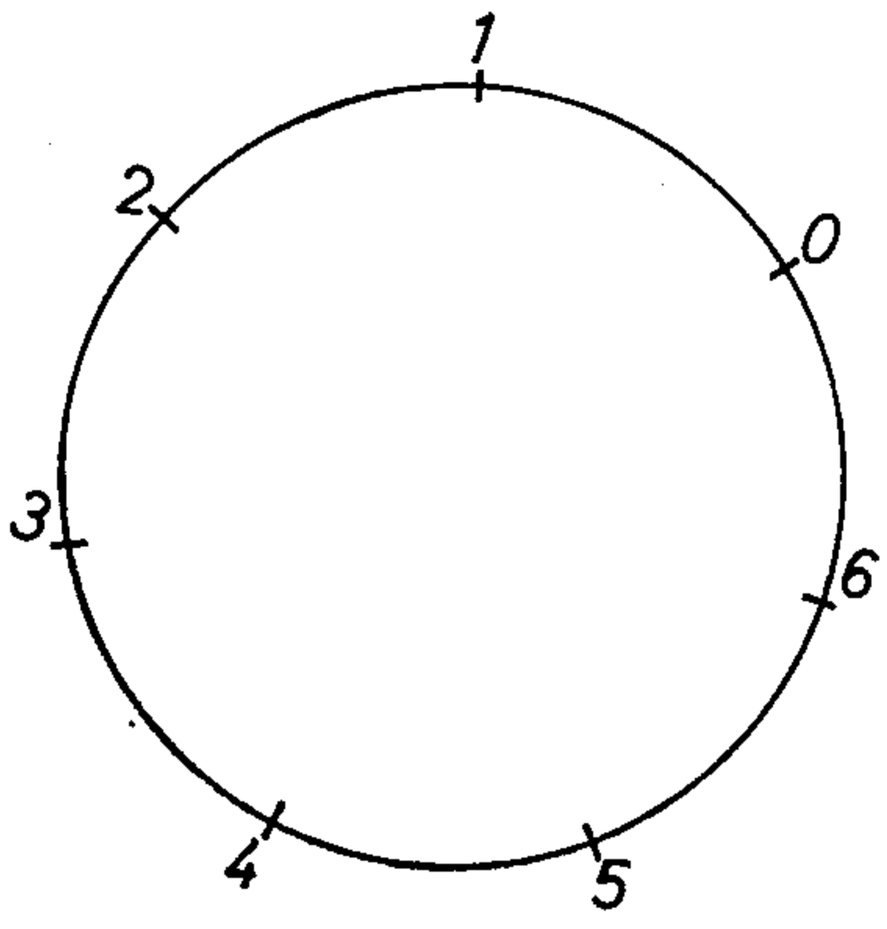
Najzad, na osnovu onog što smo rekli u prethodnoj tački, vidi se da se svaka parna permutacija može izvesti iz svake parne (neparne) permutacije jedino pomoću parnog (neparnog) broja transpozicija. Slično, svaka neparna permutacija može se izvesti iz svake parne (neparne) permutacije jedino pomoću neparnog (parnog) broja transpozicija.

8.7.2. Korolar. *Za svaki prirodni broj $n > 1$ skup $In!$ svih permutacija brojeva* 0, 1, ... $n-1$ *ima $n!/2$ parnih i $n!/2$ neparnih permutacija.*

8.8. Cikličke permutacije.

8.8.1. Tipičan primjer cikličkih permutacija imamo kad nabrajamo dane jedne sedmice: sedmicu ne moramo početi s nedjeljom, 0, nego kojim drugim danom, npr. četvrtkom — 4 — pa sedmica glasi: 4, 5, 6, 0, 1, 2, 3. Tako će glasiti sedmica boravljenja ako smo boravak započeli u četvrtak (vidi shemu!)

8.8.2. Definicija. *Cikličke* (*kružne*) *permutacije* zadanog konačnog niza f dobijaju se tako da se nizanje članova počne od bilo kojeg člana niza f i ide tako do njegova kraja, a onda se po preostale članove ide iz početka.



Sl. 3.8.8.2.

Neka je npr. zadan niz:

8 5 0 4 0 2 6;

njegova naredna ciklička permutacija dobije se počinjući ne s prvim, nego s drugim članom 5 pa se ide dalje do kraja i onda uzme preostatak; izlazi 5 0 4 0 2 6 8. Da smo u zadanom nizu otpočeli sa 4, dobili bismo cikličku permutaciju 4 0 2 6 8 5 0.

Naziv »*ciklička permutacija*« proizlazi odatle što članove niza možemo zamisliti da su raspoređeni ciklički (kružno), tj. na kružnici, u jednakim ili nejednakim razmacima i da članove nabrajamo počinjući od bilo kojeg člana, no idući uvijek u pozitivnom smislu ili uvijek u negativnom smislu.

Npr. transpozicija dvaju elemenata je određena ciklička permutacija tih elemenata.

8.8.3. Na taj način vidimo da iz svakog r-članog niza dobivamo određene cikličke permutacije, njih r na broju; za te permutacije ne smatramo da se bitno razlikuju međusobno.

Naprotiv, ako se neki niz b ne nalazi u lancu cikličkih permutacija što proizlazi iz niza a, tada se cikličke permutacije a, b smatraju bitno različnim.

Tako npr. uz niz $a = 1, 2, 3$ dolaze cikličke permutacije 2 3 1 te 3 1 2.

Ciklička permutacija $b = 3\ 2\ 1$ bitno je različna od a jer se niz b ne pojavljuje među nizovima 1 2 3, 2 3 1, 3 1 2.

8.8.4. Teorem. *Bitno različitih cikličkih permutacija od n predmeta ima* $(n-1)!$

Stvarno, ako se radi o predmetima $1, 2, \ldots, n$, onda se sve bitno različne permutacije dobijaju tako da predmet 1 ostane na miru, a permutiramo preostale predmete $2, 3, \ldots, n$ na sve moguće načine, tj. na $(n-1)!$ različnih načina.

8.8.5. Promatrajmo određenu permutaciju, npr.

$$3\ 2\ 4\ 1\ 6\ 5\ 7 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 1 & 6 & 5 & 7 \end{pmatrix}.$$

Kod te permutacije imamo »*ciklus*« ili *zatvoren lanac*

$$1 \to 3 \to 4 \to 1,$$

tj. ciklus (1 3 4); zatim imamo dvočlani ciklus (5 6) i, najzad, jednočlane cikluse 2 ili (2) te 7 ili (7).

Zato se zadana permutacija prikazuje kao produkt svojih ciklusa:

$$3\ 2\ 4\ 1\ 6\ 5\ 7 = (1\ 3\ 4)\ (2)\ (5\ 6)\ (7).$$

Također je

$$(5\ 6)\ (2)\ (1\ 3\ 4)\ (7) = (1\ 3\ 4)\ (2)\cdot(5\ 6)\ (7).$$

Naravno, zaključak je općenit:

8.8.6. Teorem. *Svaka se permutacija skupnosti Ir može prikazati kao kompozicija (produkt) određenog broja svojih cikličnih permutacija ili ciklusâ; pri tom vrijedi zakon komutacije. Ne gledajući na redoslijed ciklusâ, svaka se permutacija prikazuje na jedan jedini način kao produkt svojih ciklusa. Dva ciklusa nemaju zajedničkog člana.*

9. VEZA IZMEĐU PERMUTACIJA, VARIJACIJA I KOMBINACIJA

9.1. Primjer. Obradimo opet primjer da odredimo koliko ima 3-članih dijelova u skupu $I10$ od 10 članova.

Skup svih tih dijelova označuje se sa

$$\binom{I10}{3};$$

iz svakog takvog dijela proizlazi 3! raznih uređenih trojki.

Ako dakle svakom

$$x \in \binom{I10}{3}$$

pridružimo skup $x!$ od 3! pripadnih uređenih trojki, jasno je da su članovi od $x!$ različiti od članova u $y!$ za svako

$$y \neq x \text{ i } y \in \binom{I10}{3};$$

no svaka od $10\cdot 9\cdot 8 = (10)_3$ uređenih trojki članova iz $I10$ dobije se na taj način. Dakle je

$$3!\ k\binom{I10}{3} = (10)_3.$$

Zaključak je općenit: na sličan način dokazujemo (isp. pogl. 2, § 3.9.):

9.2. Teorem. *Za prirodne brojeve n i r vrijedi:*

$$r!\ k\binom{In}{r} = (n)_r, \text{ tj.}$$

$$k\binom{In}{r} = \frac{n\,(n-1)\,(n-2)\ldots(n-r+1)}{r!}.$$

9.3. Permutacija zadanog niza. Permutacije s ponavljanjem. Promatrajmo ova dva niza:

(1) 1, 2, 1, 3, 2, 4, 1, 5

(2) 2, 1, 2, 1, 1, 5, 4, 3;

jedan od njih nastaje permutiranjem drugoga: jedan je permutacija drugoga, jer je ispunjena:

9.3.1. Definicija. *Jedan niz je permutacija drugog niza ako oba niza imaju jednako mnogo članova te ako se svaki predmet x pojavljuje u jednom nizu upravo onoliko puta koliko se puta to x pojavljuje u drugom nizu.*[1)]

Umjesto da se govori o permutaciji zadanog niza a, govori se također o permutaciji s ponavljanjem množine predmeta koji sačinjavaju taj niz a.

Niz 1, 1, 2, 2, 3, 4, 5 nije permutacija niza (1) jer se predmet 1 u oba niza ne pojavljuje jednak broj puta.

—→ **9.3.2. Teorem.** ***Zadan je konačan niz:***

(1) $a_1, a_2, \ldots a_n$***; tada skup*** $(a_1, \ldots, a_n)$***! svih njegovih permutacija ima*** $\dfrac{n!}{\prod\limits_{x \in \{a_1, \ldots, a_n\}} (\varphi x)!}$ ***članova, tj.***

(2) $k(a_1, a_2, \ldots, a_n)! = \dfrac{n!}{\prod\limits_{x \in \{a_1, \ldots, a_n\}} (\varphi x)!}$***, pri čemu*** φx ***označuje frekvenciju predmeta x u nizu* (1)*, tj. x se pojavljuje u nizu* (1) *upravo*** φx ***puta kao član.***

Tako npr. za niz $b = 3, 1, 2, 2, 1, 1, 2, 2, 2\ 2$ imamo $n = 10$, $\{3, 1, 2, 2, 1, 1, 2, 2, 2, 2\} = \{1, 2, 3\}$; $\varphi 1 = 3$, $\varphi 2 = 6$, $\varphi 3 = 1$, pa prema obrascu (2). imamo:

$$k\,b! = \frac{10!}{3!\ 6!\ 1!} = \frac{7 \cdot 8 \cdot 9 \cdot 10}{2 \cdot 3} = 840.$$

Dokaz važne jednakosti (2) jednostavan je i zanimljiv. Ideja je da se niz (1), u kojem u općem slučaju može biti i jednakih članova, usporedi s nekim nizom *bez ponavljanja*, npr. s nizom odgovarajućih indeksa

(3) 1, 2, 3, ..., n,

za koji znamo da dopušta upravo $n!$ permutacija.

Pridružimo svakom članu a_i iz (1) skup A_i svih indeksa $r \in \{1, \ldots, n\}$ za koje je $a_i = a_r$; naravno, A_i ima φa_i članova, gdje nam φa_i kazuje koliko se

---

[1)] Općenitije, možemo izreći ovu definiciju o *permutaciji funkcija:* Ako su f, g funkcije, tada se kaže da je g *permutacija funkcije* f ako su ispunjeni ovi uslovi:

1. $\mathrm{Dom}\, f = \mathrm{Dom}\, g$;
2. $^{-}\mathrm{Dom}\, f = {}^{-}\mathrm{Dom}\, g$;
3. za svako $y \in {}^{-}\mathrm{Dom}\, f$, skupovi $^{-}f\{y\}$, $^{-}g\{y\}$ su istobrojni, tj. $k\,{}^{-}f\{y\} = k\,{}^{-}g\{y\}$.

puta predmet a_i pojavljuje kao član u nizu (1). Jasno je da iz $a_i \neq a_j$ izlazi da su A_i, A_j disjunktni skupovi.

Osim toga, svakoj permutaciji $p = p_1, p_2, \ldots, p_n$ niza (3) pridružimo permutaciju $a(p) = a_{p_1}, a_{p_2}, \ldots a_{p_n}$ niza (1). Jasno je ovo: ako permutacija p ne miješa međusobno članove iz A_i sa članovima iz A_j, onda odgovarajuća permutacija u nizu (1) ne vrši nikakve izmjene. No, svih permutacija niza (3) za koje je svaki od skupova A_i invarijantan ima:

$$\prod_x (\varphi x)! \qquad (x \in \{a_1, a_2, \ldots, a_n\}). \tag{4}$$

Za svaku permutaciju q niza (1) neka $S(q)$ označuje skup svih permutacija $p \in (3)!$ za koje je $a(p) = q$. Tada je prema pretposljednjoj rečenici:

$$k\,S(q) = (4). \tag{5}$$

Međutim, jasno je da vrijedi:

$$\bigcup_{q \in (1)!} S(q) = (3)! \tag{6}$$

No, ako su q, q' različni članovi iz (1)!, tada su skupovi $S(q)$, $S(q')$ disjunktni. Zato, prelazeći na kardinalne brojeve, relacija (6) daje:

$$\sum_{q \in (1)!} k\,S(q) = k\,(3)!;$$

zbog $k\,(3)! = n!$ i zbog (5) postaje to

$$k\,(1)!\,(4) = n!$$

A to je upravo željena jednakost (2).

9.4. Kombinacije s ponavljanjem. Nizovi

$$5,\ 1,\ 2,\ 3,\ 2,\ 3,\ 1,\ 2$$
$$1,\ 1,\ 2,\ 2,\ 2,\ 3,\ 3,\ 5$$

predstavljaju jednu te istu »*kombinaciju s ponavljanjem razreda* 8«; ta dva niza su 2 različna prikaza te kombinacije. Neka, naime, vrijedi:

9.4.1. Definicija. *Kombinacija razreda r s ponavljanjem elemenata množine M je svaki r-član niz kojemu su članovi uzeti iz M; pri čemu dva niza smatramo jednakim onda i samo onda ako je jedan permutacija drugoga.*

9.4.2. Najzgodnije je da predmete u određenoj kombinaciji r-tog razreda sredimo linearno tako da jednaki predmeti dođu do jednakih predmeta. Tako npr. „uređeni" oblik kombinacije 3, 1, 2, 1, 3, 2, 1 glasi: 1, 1, 1, 2, 2, 3, 3; te dvije kombinacije smatramo jednakima.

9.4.3. Specijalno je zgodno raditi s kombinacijama *brojeva*. Ako se radi o skupu $K_r'(n)$ svih kombinacija r-og razreda od n predmetâ, možemo za ove predmete uzeti upravo niz $In = 0, 1, 2, \ldots, n-1$. Prema tome, ako je $f' \in K_r'(n)$, onda f' u određenom obliku predstavlja određen uzlazan niz od r

članova $\in In$ i vrijedi $f_0' \leq f_1' \leq \ldots f'_{r-1}$. Neka Ir označuje identičnu transformaciju od Ir na sama sebe; tada je $f = f' + Ir$ kao niz $f_0', f_1' + 1, f_2' + 2, \ldots$ *strogo uzlazan* r-niz brojeva iz $I(n+r-1)$, tj. $f' + Ir \in K_r(n+r-1)$. No, ako su f', g' dva *različna* člana iz $K_r'(n)$, tada su f, g dva *različna* člana iz $K_r(n+r-1)$. Ako je $h \in K_r(n+r-1)$, tada je $h' = h - Ir \in K_r'(n)$. Stvarno, niz $h - Ir$ glasi h_0, $h_1 - 1$, $h_2 - 2, \ldots$; tvrdimo da je $h_0 \leq h_1 - 1 \leq h_2 - 2 \leq \ldots$ U protivnom slučaju bilo bi $i < j$, $h_i - i > h_j - j$, tj.

$$h_i - h_j > i - j, \text{ tj. } h_j - h_i < j - i. \qquad (*)$$

No, $h_j - h_i = (h_j - h_{j-1}) + (h_{j-1} - h_{j-2}) + \ldots + (h_{i+1} - h_i) \geqq j - i$, tj. $h_j - h_i \geqq j - i$ protivno pretpostavci (*).

Tako npr. kombinacije s ponavljanjem razreda 3 brojeva 0, 1, 2, 3 tj. uzlazni 3-člani nizovi brojeva 0, 1, 2, 3 oblika su h_0, $h_1 - 1$, $h_2 - 2$, gdje je $h = h_0$, h_1, h_2 bilo koji strogo uzlazan 3-član niz iz $I7 = \{0, 1, 2, 3, 4, 5, 6\}$. Npr. niz 2, 2, 4 je 2, 3 — 1, 6 — 2, tj. 2, 2, 4 = (2, 3, 6) — (0, 1 2).

Na taj način dokazali smo da veza

$$x \to x - Ir \qquad \left(x \in K_r(n+r-1) = \binom{I(n+r-1)}{r}\right)$$

predstavlja određeno tolikovanje između $\binom{I(n+r-1)}{r}$ i $K_r'(n)$; *time se uspostavlja veza između kombinacija s ponavljanjem u* In *i kombinacija bez ponavljanja s elementima u opsežnijoj množini* $I(n+r-1)$.

9.4.4 Teorem. $k K_r'(n) = k\binom{I(n+r-1)}{r}$, *tj. kombinacija s ponavljanjem razreda* r *od* n *članova ima* $\binom{n+r-1}{r}$.

9.5. Problem raspodjeljivanja.

9.5.1. Zadatak. Na koliko se načina može 8 identičkih kuglica raspodijeliti na 3 kutije tako da u svaku kutiju dođe bar jedna kuglica?

Možemo zamisliti da su kuglice nanizane linearno ovako:

$$\ldots\ldots\ldots; \text{ kutije također } \underline{|\ \ |\ \ |\ \ |}$$

(okomiti potezi su stijene kutija).

Na početku i na kraju stoji po 1 stijenka; još preostaju 2; svaku od njih treba smjestiti negdje između dvije susjedne kuglice, npr. u treći i peti međuprostor, evo ovako:

$$|\ldots|\ldots|\ldots|$$

Dakle od 7 *međuprostora treba izabrati proizvoljna* 2 *međuprostora;* to je moguće na $\binom{7}{2}$ načina; i u te međuprostore treba smjestiti preostale stijenke.

Zaključak je općenit pa imamo:

9.5.2. Teorem. *Zadanih n jednakih kuglica moguće je raspodijeliti na zadanih r kutija upravo na* $\binom{n-1}{r-1}$ *načina tako da u svaku kutiju dođe najmanje jedna kuglica. Ako se ne traži da u svakoj kutiji ima najmanje jedna kuglica, onda broj različnih raspodjela glasi:* $\binom{n+r-1}{n}$.

Prvi dio teorema je jasan jer n kuglicâ određuje $n-1$ međuprostor od kojih treba izabrati $r-1$ mjesto — stijenke kutijâ. Dokažimo i drugi dio teorema. Radeći kao maloprije, stvar se svodi na to da imamo n tačkica i $r+1$ štapić, koje treba linearno rasporediti. Na krajeve dolazi po jedan štapić (stijenka) pa se radi još o n kuglica i $r-1$ štapić. Imamo, dakle, ovakvu situaciju:

$$\Big|\ \underbrace{\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot}_{n+r-1}\ \Big|$$

Od tih $n+r-1$ mjesta treba izabrati bilo kojih n mjesta; na svako izabrano mjesto treba staviti po jednu kuglicu; time se dobije određeno razdijeljenje zadanih kuglica. Svih tih razdijeljenja ima $\binom{n+r-1}{n}$ jer se radi o izboru n predmeta od svega $n+r-1$ predmet. Da se npr. radilo o 9 kuglica pa da se u rasporedu o 11 mjesta za kuglice i preostale 2 stijenke izabralo 5. i 6. mjesto, raspored bi glasio ovako:

$$\underset{1}{|}\ \cdot\ \underset{2}{\cdot}\ \cdot\ \underset{3}{\cdot}\ \cdot\ \underset{4}{|}\ \underset{5}{|}\ \cdot\ \underset{6}{\cdot}\ \cdot\ \underset{7}{\cdot}\ \cdot\ \underset{8}{\cdot}\ \cdot\ \underset{9}{\cdot}\ \cdot\ \underset{10}{\cdot}\ \underset{11}{|}$$

To znači da bi druga kutija bila prazna; u prvoj bi bile 4 kuglice, a u trećoj preostalih 5 kuglica.

9.6. Zadaci o permutacijama, varijacijama i kombinacijama.

1. Koliko ima permutacija s elementima 1, 2, 3, 4, 5? Sredi ih abecedno i nađi 30. član. Nađi susjedne permutacije od 4, 3, 2, 1, 5.
2. Koliko ima 4-cifrenih brojeva sagrađenih od brojki 1, 2, 3, 4, 5? Nađi najmanji, najveći i srednji.
3. Nađi početni položaj slova P E T A R; je li P E T A R parna ili neparna permutacija?
4. Isto pitanje za riječi: 1) R U M A; 2) P R E D R A G, 3) N I K O L A; 4) A R H I M E D; 5) S R E Ć K O.
5. Isto pitanje za brojeve: 1) 3, 5, 1; 2) 11, 15, 103, 2; 3) 1, 7, 9, 8, 3, 4.
6. U abecednom uređenju svih permutacija brojeva 0, 1, 2, 3, 4, 5 odredi koje su po redu parne, a koje neparne permutacije. Ima li susjednih permutacija od kojih su obje: a) parne; b) neparne?
7. Koliko inverzija (poremećaja poretka) pokazuje niz: 1) 3, 1, 4; 2) 2, 1, 5, 3, 4; 3) 9, 8, 7, . . . , 1; 4) n, $n-1$, . . . , 2, 1;

5) 2, 1, 4, 3, . . . , 100, 99; 6) 3, 2, 1, 6, 5, 4; 9, 8, 7; 7) 2, 4, 6, . . . , $2n$, 1, 3, 5, . . . , $2n-1$; 8) 1, 5, 9, . . . , $4n-3$, 3, 7, . . . , $4n-1$, 2, 6, . . . , $4n-2$, 4, 8, . . . , $4n$?

8. 1) Koliko inverzija prouzrokuje broj 1 u pojedinoj permutaciji brojeva 1, 2, 3, 4, 5? 2) Koliko ima parnih, a koliko neparnih permutacija kod kojih broj 1 stoji na 4-om mjestu?

9. Koliko puta manji element dolazi prije većeg elementa u permutaciji: 1) 2, 4, 1; 2) 1, 2, 3, 4; 3) 5, 1, 2, 3, 6; 4) 1 2, 3, . . . , n; 5) u proizvoljnoj permutaciji p množine In? Označimo taj broj sa sp; za koje n će brojevi ip, sp biti oba parna ili oba neparna, a za koje n će jedan od brojeva sp, ip biti paran, a drugi neparan?

11. Nađi sumu brojeva ip kad p prolazi svim permutacijama množine $\{1, 2, \ldots, n\}$.

11. Broj inverzija permutacije $p = p_1, p_2, \ldots, p_n$ jednak je broju inverzija permutacije $r = r_1, \ldots, r_n$, pri čemu je $p_{r_1} = inf_i \{p_i\}$, $p_{r_2} = inf_i \{p_i\}$, $i \neq r_1$, $p_{r_3} = inf_i \{p_i\}$, $i\, non \in \{r_1, r_2\}$ itd.

12. Na natječaj (konkurs) za $r = 2$ mjesta javilo se $n = 6$ osoba; na koliko se načina može udovoljiti natječaju?

13. Isto pitanje ako je uređen par (n, r) jednak: 1) (8, 3); 2) (14, 7); 3) (250, 40).

14. Domaćin je pozvao 8 gostiju; nakon što je on sam sjeo, na koliko načina može razmjestiti svoje goste na preostalih 8 stolica?

15. Na koliko različnih načina može sjesti 6 osoba A, B, C, D, E, F: 1) u jednu klupu; 2) dvije klupe po 3 osobe; 3) u 3 klupe po 2 osobe; 4) za okrugao stol?

16. Na koliko načina dvije osobe A, B iz zadatka 15 mogu sjediti jedna do druge?

17. U automobilu je preostalo još 10 praznih sjedala, i to: 1) 5 na lijevoj, 5 na desnoj strani; 2) 6 na lijevoj, 4 na desnoj strani; na koliko načina može tu sjesti 8 putnika 1, 2, . . . , 8 ako putnici 1, 2, 3, 4 žele da budu na lijevoj strani?

18. Na koliko se načina mogu osobe 1, 2, 3, 4 prijaviti u 4 hotela A, B, C, D ako osobe 1, 2: 1) žele; 2) ne žele da budu u istom hotelu?

19. Na koliko se načina mogu na polici poredati 2 crvene, 3 zelene i 4 crne knjige, tako da knjige iste boje budu zajedno?

20. Na koliko se načina na stolu može poredati 10 tanjura, od kojih je 5 potpuno jednakih, a ostalih 5 međusobno su različiti?

21. Odbor od 10 članova 1, 2, 3, 4, . . . , 10 treba da izabere svojeg predsjednika, i to između 1, 2, 3, zatim svog potpredsjednika $\in \{1, 2, 3, 4\}$, tajnika $\neq 8, 9$ i blagajnika. Na koliko se načina odbor može sastaviti?

22. Na koliko se načina može nanizati 8 ključeva na kružni prsten ako su 3 ključa manja i međusobno jednaka, druga tri su međusobno jednaka i različita od preostalih ključeva; k tome su 2 preostala ključa i međusobno različita i različita od svih ostalih ključeva.

23. Koliko treba autobusnih linija da se 6 mjesta međusobno poveže, ako nijedna linija ne povezuje: 1) 3 mjesta; 2) 4 mjesta?

24. Iz vrećice sa $n=13$ kuglica, od kojih je 6 crvenih, 3 bijele i 4 žute, izaberi 7 kuglica, i to: 3 crvene, 2 bijele i 2 žute; na koliko je to načina moguće?

25. Na koliko načina može sjesti u red 5 dječaka i 5 djevojčica ako naizmjence dolaze dječaci i djevojčice?

26. Ako se istodobno protrese i ispusti na pod 6 dvodinarki, na koliko se načina može desiti da: 1) upravo 3 dvodinarke; 2) bar 3 dvodinarke pokažu „pismo“?

27. U ormaru se nalazi 8 pari cipela; ako se nasumce uzmu 4 cipele, na koliko je to načina moguće? A ako među njima ima da bude bar 1 par cipela?

28. 1) Na koliko se načina 7 jednakih čestica može rasporediti u 3 pretinca? 2) A ako u svakom pretincu treba da bude bar jedna čestica? 3) A ako ni u kojem pretincu ne smije doći svih 7 čestica?

29. Na koliko se načina 8 jednakih kuglica može rasporediti u 15 kutija tako da ni u jednoj kutiji ne bude više od: 1) jedne; 2) dvije; 3) 5 kuglica?

30. Na koliko se načina 5 jednakih bijelih i 3 jednake crvene kuglice mogu raspodijeliti na 3 kutije? Razlikuj slučaj da nijedna kutija ne bude prazna i slučaj da koja kutija može biti prazna.

31. Izreci koji zadatak sličan prethodnima.

10. NEKE SPECIJALNE VRSTE FUNKCIJA

10.1. Funkcije kojima argument leži u tijelu R realnih, odnosno u tijelu $R(i)$ kompleksnih brojeva.

10.1.1. Četiri osnovne računske operacije. Ako je M kakav skup brojeva, tada najjednostavnije funkcije od dvije varijable x_0, x_1 koje se kreću u M jesu:

10.1.1.1. Dodavanje (zbrajanje, sabiranje) $\mathbf{x_0+x_1}$; tu umjesto $f(x_0, x_1)$ pišemo x_0+x_1; drugim riječima, x_0+x_1 znači isto što i funkcionalno $+(x_0, x_1)$; varijable se zovu *pribrojnici* ili *sumandi*, a *rezultat* se zove *suma*, *zbroj* ili *zbir*.

10.1.1.2. *Oduzimanje* x_0-x_1 (prva varijabla zove se *minuend*, a druga *suptrahend*, rezultat se zove *diferencija* ili *razlika*).

10.1.1.3. *Množenje* $x_0 x_1$ (faktori; produkt).

10.1.1.4. *Dijeljenje* $x_0 : x_1$ (*dividend, divizor, kvocijent;* pretpostavlja se $x_1 \neq 0$).

Za zbrajanje i množenje vrijedi zakon asocijacije ili zakon združivanja:

$$(x_0 + x_1) + x_2 = x_0 + (x_1 + x_2), \text{ odnosno } (x_0 \cdot x_1) \cdot x_2 = x_0 (x_1 x_2).$$

Zato se umjesto tih izraza piše naprosto: $x_0 + x_1 + x_2$, odnosno: $x_0 x_1 x_2$. Funkcionalno, zakon asocijacije glasi ovako:

$$f[f(x_0, x_1), x_2] = f[x_0, f(x_1, x_2)].$$

Taj zakon ne vrijedi za oduzimanje ni za dijeljenje.

10.1.2. Nizovi. Među nizovima se ističu *aritmetički* i *geometrijski nizovi.* Kod njih je *razlika* (*kvocijent*) između svakog nepočetnog člana i člana pred njim određena *konstanta.* Ako je ta konstanta k, a početni član a, niz tada glasi:

$$a, \ a + k, \ a + 2k, \ a + 3k, \ldots,$$

odnosno

$$a, \ ak, \ ak^2, \ ak^3, \ldots$$

10.1.3. Unutrašnji ili skalarni produkt dvaju istobrojnih nizova.

Neka su $f = f_1, f_2, \ldots$ i

$$g = g_1, g_2, \ldots$$

dva *istobrojna* niza brojeva. Pomnožimo li odgovarajuće članove f_1, g_1 i f_2, g_2, itd. pa dobivene produkte zbrojimo, dobivamo tzv. *unutrašnji* ili *skalarni produkt* od f i g; označit ćemo ga sa $f \circ g$ (znak $\circ$ nas podsjeća i na znak množenja i na slovo s ili σ — početno slovo riječi *skalar*). Dakle je:

$$f \circ g = f_1 g_1 + f_2 g_2 + \ldots$$

Ako f i g imaju po n članova, onda skalarni produkt $f \circ g$ zavisi preko f i g od $2n$ članova. Posebno je $f \circ f = f_1^2 + f_2^2 + \ldots$

Analogno se definira skalarni produkt funkcija s istom oblasti.

Skalarni produkt je vanredno važna računska operacija.

Tako npr. *svaki realni broj x je skalarni produkt od izvjesnog niza cifara i određenog geometrijskog niza s kvocijentom* 10^{-1}. Npr.:

$$2\ 5\ 8,\ \ 4\ 9\ 3\ldots = 2 \cdot 10^2 + 5 \cdot 10 + 8 \cdot 10^0 + 4 \cdot 10^{-1} + 9 \cdot 10^{-2} + 3 \cdot 10^{-3} + \ldots$$

$$= (2, 5, 8, 4, 9, 3, \ldots) \circ (10^2, 10, 10^0, 10^{-1}, 10^{-2}\ 10^{-3}, \ldots).$$

10.1.4. Algebarski polinomi ili cijele racionalne funkcije u odnosu na veličinu (varijablu) x i s koeficijentima u kolu K.[1] To su skalarni produkti geometrijskog niza $1 = x^0, x, x^2, \ldots, x^n$ i istobrojnog niza sa članovima u K.

---

[1] *Kolo* ili *prsten* (odnosno *tijelo* ili *polje*) je svaki skup u kojem su definirane prve tri (četiri) računske operacije tako da pri tom vrijede uobičajena pravila.

Ako je riječ o a-nizu $a_0, a_1, \ldots, a_n$, tada je odgovarajući *a-polinom* oblika: $a_0\,1 + a_1\,x + a_2\,x^2 + \ldots + a_n\,x^n$ ili kraće:

$$\sum_{i=0}^{n} a_i\,x^i.$$

Ako je $a_n \neq 0$, kaže se da taj polinom ima *stupanj* ili *stepen n* i pišemo $st\,a = n$.

Algebarski polinom stupnja n zavisi od $1+n$ koeficijenata $a_0, a_1, \ldots, a_n$ i od veličine x, tj. on zavisi od $2+n$ veličina.

Skup svih algebarskih polinoma u odnosu na x i s koeficijentima u K označuje se sa $K[x]$; kao što vidimo, tu se pojavljuje *uglasta* zagrada.

10.1.5. Razlomljene racionalne funkcije veličine x i s koeficijentima iz tijela K jesu kvocijenti cijelih racionalnih funkcija; njihov skup označivat ćemo sa $K(x)$. Prema tome, treba razlikovati $K[x]$ od $K(x)$; jasno je da je $K[x] \subset K(x)$.

10.1.6. Linearne forme zadanih veličina. Definicija. Neka je zadan niz x veličinâ $x_1, \ldots x_n$. Skalarni produkt niza x i istobrojnog niza $a = (a_1, a_2, \ldots)$ koji ne zavisi od veličina $x_1, x_2, \ldots$ zove se *linearna forma veličina* $x_1, x_2, \ldots$ Ona je, dakle, oblika:

$$a_1\,x_1 + a_2\,x_2 + \ldots a_n\,x_n;$$

pri tom je važno da nijedan koeficijent $a_1, a_2, \ldots$ ne zavisi od $x_1, x_2, \ldots$

Umjesto izraza »*linearna forma*« služimo se izrazom »*homogena linearna funkcija.*«

10.1.7. Linearna funkcija zadanih veličina je svaka funkcija koja je *suma linearne forme tih veličina i konstante* (tj. funkcije koja ne zavisi od promatranih veličina). Npr. funkcija $z \to 3z + 2$ je linearna funkcija od z; funkcija $z \to 3z$ je linearna forma od z.

10.1.8. Algebarski monom zadanih veličina. Neka su zadane veličine $x_0, x_1, x_2, \ldots$ u konačnom broju. Najjednostavniji »*čisti*« algebarski monomi su potencije $x_k^{n_k}$, gdje je n_k redni broj (dakle je $n_k = 0$ ili prirodan broj). Produkti takvih „čistih“ monoma također su algebarski monomi; ako takav produkt pomnožimo (obično sprijeda) s kakvim članom iz kakvog kola A, dobijamo najopćenitiji »*algebarski monom zadanih veličina* $x_0, x_1, \ldots$ *s koeficijentom iz zadanog kola A*«. Formalno se taj monom prikazuje ovako:

(*) $$C\,x_o^{no}\,x_1^{n_1}\ldots;\ C \text{ ne zavisi od } x_0, x_1, \ldots,$$

ali općenito zavisi od eksponenata $n_0, n_1 \ldots$ pa se zato umjesto C može pisati $C(n_0, n_1 \ldots)$ ili $C_{n_0 n_1} \ldots$

Suma $n_0 + n_1 \ldots$ eksponenata u (*) zove se *stupanj* ili *stepen monoma* (*).

10.1.9. Algebarski polinom zadanih veličina jest suma od *konačno mnogo* algebarskih monoma tih veličina; ti se monomi zovu *članovi* ili *termi* polinoma. Pri tom koeficijenti obično leže u određenom kolu ili prstenu A.

10.1.10. Homogeni algebarski polinomi ili **algebarske forme** zadanih veličina jesu algebarski polinomi tih veličina kojima *svi članovi* imaju *isti stupanj.*

10.1.11. Što znači da je *y* algebarska funkcija od *x*? To znači da postoji algebarski polinom $P(x, y)$ veličina x i y tako da vrijedi $P(x, y)=0$ za svako promatrano x.

10.1.12. Ako funkcija $x \to fx$ (x kompleksan broj) nije algebarska, kaže se da je ona *nealgebarska* ili *transcendentna*. Takva je npr. funkcija kosinus pa $x \to e^x$, itd. Naprotiv, funkcija $y=x^{1/2}$ je algebarska jer je $y^2-x=0$.

10.2. Argument(i) ne mora(ju) biti u *R*. Vrlo je važno da se promatraju i funkcije kojima *argument nije nužno broj, nego može ležati u proizvoljnoj množini M.*

10.2.1. Permutacije ili automorfizmi zadane množine *M*. Taj smo slučaj obrađivali ranije u § 8. To je vrlo važan slučaj funkcije f s jednim argumentom koji leži u M isto kao vrijednost funkcije: $\mathrm{D}o f = {}^{-}\mathrm{D}o f = M$.

10.2.2. Funkcije s dva argumenta koji leže isto kao i vrijednosti funkcije u zadanoj množini *M*. Grupoid.

Tu polazimo od proizvoljne neprazne množine M pa *svakom uređenom paru* (x, y) članova iz M pridružimo određen član $f(x, y)$ ili xfy iz M. Tada se govori o grupoidu (M, f) kao organizaciji ili vezama f u množini M. **To je beskonačno važan primjer funkcija.** Tu je $Dom f = M^{I^2}$, ${}^{-}Dom f \subset M$. Tako npr. za skup N prirodnih brojeva imamo grupoide $(N, +)$, $(N, \cdot)$; naprotiv, $(N, -)$ nije grupoid, jer npr. nije $1-4 \in N$, mada je $1 \in N$, $4 \in N$.

Za svaki skup S imamo skup PS svih dijelova iz S te grupoide $(PS, \cup)$, $(PS, \cap)$, $(PS, \dot{-})$. Je li $(\{0, 1\}, \Rightarrow)$ grupoid? Zašto?

10.2.3. Komponiranje funkcija. Tu se radi o tome da se iz zadane dvojke (f, g) funkcija izvede njihov *spoj* ili *sastav* fg u tom smislu da vrijedi $(fg)x = f(gx)$ za svako x. O tome je također već bilo govora (v. § 2). Inače je tu riječ o funkcijama sa 2 varijable koje su i same funkcije. Specijalno smo podrobnije razmatrali komponiranje permutacija.

No dobro je da se vidi kako je oblast operacije komponiranja raznovrsna!

10.2.4. *Derivat zadanog polinoma.* Svakom polinomu $p = p_0 + p_1 x + p_2 x^2 + \ldots + p_n x^n$ pridjeljujemo njegov *derivat* ili *izvod* $p' = p_1 + 2p_2 x + 3p_3 x^2 + \ldots + np_n x^{n-1}$. Drugi izvod definira se kao izvod prvog izvoda, a označuje se sa p''; dakle $p'' = (p')'$. Slično $p^{(3)} = (p'')', \ldots, p^{(k+1)} = (p^{(k)})'$.

10.3. Zadaci o funkcijama.

1. Koje su od ovih funkcija polinomi a koje nisu algebarski polinomi u x; ako se radi o polinomu, odredi mu stepen:

   1) x; 2) $3x$; 3) $3x^2+1$; 4) $5x^2y-xy$; 6) $\cos x$; 7) $\cos^2 x - \sin^2 x$;

   8) $\cos^2 x + \sin^2 x$; 9) 3^{x^2+1}; 10) $(x+1)\cdot(x+2)\cdot(x+3)$;

11) $\operatorname{tg}(x+1)$; 12) $\frac{x-1}{x+1}$; 13) $\frac{x^2-1}{x-1}$; 14) $\frac{x^5+3x^2}{6x}$; 17) $1-x^{-2}$;
18) $\cos^2 x+\cos^2(a+x)-2\cos a\cos x\cos(a+x)$.

2. Isto pitanje ako se radi o: a) varijabli x, b) varijabli y, c) varijablama x, y:
1) 5; 2) $a^2+b^2+c^2$; 3) $x+y-z$; 4) $x+\cos y-3z$; 5) $xy^{-1}+z^{-2}$; 6) $3x^2y-2xy^2+z^{-1}$; 7) $\frac{x^2-y^2}{x^2+y^2}$; 8) $\cos(x^2+y^2)$.

3. Odredi stupanj ovih algebarskih polinoma u odnosu na:
a) x, b) y, c) x i y:
1) $x\cdot y^2-y$; 2) $xy^4-x^2y^5+5y^6+2$; 3) $-5y^3+4y^2-3x^2y^2+6x$.

4. Da li su ove funkcije algebarske forme:
1) x; 2) $x+y$; 3) $x+y+1$; 4) $xy-5x^2-7y^2$; 5) $x^3y-2x^5-y^5$; 6) $\cos(x^2+y^2+3xy)$; 7) $2x-3y-5z$; 8) $(1+x^2+y^2)(1-x^2-y^2)$; 9) $(2x+3y)(x^2+y^2)$.

5. Nađi skalarni produkt ovih nizova:
1) 2, 5, −4 i −2, 3, 4; 2) $a-b$, $a+b$, i $a+b$, $a-b$; 3) 2, 1, 2, 1, 2, 1 i 3, 5, 6, 7, −8, 7; 4) $\cos x$, $\sin x$ i $\cos x$, $\sin x$, 5) 2, −3, 4, 5 i 1, x, x^2, x^3; 6) 1, 10^{-1}, 10^{-2}, 10^{-3} i 0, 2, 5, 9.

6. Zadan je 4-član $1-2x+3x^2-x^4$; permutiraj mu koeficijente; koliko se različnih polinoma dobije? Nađi vrijednost tih polinoma za $x=2$.

7. Isto pitanje za polinom $2+3x+5x^2+3x^3+2x^4$.

8. Koliko članova ima opći polinom od x, y ako mu je stepen:
1) ≤ 1; 2) ≤ 2; 3) 5; 4) n; 5) $\leq n$.

9. Isto pitanje i za varijable x, y, z.

10. Dokaži:
1) $(a^2+b^2)(x^2+y^2)=(ax-by)^2+(bx+ay)^2$;
2) $(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2)=(ax-by-cz-dt)^2+$
$+(bx+ay-dz+ct)^2+(cx+dy+az-bt)^2+(dx-cy+bz+at)^2$;
3) $(a^2+b^2+c^2)(x^2+y^2+z^2)=(ax+by+cz)^2+(bx-ay)^2+$
$+(cy-bz)^2+(az-cx)^2$;
4) $(a_1^2+a_2^2+\ldots+a_n^2)(x_1^2+x_2^2+\ldots+x_n^2)=(a_1x_1+a_2x_2+\ldots$
$+a_nx_n)^2+(a_1x_2-a_2x_1)^2+(a_1x_3-a_3x_1)^2+\ldots+(a_{n-1}x_n-a_nx_{n-1})^2$.

11. Ako za istobrojne nizove a, b vrijedi $a\circ a=1$, $b\circ b=1$, onda je $-1\leq a\circ b\leq 1$.

12. Ako je $c^{-1}+b^{-1}+c^{-1}=(a+b+c)^{-1}$, onda je:
1) $0\in\{a+b,\ b+c,\ c+a\}$;
2) $a^{-n}+b^{-n}+c^{-n}=(a^n+b^n+c^n)^{-1}$ za $n=3,\ 5,\ 7\ldots$

13. Ako je $a+b+c=0$, onda je

$$\left(\frac{a-b}{c}+\frac{b-c}{a}+\frac{c-a}{b}\right)\left(\frac{c}{a-b}+\frac{a}{b-c}+\frac{b}{c-a}\right)=9;$$

pri tom su a, b, c nejednaki izrazi $\neq 0$.

14. Izraz $bc\dfrac{(a-\alpha)(b-\beta)(c-\gamma)}{(a-b)(a-c)}$ zavisi od a, b, c te od α, β, γ; obrazuj cikličkom permutacijom još slična dva izraza i dokaži da je suma svih tih triju izraza $=abc-\alpha\beta\gamma$.

15. Izrazi pomoću $\cos x$, $\sin x$ ove funkcije: 1) $\cos 3x$; 2) $\sin 3x$; 3) $\cos 5x$; 4) $\sin 5x$. Da li se dobijaju algebarski polinomi s obzirom na $\cos x$, $\sin x$? Stupanj?

16. Izrazi 1) $\cos 5x$; 2) $\sin 5x$ pomoću funkcija oblika $\cos kx$, $\sin kx$, gje je $k=1,\ 2,\ 3,\ 4,\ 5$.

17. Da li su $\cos x$, $\sin x$ racionalne funkcije od $\operatorname{tg}\dfrac{x}{2}$?

18. Izrazi $\operatorname{tg} 4x$, $\operatorname{tg} 6x$ pomoću $\operatorname{tg} x$.

19. Da li je $f(x)=\sum_{k=0}^{n}(-1)^k\binom{x}{k}$ algebarski polinom? Stepen? Dokaži da je $f(n')=0$ za $n'=1,\ 2,\ \ldots,\ n$.

11. TRI ZLATNA PRAVILA O FUNKCIJAMA

Ta se pravila odnose na to, da se odredi oblast svake nezavisne i zavisne varijable, oblast funkcije, protuoblast funkcije te da se utvrdi kad su dvije funkcije jednake ili ekvivalentne, a kad su nejednake.

11.1. Prvo zlatno pravilo o funkcijama traži da se odredi oblast svake nezavisne varijable i oblast funkcije. U najjednostavnijim slučajevima oblast funkcije je Kartezijev produkt oblastî njenih sviju varijabli.

11.2. Drugo zlatno pravilo o funkcijama traži da se odredi protuoblast funkcije i protuoblast svake zavisne varijable.

11.3. Treće zlatno pravilo o funkcijama traži da se specifira o kakvoj je relaciji jednakosti riječ među zadanim funkcijama.

11.4. Pođemo li npr. od dvočlanog skupa $I2=\{0,\ 1\}$ i svih pripadnih 3-članih nizova $(a_0,\ a_1,\ a_2)$, pa ako svakom tom nizu $(a_0,\ a_1,\ a_2)$ pridružimo dvočlani niz $(a_0,\ a_1)$ tada se može govoriti o »*projiciranju* p_z u smjeru z-osi na ravninu $x\,y$.« Tu se radi o jednom preslikavanju ili funkciji p_z; oblast joj je »*kub*« $I2^{I3}$, a protuoblast je „kvadrat“ $(I2^{I2},\ 0)$. Sve tri nezavisne varijable pri tom preslikavanju imaju istu oblast — to je skup $I2$. Zavisne varijable jesu:

$$x=x(a_0,\ a_1,\ a_2)=a_0,$$

$$y=y(a_0,\ a_1,\ a_2)=a_1,$$

$$z=z(a_0,\ a_1,\ a_2)=0.$$

Njihova je protuoblast $I2$, odnosno $I2$, odnosno $\{0\}$. A protuoblast funkcije je $I2 \times I2 \times \{0\}$, tj. $(I2^{I2}, 0)$, kao što smo upravo vidjeli.

11.5. Pri oduzimanju realnih brojeva riječ je o funkciji $x-y$ sa dvije varijable; oblast varijabli je R; oblast funkcije je R^{I2}, tj. — geometrijski govoreći — čitava Euklidska ravnina; protuoblast te funkcije je R.

11.6. O jednakosti i nejednakosti funkcija.

11.6.1. Govoreći funkcionalno, dvije funkcije f i g su jednake onda i samo onda ako imaju istu oblast i iste vrijednosti u svakoj tački te oblasti. To je jednakost po aktivnoj ulozi funkcija. No, osim te jednakosti dolaze vrlo raznolike druge vrste jednakosti funkcija. Jedna od njih je tzv. *formalna jednakost funkcija*: kod njih se radi o istoj oblasti i o istim operacijama što se imaju izvršiti nad argumentom (argumentima) u jednoj i drugoj vrsti funkcija. Tako su npr. dva polinoma a, b u varijabli $x \in R$ jednaka ako je $a(x) = b(x)$ za svako $x \in R$. To je uobičajena definicija jednakosti.

11.6.2. *Formalna definicija jednakosti* bila bi: Dva algebarska polinoma a, b u x jednaka su onda i samo onda, ako se podudaraju u odgovarajućim koeficijentima, tj. $a = b$ znači $a_0 = b_0$, $a_1 = b_1$, $a_2 = b_2, \ldots$, dakle je i $st\, a = s\, tb$.

Tu se stvarno ne pojavljuje argument x; no pretpostavlja da x u $a(x)$ i u $b(x)$ prolazi *istim* skupom.

Te dvije definicije jednakosti polinoma međusobno su ravnopravne, ako predmnijevamo da su koeficijenti u kolu realnih ili kompleksnih brojeva. No, ako su koeficijenti u kakvom proizvoljnom tijelu, onda funkcionalna jednakost ne mora povlačiti za sobom i formalnu jednakost.

Ima još i raznih drugih *radnih definicija jednakosti funkcija*. Npr. ako se radi o uređenim parovima brojeva, tada se susrećemo s ovim radnim definicijama jednakosti:

I. Funkcionalna jednakost $(x, y) = (x', y') \Leftrightarrow x = x',\ y = y'$ Takav je slučaj npr. kod kompleksnih brojeva, kada (x, y) stoji umjesto $x + y\, i$.

II. $(x, y) = (x', y') \Leftrightarrow x + y' = x' + y$. To dolazi npr. u slučaju kada (x, y) znači $x - y$.

III. $(x, y) = (x', y') \Leftrightarrow x\, y' = x'\, y,\ y\, y' \neq 0$. To dolazi npr. kada (x, y) znači x/y.

11.7. Kod definicije jednakosti važno je da su ispunjena ova tri uslova:

1) uslov *refleksije* (povratnosti); $x = x$;
2) uslov obrtnosti ili *simetrije*: iz $x = y$ izlazi $y = x$;
3) uslov prelaznosti ili *tranzitivnosti*: iz $x = y$ i $y = z$ izlazi $x = z$.

A ta tri uslova mogu biti ostvarena u vrlo raznovrsnim okolnostima. Zato treba uvijek paziti o kakvoj se vrsti „jednakosti“ stvarno radi! Ako su sva ta tri uslova ispunjena u nekoj množini M, kaže se da imamo posla s određenom relacijom jednakosti ili ravnopravnosti (ekvivalencije) u M.

12. RELACIJA EKVIVALENCIJE. KLASIFIKACIJA

12.0. Ideja vodilja. Zadan je skup S; njega razdjeljujemo u disjunktne (mimoležne) skupove, tzv. *razrede* ili *klase*, stavljajući u isti razred sve međusobno „ravnopravne" članove iz S; umjesto da se kaže „*x je ravno(pravno) y*", piše se $x=y$, $x\sim y$, $x\equiv y$, itd. Ako je „relacija" $=$, $\sim$, $\equiv$, $\|$, i sl. već unaprijed bila definirana, tada se skup svih razreda označuje poput razlomka $S/=$, $S/\sim$, $S/\equiv$, $S/\|$, i sl.

12.1. Relacija jednakosti $=$ je: *povratna* (*refleksivna*), tj. $x=x$; *simetrična* tj. iz $x=y$ izlazi $y=x$; *prelazna ili tranzitivna*, tj. iz $x=y$ i $y=z$ izlazi $x=z$.

Ta ista tri svojstva ispunjava i relacija *sličnosti* među skupovima, npr. među trokutima; u Euklidovu prostoru relacija paralelnosti među pravuljama također zadovoljava gornja tri uslova.

Kako se gornja tri uslova javljaju vrlo često i u raznim prilikama, uvodi se kraći način izražavanja i postavlja ova:

12.2. Definicija relacije ekvivalencije ili odnosa ravnopravnosti u zadanom skupu S. *Ako se za svaki uređen par (x, y) članova zadanog skupa S može reći da je x ravnopravno sa y (simbolički: $x\sim y$) ili x nije ravnopravno sa y (simbolički: x non$\sim y$), pa ako je ta veza $\sim$:*

1) *povratna ili refleksivna: $x\sim x$ za svako $x\in S$;*

2) *obrtna ili simetrična: iz $x\sim y$, $x\in S$, $y\in S$ izlazi $y\sim x$;*

3) *prelazna ili tranzitivna: za svaku uređenu trojku (x, y, z) članova iz S iz $x\sim y$ i $y\sim z$ izlazi $x\sim z$,*

tada se kaže da je $\sim$ određena relacija ekvivalencije ili odnos jednakosti u skupu S.

Govori se o odnosu ravnopravnosti $(S, \sim)$, imajući na umu dvoje: *prvo, množinu M*, i *drugo, samu relaciju* $\sim$ sa gornja 3 svojstva.

12.2.1. Tako npr. u skupu S diferencijâ $x-y$ prirodnih brojeva relacija

(1) $$x-y=x'-y', \text{ koja iskazuje da je } x+y'=x'+y,$$

jest relacija ekvivalencije. Naime: a) relacija (1) je povratna: $x-y=x-y$ jer je $x+y=x+y$; b) relacija (1) je simetrična: iz $x-y=x'-y'$ izlazi $x'-y'=x-y$ jer iz $x+y'=x'+y$ izlazi $x'+y=x+y'$; c) relacija (1) je prelazna: iz $x-y=x'-y'$ i $x'-y'=x''-y''$ izlazi $x-y=x''-y''$ jer iz $x+y'=x'+y$ i $x'+y''=x''+y'$ izlazi (kako! ?) $x+y''=x''+y$.

12.3. Ako u kvadratu S^{I2} promatramo skup svih $(x, y)\in S^{I2}$ za koje je $x\sim y$, dobijamo posve određen skup $E\subset S^{I2}$. Taj skup E sadrži *dijagonalu*, tj. sve tačke (x, x), zatim je simetričan prema dijagonali, tj. iz $(x, y)\in E$ izlazi $(y, x)\in E$; nadalje je skup E prelazan: iz $(x, y)\in E$ i $(y, z)\in E$ izlazi $(x, z)\in E$.

Skup E je *reprezentacija relacije* $\sim$. Zato se može izreći i ovakva:

12.3.1. Definicija relacije ravnopravnosti u S kao podskup u S^2. *Svaki podskup E iz S^{I_2} koji ima ova 3 svojstva:*

a) *skup E je povratan ili refleksivan, tj. E sadrži dijagonalu;*

b) *skup E je simetričan prema dijagonali;*

c) *skup E je prelazan ili tranzitivan: iz $(x, y)\in E$ i $(y, z)\in E$ izlazi $(x, z)\in E$,*

zove se relacija ekvivalencije ili jednakosti ili odnos ravnopravnosti u skupu S.

12.4. Razredi ili klase mnogosti M prema relaciji ravnopravnosti.

12.4.1. Definicija. Skup svih međusobno ravnopravnih članova skupnosti S zove se *razred* ili *klasa*. Specijalno, za dato $x\in S$ skup $S\{x\}$ svih $y\in S$ za koje je $x\sim y$ zove se x-razred organizacije $(S, \sim)$.

12.4.2. Skup svih razreda od $(S, \sim)$ označuje se sa $S/\sim$, dakle u obliku razlomka: gore je S, a dolje desno je $\sim$.

Tako npr. u skupu P svih pravulja imamo organizaciju $(P, \|)$ po paralelnosti; sve pravulje koje su paralelne sa zadanom pravuljom p čine određen razred. $P/\|$ je skup svih pramenova paralelnih pravulja.

Ako je q pravulja koja nije $\|p$, tada odgovarajući razred $P\{q\}$ nema nikojeg člana zajedno sa $P\{p\}$.

Zaključak je općenit:

⟶ 12.5. Teorem. *1) Za svaki uređeni par A, B razredâ ravnopravnosti organizacije $(S, \sim)$ vrijedi ili $A=B$ ili su A, B disjunktni skupovi. Drugim riječima, preslikavanje $x\to S\{x\}$ ima za vrijednosti dijelove od S koji su međusobno disjunktni i iscrpljuju čitavo S. Specijalno je $x\in S\{x\}$ za svako $x\in S$ i* $\bigcup_{R\in S/\sim} R=S$.

2) Svakoj disjunktnoj podjeli P množine S na neprazne dijelove odgovara izvjesna relacija ravnopravnosti $\sim(P)$ za koju je $S/\sim(P)=P$.

Dokaz. Pretpostavimo da A, B imaju neki član e zajednički; tvrdimo da je $A=B$, tj. $\dot{A}\in B$ i $\dot{B}\in A$. Naime, $\dot{A}\sim e$ jer su $\dot{A}$, e u istom razredu A; isto tako je $e\sim\dot{B}$ jer su e, $\dot{B}$ u razredu B; dakle je $\dot{A}\sim e$ i $e\sim\dot{B}$, pa po svojstvu prelaznosti izlazi $\dot{A}\sim\dot{B}$, tj. $\dot{A}$ i $\dot{B}$ su u istom razredu, dakle je $\dot{A}\in B$; jer je $\dot{B}\in B$; iz istog razloga je $\dot{A}\in B$. Dakle je $A=B$.

Dokažimo 2). Stvarno, dovoljno je definirati relaciju $\sim(P)$ u S zahtjevom da za $(x, y)\in S^{I_2}$ vrijedi $x\sim_P y$ onda i samo onda ako skup $\{x, y\}$ leži u nekom članu podjele P.

Tako npr. podjeli množine D cijelih brojeva na skup $2D$ parnih brojeva i skup $2D+1$ neparnih brojeva odgovara relacija ravnopravnosti $x\sim y$ koja iskazuje: »*x i y su parni brojevi* ili x i y su neparni brojevi«, a može se kraće izreći ovako: „*Razlika $x-y$ je djeljiva sa* 2.“

12.6. Ne plaši se oznake $S/\sim$, $S/=$, $S/\equiv$ i sl.; sprijatelji se s njima: one označuju naprosto da smo skup S raskomadali, rasparcelirali na *disjunktne* (*mimoležne*) dijelove.

12.7. Izomorfnost ili sličnost klasifikacija. Kaže se da je klasifikacija $(S, \sim)$ izomorfna s klasifikacijom $(S', \sim')$ ako postoji tolikovanje t (tj. obostrano jednoznačno preslikavanje) od S na S' sa svojstvom da bude $tS = S'$ i da je ispunjen uslov:

$$x \sim y \text{ u } S \text{ onda i samo onda ako } tx \sim' ty \text{ u } S'.$$

Tako npr. klasifikacija od $I5 = \{0, 1, 2, 3, 4\}$ u $\{0, 1\}$ i $\{2, 3, 4\}$ izomorfna je s klasifikacijom od $I5$ u $\{0, 4\}$, $\{1, 2, 3\}$, kao što to pokazuje tolikovanje:

$$\begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & 4 & 1 & 2 & 3. \end{array}$$

Naprotiv, te dvije izomorfne klasifikacije nisu izomorfne npr. s klasifikacijom $\{0\}$, $\{1, 2, 3, 4\}$ ni s klasifikacijom $\{0\}$, $\{1, 2\}$, $\{3, 4\}$.

12.8. Definicija dvočlane relacije. Neka je S zadan skup; svaki podskup A Deskartesova kvadrata S^2 skupnosti S zove se *dvočlano srodstvo* ili *dvočlana relacija u skupu S*.

Ako je $(x, y) \in A$, kaže se da je x u *srodstvu* (*relaciji*) A sa y i piše također xAy.

12.9. Definicija n-člane relacije.

Slično za svaki prirodni broj $n > 1$ imamo hiperkub $S^n = S^{\{1, 2, \ldots, n\}}$ skupnosti S; veza $A \subset S^n$ iskazuje se i ovako: *A je n-člana relacija u S.*

12.9.1. Primer. Pomoću $x + y = z$ određena je 3-člana relacija B među brojevima x, y, z, a predstavljena je skupom svih trojki $(x, y, z) \in R^3$ za koje je $x + y = z$.

12.9.2. Ako je E_3 Euklidov prostor od tri dimenzije pa ako za svaki 4-člani niz tačaka

$$T_i \in E_3 \quad (i = 1, 2, 3, 4) \tag{1}$$

pišemo $P(T_1, T_2, T_3, T_4)$ onda i samo onda ako sve te tačke (1) leže u nekoj ravnini tada se u E_3 dobije određena 4-člana relacija P.

12.10. Zadaci o klasifikaciji.

1. Ako $x =_3 y$ znači „$x - y$ je djeljivo sa 3“, da li je $=_3$ relacija ekvivalencije u skupu D svih cijelih brojeva?
1. Isti zadatak pišući umjesto 3 svuda 4, 5, 10, 25, n.
3. Odredi $D/=_n$ za $n = 2, 3, 5$.
4. Ako je r ravnina, a $1(r)$ skup svih njenih pravulja, je li $\parallel$ relacija ravnopravnosti? Odredi joj razrede. Ako je ravnina r snabdjevena Descartesovim koordinatnim sistemom, odredi razred što pripada pravulji: 1) $y = 2x$; 2) $y = -2x + 5$; 3) $y = 2$.

5. Je li relacija okomitosti $\perp$ među pravuljama relacija ravnopravnosti? Zašto nije?
6. Prosmatraj skup $I10=\{0, 1, \ldots, 9\}$ i njegovu disjunktnu podjelu: 1) $\{0, 2, 4, 6, 8\}$, $\{1, 3, 5, 7, 9\}$; 2) $\{0, 9\}$, $\{1, 8\}$, $\{2, 7\}$, $\{3, 6\}$, $\{4, 5\}$; 3) $\{0, 9\}$, $\{1, 2, 7, 8\}$, $\{3, 4, 5, 6\}$.
   Ako odgovarajuće relacije ravnopravnosti označimo po redu sa a, b, c, nađi x iz $1\,x\,8$, $x\in\{a, b, c\}$.
7. Koliko ima disjunktnih podjela množine:
   1) $I3=\{0, 1, 2\}$; 2) $I6$; 3) In?
8. Koliko ima neizomorfnih klasifikacija množine $I5$? Navedi ih sve.
9. Dokaži da je izomorfizam među skupovima određena klasifikacija.
10. Dokaži da je izomorfizam u svakom skupu klasifikacijâ određena klasifikaciona relacija.

13. UREĐAJNA RELACIJA. POREDAK

13.0. Ideja vodilja. U praksi i teoriji često se služimo pojmovima: *prije*, odnosno *poslije*; *veći*, odnosno *manji*; *lakši*, odnosno *teži*; *topliji*, odnosno *hladniji*, itd. Pri tom se radi o *prelaznoj* relaciji. Tipičan slučaj je veza $A\supset B$ među skupovima: ona je *povratna*, *prelazna* i *antisimetrična*. Time se uvode *uređeni* skupovi i *uređene relacije*.

13.1. Relacija inkluzije $\subset$ među skupovima ima ova 3 svojstva:

(*r*) *relacija je refleksivna* ili povratna, tj. $A\subset A$ za svaki skup A;

(*t*) *relacija* $\subset$ *je tranzitivna* ili prelazna;

(*a*) *relacija je antisimetrična*: iz $A\subset B$ i $B\subset A$ izlazi $A=B$.

Na osnovu toga tipičnog i svakidašnjeg primjera uvodi se:

13.1.1. ***Definicija uređajne relacije i uređenih skupova.*** *Ako je M neka mnogost pa ako za svako $(x, y)\in M^2$ možemo reći da li je x ispred y ili x nije ispred y, simbolički $x\prec y$, odnosno x non $\prec y$, onda se kaže da je mnogost M uređena relacijom $\prec$ ako je relacija $\prec$ povratna, prelazna i antisimetrična. Kaže se da je $\prec$ uređajna relacija u M.*[1]

Ako vrijedi $x\prec y$ ili $y\prec x$, kaže se da su x i y međusobno *usporedljivi ili komparabilni;* inače su x, y međusobno *neusporedljivi* ili *inkomparabilni*.

13.2. Oznaka uređenih skupova. Neka $(M, \prec)$ označuje da imamo posla sa skupom M uređenim relacijom $\prec$. Uređajne relacije označujemo sa $\prec$, $<$, $\leq$, $\subseteq$, itd.

13.3.—13.3.1. Primjer. Ako je O bilo kakva obitelj skupova, tada $(O, \subset)$ označuje da obitelj O smatramo uređenom pomoću $\subset$ (a ne npr. pomoću $\supset$).

U općem slučaju, to je uređenje *djelomično* ili *nepotpuno*, jer će sadržavati i *neuporedljivih elemenata* A, B, tj. takvih za koje ne vrijedi ni $A\subset B$ ni $A\supset B$.

[1] Kraće možemo reći ovako: Svaka *dvočlana* relacija koja je *povratna*, *prelazna* i *antisimetrična* zove se *uređajna relacija*.

13.3.2. Primjer (glavno uređenje). Ako je X bilo kakav skup, pa ako R^X znači skup svih jednoznačnih funkcija od X prema skupu R realnih brojeva, neka za $f, g \in R^X$ simbol $f \leq g$ znači da je $f \dot{R} \leq g \dot{R}$; tada $(R^X, \leq)$ označuje određeno uređenje mnogosti R^X; to je uređenje djelomično, jer u općem slučaju ima u njemu neusporedljivih elemenata.

1.3.3.3. Primjer. Ako je p permutacija mnogosti In, dobijemo uređenje:

$$p_1 \prec p_2 \prec p_3 \prec \ldots \prec p_n \text{ od } In.$$

13.4. Lanci. Antilanci. Uređenje $(M, \prec)$ je totalno (posve[mašnje], skroz, linearno, lančasto, ili lanac) ako u njemu nema neusporedljivih elemenata. Ako u uređenju nema usporedljivih elemenata, zove se ono antilanac. Prazni skup i svaki jednočlani skup smatramo lancem i antilancem prema svakoj uređajnoj relaciji.

Shematski, lanac se označuje strelicom, i to vertikalno ↑ ili horizontalno →; antilanac se označuje kao nakupina tačaka, bez strelice, npr. · · · · · · ili ___ ili |; obično ćemo lanac zamišljati u vertikalnom položaju sa strelicom prema gore, a antilanac u horizontalnom položaju.

Tako npr. za skup $I3 = \{0, 1, 2\}$ imamo ovih 6 lanaca:

↑	2	1	2	0	1	0
|	1	2	0	2	0	1
|	0	0	1	1	2	2.

Zatim imamo ovaj antilanac: 0 1 2. U uređaju 1 \ / 2 član 0 je početni, a 1, 2 su dva završna neusporedljiva člana. 0

13.5. Dobro uređeni skupovi. Definicija. *Uređen skup M je dobro uređen ako mu svaki neprazni dio X ima svoj određen prvi član*, tj. takav član $a \in X$ da bude $a \leq \dot{X}$. Prazan skup smatramo dobro uređenim.

Npr. skup prirodnih brojeva uređen po veličini dobro je uređen (na to se u suštini svodi princip totalne indukcije). Skup $(D, \leq)$ svih cijelih racionalnih brojeva nije dobro uređen jer npr. sâmo D nema najmanjeg člana. Skup $(R, \leq)$ nije dobro uređen, no posjeduje raznovrsne dobro uređene dijelove.

13.6. Intervali. Ako je $(M, \leq)$ uređen skup, tada za uređen par $a, b \in M$, za koji je $a \leq b$ sa $M[a, b]$ ili $M[b, a]$, označujemo skup svih x iz M za koje je $a \leq x \leq b$, tj. $M[a, b] = \{x;\ x \in M,\ a \leq x \leq b\}$. Slično se stavlja

$$M[a, b) = \{x;\ x \in M,\ a \leq x < b\},\ M(a, b] = \{x:\ x \in M,\ a < x \leq b\};$$

$$M(a, b) = \{x;\ x \in M,\ a < x < b\}.$$

$M[a, b]$ se zove *zatvoreni* interval ab *od* M; $M(a, b)$ se zove *otvoreni* interval ab od M.

13.7. Ideali uređenog skupa M. Svaki dio I uređenog skupa M sa svojstvom da iz $x \in I$ izlazi $M(\cdot, x) \subset I$ zove se *ideal ili početni odlomak mnogosti M; dualni ideal* ili *završni odlomak mnogosti* $(M; \leq)$ zovu se ideali dualnog uređaja $(M, \geq)$. Stavljamo: $M(\cdot, a] = \{x;\ x \in M,\ x \leq a\}$;

$$M[a, \cdot) = \{x;\ x \in M;\ a \leq x\};\ M(\cdot, a) = \{x;\ x \in M,\ x < a\}.$$

Specijalno, skupovi oblika $M(\cdot, a]$, gdje je $a \in M$ zovu se *glavni ideali od* $(M, \leq)$.

13.8. Izomorfizam (sličnost) uređenih skupova. Kaže se da je uređeni skup $(S, \leq)$ *sličan* (*izomorfan*) s uređenim skupom $(S', \leq')$, ako postoji tolikovanje t od S na čitavo S' sa svojstvom da vrijede ovi uslovi:

ako je $x < y$ u S, onda je $t\,x <' t\,y$ u S'; i obrnuto;

ako je $x \parallel y$ u S, onda je $t\,x \parallel' t\,y$ u S'; i obrnuto.

Tako je npr. lanac $2 \prec 3 \prec 1 \prec 0$ množine $I4$ sličan lancu

$$3 \prec' 2 \prec' 0 \prec' 1,$$

kao što to pokazuje pridruživanje odgovarajućih članova po redu:

$$\begin{array}{cccc} 2 & 3 & 1 & 0 \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 3 & 2 & 0 & 1. \end{array}$$

Naprotiv, lanac $1 < 2 < 3 < 4 \ldots$ svih prirodnih brojeva nije sličan dualnom lancu... $< 4 < 3 < 2 < 1$, jer ovdje nema početnog člana.

13.9. Majoranta i minoranta zadanog podskupa. Definicija. Neka je $(M, \leq)$ uređen skup, a S njegov neprazan podskup; svako x za koje je $\dot{S} \leq x$ (odnosno $x \leq \dot{S}$) zove se *majoranta* (odnosno *minoranta*) od S.

Tako je npr. svaki pozitivni broj i 0 majoranta svih negativnih brojeva; 0 je najmanja majoranta negativnih brojeva i zove se *supremum* negativnih brojeva.

13.10. Supremum i infimum zadanog skupa. Definicija. Neka je X neprazan dio uređenog skupa $(M, \leq)$; *najmanja majoranta* od X zove se *supremum* ili *gornja ograda skupnosti X;* označuje se sa sup X ili sup $\dot{X}$ ili $\sup\limits_{x \in X} x$.

Ako X nema nikakve majorante, stavlja se sup $X = \infty$.

Ako je sup $X \in X$, kaže se da je sup X *maksimum od* X.

Dualno se definira *infimum* ili *donja ograda od X*; označuje se sa inf X ili inf $\dot{X}$ ili $\inf\limits_{x \in X} x$.

Ako X nema ni jedne minorante, stavlja se inf $X = -\infty$.

Ako je inf $X \in X$, onda se inf X zove *minimum* od X.

Npr. sup $R(0, 1) = 1$; max $R(0, 1)$ ne postoji; sup $N = \infty$, inf $D = -\infty$.

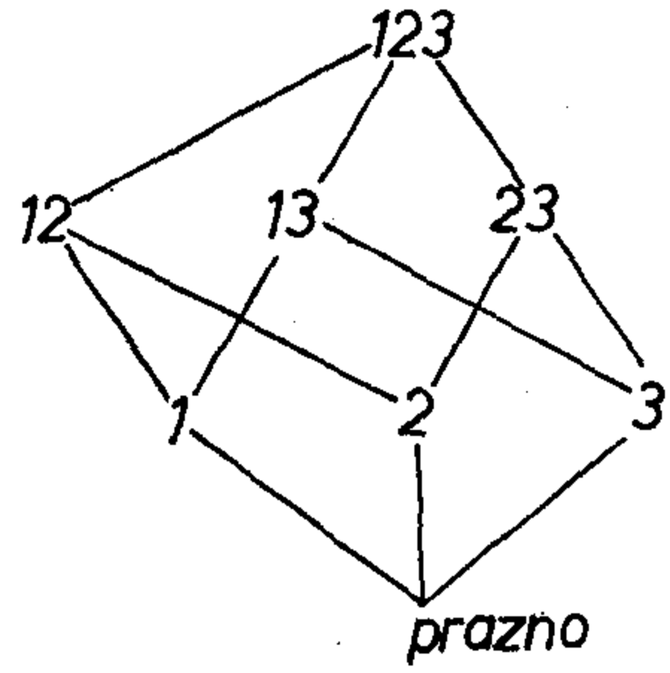
Operacija $X \to \sup X$ i dualna operacija $X \to \inf X$ od vanredno su velike važnosti.

13.11. Mreže. Od specijalnog su interesa uređeni skupovi $(M, \leq)$ sa svojstvom da iz $x, y \in M$ izlazi sup $\{x, y\} \in M$, inf $\{x, y\} \in M$. To su tzv. *mrežasti skupovi ili mreže.*[1)]

Poslije 1930. godine ti su skupovi mnogo izučavani (isp. Birkhoff [1]).

[1)] Rus.: структура; engl.: lattice; franc.: treillis; njem.: Verband.

13.11.1. Primjer $(P\,S, \subset)$ je određena mreža za svaki skup S; specijalno je $\inf S =$ prazni skup $\varnothing$. Evo npr. grafa mreže od $(P\{1, 2, 3\})$. (gledaj sliku!).



Sl. 3.13.11.1.

13.12. Zadaci o uređenim skupovima.

1. Navedi sva totalna uređenja skupa:
   1) $I3$; 2) In. Koliko ih ima? 3) Je li svako to uređenje dobro uređenje?

2. 1) Zašto su sva potpuna uređenja skupnosti $I4$ međusobno izomorfna?
   2) Vrijedi li to i za skup In, gdje je n prirodan broj?
   3) A za skup N prirodnih brojeva?

3. Odredi sve lance i sve antilance u glavnom uređenju kvadrata:
   1) $I2^{I2}$; 2) N^{I2}; 3) R^{I2} (isp. § 3.2).

4. Neka je Gn broj neizomorfnih uređenja od n članova; dokaži da je:
   1) $G2 = 2$; 2) $G3 = 5$; 3) $G4 = 16$; 4) $G5 = 63$.

5. Dokaži da je sličnost među uređenim skupovima određena relacija ravnopravnosti.

6. Uredi prirodne brojeve u obliku drveta; ako u tom uređenju T pišemo $x \sim y$ onda i samo onda ako su pripadni ideali $T(\cdot, x)$, $(T\cdot, y)$ identični, 2) jednakobrojni, dokaži da je $\sim$ relacija ekvivalencije. Odredi pripadne razrede.

7. U latinskom i ćirilskom alfabetu uredi abecedno riječi: olovka, pero, knjiga, aritmetika, broj, brojka, brojevan, brojčan, brojiti, brojni, brojnost, brojevnost, brojen, brojan.

Literatura

Kurepa Đuro [1], [2], Kurepa Sv. [2].

POGLAVLJE 4.

VRSTE BROJEVA

1. PREGLED I NAZIVI TRIJU PRAVILA O RAČUNANJU

1.1. Ne ulazeći u stroge definicije, ovde ćemo navesti glavne vrste brojeva: *prirodni brojevi* i njihov skup N, *cijeli racionalni brojevi* i njihov skup D, *racionalni brojevi* i njihov skup Q, *realni brojevi* i njihov skup R te kompleksni brojevi i njihov skup $R(i)$ ili C ili K.

1.2. Zakoni o udruživanju (asocijaciji), raspodjeli (distribuciji) i razmjeni (komutaciji). Za 4 osnovne operacije (zbrajanje, oduzimanje, množenje i dijeljenje) vrijede pravila:

1.2.1. Zakon asocijacije ili udruživanja vrijedi i za zbrajanje i za množenje brojeva:

$$(a+b)+c=a+(b+c) \qquad (ab)\,c=a\,(bc).$$

Npr. $(3+7)+4=3+(7+4)$.

1.2.2. Taj zakon ne vrijedi za oduzimanje ni za dijeljenje; tako npr. $(3-7)-4$ nije $3-(7-4)$.

1.2.3. Zakon raspodjele ili distribucije množenja prema zbrajanju ili oduzimanju vrijedi:

$$(a+b)\,c=ac+bc, \qquad (a-b)\,c=ac-bc.$$

1.2.4. Naprotiv, nijedna druga od 4 računske operacije nije distributivna ili razdjelna prema kojoj od četiriju računskih operacija.

1.2.5. Zakon komutacije ili razmjene vrijedi za zbrajanje i za množenje: $a+b=b+a, \qquad ab=ba.$

1.2.6. *Za oduzimanje i dijeljenje vrijedi zakon kose razmjene:*

$$a-b=-(b-a), \qquad a:b=(b:a)^{-1}$$

(u posljednjem slučaju pretpostavlja se $a\neq 0$ i $b\neq 0$).

2. PRIRODNI BROJEVI. SKUP N

2.1. Pod *glavnim prirodnim brojevima* razumijevamo brojeve: jedan (1), dva (2), tri (3), ... Nekad se i nula (0) označuje kao jedan glavni prirodni broj.

Redni prirodni brojevi jesu: početni ili nulti (0.), prvi (1.), drugi (2.), ...

2.2. Skup svih prirodnih brojeva označujemo sa N; dakle: $N=\{1, 2, 3, \ldots\}$.

2.3. Skup svih rednih prirodnih brojeva označuje se sa $I\omega$ ili N_0; dakle:

$$I\omega=\{0,\ 1,\ 2, \ldots\}=N_0;$$

pri tom ω označuje tzv. prvi beskonačni redni broj; također je (v. 3 § 3.2.3)

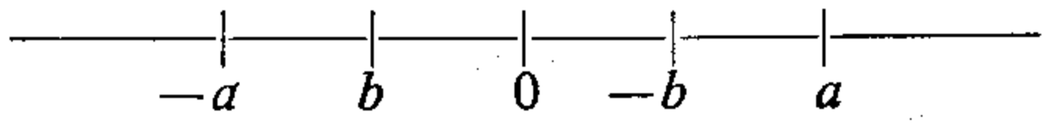
$$1\,(\omega)=\{1,\ 2,\ 3, \ldots\}=N.$$

3. CIJELI RACIONALNI BROJEVI, SKUP $D=\{\ldots, -2, -1, 0, 1, 2, \ldots\}$

3.1. Brojevi ... -2, -1, 0, 1, 2, ... zovu se *cijeli racionalni brojevi.* Njihov skup označuje se sa D (početno slovo riječi »*diferencija*« = razlika; svaki se, naime, cijeli racionalni broj prikazuje kao diferencija ili razlika dvaju prirodnih brojeva; isp pogl. 17, § 13.4.1).

3.2. Na brojevnoj crti skup D se predočuje kao skup koji je centralno simetričan i prema 0 i prema svakom svojem članu.

3.3. Parovi brojeva koji su simetrično položeni prema 0 zovu se *suprotni brojevi*; suprotan broj od broja x označuje se $-x$ ili $-1\cdot x$. Na taj način, *množenje s* -1 *odgovara simetriji ili zrcaljenju s obzirom na* 0, *odnosno rotaciji za* π *oko* 0.



4. RACIONALNI BROJEVI. SKUP Q

4.1. Definicija. *Racionalni brojevi jesu kvocijenti cijelih racionalnih brojeva* (isp. pogl. 17, § 13.3.1).

Prema tome, svaki racionalni broj može se predočiti kao razlomak a/b, pri čemu su a, b članovi u D i $b\neq 0$. Specijalno, svaki *cio racionalan broj* x je racionalan jer je $x=x/1$. Također, *osnovni razlomci* tj. recipročne vrijednosti cijelih racionalnih brojeva, jesu racionalni brojevi: evo ih *uređenih po veličini*:

$$-1,\ -1/2,\ -1/3, \ldots,\ 1/3,\ 1/2,\ 1.$$

4.2. *U pozicionom brojevnom sistemu sa bazom* 10 (ili kojom drugom bazom) svaki racionalni broj prikazuje se kao *periodski* razlomak; npr.

$$3/2=1{,}5=1{,}5000 \text{ (tu cifra 0 čini periodu);}$$

$$1/6=0.1666\cdots;\ 253\,\frac{437203}{999900}=253,\ 43\,[7246].$$

Obrnuto, npr. $0,[7243]=\frac{7243}{9999}$; $0,20\,[354035]=\frac{20354035-20}{99999900}=$

$$=\frac{20354015}{99999900}.$$ Zapišimo to:

4.3 Teorem **(pravilo o vezi između razlomaka prirodnih brojeva i pozitivnih periodskih decimalnih brojeva).**

Za periodske decimalne brojeve imamo:

$$0,AP=\frac{(AP)-(A)}{\underbrace{99\ldots9}_{p}\;\underbrace{00\ldots0}_{a}};$$

pri tom je (A) prirodni broj sastavljen od brojaka pretperiode A; (AP) je prirodni broj sastavljen od pretperiode i periode zadanog periodskog broja; a, odnosno p, kazuje koliko perioda, odnosno pretperioda, ima decimalnih mjesta.

5. REALNI BROJEVI. SKUP *R*. IRACIONALNI BROJEVI

5.1. Definicija. Decimalne razlomke (s konačno i beskonačno mnogo znamenaka) zovemo *realni (stvarni) brojevi*. *R* označuje skup svih realnih brojeva.

O aksiomatskoj definiciji mnogosti *R* isp. 32, § 8.9.11.

5.2. Definicija. Realne brojeve koji nisu racionalni brojevi zovemo *iracionalni brojevi*. Drugim riječima, svaki decimalni broj koji nije periodski zove se iracionalan realan broj. Takav je npr. broj 0, 10 1 0 0 1 0 0 0 1... (poslije svakog 1 piše se uzastopce onoliko znakova 0 koliko ispred toga 1 ima već znakova 1). Već u srednjoj školi dokazuje se da je i broj $2^{1/2}$ iracionalan broj; uopće broj $+m^{1/n}$ je ili cio ili iracionalan za svako $m, n\in N$.

5.3. Intervali. Definicija. Ako su a, b dva $\neq$ realna broja, tada se pod *otvorenim intervalom a, b* realnih brojeva razumijeva množina svih realnih brojeva koji su smješteni između a, b; on se označuje sa $R(a,b)$ ili sa $R(b,a)$.

Prema tome, ako je $a<b$, onda je $R(a,b)=R(b,a)=$skup svih x za koje je $x\in R$ i $a<x<b$. *Zatvoreni* interval ab označuje se sa $R[a,b]$ ili $R[b,a]$; to je skup svih x za koje je $a\leqslant x\leqslant b$, odnosno $a\geqslant x\geqslant b$. Drugim riječima:

$$R(a,b)=\{x;\, x\in R\wedge((a<x<b)\vee(a>x>b))\}$$

$$R[a,b]=\{x;\, x\in R\wedge((a\leqslant x\leqslant b)\vee(a\geqslant x\geqslant b))\}.$$

Slično se definiraju *poluzatvoreni intervali* $R[a,b)$, $R(a,b]$. (isp. pogl. 3, § 13.6).

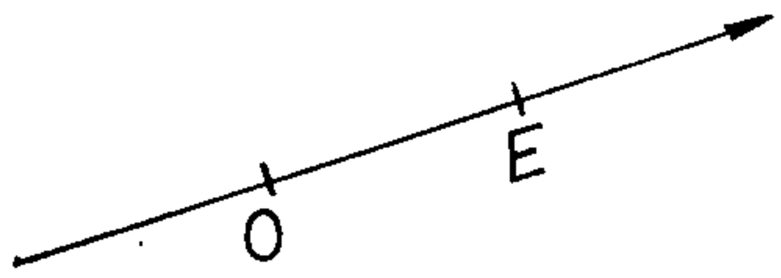
5.4 Okoline. Definicija. *Okolina broja a* jest svaki skup koji obuhvata neki otvoren interval u kojem se nalazi *a*.

Prema tome, zatvoreni interval $R[a,b]$ nije okolina *krajeva a*, odnosno *b*.

5.5 Brojevna pravulja[1]. Neka su O, E dvije različne tačke; promatrajmo vektor $\overrightarrow{OE}$ i vektor $x \cdot \overrightarrow{OE}$ za svaki realni broj x; početak toga vektora je O; označimo njegov završetak sa X; tada je X potpuno određena tačka pravca ili pravulje OE, pa je

$$\overrightarrow{OX} = x \cdot \overrightarrow{OE}. \tag{1}$$

Ako je x' realan broj $\neq x$, tada je $\overrightarrow{OX'} \neq \overrightarrow{OX}$; na taj se način vezom (1) uspostavlja *obostrano jednoznačna veza* ili *tolikovanje* između množine R svih realnih brojeva i tačaka proizvoljne pravulje OE. Ta je veza tako prisna da je zgodno za tačku X pravulje uvesti i *numeričku oznaku* (x) ili čak x i govoriti o *tački* (x), pa čak i o tački x uređene ili orijentirane pravulje OE. Tako bi npr. tačka E imala *numeričku oznaku i ime* (1) ili 1; 0, odnosno (0), značilo bi tačku O. Isto tako, *radi kratkoće* možemo govoriti o *broju* x za svaku tačku X uređene pravulje $\overrightarrow{OE}$ misleći pri tom na mjerni broj x dobiven osnovnom vezom (1).[2]



Sl. 4.5.5.

Pojam intervala i okoline postaju vrlo pregledni ako se služimo brojevnom pravuljom.

5.6. Množenje s — 1. Svakom broju a odgovara *suprotan* broj $-a$ pa uzimamo da je $-a = -1 \cdot a$; na taj način *množenju broja x s* — 1 *odgovara simetrična slika tačke x s obzirom na O* kao središtem simetrije. Na taj način *množenje* s — 1 kao *aritmetička operacija* u skupu R i *rotacija* za π oko O kao *geometrijska operacija* na koordinatnoj pravulji odgovaraju jedno drugom. Isto tako, množenje s 1 kao aritmetičke operacije i rotacija za 2π oko O odgovaraju jedno drugom.

6. KOMPLEKSNI BROJEVI. SKUP $R(i)$

6.1. Ovdje nećemo dati strogu definiciju kompleksnih brojeva; zadovoljimo se napomenom da su oni oblika $a+bi$, gde je $i^2 = -1$; pri tom su a, b proizvoljni *realni* brojevi; i da se s $a+bi$ računa kao i s drugim binomima; slovo i označuje jedno »*određeno rješenje*« jednažbe $i^2 = -1$; važno je da izraze oblika $a+bi$ smatramo *binomima* i da se baratanje s njima vrši kao i s drugim binomima (isp. 23, § 8.4). Skup svih kompleksnih brojeva može se označiti sa $R(i)$.

Vrlo je slikovito i zgodno *uvesti* kompleksne brojeve i *geometrijski, interpretirajući množenje s i kao rotaciju za* $\pi/2$ *koordinatne ravnine oko koordinatnog početka.*

---

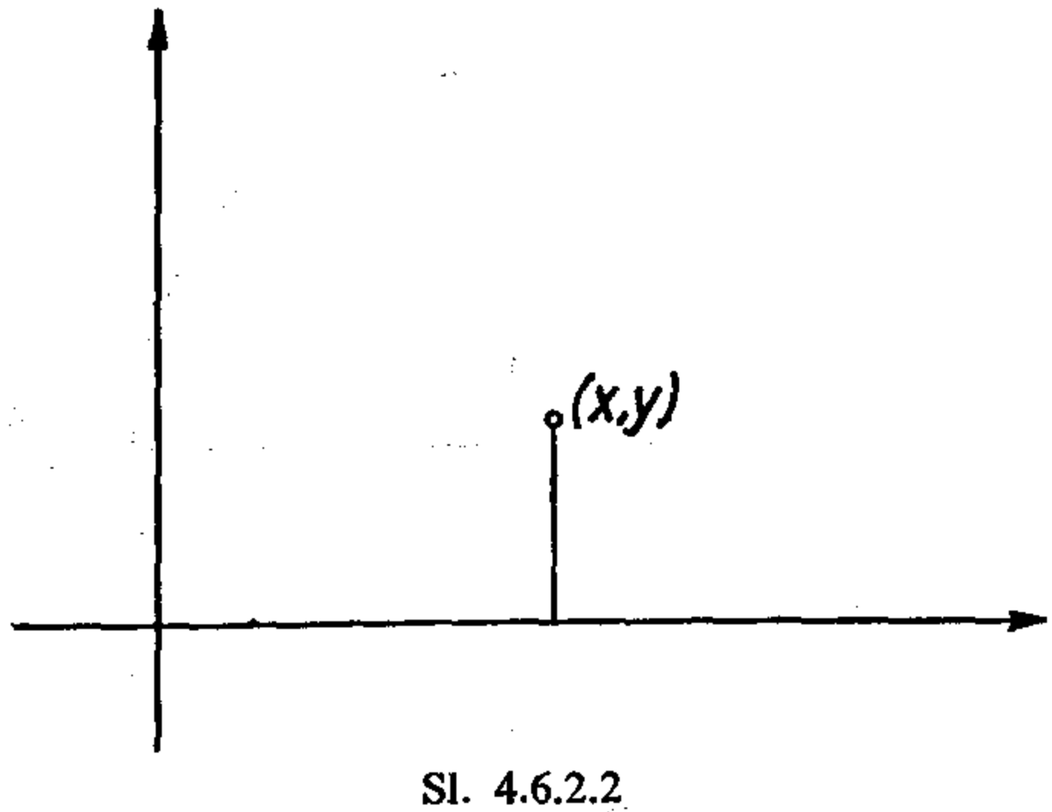
[1] Predlažem naziv »*pravulja*« umesto »*pravac*« ili »*prava*« jer tačnije i potpuno jednoznačno određuje onaj skup tačaka koji želimo izučavati.

[2] Jasno je da čitalac neće pomiješati npr. oznaku (1) *za gornju formulu* i oznaku (1) za *tačku E.*

6.2. Koordinatna ravnina. Brojevna ravnina.

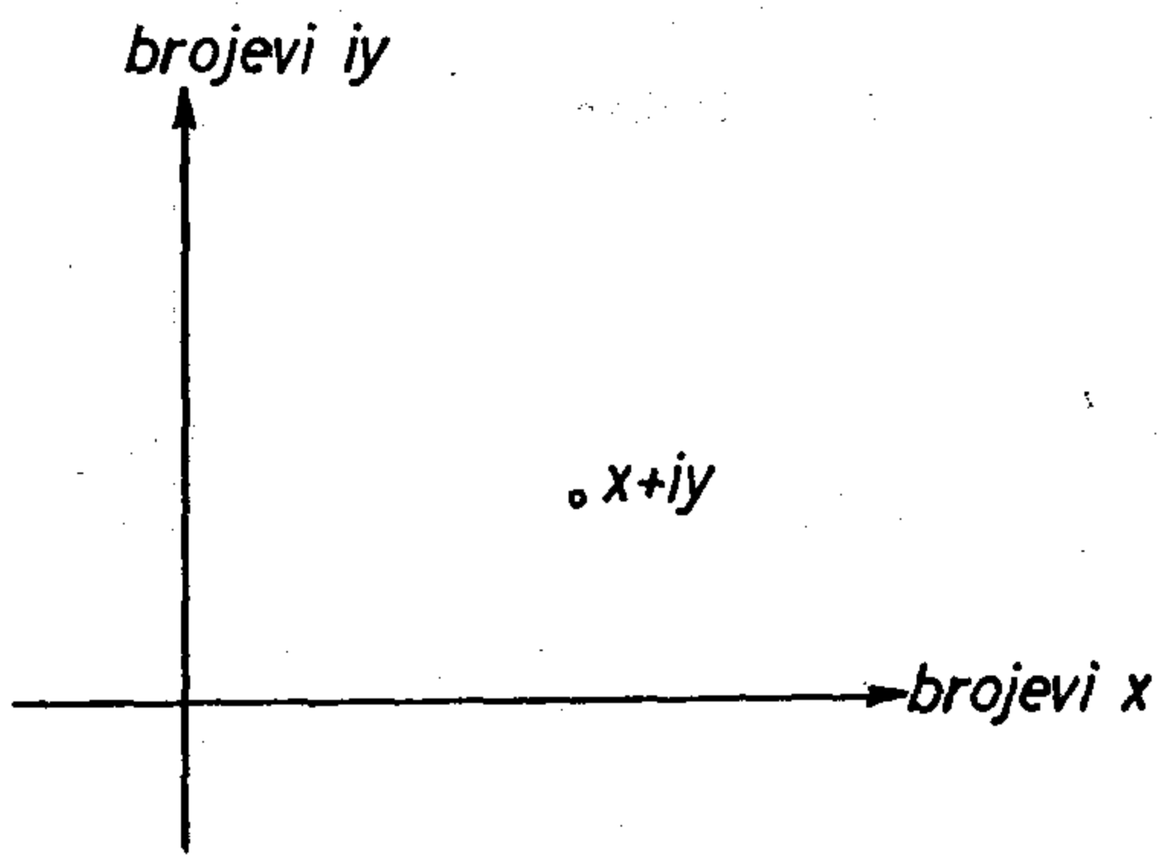
6.2.1. Definicija. *Koordinatna ravnina je svaka ravnina* u kojoj je zadan određen *koordinatni sistem* (obično pravokutni Kartezijev koordinatni sistem). Koordinatnom ravninom se postiže tolikovanje između tačaka ravnine i uređenih parova (x, y) realnih brojeva. Može se govoriti o (x, y) kao *analitičkoj oznaci za tačku* kojoj je x apscisa, a y ordinata u promatranom Descartesovu sistemu.

Vrlo je praktično uz *tačku T* analitičke oznake (a, b) promatrati i kompleksni broj $a+bi$; čak taj broj možemo upisati tamo gdje je smještena tačka T; možemo čak i govoriti o *tački oznake* $a+bi$, odnosno o *tački* $a+bi$. Time ravnina postaje nosiocem brojeva pa je zovemo *brojevna ravnina*. *Prva* ili *apscisna os* je nosilac *realnih brojeva*; *druga* ili ordinatna *os* je nosilac brojeva oblika bi *(čisto imaginarni brojevi)*.



Sl. 4.6.2.2

6.2.2. Definicija. ***Brojevna ravnina je svaka ravnina s okomitim Kartezijevim sistemom koordinata pri čemu tačku analitičkog imena (x, y) zapisujemo kao kompleksni broj $z=x+yi$. Realna os je nosilac realnih brojeva; ordinatna***



Sl. 4.6.2.2′.

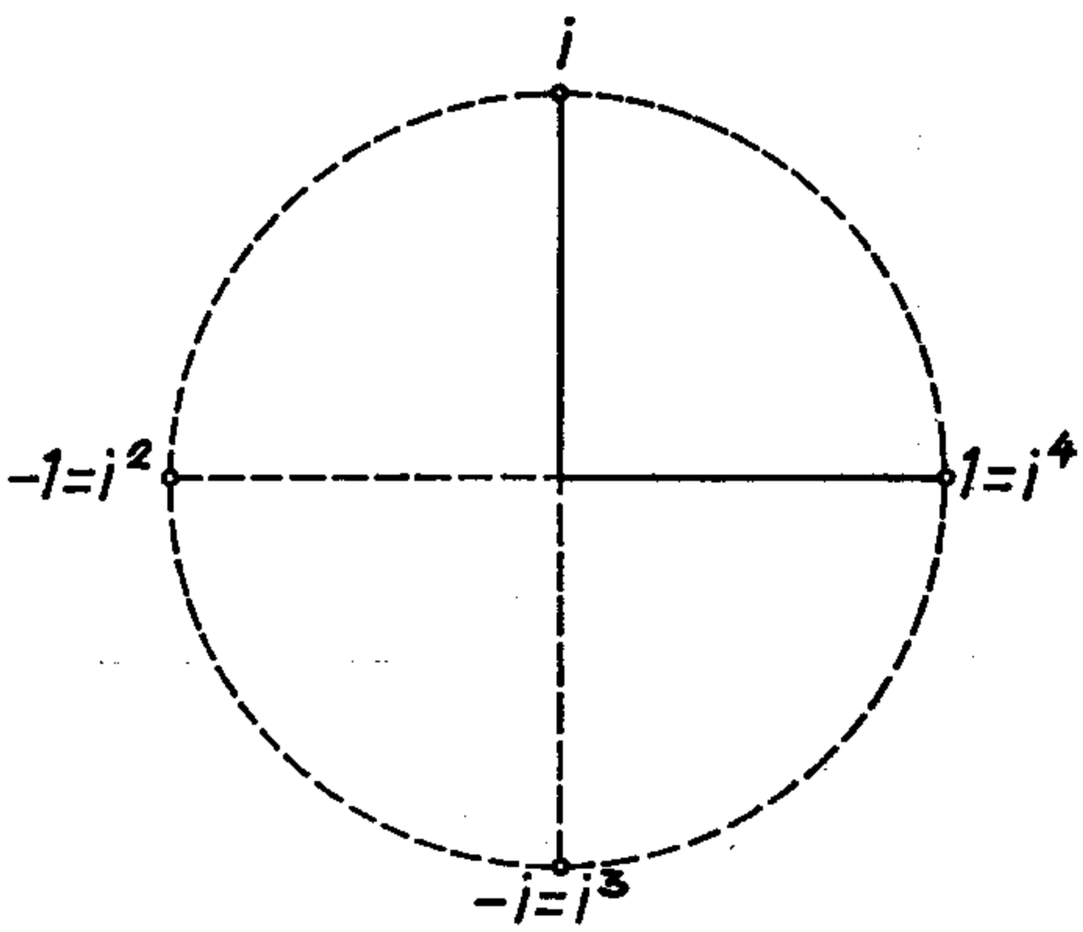
os brojevne ravnine zove se čisto imaginarna os brojevne ravnine i nosilac je čisto imaginarnih brojeva.

Neće biti zabune ako miješamo nazive: *apscisna os* i ***realna os***, te nazive *ordinatna os* i *čisto imaginarna os*.

6.2.3. Brojevi — 1, i; rotacije oko *O*. Promatrajmo npr. brojeve 3, $3i$ u brojevnoj ravnini; tačka imena 3 u toj ravnini nalazi se na x-osi; rotacijom

oko O za $\pi/2$ prelazi ta tačka u tačku imena $3i$ na drugoj koordinatnoj osi. Na taj način, *geometrijska rotacija* za $\pi/2$ oko O i *algebarsko množenje* s i *odgovaraju jedno drugom.* Čak se postavlja:

Definicija. *Za svaku tačku T ravnine neka $i \cdot T$ znači tačku u koju dolazi T rotacijom oko O za $\pi/2$ u pozitivnom smislu.*



Sl. 4.6.2.3.

To specijalno znači da tačka 1 prelazi tom rotacijom u $i \cdot 1$ ili kraće i, a ova u $i \cdot i$, dakle u -1, što znači da je $i^2 = -1$ (stavljajući $i \cdot i = i^2$); iz istog razloga je i^3 kao $i \cdot i^2$ jednaka $-i$; najzad $i^4 = 1$ jer nakon uzastopne *četiri* rotacije oko O za $\pi/2$ u pozitivnom smislu dolazi tačka 1 u svoj početni položaj 1.

Isporedi množenje s -1 kao rotaciju za π oko O!

6.3. Realni i imaginarni dio. Ako su a, b realni brojevi, tada se a zove *realni dio kompleksnog* ili *složenog broja* $a+bi$; bi se zove *imaginarni dio* od $a+bi$; b se zove *koeficijent imaginarnog dijela broja* $a+bi$; pišemo:

$$Re\,(a+bi) = a, \qquad Im\,(a+bi) = b.$$

6.4. Jednakost kompleksnih brojeva. Definicija

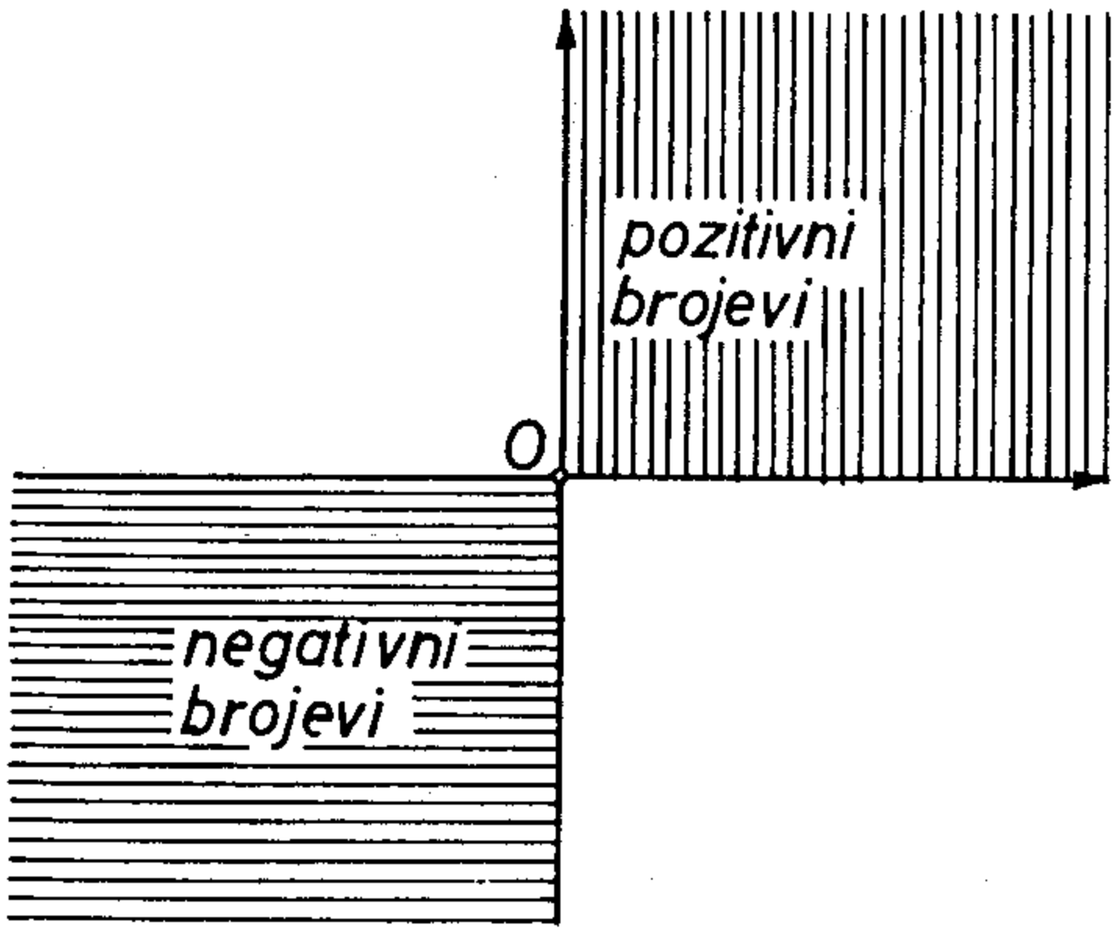
$$a+bi = a'+b'i \Leftrightarrow a = a' \wedge b = b';$$

drugim riječima: *za kompleksne brojeve z, z' jednakost $z = z'$ vrijedi isto što* i postojanje *obiju* jednakosti: $Re\,z = Re\,z'$, $Im\,z = Im\,z'$.

Posebno,

$$a+bi = 0 \Leftrightarrow a = 0 \wedge b = 0.$$

Definiramo $z \neq z'$ kao negaciju od $z = z'$, tj. $z \neq z' \Leftrightarrow \neg(z = z')$.



Sl. 4.6.5.

6.5. Glavno uređenje kompleksnih broveva. Definicija.

$$z < z' \Leftrightarrow (Re\,z < Re\,z') \wedge (Im\,z < Im\,z'); \quad z \lessdot z' \Leftrightarrow (z < z') \wedge (z \neq z').$$

Znak $\wedge$ čitaj „i“ ili „te“.

Tako npr. $2+5i<5+10i$ jer je $2<5$, $5<10$;

$2+5\ \ i<2+100i.$

Nije ni $1\leqslant i$ ni $1>i$; brojevi 1, i su *neusporedljivi.*

Brojevi >0 zovu se *pozitivni*; oni s 0 ispunjavaju *prvi zatvoreni kvadrant brojevne ravnine.*

Negativni brojevi, tj. brojevi koji su <0, ispunjavaju čitav *treći zatvoreni kvadrant iz kojeg je uklonjen vrh.*

Osim pozitivnih brojeva, negativnih brojeva i 0 dolaze još brojevi iz *otvorenog* 2. *i otvorenog* 4. *kvadranta;* oni su *neusporedljivi s* 0; svaki broj iz otvorenog drugog kvadranta neusporedljiv je sa svakim brojem iz otvorenog 4. kvadranta. (gl. sliku 4.6.5).

6.6. Zbrajanje kompleksnih brojeva. Definicija.

$$(a+bi)+(a'+b'i)=(a+a')+(b+b')i, \text{ tj.}$$

$$Re\,(z+z')=Re\,z+Re\,z'$$

$$Im\,(z+z')=Im\,z+Im\,z'.$$

Drugim riječima *radijus-vektor* $\overrightarrow{Oz}$ *broja z plus radijus-vektor* $\overrightarrow{Oz'}$ *što pripada broju z' daje radijus-vektor sume* $z+z'$ *brojeva z, z'*:

$$\overrightarrow{O\,(z+z')}=\overrightarrow{Oz}+\overrightarrow{Oz'}.$$

7. ODUZIMANJE KOMPLEKSNIH BROJEVA. SUPROTNI BROJEVI

Oduzimanje se *definira* kao *operacija obratna* od zbrajanja:

Definicija. *Diferencija* ili razlika $z'-z$ zadanih brojeva z', z definira se kao rješenje jednakosti

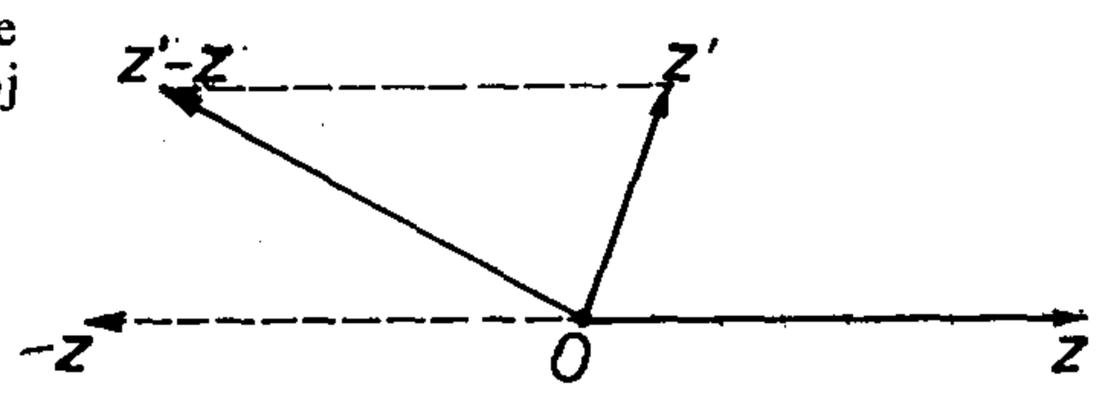
$$x+z=z';$$

specijalno se umjesto $0-z$ piše $-z$; $-z$ se zove *suprotni* broj od z.

Vidi se da je

$$(a+bi)-(a'+b'i)=$$

$$=(a-a')+(b-b')i;$$



Sl. 4.7.

posebno, $-(a+bi)=-a-bi$.

Vidi se da je $z'-z=z'+(-z)$.

Geometrijski, razlika $z'-z$ ***je vektor od*** z ***do*** z', jer taj vektor dodan suptrahendu z daje minuend z'.

8. MNOŽENJE KOMPLEKSNIH BROJEVA

Definicija. $(x+iy)(x'+iy')=(xx'-yy')+i(xy'+x'y)$.

To znači da se množenje kompleksnih brojeva $x+iy$, $x'+iy'$ izvodi kao da množimo dvočlan $x+iy$ dvočlanom $x'+iy'$ imajući na umu da je $i^2=-1$.

Poslije ćemo vidjeti (u § 16, posebno 16.6) kako se množenje vrši geometrijski.

9. DIJELJENJE KOMPLEKSNIH BROJEVA

9.1. Dijeljenje se *definira kao obrat* množenja:

Definicija. Ako su $a+bi$, $c+di$ zadani kompleksni brojevi, tada se rješenje $z=x+iy$ jednadžbe

$$(a+bi)z=c+di \tag{1}$$

zove *kvocijent broja* $c+di$ i broja $a+bi$; označuje se sa

$$(c+di):(a+bi) \text{ ili } \frac{c+di}{a+bi} \text{ ili } (c+di)(a+bi)^{-1}.$$

Pretpostavlja se $a+bi\neq 0$.

No jednakost (1) postaje za $z=x+iy$ nakon izmnažanja:

$$(ax-by)+i(bx+ay)=c+di. \tag{2}$$

Na osnovu jednakosti kompleksnih brojeva (t. 4) znači (2) da vrijedi:

$$ax-by=c$$

$$bx+ay=d.$$

Iz te dvije jednadžbe dobijemo $x=\frac{ac+bd}{a^2+b^2}$, $y=\frac{ad-bc}{a^2+b^2}$.

Na taj smo način dobili:

9.2. Teorem. $\frac{c+di}{a+bi}=\frac{ac+bd}{a^2+b^2}+\frac{ad-bc}{a^2+b^2}i$, pri tom je $c+di\neq 0$, tj. $a^2+b^2\neq 0$.

O geometrijskoj strani dijeljenja brojeva v. t. 16.7.

10. KONJUGIRANI [1] ILI SPREGNUTI BROJEVI

Definicija. Svakom broju $z = x + iy$ pripada određen *konjugirani* ili *spregnuti* broj $\bar{z}$ kao simetrična slika prema realnoj osi:

$$Re\, z = Re\, \bar{z},\ Im\, z = -Im\, \bar{z},$$

tj. realni dijelovi su jednaki, a imaginarni dijelovi od z i $\bar{z}$ su suprotnojednaki.

Dakle je $a + b\,i = a - b\,i$.

Kao vježba lako se dokazuje ovo:

ako je $\bar{z} = z$, onda je z realan broj; i obrnuto;

ako $z = -\bar{z}$, onda je z čisto imaginaran broj; i obrnuto;

$z\bar{z} = x^2 + y^2 \geqq 0$; $z\bar{z} = 0 \Leftrightarrow z = 0$.

11. APSOLUTNA VRIJEDNOST ILI MODUL KOMPLEKSNOG BROJA. SIGNUM ILI ZNAK KOMPLEKSNOG BROJA

11.1. Definicija. *Apsolutna vrijednost ili modul kompleksnog broja* $z = x + iy$ jest neodrečni broj $+(x^2 + y^2)^{1/2}$; označuje se sa $|z|$, odnosno $|x + iy|$ (okomite zagrade); geometrijski, *znači* $|z|$ *udaljenost između* O i z (isp. pogl. 3. § 2.1.1.). Npr. $|3 + 4\,i| = +(9 + 16)^{1/2} = 5$.

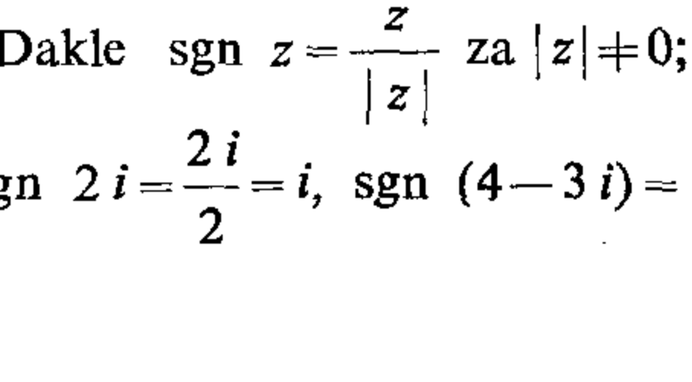
11.1.1. Definicija. **Signum** ili **znak (predznak) kompleksnog broja** $z \neq 0$ jest kvocijent $z : |z|$; označuje se sa sgn z. Dakle $\operatorname{sgn} z = \dfrac{z}{|z|}$ za $|z| \neq 0$; stavlja se sgn $0 = 0$. Npr. $\operatorname{sgn} -5 = \dfrac{-5}{5} = -1$, $\operatorname{sgn} 2\,i = \dfrac{2\,i}{2} = i$, $\operatorname{sgn}(4 - 3\,i) =$

$$= \frac{4 - 3\,i}{+(4^2 + (-3)^2)^{1/2}} = \frac{4}{5} - \frac{3}{5}\,i.$$

11.2. Modul razlike. ***Najvažnije geometrijsko svojstvo apsolutne vrijednosti sastoji se u tome da apsolutna vrijednost diferencije dvaju brojeva znači međusobnu razdaljinu tih brojeva:***

$|z - z'|$ *znači međusobni razmak brojeva (tačaka)* z, z'.

U paralelogramu kojemu su vrhovi O, $z - z'$, z, z' nasuprotne stranice O do $z - z'$ i z, z' međusobno su jednake; no dužina prve iznosi $|z - z'|$.



Sl. 4.11.

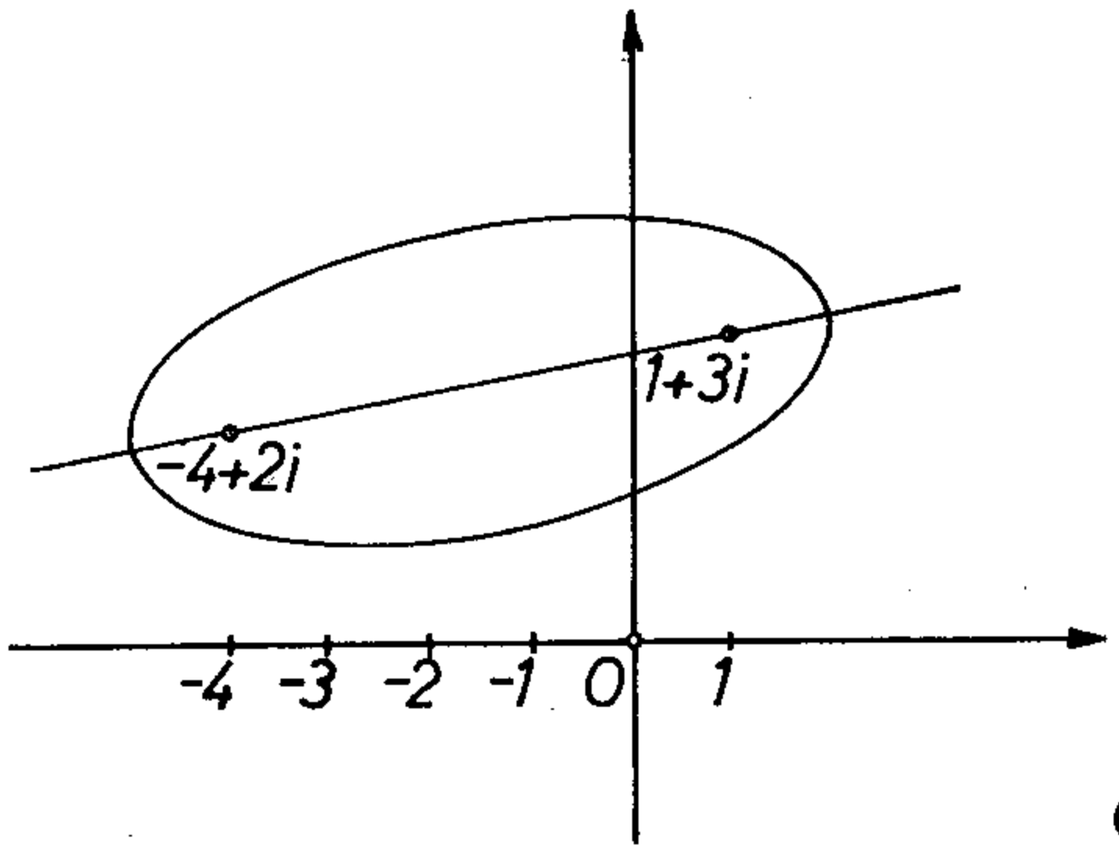
Dva primjera. $|z - 1| = 2$ je kružnica kojoj je radijus 2, a središte u broju 1.

Isto tako

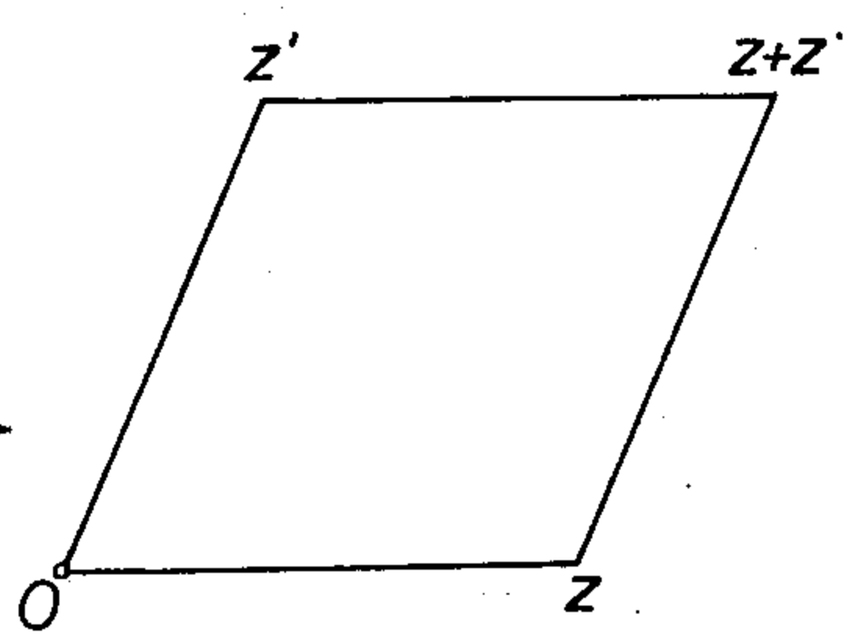
$$|z - (1 + 3\,i)| + |z + 4 - 2\,i| = 14$$

[1] Tu su *n*, *j* samostalni glasovi, ćirilski конјугирани.

predočuje skup tačaka z kojima je suma udaljenosti od tačaka $1+3i$, $-4+2i$ jednaka 14; to je, dakle, jednadžba elipse kojoj je velika os 7, a fokusi su joj u $1+3i$, $-4+2i$ (gledaj sliku 4.11.2).



Sl. 4.11.2.



Sl. 4.11.3.

11.3. Modul zbroja. 1. *Brojevi O, z, $z+z'$ lli leže na istoj pravulji ili određuju trokut kojemu su dužine stranica*: $|z|$, $|z'|$, $|z+z'|$.

No iz planimetrije znamo da je svaka stranica u svakom $\triangle$ manja od sume ostalih dviju stranica toga trokuta. Primijenimo li to na trokut kojemu su vrhovi O, z, $z+z'$ i uzimajući u obzir slučaj da te tri tačke mogu ležati na istoj pravulji, dobijemo:

$$|z+z'| \leqslant |z| + |z'|. \tag{1}$$

To se lako može dokazati.

U relaciji (1) vrijedi znak $=$ onda i samo onda ako su tačke O, z, z' na istoj pravulji i da O ne leži između z i z'.

Općenito:

$$\Big|\sum_{k=1}^{n} z_k\Big| \leqslant \sum_{k=1}^{n} |z_k| \text{ za bilo koji prirodni broj } n \text{ i bilo koji niz } z_1, z_2, \ldots, z_n \in R(i).$$

11.4. Apsolutna vrijednost i signum produkta. *Apsolutna vrijednost produkta od dva ili konačno mnogo brojeva jednaka je produktu apsolutnih vrijednosti tih brojeva*:

$$|z\,z'| = |z| \cdot |z'|, \qquad |z^2| = |z|^2 \tag{1, 2}$$

$$\Big|\prod_{k=1}^{n} z_k\Big| = \prod_{k=1}^{n} |z_k|, \qquad |z^n| = |z|^n \ (n \in N). \tag{3, 4}$$

Isto tako

$$\operatorname{sgn}(z\,z') = \operatorname{sgn} z \cdot \operatorname{sgn} z'$$

$$\operatorname{sgn} \prod_{k=1}^{n} z_k = \prod_{k=1}^{n} \operatorname{sgn} z_k, \ (n \in N).$$

Zadovoljimo se da dokažemo (1); ostali slučajevi (2), (3) i (4) lako izlaze iz (1).

Neka je $z = a + b\,i$, $z' = a' + b'\,i$, dakle $z\,z' = (a\,a' - b\,b') + (a\,b' + a'\,b)\,i$. Odredimo module: $|z\,z'| = |(a\,a' - b\,b') + i\,(a'\,b + a'\,b)| =$ prema definiciji $= [(a\,a' - b\,b')^2 + (a\,b' + a'\,b)^2]^{1/2}$; ovo je, kao što se lako može provjeriti $= (a^2 + b^2)^{1/2}\,(a'^2 + b'^2)^{1/2}$; dakle je $= |z| \cdot |z'|$.

11.5. Modul i signum kvocijenta. Čitalac neka sam dokaže da je

$$\left|\frac{z}{z'}\right| = \left|\frac{z}{z'}\right|, \quad \operatorname{sgn}\frac{z}{z'} = \frac{\operatorname{sgn} z}{\operatorname{sgn} z'} \text{ ako je } z' \neq 0.$$

11.6. Teorem. $z \neq 0 \Leftrightarrow |\operatorname{sgn} z| = 1$.

12. NORMA KOMPLEKSNOG BROJA

12.1. Definicija. *Kvadrat apsolutne vrijednosti kompleksnog broja z zove se norma broja z;* označuje se sa $N\,z$; dakle je $N\,z = |x + i\,y|^2 = x^2 + y^2$.

12.2. Kako se norma vlada prema računskim operacijama? Svojstva. Najvažnije svojstvo norme sastoji se u tome da je *norma realan* broj > 0 *i da je norma produkta jednaka produktu normi faktorâ*:

$$N(z\,z') = N(z) \cdot N(z'),$$

odnosno:

$$N \prod_k z_k = \prod_k N(z_k).$$

To se može izreći i ovako:

12.3 Teorem. *Normin operator N distributivan je u odnosu na množenje kompleksnih brojeva,* ili još ovako: *operatori N i* $\prod_k$ *međusobno su komutativni.*

Prepuštamo čitaocu da dokaže taj obrazac kao i obrasce:

$$N(z^n) = (N\,z)^n,$$

$$N\left(\frac{z}{z'}\right) = \frac{N(z)}{N(z')} \text{ ako je } z' \neq 0,$$

$$N(z + z') = N(z) + N(z') + 2\,Re\,(z)\,Re\,(z') + 2\,Im\,(z) \cdot Im\,(z'),$$

$$N|z| = |N(z)| = |z|^2,$$

$$N\,\bar{z} = N(z).$$

13. ARGUMENT KOMPLEKSNOG BROJA *Z* (OPEPATOR ARG *Z*)

U brojevnoj ravnini broju $z = x + i\,y$ odgovara određena tačka; njene su Descartesove koordinate x, y u odnosu na realnu i imaginarnu os kao koordinatne osi. No osim tih koordinata služimo se i *polarnim koordinatama* s *x-osi i*

početkom O: radi se *o razdaljini O z*, koju smo nazvali *modulom broja z*, i o $\sphericalangle(1, O, z)$; odnosno o mjernom broju toga kuta i zvat ćemo ga *argument broja z*.

13.1. Definicija. *Argument kompleksnog broja z jeste svaki mjerni broj kuta* $\sphericalangle(1, O, z)$; označuje se sa *Arg z*; definiran je za svako $z \neq 0$; Arg ima beskonačno mnogo vrijednosti; *Arg O nije definirano.*

Npr. Arg $1 = 0,\ 2\pi,\ -2\pi,\ 4\pi,\ -4\pi, \ldots, \ldots, k \cdot 2\pi, \ldots$ za svako $k \in D$ (D = skup svih cijelih brojeva); tj.

$$\text{Arg } 1 = \dot{D}\, 2\pi;\ \text{Arg } i = \frac{\pi}{2} + \dot{D}\, 2\pi.$$

⟶ **13.2. Teorem.** ***Za svako $z \neq 0$ ima Arg z beskonačno mnogo vrijednosti; ako je φ jedna vrijednost od Arg z, onda je svaka vrijednost od Arg z oblika $\varphi + \dot{D} \cdot 2\pi$, dakle Arg $z = \varphi + \dot{D}\, 2\pi$.***

To je osnovna činjenica.

13.3. Arg z i arg z. Posebno ćemo sa arg z (malo poč. slovo!) označivati onu vrijednost Arg z koja leži u *poluzatvorenom intervalu* $[0, 2\pi)$, za koj; je dakle, $0 \leqslant \arg z < 2\pi$. To je tzv. *glavna neodrečna mjerna vrijednost kuta*i često se $\arg z$ definira tako da bude $-\pi < \arg z \leqslant \pi$; time mjerni broj kuta ue bi nikad bio po modulu veći od π (ispružen kut).

13.4. Lema. *Za svako kompleksno $z \neq 0$ i svako realno pozitivno c vrijedi;*

$$Arg\ c\, z = Arg\ z.$$

$$\text{sgn } c\, z = \text{sgn } z.$$

Stvarno, iz razloga što je realan broj c pozitivan izlazi da su točke O, z, $c\, z$ na jednoj te istoj zraci; a za sve tačke jedne te iste zrake sastavljen je skup $\{\text{Arg } z\}$ svih Arg z od istih brojeva.

13.5. Lema. *Za svaki realan broj x ispunjavaju brojevi −Arg x (anti-argument od x) cijelu otvorenu zraku koja s pozitivnom x-poluosi čini kut veličine x.*

14. TRIGONOMETRIJSKI OBLIK KOMPLEKSNIH BROJEVA

Zadan je broj $z = a + i\,b$; njegov je modul $|z| = \sqrt{a^2 + b^2}$, a argument mu je također određen: Arg z. No, tačka z je potpuno određena svojim polarnim koordinatama $|z|$, Arg z.

Očigledno je

$$a = |z| \cos \text{Arg } z \qquad b = |z| \sin \text{Arg } z,$$

pa je

$$z = a + i\,b = |z| \cos \text{Arg } z + i\,|z| \sin \text{Arg } z, \text{ tj.}$$

$$z = |z| \cdot (\cos \text{Arg } z + i \sin \text{Arg } z). \tag{1}$$

To je tzv. *trigonometrijski oblik broja z.* U obliku (1) dobro se vide *polarne koordinate* $|z|$, Arg z tačke u kojoj leži broj z. Primetimo da je cos Arg z posve određen broj; to vrijedi i za sin Arg z, jer se različite vrijednosti Arg z razlikuju za cjelobrojni mnogokratnik punoga kuta, pa im zato pripada isti sinus i isti kosinus.

Tako npr. broj -1 ima trigonometrijski oblik $\cos(-\pi)+i\sin(-\pi)$, odnosno $\cos(-\pi+2\pi\dot{D})+i\sin(-\pi+2\pi\dot{D})$. Također je

$$2-3i=+\sqrt{13}\,(\cos\alpha+i\sin\alpha),$$

gdje je α mjerni broj kuta iz 4. kvadranta kojemu je tangens $-\frac{3}{2}$.

15. EKSPONENCIJALNI ILI POLARNI OBLIK KOMPLEKSNIH BROJEVA. EULEROVA JEDNAKOST

15.1. Pravila

$$(\cos\alpha+i\sin\alpha)(\cos\alpha'+i\sin\alpha')=\cos(\alpha+\alpha')+i\sin(\alpha+\alpha')$$

$$(\cos\alpha+i\sin\alpha):(\cos\alpha'+i\sin\alpha')=\cos(\alpha-\alpha')+i\sin(\alpha-\alpha')$$

o množenju i dijeljenju *unimodularnih brojeva*, tj. brojeva modula 1, podsjećaju nas na pripadna računanja s *potencijama iste baze*, naime:

$$x^{\alpha}\cdot x^{\alpha'}=x^{\alpha+\alpha'}$$

$$x^{\alpha}:x^{\alpha'}=x^{\alpha-\alpha'}.$$

Zato bismo mogli očekivati da će se unimodularni brojevi moći prikazati kao potencija sa zadanom bazom.

15.2. Eulerova jednakost. [1] Označujući kao obično

$$e=\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^{n}=2,718281\ldots,$$

može se pokazati da je *za svako realno* x *zaista*

$$\cos x+i\sin x=e^{ix}.$$

To je tzv. Eulerova *trigonometrijsko-eksponencijalna jednakost*. Mi je ovdje možemo shvatiti tako da njome *definiramo prirodnu eksponencijalnu funkciju* e^x također na *imaginarnoj osi*: po realnoj osi definira se

$$e^{x}=\lim_{n}\left(1+\frac{x}{n}\right)^{n};$$

definiramo li za proizvoljne realne brojeve x, y da je

$$e^{x+iy}=e^{x}\cdot e^{iy},$$

L. Euler (1707 — 1783), veliki švicarski matematičar

[1] L. Euler [Ojler] (1707 — 1783), veliki švicarski matematičar

definirana je time eksponencijalna funkcija $e^z \mid C$ za svako kompleksno z, tj. za $z \in C$; C je skup svih kompleksnih brojeva.

Lako se dokaže da ta funkcija zadovoljava slične relacije kao pripadna funkcija $e^x \mid R$, kad je x realno, posebno da je

$$e^z \cdot z' = e^{z+z'}, \quad e^z : e^{z'} = e^{z-z'}.$$

Valja, dakle, upamtiti da je za svako $z \neq 0$

(1) $$e^{i \operatorname{Arg} z} = \cos \operatorname{Arg} z + i \sin \operatorname{Arg} z,$$

odakle izlazi:

$$\operatorname{Arg} e^{i \operatorname{Arg} z} = \operatorname{Arg} (\cos \operatorname{Arg} z + i \sin \operatorname{Arg} z) = \operatorname{Arg} z,$$

tj. identički:

$$\operatorname{Arg} e^{i \operatorname{Arg} z} = \operatorname{Arg} z \text{ za svako } z \neq 0, \text{ te}$$

15.2.1. $\operatorname{sgn} z = e^{i \operatorname{Arg} z}$ za $z \neq 0$.

15.3. Eksponencijalno-polarni oblik kompleksnih brojeva. Na osnovu obrasca (1) prelazi trigonometrijski oblik

$$z = |z| (\cos \operatorname{Arg} z + i \sin \operatorname{Arg} z)$$

u ovaj *osnovni i vrlo sugestivni eksponencijalni ili polarni oblik*:

(2) $$z = |z| e^{i \operatorname{Arg} z}, \quad e^{i \operatorname{Arg} z} = \operatorname{sgn} z \text{ za } z \neq 0$$

u kojem se na izrazit način javlja apsolutna vrijednost i argument te signum.

15.3.1. Teorem. ***Izraz $r e^{i\alpha}$ za bilo kakve realne brojeve $r > 0$, α predstavlja kompleksni broj kojemu je broj r apsolutna vrijednost, broj α argument. Izraz $e^{i\alpha}$ naznačuje jedinični radijus-vektor koji s realnom osi čini kut veličine α.***

15.3.2. *Za $z = -1$ daje veza* (2) *ovu glasovitu Eulerovu jednakost*:

$$-1 = e^{i\pi},$$

kojom su međusobno povezani glasoviti brojevi: -1, e, i, π.

16. MNOŽENJE I DIJELJENJE KOMPLEKSNIH BROJEVA U POLARNIM KOORDINATAMA

16.1. Pregled. U §§ 8, i 9. obradili smo množenje i dijeljenje kompleksnih brojeva u *Descartesovim koordinatama*; te su koordinate vrlo podesne za *zbrajanje i oduzimanje* kompleksnih brojeva, no one ne daju preglednih rezultata za *množenje i dijeljenje* kompleksnih brojeva; za ovu svrhu polarne koordinate su od vanredne koristi.

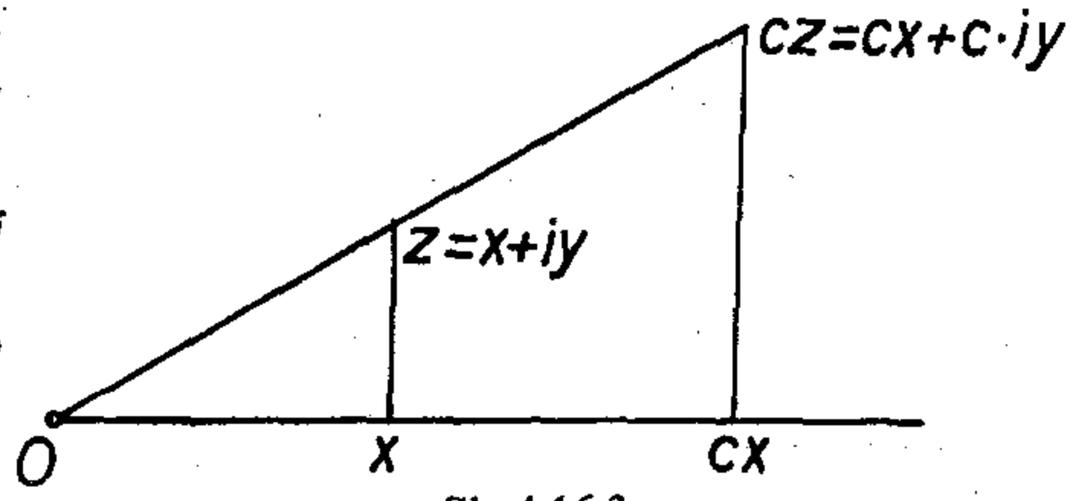
Već znamo da je modul produkta jednak produktu modulâ faktora; još *preostaje da ispitamo kako se vlada druga polarna koordinata-argument*. Ako je $z = r e^{i\alpha}$, $z' = r' e^{i\alpha'}$, tada je $z z' = r e^{i\alpha} \cdot r' e^{i\alpha'}$, što će prema očekivanju biti =

$= (r\,r')\,e^{i\,(\alpha+\alpha')}$, tj. $z\,z' = (r\,r')\,e^{i\,(\alpha+\alpha')}$. To bi značilo da je $\operatorname{Arg}(z\,z') = \operatorname{Arg} z + \operatorname{Arg} z'$. A to ćemo stvarno i pokazati.

16.2. Geometrijsko množenje s realnim brojem $c>0$:

$c\,(x+i\,y) = c\,x + i\,c\,y$. Prema tome,

polazni $\triangle O\,x\,z$ i *dobiveni* $\triangle O\,(cx)\,(cz)$ *su slični* jer su im stranice proporcionalne.



Sl. 4.16.3.

16.3. Lema. *Pomnožiti broj z s unimodularnim brojem $\cos\alpha + i\sin\alpha = e^{i\alpha}$* znači rotirati z oko O za kut α.

Stvarno, $z = x + i\,y = |z|\,(\cos \operatorname{Arg} z + i \sin \operatorname{Arg} z)$, pa je $z e^{i\alpha} = |z|\,(\cos \operatorname{Arg} z + i \sin \operatorname{Arg} z)\,(\cos\alpha + i\sin\alpha) = |z|\,([\cos \operatorname{Arg} z \cos\alpha - \sin \operatorname{Arg} z \sin\alpha] + i\,[\sin \operatorname{Arg} z \cos\alpha + \cos \operatorname{Arg} z \sin\alpha]) = |z|\,(\cos \operatorname{Arg}(z+\alpha) + i \sin(\operatorname{Arg} z + \alpha))$.

To znači da je $|z\,e^{i\alpha}| = |z|$, $\operatorname{Arg}|z\,e^{i\alpha}| = \operatorname{Arg} z + \alpha$, dakle zaista produkt $z\,e^{i\alpha}$ nastaje rotirajući z oko O za α.

16.4. Teorem. ***Modul produkta dvaju brojeva jednak je produktu modulâ tih brojeva:*** $|z\,z'| = |z| \cdot |z'|$.

Argument produkta $z\,z'$ jest suma argumenata faktora:

$$\operatorname{Arg} z\,z' = \operatorname{Arg} z + \operatorname{Arg} z'.$$

Ukratko $$z\,z' = |z| \cdot |z'|\,e^{i(\operatorname{Arg} z + \operatorname{Arg} z')}.$$

Ili još općenitije:

Za konačan niz $z_1, z, \ldots, z_n$ kompleksnih brojeva imamo ove dvije formule

$$|z_1 \cdot z_2 \cdot \ldots \cdot z_n| = |z_1| \cdot |z_2| \cdot \ldots \cdot |z_n|$$

$$\operatorname{Arg}(z_1\,z_2 \cdot \ldots \cdot z_n) = \operatorname{Arg} z_1 + \ldots + \operatorname{Arg} z_n.$$

Ili kraće:

$$\Big|\prod_{k=1}^{n} z_k\Big| = \prod_{k=1}^{n} |z_k|$$

$$\operatorname{Arg}\prod_{k=1}^{n} z_k = \sum_{k=1}^{n} \operatorname{Arg} z_k, \quad \textit{odnosno}$$

$$\prod_{k} z_k = \prod_{k} |z_k| \cdot \Big(\cos \sum_{k=1}^{n} \operatorname{Arg} z_k + i \sin \sum_{k=1}^{n} \operatorname{Arg} z_k\Big), \quad \textit{tj.}$$

$$\prod_{k=1}^{n} z_k = \prod |z_k| \cdot e^{i \sum_{k=1}^{n} \operatorname{Arg} z_k}.$$

Dokažimo gornje formule za slučaj da imamo dva faktora z, z'; nadalje se zaključuje da isti obrasci vrijede za 3 faktora, pa 4 faktora, itd.

$$\text{No, } z\,z' = |z|(\cos \operatorname{Arg} z + i \sin \operatorname{Arg} z)\,|z'|(\operatorname{Arg} z' + i \sin \operatorname{Arg} z') =$$
$$= |z|\,|z'|[(\cos \operatorname{Arg} z \cos \operatorname{Arg} z' - \sin \operatorname{Arg} z \sin \operatorname{Arg} z') +$$
$$+ i(\sin \operatorname{Arg} z \cos \operatorname{Arg} z' + \cos \operatorname{Arg} z \sin \operatorname{Arg} z')] =$$
$$= (\text{po adicionom teoremu za cos i sin}) =$$
$$|z|\,|z'|(\cos(\operatorname{Arg} z + \operatorname{Arg} z') + i \sin(\operatorname{Arg} z + \operatorname{Arg} z'). \text{ Dakle:}$$
$$z\,z' = |z|\,|z'|(\cos(\operatorname{Arg} z + \operatorname{Arg} z') + i \sin(\operatorname{Arg} z + \sin \operatorname{Arg} z')).$$

Odatle se vidi da su *polarne* koordinate produkta $z\,z'$ veličine $|z| \cdot |z'|$, $\operatorname{Arg} z + \operatorname{Arg} z'$. A to se i tvrdi!

16.5. Teorem. ***Za svaki kompleksni broj z i svaki cio broj n vrijedi:***

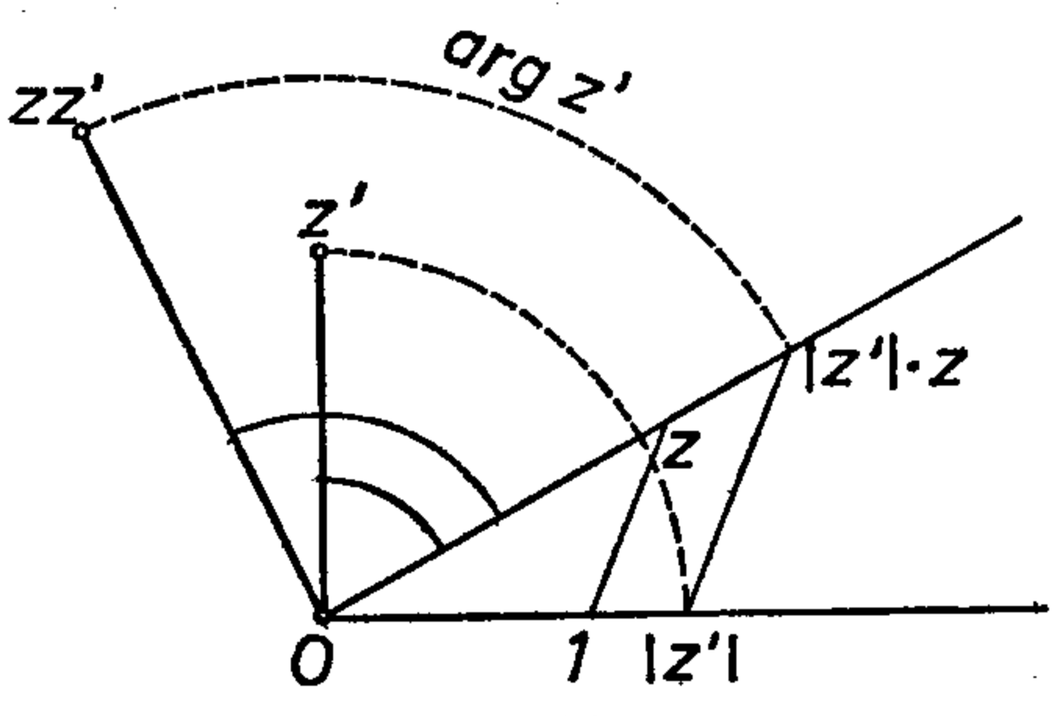
$$z^n = |z^n|\,(\cos n \operatorname{Arg} z + i \sin \operatorname{Arg} z), \text{ dakle:}$$
$$|z^n| = |z|^n, \ \operatorname{Arg} z^n = n \operatorname{Arg} z; \text{ specijalno je}$$
$$(M) \qquad (\cos \varphi + i \sin \varphi)^n = \cos n\varphi + i \sin n\varphi$$
$$(\cos \varphi - i \sin \varphi)^n = \cos n\varphi - i \sin \varphi$$

za svaki realan broj φ ***i svako cijelo n*** (Moivreov teorem)[1].

Teorem je specijalan slučaj rezultata u t. 16.4.: dovoljno je staviti $z_k = z$ za $k = 1, 2, \ldots, n$. Posljednja formula u teoremu dobije se iz pretposlednje pišući $-\varphi$ umjesto φ i imajući na umu da je

$$\cos -\varphi\, n = \cos \varphi\, n, \ \sin -\varphi\, n = -\sin \varphi\, n.$$

Formula (M) je značajna jer povezuje brojeve $\cos \varphi$, $\sin \varphi$, $\cos n\varphi$, $\sin n\varphi$.



Sl. 4.6.16.6.

16.6. Geometrijska konstrukcija produkta $z\,z'$**:** rastegni $\Delta O\,1\,z$ u omjeru, $|z'| : 1$; rotiraj z' u $|z'|$ pa kroz $|z'|$ povuci $\parallel 1\,z$; dobiveni $\Delta O\,|z'|$ $(z\,|z'|)$ rotiraj oko O za $\operatorname{Arg} z'$; izlazi $\Delta O\,z'$ $(z\,z')$ sa željenim vrhom $z\,z'$.

16.7. Recipročna vrijednost. Ako je $z \neq O$, tada se *recipročna vrijednost* z^{-1} definira relacijom $z \cdot z^{-1} = 1$. Odatle proizlazi $|z \cdot z^{-1}| = 1$ i $\operatorname{Arg} z\,z^{-1} = \operatorname{Arg} 1 = 0$. Dalje, na osnovu § 16.4, prelaze te dvije jednakosti u ove dvije: $|z|\,|z^{-1}| = 1$, $\operatorname{Arg} z + \operatorname{Arg} z^{-1} = 0$; dakle je

$$|z^{-1}| = |z|^{-1}, \ \operatorname{Arg} z^{-1} = -\operatorname{Arg} z.$$

---

[1]) A. de Moivre [Moavr] (1667—1754); formula je nađena oko god. 1707; definitivni oblik potječe 1748. od Eulera; Euler je pokazao da formula vrijedi za kakve god realne eksponente n.

Na osnovu te dvije jednakosti konstruira se z^{-1} ovako (imajući na umu da konjugirano $\overline{z}$ ima argument $= -\operatorname{Arg} z$): tačke z, $|z|$, $\overline{z}$ su na istoj kružnici oko O; z^{-1}, $\overline{z}$ su na istoj zraci iz O; $\overline{z}$ je simetrična slika od z prema x-osi; nađi $\overline{z}/|z|$ kao sjecište zrake $O\overline{z}$ i jedinične kružnice; z^{-1} je sjecište zrake $O\overline{z}$ i paralele kroz 1 sa spojnicom $|z|$, $\dfrac{\overline{z}}{|z|}$.

Još je bolja ova konstrukcija: nađi $|z|$ kao sjecište x-osi i kružnice oko O kroz z; ako $|z|>0$, nađi $|z|^{-1}$ kao x-projekciju dirališta tangente iz $|z|$ na jediničnu kružnicu; kružnica oko O kroz $|z|^{-1}$ siječe zraku $O|\overline{z}|$ u z^{-1}. Zaključi odatle kako se nalazi z^{-1} pri $0<|z|<1$.

16.8. Teorem. *Modul kvocijenta dvaju brojeva jednak je kvocijentu modula tih brojeva:*

$$\left|\frac{z'}{z}\right| = \frac{|z'|}{|z|}.$$

Argument kvocijenta dvaju brojeva jednak je razlici argumenta dividenda i argumenta divizora:

$$\operatorname{Arg}\frac{z'}{z} = \operatorname{Arg} z' - \operatorname{Arg} z.$$

Ukratko:

$$z' : z = \frac{|z'|}{|z|}\, e^{i(\operatorname{Arg} z' - \operatorname{Arg} z)}.$$

Dokaz izvire iz odgovarajućeg teorema za produkt dvaju brojeva.

17. ZAVISNOST $\cos n\varphi$ OD $\cos\varphi$, $\sin\varphi$

Pođimo od Moivreove formule:

$$(M) \qquad (\cos\varphi + i\sin\varphi)^n = \cos n\varphi + i\sin n\varphi.$$

Razvijmo lijevu stranu po Newtonovu binomskom stavku, tako dobivenu lijevu stranu sredimo odjeljujući realni dio od čisto imaginarnog dijela držeći se pravila da je niz i^k $(k=0, 1, 2, \ldots)$ čisto periodičan: s periodom 1, i, -1, $-i$; time (M) postaje:

$$\sum_{k=0}^{n}(-1)^k\binom{n}{2k}\cos^{n-2k}\varphi\sin^{2k}\varphi + i\sum(-1)^k\binom{n}{2k-1}\cos^{n-2k-1}\varphi\sin^{2k+1}\varphi =$$

$$= \cos n\varphi + i\sin n\varphi.$$

Ta *kompleksna jednakost* ravnopravna je s ove dvije jednakosti:

17.1. Teorem.

$$\cos n\varphi = \sum_{2k=0}^{\leqslant n} (-1)^k \binom{n}{2k} \cos^{n-2k}\varphi \sin^{2k}\varphi$$

$$\sin n\varphi = \sum_{2k=0}^{\leqslant n} (-1)^k \binom{n}{2k+1} \cos^{n-2k-1}\varphi \sin^{2k+1}\varphi;$$

pri tome je n bilo koji prirodni broj.

Tim se formulama $\cos n\varphi$, $\sin n\varphi$ prikazuju kao *homogene* funkcije stupnja n veličinâ $\cos\varphi$, $\sin\varphi$.

Tako npr. za $n=2$ i $n=3$ gornje formule daju ove homogene funkcije od $\cos\varphi$, $\sin\varphi$:

$$\cos 2\varphi = \cos^2\varphi - \sin^2\varphi, \quad \sin 2\varphi = 2\sin\varphi\cos\varphi$$

$$\cos 3\varphi = \cos^3\varphi - 3\cos\varphi\sin^2\varphi, \quad \sin 3\varphi = 3\cos^2\varphi\sin\varphi - \sin^3\varphi.$$

Formula za $\cos n\varphi$ kazuje da zbog $\sin^2\varphi = 1-\cos^2\varphi$ izraz $\cos n\varphi$ jest polinom n-tog stupnja od $\cos\varphi$, tj. $\cos n\varphi = P_n(\cos\varphi)$; P_n se zove *polinom Čebiševa* (isp. pogl. 7. § 12.8.6.).

18. ZATVORENI IZRAZI ZA $\sum \cos \dot{n}\varphi$, $\sum \sin \dot{n}\varphi$
(tu $\dot{n}$ prolazi $0, 1, \ldots, n-1$)

Polazimo od obrasca $\sum z^{\dot{n}} = \dfrac{z^n-1}{z-1}$ za $z \neq 1$. Stavimo tu specijalno $z = \cos\varphi + i\sin\varphi$ i primijenimo formulu (M); izlazi:

$$\sum(\cos\dot{n}\varphi + i\sin\dot{n}\varphi) = \frac{(\cos n\varphi + i\sin n\varphi)-1}{(\cos\varphi + i\sin\varphi)-1};$$

ovaj razlomak zbog $\cos n\varphi - 1 = -2\sin^2\dfrac{n\varphi}{2}$, $\sin n\varphi = 2\sin\dfrac{n\varphi}{2}\cos\dfrac{n\varphi}{2}$ postaje dalje

$$= \frac{-2\sin^2\frac{n\varphi}{2} + 2i\sin\frac{n\varphi}{2}\cos\frac{n\varphi}{2}}{-2\sin^2\frac{\varphi}{2} + 2i\sin\frac{\varphi}{2}\cos\frac{\varphi}{2}} = \frac{\sin\frac{n\varphi}{2}}{\sin\frac{\varphi}{2}} \cdot \frac{-\sin\frac{n\varphi}{2} + i\cos\frac{n\varphi}{2}}{-\sin\frac{\varphi}{2} + i\cos\frac{\varphi}{2}} =$$

$$= \frac{\sin\frac{n\varphi}{2}}{\sin\frac{\varphi}{2}} \cdot \frac{\left(-\sin\frac{n\varphi}{2} + i\cos\frac{n\varphi}{2}\right)\left(-\sin\frac{\varphi}{2} - i\cos\frac{\varphi}{2}\right)}{\left(-\sin\frac{\varphi}{2} + i\cos\frac{\varphi}{2}\right)\left(-\sin\frac{\varphi}{2} - i\cos\frac{\varphi}{2}\right)} =$$

$$= \frac{\sin n\frac{\varphi}{2}}{\sin\frac{\varphi}{2}}\left(\cos\frac{n-1}{2}\varphi + i\sin\frac{n-1}{2}\varphi\right).$$

Dakle:

$$\sum(\cos \dot{n}\varphi + i \sin \dot{n}\varphi) = \frac{\sin \frac{n\varphi}{2}}{\sin \frac{\varphi}{2}} \left(\cos \frac{n-1}{2}\varphi + i \sin \frac{n-1}{2}\varphi\right).$$

Ta jednakost u kompleksnom području znači da je na snazi:

18.1. Teorem.

$$\sum_{\dot{n}} \cos \dot{n}\varphi = \frac{\sin \frac{n\varphi}{2}}{\sin \frac{\varphi}{2}} \cos \frac{n-1}{2}\varphi$$

$$\sum_{\dot{n}} \sin \dot{n}\varphi = \frac{\sin \frac{n\varphi}{2}}{\sin \frac{\varphi}{2}} \sin \frac{n-1}{2}\varphi, \quad (\dot{n} = 0, 1, \ldots, n-1).$$

Izvođenje teorema 18.1, kao i 17.1, poučan je primjer kako se *upotrebom kompleksnih brojeva dolazi na jednostavan način do raznih formula među realnim* veličinama.

19. KORJENOVANJE

19.1. Definicija. Neka je n prirodan broj. Naći *n-ti korijen* broja a znači naći *svaki* broj z za koji je

(1) $z^n = a$; *svaki* takav broj z označujemo sa

(2) $$\sqrt[n]{a} \text{ ili } a^{\frac{1}{n}}.$$

Skup svih brojeva z za koje vrijedi (1) označujemo sa $\{a^{\frac{1}{n}}\}$. Naravno:

$$\{a^{1/n}\}^n = \{a\}.$$

Definicija. Onaj broj z iz skupa $\{a^{1/n}\}$ kojemu je argument *najmanji* broj iz poluzatvorenog intervala $[0, 2\pi)$ označujemo sa

$$+a^{1/n} \text{ ili } +\sqrt[n]{a} \text{ (znak } + \text{ čitaj plus, a ne „pozitivno“).}$$

Npr. $9^{1/2} = 3, \ -3; \ +9^{1/2} = 3, \ \{9^{1/2}\} = \{3, \ -3\}.$

Neka je

(3) $$a = |a|(\cos \operatorname{Arg} a + i \sin \operatorname{Arg} a)$$

trigonometrijski oblik zadanog broja a; isto tako neka je traženi broj:

$$z = r(\cos\varphi + i\sin\varphi),\ r \geqslant 0. \tag{4}$$

Najprije, prema Moivreovu obrascu, jasno je da je *svaki* broj oblika

$$+|a|^{\frac{1}{n}}\left(\cos\frac{\operatorname{Arg} a}{n} + i\sin\frac{\operatorname{Arg} a}{n}\right) \tag{4'}$$

jedno rješenje jednadžbe (1). Pri tome je *bitno da imamo na umu* ***mnogoznačnost*** *funkcije* $\operatorname{Arg} z$. Jedino još treba da se ispita *koliko ima različitih brojeva oblika* (4'). No, $\operatorname{Arg} a = \arg a + 2\pi\dot{D}$; dakle je:

$$\frac{\operatorname{Arg} a}{n} = \frac{\arg a}{n} + \frac{2\pi}{n}\dot{D}. \tag{5}$$

Tu $\dot{D}$ prolazi $0, \pm 1, \pm 2, \ldots$; posebno, vrijednosti $\dot{D} = \dot{n} = 0, 1, 2, \ldots, n-1$ određuju pripadnih n brojeva (5), a time i n *različitih* zraka oko 0; tih n zraka siječe kružnicu $|z| = +|a|^{\frac{1}{n}}$ u n vrhova *pravilna n-terokuta* u kojemu su smješteni brojevi $+|a|^{1/n}\cdot e^{i\left(\frac{\arg a}{n}+\frac{2\pi}{n}\dot{n}\right)}$, tj. brojevi:

$$+|a|^{1/n}\cdot\left[\cos\left(\frac{\arg a}{n}+\frac{2\pi}{n}\dot{n}\right)+i\sin\left(\frac{\arg a}{n}+\frac{2\pi}{n}\dot{n}\right)\right]. \tag{6}$$

Tih n različitih brojeva (6) *upravo su sva tražena rješenja* jednadžbe (1).

Stavimo li $+a^{1/n} = +|a|^{1/n}\cdot e^{i\frac{\arg a}{n}}$, postaju brojevi (6) oblika $+a^{1/n}\cdot e^{i\frac{2\pi\dot{n}}{n}}$; to znači da oni nastaju iz $+a^{1/n}$ rotiranjem oko O za kut veličine $\frac{2\pi}{n}\dot{n}$.

Time smo dokazali ovaj elegantni izraz:

⟶ **19.2. Teorem. (Moivre 1737).** ***Za svaki kompleksni broj*** $a \neq 0$ ***i svaki prirodni broj*** n ***ima jednadžba*** $z^n = a$ ***upravo ovih*** n ***brojeva kao svoja rješenja:*** $a^{1/n} = +a^{1/n}\cdot e^{i\frac{2\pi}{n}\dot{n}}$ ***(kao obično,*** $\dot{n}$ ***znači brojeve*** $0, 1, 2, \ldots, n-1$***); sva ta rješenja izlaze rotiranjem oko*** O ***broja*** $+a^{1/n} = +|a|^{1/n}\cdot e^{i\frac{\arg a}{n}}$ ***za kut*** $\frac{2\pi}{n}\dot{n}$***. Jednadžba*** $z^n = 0$ ***ima jedno jedino rješenje, i to broj*** 0 ***(no to je rješenje „n-struko“).***

Tako npr. jednadžba $z^4 = 1$ ima ova rješenja (tu je $a = 1$, $|a| = 1$, $\arg a = 0$):

$\cos\frac{2\pi}{4}\dot{4} + i\sin\frac{2\pi}{4}\cdot\dot{4}$; stavljajući tu po redu $\dot{4} = 0, 1, 2, 3$, dobivamo brojeve

$$1,\ i,\ -1,\ -i$$

kao sva rješenja zadane jednadžbe.

Drugim riječima:

$$\{1^{1/4}\} = \{1,\ i,\ -1,\ -i\}.$$

Analogno se dokazuje da je

$$\{1^{1/3}\} = \left\{1,\ -\frac{1}{2} + \frac{i}{2}\sqrt{3},\ -\frac{1}{2} - \frac{i}{2}\sqrt{3}\right\}.$$

20. PRIRODNA EKSPONENCIJALNA FUNKCIJA e^z

D e f i n i c i j a. Za *svaki par* realnih brojeva x, y stavlja se $e^{x+iy} = e^x e^{iy} = e^x(\cos y + i \sin y)$.

Time je e^z definirano za *svako* kompleksno z.

Ako se tu y promijeni za cio kratnik $k \cdot 2\pi$ broja 2π, broj e^z se ne mijenja tj. $e^{z+ik2\pi} = e^z$; to znači da je broj $2\pi i$ *perioda* funkcije e^z.

21. PRIRODNI LOGARITAM

Za svaki broj a definira se prirodni logaritam broja a kao rješenje jednadžbe $e^z = a$; označuje se sa $\operatorname{Ln} a$ (logaritam naturalis); dakle po definiciji $e^{\operatorname{Ln} a} = a$; definira se *glavna vrijednost* $\ln a := +\operatorname{Ln} a$, tj. kao ono $\operatorname{Ln} a$ kojemu je argument u $[0,\ 2\pi)$.

Iz osnovne jednakosti $a = |a| e^{i \operatorname{Arg} a}$ za $a \neq 0$ zaključujemo da je

$$\operatorname{Ln} a = \ln |a| + i \operatorname{Arg} a.$$

Odatle vidimo da, poput $\operatorname{Arg} a$, također $\operatorname{Ln} a$ ima beskonačno mnogo vrijednosti. Tako npr. za svaki realni broj $x > 0$ imamo $|x| = x$, $\operatorname{Arg} x = 2\pi \dot{D}$, pa je zato $\operatorname{Ln} x = \ln x + i \cdot 2\pi \dot{D}$; npr.

$$\operatorname{Ln} 1 = 0 + i \cdot 2\pi \dot{D}, \text{ tj. } \operatorname{Ln} 1$$

je ne samo 0 nego i *svaki* od čisto imaginarnih brojeva

$$\pm 2\pi i,\ \pm 4\pi i,\ \pm 6\pi i, \ldots$$

Isto tako može se provjeriti da je

$$\operatorname{Ln}(3 + 4i) = \ln 5 + i \operatorname{Arg}(3 + 4i),$$

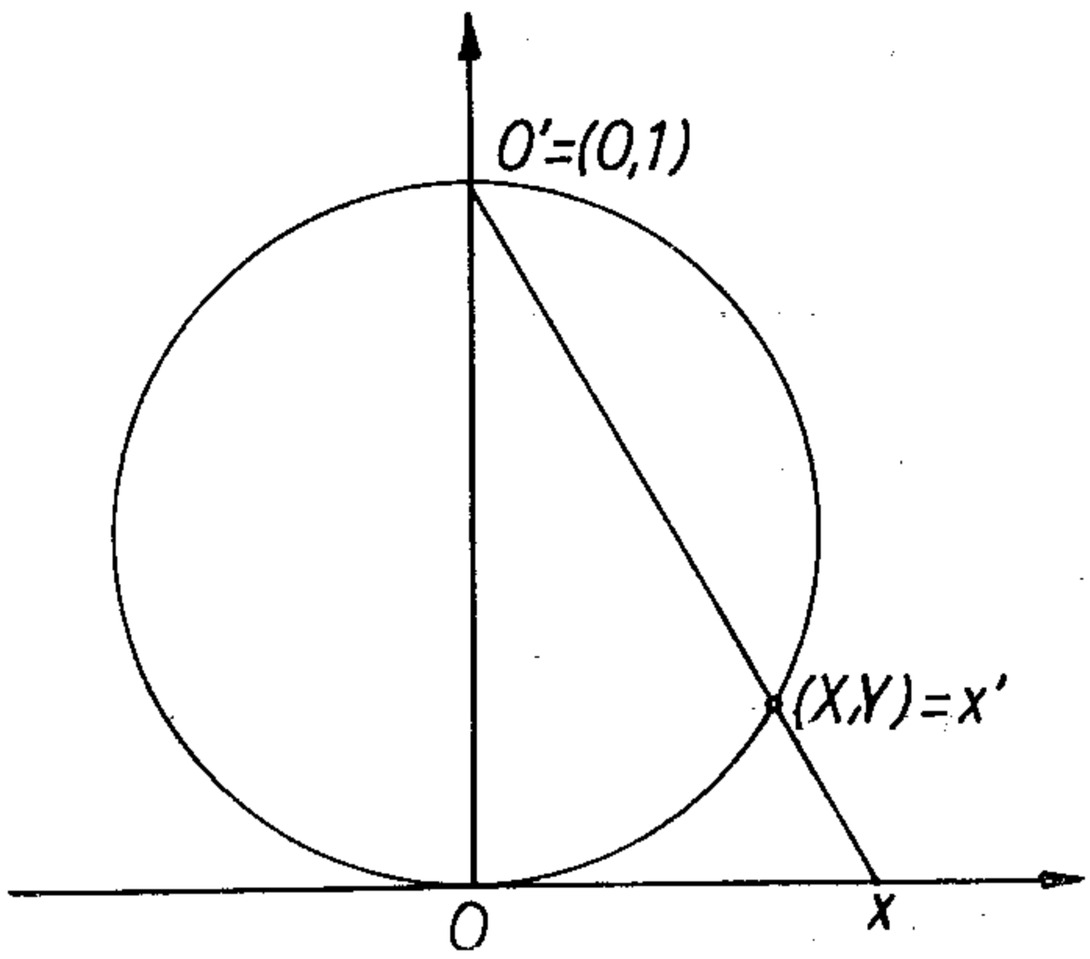
pri čemu je $$\arg(3 + 4i) = 53^\circ\, 7'\, 47''.$$

22. OPĆA POTENCIJA. OPĆA EKSPONENCIJALNA FUNKCIJA

Definiramo $a^b = e^{b \operatorname{Ln} a}$ *za bilo kakve brojeve* a, b, *pri čemu je* $a \neq 0$; *stavlja se* $0^b = 0$ *za svako* $b > 0$.

23. STEREOGRAFSKA PROJEKCIJA. BROJEVNA LOPTA

23.1. Broju x možemo pridijeliti tačku $x' = (X, Y)$ na kružnici $X^2 + (Y-0{,}5)^2 = 0{,}5^2$ tako da tačke x, x', (0, 1) budu na istoj pravulji. Time i svakoj tački $x' \neq 0'$ odgovara jedan jedini realni broj x. Takvo preslikavanje (brojevne) pravulje na kružnicu zove se *stereografska projekcija pravulje na kružnicu.*



Sl 4.23.1.

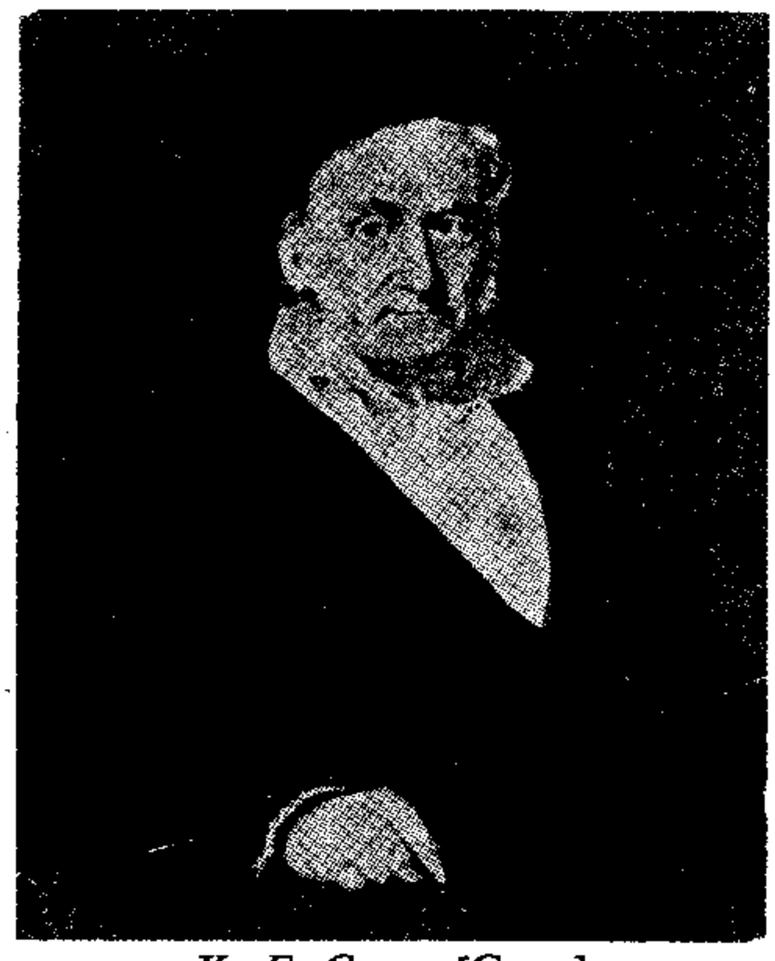
Slično ćemo imati i stereografsku projekciju ravnine na loptu.

23.2. Brojevna lopta.[1]) Radi potpunosti spomenimo da se kompleksni brojevi mogu smjestiti i na loptu (Gauss, 1800). U tu svrhu zamislimo loptu promjera (dijametra) 1 položenu na brojevnu ravninu tako da je dodiruje u polaznoj tački O; ako je O' dijametralno suprotna tačka lopte, tada ćemo svakom kompleksnom broju $z \neq 0$ pridijeliti na lopti tačku z' u kojoj pravulja $O'z$ probada loptu. Takvo preslikavanje brojevne ravnine na loptu zove se *stereografska projekcija ravnine na loptu.*

Zamislimo li da je broj z smješten ne u tački z brojevne ravnine, nego u odgovarajućoj tački z' lopte, *postaje time lopta spremištem svih kompleksnih brojeva: svaki kompleksni broj ima posve određen položaj na površini kugle tj. na lopti;* i obrnuto: *svaka tačka na kuglinoj površini izuzev jedino pol O' — određeno je mjesto jednog jedinog kompleksnog broja.* Radi potpunosti se kaže da je sam pol O' *sijelo beskonačnosti.*

Od interesa je činjenica da se pri *stereografskom preslikavanju veličina kutova u ravnini ne mijenja; također kružnicama*[2]) *u brojevnoj ravnini odgovaraju kružnice na lopti i obrnuto.*

U teoriji kompleksnih funkcija — važnoj matematičkoj grani — pobliže se ispituje narav stereografske projekcije, a posebno kako se *ona vlada prema pojedinim računskim operacijama.*


K. F. Gauss [Gaus]
(30. 4. 1777 — 23. 02. 1855.),
veliki njemački matematičar.

23.3. Nađimo *analitičku vezu* između tačaka $z = x + iy$ i z'; odaberimo u prostoru koordinatni sistem s osima X, Y, Z time da

[1]) Lopta omeđuje kuglu; lopta je skup od dvije dimenzije a kugla je skup od 3 dimenzije. Veza *lopta* ↔ *kugla* odgovara vezi *kružnica* ↔ *krug*.

[2]) Naravno, pravulje smatramo „specijalnim" kružnicama — kružnicama kojima je radijus beskonačan.

osima x i y dodamo još os $\overrightarrow{O\,O'}$ kao Z-os; neka tačka z' nosi ime (X, Y, Z) u tom sistemu. Tada središte lopte glasi $(0, 0, 1/2)$ pa je jednadžba lopte $X^2+Y^2+(Z-1/2)^2=1/4$. Međutim, činjenica da tačke $z=(x, y, 0)$, $z'=(X, Y, Z)$ i $O'=(0, 0, 1)$ leže na *istoj pravulji* izražava se jednadžbama:

$$\frac{X-0}{x-0}=\frac{Y-1}{0-1}=\frac{Z-1}{0-1}.$$ Odatle: $x=\frac{X}{1-Z}$, $y=\frac{Y}{1-Z}$, dakle:

$$z=x+iy=\frac{X+iY}{1-Z}, \quad \text{tj.} \quad x=\frac{X}{1-Z}, \quad y=\frac{Y}{1-Z}. \tag{1}$$

Time smo zadanoj tački $z'=(X, Y, Z)$ sa brojevne lopte odredili pripadni broj $z=x+iy$ *u brojevnoj ravnini.*

Sad ćemo obrnuto: *izraziti z' pomoću z.* No,

$$|z|^2=x^2+y^2=\frac{X^2+Y^2}{(1-Z)^2}=\frac{\frac{1}{4}-(Z-1/2)^2}{(1-Z)^2}=\frac{Z(1-Z)}{(1-Z)^2}=\frac{Z}{1-Z}.$$

Dakle: $x^2+y^2=\frac{Z}{1-Z}$; odatle:

$$Z=\frac{x^2+y^2}{x^2+y^2+1}. \tag{2}$$

Uvrstimo taj izraz za Z u (1); najprije je

$$1-Z=\frac{1}{x^2+y^2+1}.$$

pa (1) postaje:

$$x+iy=X(x^2+y^2+1)+iY(x^2+y^2+1). \tag{3}$$

Formulama (2) i (3) izražava se z' pomoću z, pa u konačnom obliku imamo:

$$X=\frac{x}{x^2+y^2+1}, \quad Y=\frac{y}{x^2+y^2+1}, \quad Z=\frac{x^2+y^2}{x^2+y^2+1}. \tag{4}$$

Formule (1) i (4) pokazuju da se veličine x, y izražavaju pomoću X, Y, Z na racionalan način (tj. pomoću racionalnih funkcijâ), kao i obrnuto: X, Y, Z *izražavaju se pomoću x, y na racionalan način.* Tako imamo primjer *»biracionalnih« transformacija.*

24. ZADACI O BROJEVIMA I RAČUNSKIM OPERACIJAMA

1. U koju vrstu brojeva (prirodni, cijeli, racionalni, iracionalni, realni, kompleksni, čisto imaginarni) spadaju brojevi: 0) 0; 1) 5; 2) -5; 3) $+5^{1/2}$; 4) $5^{1/2}$; 5) $2i$; 6) $3+4i$; 7) $\pi+ie$; 8) i^2; 9) $(1+i)^2$; 10) $(3+4i)\cdot(3-4i)$; 11) $0{,}2\,4\,24\,24\ldots$; 12) $0{,}7\,9\,(3\,4\,5\,4)$;
13) $0{,}0\,2\,4\,0\,0\,2\,4\,0\,0\,0\,2\,4\,0\,0\,0\,0\,2\,4\,0\ldots$?

2. Napiši po dva broja od svake navedene vrste brojeva.

3. Uredi brojeve: $5,\ -4i+1,\ (3+i)^2,\ 10-5i,\ (3+4i)\cdot(5-i)$.

4. Promatraj brojeve: $a=3+4i,\ b=5-2i$; nađi (računski i po mogućnosti crtnjom): 1) $a+b$; 2) $a-b$; 3) ab; 4) $a:b$; 5) a^2-b^2; 6) $a^{1/2}$; 7) $a^{1/2}+b^{1/3}$; 8) $\overline{a^2}\,b^3$; 9) a^3-b^3; 10) a^b; 11) b^a; 12) 1^a; 13) $\overline{ab}+a\overline{b}$; 14) $3\overline{a}-2b+4\overline{ab}$; 15) $\ln a$; 16) $\log_b a$.

5. Dokaži da i za kompleksne brojeve vrijede zakoni udruživanja (asocijacije) i obrtanja (komutacije) za zbrajanje i množenje te zakon raspodjele (distribucije) množenja prema zbrajanju i prema oduzimanju.

6. Odredi polarni oblik ovih brojeva: 1) $5-2i$; 2) $(4+5i)\cdot(2-i)$; 3) $\cos\varphi+i\sin\varphi$; 4) $i^{23}-1$); 5) z^2+3z-1 6) $\dfrac{z+1}{z-1}$; 7) $\dfrac{z-1}{z^2+z+1}$.

7. Nađi stereografsku sliku brojeva iz zadatka 6.

8. Dokaži: $z\neq 1\Rightarrow\left|\dfrac{1}{1-z}\right|\leq\left|\dfrac{1}{1-|z|}\right|$.

9. Promatraj trotačku z_1, z_2, z_3; dokaži da je: $\sphericalangle(0x, z_1z_2)=\arg(z_2-z_1)$, $\sphericalangle(z_2z_1z_3)=\arg\dfrac{z_3-z_1}{z_2-z_1}$; tačke z_1, z_2, z_3 leže na pravulji onda i samo onda ako je $(z_3-z_1)\cdot(z_2-z_1)^{-1}$ realno.

10. $|z_1-z_2|^2+|z_1+z_2|^2=2|z_1|^2+2|z_2|^2$. Dokaz.

11. Što predstavlja jednadžba: 1) $|z-1|=4$; 2) $|z-5+4i|=5$; 3) $\left|\dfrac{z-1}{z+1}\right|=2$; 4) $\left|\dfrac{z-5+2i}{2z-1}\right|=1$; 5) $|z-5|+|z-4|=8$, 6) $\arg(z-5+2i)=\dfrac{\pi}{3}$?

12. Ako je $|z|=1$, gdje leži: 1) $z+5$; 2) $z+5-2i$; 3) $z+6i+5$?

13. Odredi: $z^{1/2},\ z^{1/3},\ z^{1/4}$ za $z=5+6i$.

14. Dokaži: $(1+i)^n=2^{\frac{n}{2}}\left(\cos\dfrac{n\pi}{4}+i\sin\dfrac{n\pi}{4}\right)$.

15. $z+z^{-1}=2\cos\alpha\Rightarrow z^n+z^{-n}=2\cos n\alpha$.

16. $\left(\dfrac{1+i\operatorname{tg}\alpha}{1-i\operatorname{tg}\alpha}\right)^n=\dfrac{1+i\operatorname{tg}n\alpha}{1-i\operatorname{tg}n\alpha}$.

17. Izrazi pomoću $\cos x$, $\sin x$ ove izraze: 1) $\cos 4x$; 2) $\cos 5x$; 3) $\sin 6x$.

18. Izrazi: 1) $\operatorname{tg}3x$; 2) $\operatorname{tg}6x$ pomoću $\operatorname{tg}x$.

19. Izrazi: 1) $\sin^3 x$; 3) $\cos^5 x$; 3) $\cos^6 x$ pomoću kosinusa i sinusa kratnika broja x.

20. Dokaži: $\cos^2 x + \cos^2 2x + \cos^2 3x + \ldots + \cos^2 nx = \frac{2n-1}{4} + \frac{\sin(2n+1)x}{4\sin x}$.

21. Ako je $\left|\sum_{k=1}^{n} z_k\right| = \sum_{k=1}^{n} |z_k|$, onda je $\arg z_k = \text{konst}$; i obrnuto.

22. Promatraj zadanu kružnicu $k\ |z-c|=r$ i jednu njenu tačku z_0 te određenu vrijednost α_0 za $\operatorname{Arg} z_0$; ako se tačka kreće po k u pozitivnom smislu za: 1) $\frac{\pi}{2}$; 2) $\frac{3\pi}{4}$; 3) 6π; 4) -12π; 5) $n\cdot 2\pi$, u koju se tačku z' nailazi i kolika je ona vrijednost broja $\operatorname{Arg} z'$ što na neprekidan način odgovara vrijednosti α_0 za $\operatorname{Arg} z_0$?
Uzmi konkretne slučajeve: $c=0,\ 1,\ i,\ 1+2i$.

23. Odredi sve tačke z za koje je: 1) $|z|\leq 1$; 2) $\operatorname{Re} z\leq 1$; 3) $-1<\operatorname{Re} z<1$; 4) $-1<\operatorname{Im} z<1$; 5) $-1<\arg z<1$; 6) $\operatorname{Im} z\leq 1$; 7) $|z^2|\leq 1$; 8) $\operatorname{Re} z^2=1$; 9) $\operatorname{Im} z^2=1$; 10) $\operatorname{Re} e^z=1$; 11) $\operatorname{Im} e^z=1$; 12) $|e^z|=1$, 13) $\left|\frac{z-1}{z+1}\right|=a$ te $\arg\frac{z-1}{z+1}=b$ su kružnice koje su međusobno okomite (a, b su proizvoljni realni brojevi; $a>0$).

24. 1) Ako je $|z|\leq 1 \wedge |\alpha|<1$, onda je $\left|\frac{z-\alpha}{1-z\bar{\alpha}}\right|\leq 1$;

2) Ako je $|z|\leq 1 \wedge |\alpha|>1$, onda je $\left|\frac{z-\alpha}{1-z\bar{\alpha}}\right|\geq 1$. Što to znači geometrijski?

25. Zadan je kompleksni broj $z_0=x_0+iy_0$ i realan broj $r>0$;
1) što znači skup svih z za koje je $|z-z_0|=r$?

2) nađi $z'=z_0+\frac{r^2}{\bar{z}-\bar{z}_0}$ za zadano z i dokaži da je $|z'|'=z$ te da su tačke z, z' položeno simetrično prema kružnici $k(z_0, r)$.

26. Za zadane tačke z_1, z_2 i realan broj λ odredi tačku $\frac{z_1-\lambda z_2}{1-\lambda}$ i dokaži da ona odrezak $z_1\ z_2$ dijeli u omjeru $\lambda:1$.

27. Dokaži pomoću kompleksnih brojeva ovo: 1) srednjice trokuta $z_1\ z_2\ z_3$ dijele se međusobno u omjeru $2:1$ računajući od vrha, i to tačkom $\frac{1}{3}(z_1+z_2+z_3)$; 2) dijagonale paralelograma se raspolavljaju, t.j. jedna drugu raspolavlja; 3) dijagonale u rombu međusobno su okomite.

28. Zadan je 4-člani niz z_0, z_1, z_2, z_3; dvoomjer tog niza definira se prema Möbiusu[1] ovako: $(z_0, z_1, z_2, z_3) = \frac{z_2 - z_0}{z_1 - z_2} : \frac{z_3 - z_0}{z_1 - z_3}$;

1) nađi dvoomjer ovih nizova: $(1, 2, 3, 4)$, $(1, i, -1, -i)$, $(3, 5-2i, 4+2i, -3-2i)$;

2) ako je $z'_i = \frac{a z_i + b}{c z_i + d}$, onda je $(z_0, z_1, z_2, z_3) = (z'_0, z'_1, z'_2, z'_3)$;

3) ako su tačke z_i na istoj kružnici, onda je $\operatorname{Im}(z_0, z_1, z_2, z_3) = 0$, i obrnuto (pri tom i pravac smatramo kružnicom beskonačnog prečnika);

4) dokaži pomoću 2) i 3) da transformacija $z \to \frac{a z + b}{c z + d}$ prevodi kružnicu u kružnicu.

Literatura

Kurepa Đ. [1], Kurepa Sv. [1].

[1] A. Möbius (1790—1868), njem. matematičar.

POGLAVLJE 5.

ALGEBARSKE JEDNADŽBE STUPNJA 1, 2, 3, 4 S JEDNOM NEPOZNANICOM

P r e d g o v o r. Danas nam se čini tako jednostavno kad promatramo jednadžbe stupnja 1, 2, 3, 4. Međutim, čovječanstvu je trebalo mnogo vremena da nađe rješenja tih jednadžba. Rješenja jednadžba stupnja 3, 4 nađena su tek u kasnoj renesansi, u 16. st. u Italiji, nekoliko stoljeća nakon pronalaska rješenja opće kvadratne jednadžbe (poglavito Indija, 8—12. st.). Time je udaren pečat na jednu matematičku metodu, jer, kao što se pokazalo tek početkom 18. st., analogan poduhvat za jednadžbe 5, 6, ... stupnja nije moguć: rješenja algebarskih jednadžbi stupnja >4 ne mogu se lako izraziti pomoću koeficijenata kao što je to moguće za jednadžbe stupnja <5. Potrebne su nove metode, nova sredstva i nova shvatanja (upletanje teorije funkcija, teorije grupa i sl.).

1. LINEARNE JEDNADŽBE

Linearna jednadžba s nepoznanicom x je oblika:

$$ax+b=0, \quad a\neq 0; \tag{1}$$

pri tom se x ne pojavljuje u a i b; »*koeficijenti*« a i b ne zavise od x.

»*Separirani*« (*odvojeni*) oblik jednadžbe (1) glasi:

$$ax=-b; \tag{2}$$

tu je *poznata strana* $-b$ odvojena od preostalog dijela jednadžbe (1). »*Normiramo*« li jednadžbu (1) ili (2), tj. prevedemo li je u oblik u kojem je koeficijent nepoznanice $=1$, dobijemo jednadžbu:

$$x+a^{-1}b=0, \quad \text{odnosno} \quad x=-a^{-1}b.$$

Tu se odmah vidi i *rješenje* $-a^{-1}b$ zadane jednadžbe.

To je tako ako su koeficijenti a, b zadani brojevi (npr. racionalni brojevi, realni brojevi, kompleksni brojevi, brojevi oblika $u+v\cdot\sqrt{2}$, gdje su u, v racionalni brojevi, itd.). Stvar je vrlo laka! Međutim, dobar dio ove knjige govorit će o linearnoj jednadžbi s 1 nepoznatom, ali uz pretpostavku da koeficijenti

a, b, (a zato općenito ni x) više nisu brojevi u navedenom smislu nego npr. „matrice“ ili kakvi drugi predmeti uzeti iz jedne cjeline u kojoj znamo vršiti bar 3 računske operacije.

Zato neka čitaoca ne smeta ako ponekad spomenemo da koeficijente jednadžbe uzimamo npr. u „tijelu“ racionalnih brojeva, u tijelu kompleksnih brojeva itd. Time hoćemo automatski naglasiti da se postavlja pitanje: šta će biti s jednadžbom i s pripadnim rješenjima kad se odlučimo za izbor koeficijenata u kakvoj drugoj „oblasti“, kolu, tijelu itd.

2. KVADRATNE JEDNADŽBE S JEDNOM NEPOZNANICOM

2.0. Oblik. Kvadratna jednadžba ima oblik:

$$ax^2+bx+c=0, \quad a\neq 0. \tag{1}$$

Pri tom se x ne pojavljuje ni u jednom od koeficijenata a, b, c. Koeficijent a uz najvišu potenciju x^2 nepoznanice zove se *najstariji* ili *vodeći* koeficijent. On je $\neq 0$, jer bi inače stupanj jednadžbe bio <2, a ne 2.

Da se lakše sagleda položaj koeficijenta, zgodno mu je dati indeks, i to isti indeks koji se pojavljuje u eksponentu nepoznate veličine x. Na taj bi način bilo $a=a_2$, $b=a_1$, $c=a_0$, pa bi jednadžba (1) glasila:

$$a_2 x^2+a_1 x+a_0=0, \text{ ili redajući uzlazno:} \tag{1'}$$

$$a_0+a_1 x+a_2 x^2=0, \quad a_2\neq 0. \tag{1''}$$

Jednadžbu (1) možemo »*normirati*«, tj. prevesti u ekvivalentnu jednadžbu u kojoj će „treći“ koeficijent biti $=1$. Pomnožimo li (1) sa a^{-1}, dobijemo pripadni normirani oblik:

$$x^2+a^{-1}bx+a^{-1}c=0.$$

2.1. Rješenje kvadratne jednadžbe. Prethodnu jednadžbu možemo pisati i ovako:

$$\begin{aligned} &(x+2^{-1}a^{-1}b)^2=2^{-2}a^{-2}b^2-a^{-1}c \\ &\Updownarrow \\ &x+2^{-1}a^{-1}b\ =(2^{-2}a^{-2}b^2-a^{-1}c)^{1/2} \\ &\Updownarrow \\ &x=2^{-1}a^{-1}[-b+(b^2-4ac)^{1/2}]. \end{aligned} \tag{2}$$

Tu se pojavljuje izraz:

$$b^2-4ac, \tag{3}$$

a zove se *diskriminanta kvadratne jednadžbe* (1), odnosno kvadratnog polinoma $(1)_1$, gdje $(1)_1$ označuje *prvu stranu* relacije (1).

2.2. Diskriminanta. Stavimo li

$$D=b^2-4ac, \tag{4}$$

tada jednadžba (2) postaje:

$$x=2^{-1}a^{-1}(-b+D^{1/2}). \tag{5}$$

Ako je $D \neq 0$, tada $D^{1/2}$ ima dvije različite vrijednosti. Ako je još i $D > 0$, tada je $D^{1/2}$ jednako $+D^{1/2}$ i $-D^{1/2}$; pripadne vrijednosti za x glase:

$$x_1 = 2^{-1} a^{-1} [-b + |D^{1/2}|], \quad x_2 = 2^{-1} a^{-1} [-b - |D^{1/2}|]. \tag{6}$$

Ako je $D < 0$, tada $D^{1/2}$ nije realan broj, nego čisto imaginaran broj $\pm |(-D)^{1/2}| i$, pa tražena rješenja izgledaju ovako:

$$x_1 = 2^{-1} a^{-1} [-b + |D|^{1/2} i], \quad x_2 = 2^{-1} a^{-1} [-b - |(-D)^{1/2}| i]. \tag{7}$$

2.3. Viètеove formule. Iz (6) i (7) odmah izlaze ove formule:

$$x_1 + x_2 = -a^{-1} b$$
$$x_1 x_2 = a^{-1} c \text{ (Viètove formule [1]).} \tag{8}$$

Na taj smo način pokazali da rješenja x_1, x_2 kvadratne jednadžbe (1) zadovoljavaju jednadžbama (8). Vrijedi i obrat: iz jednadžba (8) izlazi da x_1 i x_2 zadovoljavaju (1).

Dokažimo npr. da x_2 zadovoljava (1). No, iz prve jednadžbe (8) izlazi:

$$x_1 = -a^{-1} b - x_2,$$

što uneseno u drugu jednadžbu (8) daje jednadžbu:

$$-a^{-1} b x_2 - x_2^2 = a^{-1} c,$$

iz koje odmah izlazi da x_2 zadovoljava (1).

2.4. Posebno (za $a = 1$) imamo ovo:

Ako je $x_1 + x_2 = s, x_1 x_2 = p$, *tada brojevi* x_1, x_2, *zadovoljavaju kvadratnu jednadžbu* $x^2 - sx + p = 0$.

Time smo ujedno riješili zadatak da se iz sume i produkta dvaju brojeva x_1, x_2 odrede i ti sami brojevi x_1, x_2.

2.5. Antikvadriranje kompleksnog broja. Geometrijski znamo naći $z^{1/2}$ ako je z zadano, jer je $arg\, z^{1/2} = 2^{-1}\ arg\, z$ i $|z^{1/2}| = +|z|^{1/2}$ (gl. sliku na str. 112).

Radimo analitički s konkretnim primjerom $z = 3 + 2i$. Rezultat $(3 + 2i)^{1/2}$ će svakako biti kompleksan broj, recimo $x + iy$, gdje su x, y realni brojevi:

$$x + iy = (3 + 2i)^{1/2}$$
$$\Downarrow$$
$$x^2 - y^2 + 2ixy = 3 + 2i$$
$$\Downarrow$$
$$x^2 - y^2 = 3$$
$$2xy = 2 \text{ (eliminacijom } y\text{):}$$
$$\Downarrow$$
$$x^2 - x^{-2} = 3$$
$$(x^2)^2 - 3x^2 - 1 = 0$$

[1] Fr. Viete [Vjet] (1540—1603), francuski matematičar; prijateljevao je s našim matematičarem Marinom Getaldićem (1566—1626).

$$x^2 = \frac{3}{2} \pm \frac{\sqrt{13}}{2}$$

$$x = \pm\left(\frac{3 \pm 13^{1/2}}{2}\right)^{1/2};$$

u zagradi znak $\pm$ može biti samo $+$ jer je x realno; dakle

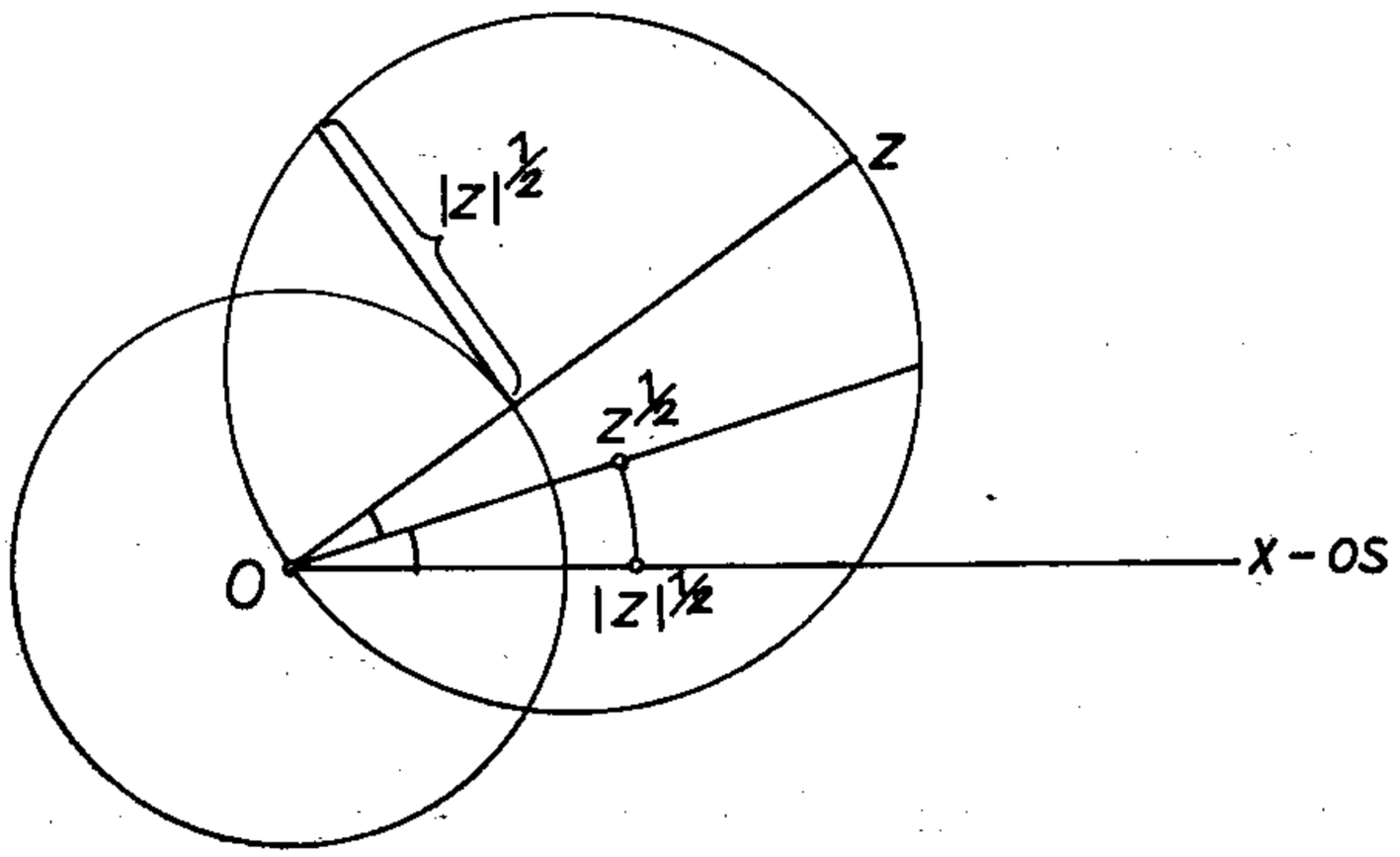
$$x = \pm\left(\frac{3 + 13^{1/2}}{2}\right)^{1/2}.$$

Pripadno y glasi:

$$y = x^{-1} = \pm\left(\frac{2}{3 + 13^{1/2}}\right)^{1/2}.$$

Dakle je najzad:

$$\left(3 + 2i\right)^{1/2} = \pm\left[\left(\frac{3 + 13^{1/2}}{2}\right)^{1/2} + i\left(\frac{3 - 13^{1/2}}{2}\right)^{1/2}\right].$$



Sl. 5.2.5. Gledaj kako se iz z dolazi do $z^{1/2}$

2.6. Trigonometrijsko rješavanje kvadratne jednadžbe. Pođimo od kvadratne jednadžbe s realnim (stvarnim) koeficijentima i realnim rješenjem; možemo je pisati u obliku:

$$ax^2 + bx + c = 0, \quad a > 0, \quad c \neq 0. \tag{1}$$

Naime, ako je $a < 0$, dovoljno je promatrati jednadžbu pomnoženu s -1; slučaj $c = 0$ nije od interesa, jer tada imamo odmah rješenje: to su brojevi 0 i $a^{-1}b$.

P r v i s l u č a j: $c > 0$. Kako je zbog realnosti korijena nužno $b^2 - 4ac \geqq 0$, dakle $b \neq 0$, izlazi odatle

$$1 \geqq b^{-2} \cdot 4ac \geqq 0.$$

Zato možemo staviti

$$b^{-2}\, 4ac = \sin^2 \varphi, \quad 0 < \varphi < \pi/2, \tag{2}$$

pa je

$$x_1 = -2^{-1}\, a^{-1}\, b\,[1 + (1 - b^{-2}\, 4ac)^{1/2}] = -2^{-1}\, a^{-1}\, b\,[1 + \cos\varphi]$$

i odatle:

$$x_1 = -a^{-1}\, b \cos^2 2^{-1}\varphi;$$

slično:

$$x_2 = -a^{-1}\, b \sin^2 2^{-1}\varphi.$$

Iz (2) imamo:

$$(2') \qquad b = \pm 2\,|\,ac\,|^{1/2} \sin^{-1}\varphi = \operatorname{sgn} b \cdot 2\,|\,(ac)^{1/2}\,|\,\sin^{-1}\varphi,$$

jer je

$$2\,|\,(ac)^{1/2}\,|\,\sin\varphi > 0.$$

Zato posljednji izrazi za x_1 i x_2 postaju:

$$(3) \qquad \begin{aligned} x_1 &= -\operatorname{sgn} b \cdot 2\,|\,a^{-1}\, c\,|^{1/2} \operatorname{ctg} 2^{-1}\varphi. \\ x_2 &= -\operatorname{sgn} b \cdot 2\,|\,a^{-1}\, c\,|^{1/2} \operatorname{tg} 2^{-1}\varphi. \end{aligned}$$

Drugi slučaj: $c<0$, dakle $-c>0$. Diskriminanta je

$$D = b^2 - 4ac = b^2\,(1 - 4b^{-2}\, ac).$$

Dakle je $1 - 4b^{-2}\, ac > 0$ pa možemo odrediti broj φ tako da bude:

$$(4) \qquad \operatorname{tg}^2\varphi = -4ab^{-2}\, c, \quad 0 < \varphi < \frac{\pi}{2}.$$

Za rješenja x_1, x_2 jednadžbe (1) imamo:

$$x_{1,2} = -2^{-1}\, a^{-1}\, b\,[1 \pm (1 - 4ab^{-2}\, c)^{1/2}] \quad \text{tj.}$$

$$\begin{aligned} x_{1,2} &= -2^{-1}\, a^{-1}\, b\,[1 \pm (1 + \operatorname{tg}^2\varphi)^{1/2}] = -2^{-1}\, a^{-1}\, b\,(1 \pm \cos^{-1}\varphi) \\ &= -2^{-1}\, a^{-1}\, b\,(\cos^2 2^{-1}\varphi + \sin^2 2^{-1}\varphi \pm [\cos^2 2^{-1}\varphi + \sin^2 2^{-1}\,\varphi])\cos^{-1}\varphi; \end{aligned}$$

odatle (označujući vrijednost prethodnog izraza sa x_1 za $\pm = +$ odnosno x_2 za $\pm = -$):

$$(5) \qquad \begin{aligned} x_1 &= -a^{-1}\, b \cos^{-1}\varphi \cos^2 2^{-1}\varphi; \\ x_2 &= a^{-1}\, b \cos^{-1}\varphi \sin^2 2^{-1}\varphi. \end{aligned}$$

No, (4) daje $b = \operatorname{sgn} b \cdot 2\,|\,(ac)^{1/2}\,|\,\operatorname{tg}^{-1}\varphi$. Uvrsti li se taj izraz u (5), dobije se nakon kraćeg računanja

$$(6) \qquad \begin{aligned} x_1 &= -\operatorname{sgn} b \cdot |\,a^{-1}(-c)\,|^{1/2} \operatorname{ctg}\varphi/2 \\ x_2 &= \operatorname{sgn} b \cdot |\,a^{-1}(-c)\,|^{1/2} \operatorname{tg}\varphi/2, \quad \operatorname{tg}^2\varphi = -4ab^{-2}\, c \quad 0 < \varphi < \pi/2. \end{aligned}$$

Rezimirajući, možemo reći — a to se lako provjeri npr. pomoću Vièteovih formula, da vrijedi:

⟶ **2.6.1.** Teorem. *Jednadžba* $ax^2+bx+c=0$ *uz uslove* $a>0$, $b^2-4ac\geq 0$, $c\neq 0$ zadovoljena je brojevima:

$$x_1 = -\operatorname{sgn} b \cdot |a^{-1/2}|c|^{1/2}| \operatorname{ctg} \varphi/2 \tag{7}$$

$$x_2 = -\operatorname{sgn}(bc) \cdot |a^{-1/2}|c|^{1/2} \operatorname{ctg} \varphi/2;$$

pri tom je broj φ jednoznačno određen iz uslovâ:

$$\sin^2\varphi = 4ab^{-2}c, \quad 0<\varphi<\pi/2 \text{ za slučaj } c>0, \tag{8}$$

$$\operatorname{tg}^2\varphi = 4ab^{-2}|c|, \quad 0<\varphi<\pi/2 \text{ za slučaj } c<0. \tag{8'}$$

Na osnovu (7), (8) i (8′) mogu se brojevi x_1, x_2 lako izračunati služeći se tablicama.

2.6.2. Primjer. $2{,}478\,x^2+25{,}484\,x+1{,}959=0$.

Odredimo li φ po (8), dobije se $\varphi = 9^0\,57'\,25''$.

Formule (7) daju

$$x_1 = -10{,}207; \qquad x_2 = -0{,}07745.$$

Kontrola: $x_1+x_2=-10{,}28445$; $x_1 x_2 = 0{,}79053$.

Prava vrijednost prema Viètеovim formulama treba biti:

$$x_1+x_2 = -a^{-1}b = -10{,}284, \quad x_1 x_2 = a^{-1}c = 0{,}79055.$$

2.6.3. Pišemo li u gornjem primjeru $-1{,}959$ umjesto $1{,}959$ tada ćemo određivati φ po obrascu (8′); izlazi

$$\varphi = 9^0\,48'\,36'' \text{ pa (7) daje } x_1 = -10{,}36; \quad x_2 = 0{,}0763.$$

Kontrola: $x_1+x_2=-10{,}2837$; $x_1 x_2 = -0{,}79053$.

Inače, prema Viètеovim obrascima treba biti

$$x_1+x_2 = -a^{-1}b = -10{,}284; \quad x_1 x_2 = a^{-1}c = -0{,}79055.$$

2.7. Historijat kvadratnih jednadžbi.

1. Sa kvadratnim jednadžbama susreli su se već grčki matematičari. Oni su ih rješavali pomoću geometrijskih konstrukcija ali su izbjegavali slučaj kad su sva tri koeficijenta a, b, c u $ax^2+bx+c=0$ pozitivna; tada naime jednadžba ne može imati pozitivna rješenja — a Grci su dopuštali samo pozitivna rješenja. Specijalno su Euklid (—3. v.), Hiparh (—2. v.) te Heron (—2. v.) i Diofant (3. v.) rješavali kvadratne jednadžbe: prva dvojica konstruktivno, a druga dvojica i računski. U Indiji promatra Brahmagupta (6. v.) i jednadžbe s *negativnim* koeficijentima, iako dopušta samo pozitivna rješenja; tako npr. promatra on jednadžbu $-9=x^2-10x$ (on piše $\dot{9}$ umjesto -9) i to je prvi put da se razlikuje pozitivno od negativnog. Baskara (12. v.) dotjeruje Heronovu metodu nadopunjavanja na kvadrat i rješava kvadratne jednadžbe kao što to radimo i danas (odatle naziv: *indijska metoda*). Baskara daje ovaj recept za

rješavanje jednadžbe $ax^2+bx=c$: „Uzmi broj 4, pomnoži ga s koeficijentom kvadrata nepoznanice, pa s tim produktom pomnoži obje strane jednadžbe; s obje strane dodaj kvadrat koeficijenta nepoznanice, transformiraj, pa ćeš lako naći vrijednost nepoznanice“. Arapin Omar Alkhayami (11. v.) obrađivao je kvadratne jednadžbe i algebarski i geometrijski. Niti Viète (16/17 v.) ne dopušta dvoznačnost rješenja kvadratne jednadžbe, osim kad su oba rješenja pozitivna. Od njega potječe rješavanje jednadžbe $ax^2+bx+c=0$ supstitucijom $x=y+z$. Jednadžba $x^2=-4x-3$ je *prva kvadratna poznata jednadžba* kojoj su oba rješenja naznačena kao negativna: $x_1=-3$, $x_2=-1$ (A. Girard, *Invention nouvelle en algèbre* [Nov pronalazak u algebri], Amsterdam, 1629.). Istom kad je Kardano 1545, u djelu *Ars magna* (Veliko umijeće) obrađivao i negativne i kompleksne brojeve bila je opća kvadratna jednadžba potpuno riješena. No, zbog nepriznavanja negativnih rješenja i rješenja koja nisu realni brojevi, može se reći da je istom na prijelazu 18/19 vijeka svijesno spoznato i priznavano da svaka algebarska jednadžba stupnja 2 kojoj su koeficijenti realni brojevi ima dva (jednaka ili nejednaka) rješenja. To je saznanje stečeno gotovo istodobno kad i odgovarajuće saznanje za jednadžbe stupnja n.

2. Zanimljivo je istaknuti da se u vezi s rješavanjima kvadratnih jednadžaba čine dva bitna proširenja brojeva: proširenje racionalnih brojeva uvođenjem *iracionalnih* brojeva (npr. rješavajući $x^2=2$) te proširenje realnih brojeva uvođenjem čisto imaginarnih i kompleksnih brojeva (npr. rješavajući $x^2=-1$).

3. Prvi pokušaj da se kvadratna jednadžba riješi pomoću trigonometrijskih funkcija potječe od B. Kavalieri-a (Bologna, 1639); opće trigonometrijsko rješenje je prvi dao A. Cagnoli (č. Kanjoli) 1786.

2.8. Zadaci o trigonometrijskom rješavanju kvadratnih jednadžba.

Riješi pomoću trigonometrijskih funkcija:

$1^{\pm}$. $3456\,x^2 \pm 75278\,x + 96548 = 0.$

$2^{\pm}$. $3456\,x^2 \pm 75278\,x - 96548 = 0.$

$3^{\pm}$. $2{,}478\,x^2 + 25{,}484\,x \pm 1{,}959 = 0.$

$4^{\pm}$. $2{,}478\,x^2 - 25{,}484\,x \pm 1{,}959 = 0.$

$5^{\pm}$. $26{,}549\,x^2 + 68{,}735\,x \pm 12{,}783 = 0.$

$6^{\pm}$. $26{,}549\,x^2 - 68{,}735\,x \pm 12{,}783 = 0.$

$7^{\pm}$. $7777\,x^2 + 9999\,x \pm 1111 = 0.$

$8^{\pm}$. $7777\,x^2 - 9999\,x \pm 1111 = 0.$

$9^{\pm}$. $1681907\,x^2 + 30101919\,x \pm 2011950 = 0.$

$10^{\pm}$. $1681907\,x^2 - 30101919\,x \pm 2011950 = 0.$

11. $17\sqrt{111}x^2 + 108\sqrt[3]{18}\,x + 2\sqrt[4]{3} = 0.$

12. $\sqrt[5]{8}\,x^2 + 4\,x - \sqrt[10]{2} = 0.$

3. O POLOŽAJU NULA-TAČAKA KVADRATNOG POLINOMA PREMA ZADANOM INTERVALU BROJEVA

3.0. Služimo se indeksima za označivanje koeficijenata. Na taj način opći oblik kvadratnog polinoma je $a_0 + a_1 x + a_2 x^2$; taj ćemo trinom označivati sa a. Tako npr. ako a označuje trinom

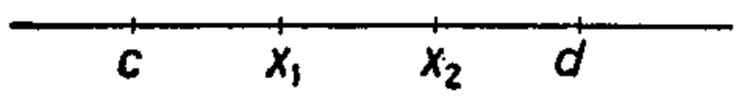
$$5 - 3x^2 + 4x, \quad \text{tada je } a_0 = 5, \quad a_1 = 4 \text{ (ne } -3), \quad a_2 = -3.$$

3.1. Neka su c, d dva realna broja i $c < d$. Neka je

$$a(x) = a_2 x^2 + a_1 x + a_0$$

kvadratni polinom s realnim (stvarnim) koeficijentima, a x_1, x_2 njegove nula-tačke. Nastaje pitanje: *kada će oba broja* x_1, x_2 *pasti u zatvoreni interval* $R[c, d]$ ili u njegovu nutrinu $R(c, d)$, odnosno koliko će nula-tačaka funkcije a pasti u interval $R(c, d)$[1]?

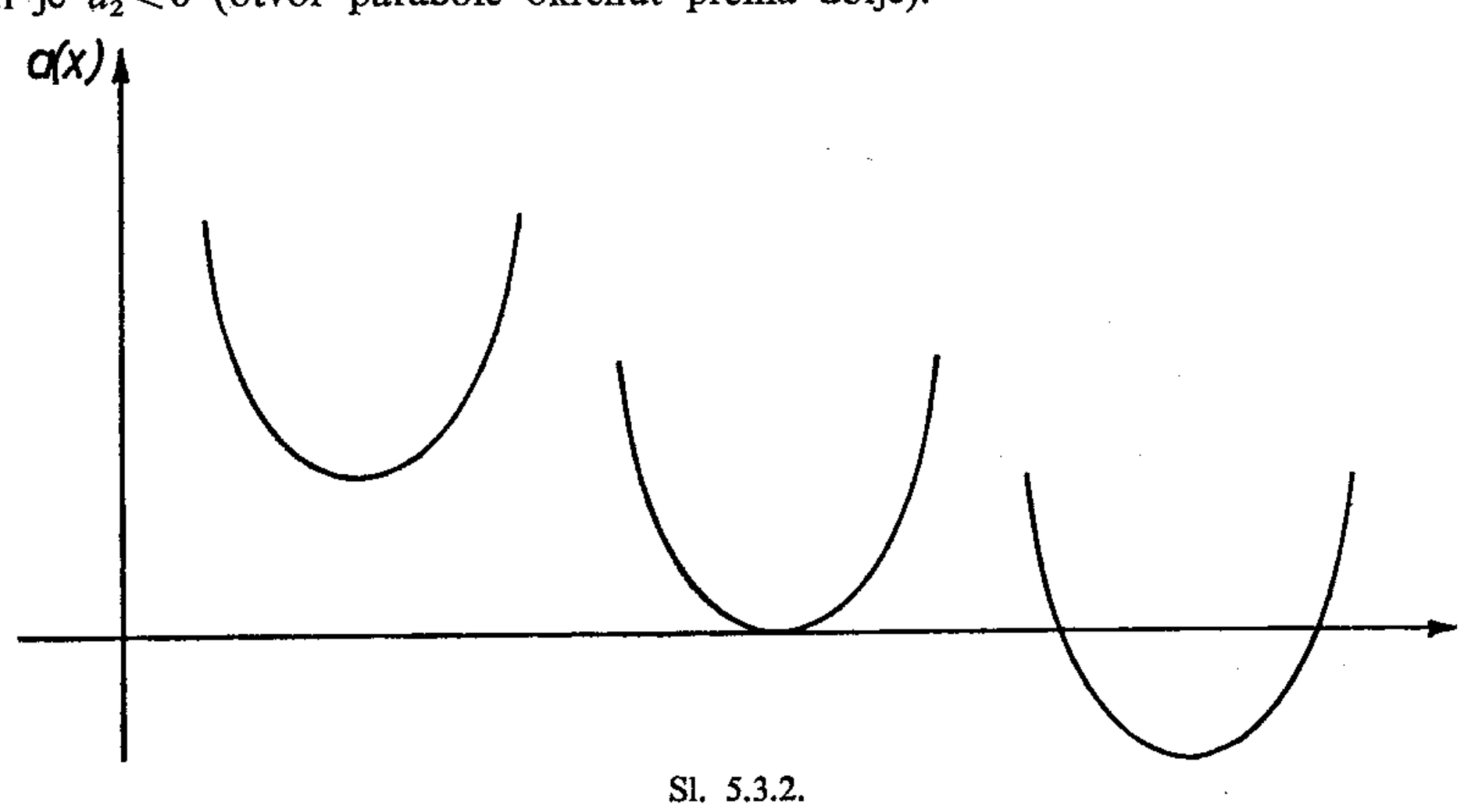
Tako npr. što je nužno i dovoljno da se nula-tačke od $a(x)$ mogu prikazati u obliku $\cos x$, za realno x? To će biti onda i samo onda ako je



Sl. 5.3.1

$$x_1, x_2 \in R[-1, 1].$$

3.2. No, jednadžbom $y = a(x)$ predočena je određena parabola; os joj je $\perp$ x-os; neka je $(x_t;\ a(x_t))$ tjeme parabole; to znači da funkcija a postaje ekstremalnom u x_t, tj. broj $a(x_t)$ je *najmanja*, odnosno *najveća* vrijednost funkcije a, već prema tome da li je $a_2 > 0$ (otvor parabole okrenut prema gore) ili je $a_2 < 0$ (otvor parabole okrenut prema dolje).



Sl. 5.3.2.

No,

$$x_t = 2^{-1}(x_1 + x_2)$$

jer je parabola simetrična prema pravcu $x = x_t$; s obzirom na Viètеove formule, daje to:

$$x_t = -2^{-1} a_2^{-1} a_1. \tag{1}$$

[1]) Slično pitanje za bilo koji polinom $a(x)$ — a ne samo za slučaj da je $st\, a = 2$ — obradit ćemo kasnije (*Sturmov teorem, v. 29 § 5.4.*). Sjetimo se da je R skup svih realnih brojeva a da $R(c, d)$ označuje skup svih $x \in R$ za koje je x između c *i* d.

Ako parabola presijeca x-os u x_1, x_2, tada je produkt

$$a_2 \cdot a \leq 0$$

u zatvorenom intervalu $R[x_1, x_2]$; izvan toga intervala vrijedi:

$$a_2\, a > 0.$$

Prema tome:

(2) $$x \in R(x_1, x_2) \Leftrightarrow a_2\, a(x) < 0.$$

Ako je $c \leq \inf\{x_1, x_2\}$, onda je $D \geq 0$, a k tome $c \leq -2^{-1} a_2^{-1} a_1$, jer u broju $-2^{-1} a_2^{-1} a_1$ kvadratna funkcija hvata svoj ekstrem (minimalnu vrijednost ako je $a_2 > 0$, a maksimalnu ako je $a_2 < 0$).

Prema tome, ako je

(3) $$R[c, d] \supset R[x_1, x_2] \neq \varnothing, \quad \text{onda je:}$$

(4) $$D \geq 0, \text{ jer su } x_1, x_2 \text{ realni;}$$

(5) $$a_2 \cdot a(c) \geq 0 \quad \text{(jer je } c \text{ izvan } R(x_1, x_2)\text{);}$$

(6) $$a_2 \cdot a(d) \geq 0 \quad \text{(jer je } d \text{ izvan } R(x_1, x_2)\text{);}$$

(7) $$c \leq -2^{-1} a_2^{-1} a_1 \leq d, \quad \text{(jer u } x_t = -2^{-1} a_2^{-1} a_1$$

prima funkcija a svoju ekstremalnu vrijednost).

3.3. *Vrijedi i obrat: iz uslova* (4)—(7) *proizlazi uslov* (3). Stvarno, iz (4) proizlazi da su brojevi x_1, x_2 realni; iz (5) i (6) proizlazi da brojevi c i d ne leže između x_1, x_2, a iz (7) proizlazi da je $c \leq x_t$, a time i $c \leq \inf [x_1, x_2]$; analogno: $x_t \leq d$ znači da je $sup\{x_1, x_2\} \leq d$. A sve to upravo znači da vrijedi (3).

Tako npr. da oba korijena leže u $R[-1, 1]$, nužno je i dovoljno da bude $D \geq 0$, $a_2 \cdot a(-1) \geq 0$, $a_2 \cdot a(1) \geq 0$, $-1 \leq x_t \leq 1$.

3.4. Primjer. Odredi m tako da polinom

$$a(x) = 5x^2 - 4x - m$$

ima svoje nula-tačke u intervalu $R[-1, 1]$. Tu je $a_0 = -m$, $a_1 = -4$, $a_2 = 5$,

Uslov $D \geq 0$, tj.

$$(-4)^2 - 4 \cdot 5(-m) \geq 0, \text{ daje:}$$

(8) $$m \geq -5^{-1} \cdot 4.$$

Uslov $-1 \leq x_t \leq 1$ je ispunjen za svako m (čak i za svako kompleksno m, jer je $x_t = -2^{-1} 5^{-1} . -4 = 0{,}4$).

Uslov $a_2\, a(-1) \geq 0$ tj. $5(5 + 4 - m) \geq 0$, daje:

(9) $$m \leq 9.$$

Najzad, uslov $a_2\, a(1) \geq 0$, tj. $5(5 - 4 - m) \geq 0$, daje:

(10) $$m \leq 1.$$

Skupimo li uslove (8), (9), (10), izlazi:

$$-5^{-1}\,4 \leq m \leq 1$$

kao odgovor na zadatak.

Tako npr. sa $m=8$ izlazi polinom $5x^2-4x-8$, za koji su ispunjeni svi uslovi osim onog koji kaže da je $1 \geqq \sup\{x_1, x_2\}$. A to znači da je broj 1 smješten između x_1 i x_2; uistinu je

$$a_2\, a(1) = 5 \cdot (5-4-8) < 0,$$

a to prema (2) znači da je $1 \in R(x_1, x_2)$.

Zaključujemo da je

$$-1 < x_1 < 1 < x_2, \tag{11}$$

tj. intervali $R(-1,\ 1)$, $R(x_1, x_2)$ se isprepleću. To zaključujemo a da i ne računamo koliko je x_1 i x_2. Inače, izračunamo li x_1 i x_2 za polinom $5x^2-4x-8$, izlazi $x_1 = -0{,}9\ 2\ 6\ 6\cdots$, $x_2 = 1{,}7\ 2\ 6\ 6$, pa tako i na drugi način vidimo da je rezultat (11) ispravan.

4. SVOJSTVA ALGEBARSKOG POLINOMA STUPNJA 2. POOPĆENJE NA STUPANJ $n=3, 4, \ldots$

4.1. Neka je a algebarski polinom stupnja 2 u varijabli x, tj.:

$$a(x) = a_0 + a_1 x + a_2 x^2,\ a_2 \neq 0.$$

Nema bitnog ograničenja ako pretpostavimo da je polinom normiran, tj. $a_2 = 1$. To ćemo, dakle, i pretpostaviti.

Imamo ove činjenice:

4.1.1. Teorem. *Ako su koeficijenti polinoma realni, pa ako je z nula-tačka toga polinoma, onda je i konjugirani (spregnut) broj* $\bar{z}$ *nula-tačka istog polinoma.*

4.1.2. Teorem. *Ako je z nula-tačka polinoma* $a(x)$, *tada je* $a(x)$ *djeljivo s normiranim linearnim faktorom* $x-z$; *i obrnuto, tj.* $a(x) = (x-z)\cdot q(x)$, *gdje je* $q(x)$ *određen polinom.*

4.1.3. Teorem. *Svaki algebarski polinom* $a(x)$ *stupnja 2 ima 2 nula-tačke (one mogu biti jednake ili različite).*

4.1.4. Teorem. *Normirani polinom je produkt svojih normiranih linearnih faktora, pri čemu svaki linearni faktor ima kratnost istu koliku ima i dotična nula-tačka.*

Gornji teoremi 1.1, 1.2 1.3, i 1.4 lako se dokazuju; međutim, od interesa je da *odgovarajući teoremi postoje i za svaki (normirani) algebarski polinom a stupnja n*

$$a = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} + a_n x^n,\ a_n \neq 0.$$

4.2.—4.2.1. Specijalno, iskaz 4.1.3. vrijedi za svaki algebarski polinom $a(x)$: za svaki prirodni broj n, *svaki algebarski polinom stupnja n u jednoj varijabli ima n nula-tačaka* (*svaka brojena svojom kratnošću*). To je tzv. *osnovni ili fundamentalni teorem algebre.* Nakon mnogih pokušaja raznih matematičara (d'Alembert, Euler, Lagrange i dr.) tek je Gaussu god. 1799. pošlo za rukom taj stavak potpuno pokazati (v. 7 § 13).

Pri tom važi ova definicija:

4.2.2. *Definicija kratnosti nula-tačke zadane funkcije.* Neka je $f(x)$ funkcija varijable x; svako z za koje je $f(z)=0$ zove se *nul-tačka* ili *nula-tačka* ili *ništična tačka* ili *ništište* funkcije f. Nula-tačka z je *jednostruka* ako je $f'(z)\neq 0$. Nula-tačka z je *dvostruka* ako je

$$f(z)=0, \quad f'(z)=0, \quad f''(z)\neq 0.$$

Uopće neka je k prirodni broj; kaže se da je z k-struka nula-tačka funkcije f ili *nultačka kratnosti* k, ako je

$$0=f(z)=f'(z)=f''(z)=\ldots=f^{(k-1)}(z),\ f^{(k)}(z)\neq 0.$$

⟶ **4.2.3.** T e o r e m. *Za svaki algebarski polinom* $a(x)$ *s realnim koeficijentima jednadžba* $a(z)=0$ *daje jednadžbu* $a(\overline{z})=0$.

D o k a z. Najprije se vidi da je za kompleksne brojeve r, s uvijek:

$$\overline{r+s}=\overline{r}+\overline{s}, \tag{1}$$

$$\overline{rs}=\overline{r}\cdot\overline{s}, \tag{2}$$

$$\overline{r^n}=\overline{r}^n \quad (n=1, 2, 3, \ldots). \tag{3}$$

Pa neka je $a(z)=0$; neka je $z=c+id$ (c i d su realni brojevi), tj. $a(z)=a(c+id)$; to znači da je a, preko $c+id$, funkcija od c, d; rastavimo a na realni i čisto imaginarni dio:

$$a(z)=a(c+id)=u(c,d)+iv(c,d),$$

pri čemu su u i v realni. Ako je $a(c+id)=0$, znači to da je

$$u(c,d)=0, \quad v(c,d)=0.$$

Ako dokažemo da je

$$a(c-id)=u(c,d)-iv(c,d),$$

bit će time dokazano svojstvo u čl. 2.3.

No, $a(\overline{z})=(\overline{z})^n+a_1(\overline{z})^{n-1}+\cdots$ (po svojstvu (3)) $=\overline{z^n}+a_1\overline{z^{n-1}}+\cdots=$ (svojstva (1) — (3), jer je $\overline{a_k}=a_k$) $=\overline{a(z)}=u(x,y)-iv(x,y)$ pa zbog pretpostavki $u(x,y)=0=v(x,y)$ izlazi $u(\overline{z})=0$.

⟶ **4.2.4.** Teorem. *Ako je* $a(z)=0$, *tada je* $a(x)$ *djeljivo s* $x-z$.

Stvarno je

$$a(x)=a(x)-0=a(x)-a(z)=(x^n-z^n)+$$

$$+a_1(x^{n-1}-z^{n-1})+\cdots+a_{n-1}(x-z).$$

Kako je u posljednjoj jednadžbi svaki član na desnoj strani djeljiv sa $x-z$, djeljiva je sa $x-z$ i čitava desna strana, pa tako i lijeva strana, tj. $a(x)$.

4.2.5. Teorem. 4.1.4. je evidentan za *st.* $a=2$, naime po Viète ovim formulama imamo $-(x_1+x_2)=a_1$, $x_1x_2=a_2$, pa relacija

$$(x-x_2)(x-x_2)=x^2-(x_1+x_2)x+x_1x_2$$

prelazi u traženu jednakost:

$$(x-x_1)(x-x_2)=x^2+a_1x+a_0.$$

U općem slučaju, iskaz 4.1.4. izlazi iz § 4.2.1. i § 4.1.2. Naime, prema § 4.2.1. postoji broj x_1 za koji je $a(x_1)=0$; to prema § 4.1.2. znači da je

$$a(x)=(x-x_1)q(x);$$

ako je *st.* $q>0$, tada analogno postoji broj x_2 i rastav

$$q(x)=(x-x_2)r(x), \quad \text{dakle:}$$

$$a(x)=(x-x_1)(x-x_2)r(x),$$

gdje je $r(x)$ polinom stupnja $n-2$ (tu je $n=st.\,a$). Postupno dolazimo do niza brojeva $x_1, x_2, \cdots x_n$ sa svojstvom da je

$$a(x)=(x-x_1)(x-x_2)\cdots(x-x_n)\cdot K, \quad K \text{ konstanta.}$$

Naravno, $K=1$. Na sličan se način dokazuje:

⟶ **4.2.6.** Teorem. *Svakom algebarskom polinomu* $a(x)=\sum_{\nu=0}^{n}a_\nu x^\nu$ *stupnja* n (*dakle je* $a_n\neq 0$), *pripada niz od* n *brojeva*

(5) $$x_1, x_2, \cdots x_n$$

sa svojstvom

(6) $$a(x)=a_n(x-x_1)(x-x_2)\cdots(x-x_n) \text{ za svako } x.$$

Naravno, u nizu (5) može biti i jednakih članova. Ako se npr. broj x_1 pojavljuje u nizu (5) upravo α puta, onda to znači da se i faktor $x-x_1$ u $(6)_2$ pojavljuje α puta, pa je, dakle, $a(x)$ djeljivo sa $(x-x_1)^\alpha$. Stavimo

$$a(x)(x-x_1)^{-\alpha}=f(x), \quad \text{tj.}$$

(7) $$a(x)=f(x)(x-x_1)^\alpha.$$

Može se pokazati da je broj α upravo kratnost nul-tačke x_1 za polinom $a(x)$ i (§ 4.2.2.) da vrijedi:

⟶ **4.2.7.** Teorem. *Neka je $a(x)$ algebarski polinom u x; ako je z nula-tačka reda α za polinom a, tada je a djeljivo sa $(x-z)^\alpha$, ali nije djeljivo sa $(x-z)^{\alpha+1}$, tj. postoji algebarski polinom $q(x)$ sa svojstvom:*

$$a(x) = (x-z)^\alpha q(x) \tag{1}$$

$$q(z) \neq 0. \tag{2}$$

I obrnuto: ako je α prirodan broj ili 0, pa ako za algebarske polinome $a(z), q(x)$ vrijede relacije (1), (2), tada je z nula-element ili ništište reda a za algebarski polinom a.

Dokaz. Služit ćemo se Taylorovim teoremom; to je osnovni teorem, a kaže da je

$$a(x) = \sum_{k=0}^{\infty} \frac{a^{(k)}(z)}{k!} (x-z)^k; \text{ tu je } a^{(k)}(z) = 0 \text{ za } k > st\, a. \tag{3}$$

1. No, prema pretpostavci, z je nul-element reda α za polinom a; dakle je

$$a^{(k)}(z) = 0 \text{ za } k = 0, 1, 2, \cdots, \alpha-1 \tag{4}$$

$$a^{(\alpha)}(z) \neq 0. \tag{5}$$

Prema tome, polinom $(3)_2$ počinje članom $\frac{a^{(\alpha)}(z)}{\alpha!}(x-z)^\alpha$; svi naredni njegovi članovi sadrže $(x-z)^{\alpha+1}$ kao faktor; zato je

$(3)_2 = (x-z)^\alpha g(x)$, $g(x) = \frac{a^{(\alpha)}(z)}{\alpha!} + (x-z)h(x)$, gdje su $g(x)$ i $h(x)$ polinomi; stavimo li tu $x = z$, izlazi $g(z) = \frac{a^{(\alpha)}(z)}{\alpha!}$, dakle zbog (5) $g(z) \neq 0$. Prema tome relacije (1) i (2) su zadovoljene — $q(x)$ je upravo dobiveni polinom $g(x)$.

2. Dokažimo obrat: iz (1) i (2) izlazi (4) i (5), tj. z je zbilja za funkciju a nul-element reda α.

Najprije iz (1) proizlazi da je $a^{(0)}(z) = 0$ ako je $\alpha \geq 1$. Nadalje, primjenjujući obrazac $D(ab) = Da \cdot b + a\ Db$ o deriviranju produkta dviju funkcija dolazimo iz (1) do nove jednakosti:

$$a'(x) = \alpha(x-z)^{\alpha-1}\ q(x) + (x-z)^\alpha\ g_1(x); \tag{1.1}$$

tu je $g_1(x)$ određena funkcija (stvarno je $g_1(x) = q'(x)$).

Deriviranjem jednakosti (1.1) izlazi jednakost:

$$a^{(2)}(x) = (\alpha-1)\,\alpha\,(x-z)^{\alpha-2} q(x) + (x-z)^{\alpha-1} g_2(x); \tag{1.2}$$

$g_2(x)$ je određena funkcija.

. . . . . .

$$a^{(\alpha)}(x) = \alpha!\, q(x) + (x-z)\, g_\alpha(x), \tag{1.α}$$

gdje je $g_\alpha(x)$ određeno.

Iz jednakosti (1.1), (1.2), $\cdots$, (1.α) izlaze, stavljajući u njih $x=z$, upravo relacije (4) i (5); specijalno je $a^{(\alpha)}(z)=\alpha!\,q(z)$, a ovo je $\neq 0$ zbog pretpostavke (2).

Teorem je potpuno dokazan.

4.2.8. O kratnosti nul-elemenata funkcijâ s dvije i više varijabli isp. pogl. 20. § 6.3.

4.3. Zadaci o jednadžbama i polinomima stupnja ≤ 2.

Nađi nula-tačke ovih polinoma:

1) $+3x^2-5x+4$, 2) ix^2-x+1, 3) $\cos a\cdot x^2+\sin a\cdot x+1$,

4) $(2+5i)x^2-(4+2i)x+1$; 5) $1,25x^2-3,42x+17{,}039$.

2. Riješi jednadžbu:

1) $3x^2+2x-65=0$; 2) $21x^2+40x+16=0$;

3) $x^2(a^2-b^2)-2a(a^2+b^2)x+(a^2+b^2)^2=0$;

4) $x^2-3ax+3bx-9ab+2(a+b)^2=0$;

5) $8ax^2-(a^2+64)x+a^2-64=0$;

6) $$\frac{4x+2}{x^2+4x+4}-\frac{11x+7}{x^2+4x+4}=\frac{77-7x^2}{x^3+8};$$

7) $$\frac{1}{x^2-1}-\frac{1}{x^2-x}=\frac{2}{15x}-\frac{1}{x^2-x};$$ 8) $$\frac{a^2-b^2}{2x}=\frac{a^2+b^2}{x^2+1};$$

9) $$\frac{x+2}{10x^2-5x}=\frac{3}{x}+\frac{16x}{4x^2-1};$$ 10) $$\frac{x+2-3i}{x-i}=x+3i.$$

3. Neka se odrede predznaci korijenâ kvadratne jednadžbe, a da se ne riješi sama jednadžba:

1) $5x^2-12x+7=0$; 2) $12x^2-4x-5=0$;

3) $40x^2-49x+15=0$.

4. Za koju su vrijednost od m oba korijena jednadžbe $(m-2)x^2-(m+1)x+2m-2=0$: a) jednaka, b) protivna, c) recipročna d) za koju je vrijednost od m jedan korijen jednak 1?

5. Za koju vrijednost od m imaju obje jednadžbe $x^2-(m+2)x+2m=0$, $x^2-(m-1)x-3m+1=0$ jedan korijen zajednički i koji je to korijen?

6. Za koju je vrijednost od m zbroj kvadrata korijena jednadžbe $(m-1)x^2-(2m+1)x+2m+2=0$ jednak 13?

7. Za koju je vrijednost od m $y=(m-3)x^2-(m+2)x+2m+1$ potpuni kvadrat?

8. Ako su nula-tačke izraza $ax^2+2bx+c$ realne, tad su i nula-tačke polinoma $ax^2+2(ac+b)x+ac^2+2bc+c$ realne.

9. Dužinu 1) 5; 2) $3\frac{1}{2}$; 3) od (2, 3) do (7, 10), 4) od $2+5i$ do $8-12i$ podijeli po „zlatnom pravilu“ (cijelo prema većem odresku

odnosi se kao veći odrezak prema manjem odresku); odredi omjer podjele λ.

10. Odredi realne brojeve m za koje će izraz $2x^2-3mx+1$ imati nula-tačke: 1) realne; 2) >0; 3) u odresku $[-1, 1]$; 4) u $[3, 10]$.

11. Riješi ove nejednadžbe:

1) $x^2-2x-15>0$; 2) $5x^2+7x-24<0$; 3) $-6x^2+5x+1>0$;

4) $24x^2-14x-3<0$; 5) $\frac{2x-5}{3-2x}>0$; 6) $\frac{3x-4}{2x-3}>5$;

7) $\frac{5x-6}{7x-8}<2$; 8) $(x^2+x-56)(x^2-12x+35)<0$;

9) $\frac{x^2+2x-48}{x^2-x-20}>0$; 10) $\frac{x^2-5x-6}{x^2-10x+16}>1$; 11) $\frac{6}{x-1}+\frac{10}{x-1}>\frac{7}{x-3}$; 12) $\frac{x+18}{x+6}>\frac{6}{x-3}$; 13) $\frac{x+3}{x-2}-\frac{x+8}{x+15}>\frac{5}{12}$;

14) $\frac{1}{x^2-5x+6}>\frac{1}{x^2-4x-32}$.

12. U rombu sa stranicom 41 cm obje se dijagonale razlikuju za 62 cm. Kolike su dijagonale?

13. Neka se odrede katete pravokutnog trokuta, komu je opseg $2s$ (36 cm) i hipotenuza c (15 cm).

14. U zadanu kuglu upiši valjak zadanog plašta p.

15. Dva se tijela gibaju po krakovima pravoga kuta jednoliko prema vrhu. Na početku je prvo tijelo udaljeno od vrha a_1 (50 m), drugo a_2 (36 m), nakon t_1 (1) sekundi njihova međusobna udaljenost je d_1 (53 m), nakon t_2 (3) sekundi d_2 (37 m). Kolika je brzina obaju tijela?

16. Dužina drvenog trupca obujma 348,54 dm^3 je 9 dm, a razlika površina jednog i drugog prereza 21,98 dm^2. Kolika je debljina trupca na dnu i na vrhu?

17. Dvije tvornice, koje proizvode istu robu obavežu se da će zajedno svršiti za 20 dana izvjesnu partiju robe široke potrošnje i predati je u distribucioni centar. Da su obje tvornice imale veći kapacitet proizvodnje, svršile bi posao za 8 dana ranije. No u tom bi slučaju prva tvornica mogla sama svršiti taj posao 15 dana ranije nego što sada sama može, a druga za 17 dana ranije nego što bi to sama mogla obaviti. Za koliko bi dana mogla (uz normalni kapacitet) svaka od tvornica sama svršiti posao?

18. Nabavljačko-potrošačka zadruga dobila je naručene dvije bale tkanine s računom na 360 dinara. Prigodom pregleda robe ustanovilo se, da je poslano 3 m tkanine manje nego što je naručeno, ali zato je kvalitet robe bolji i 1 m poslane tkanine treba prodati za cijenu 2 dinara veću od 1 m tkanine, koja se naručila. Kako je račun za poslanu

tkaninu bio opet 360 din, zadruga je zadržala robu i prodala je. Koliko je bilo m tkanine i koliko je stajao 1 m?

19. Od komada kvadratna lima treba napraviti otvorenu uspravnu prizmatičnu posudu od 8 *l* tako da se u uglovima lima odreže kvadratni komad po 8 cm dug i da se onda ostatak lima previje i susjedne strane slijepe. Koliko je potrebno lima?

20) Riješi: 1) $x + x^{-1} = 4$; 2) $x^{1/2} + x = 8$; 2) $x^{1/2} + x^{-1/2} = 15$;
4) $l = \pi r (r^2 + x^2)^{1/2}$; 5) $(x-a)^{1/2} + (2x + 3a)^{1/2} = (5a)^{1/2}$.

5. KUBIRANJE. ANTIKUBIRANJE

5.1. Zadan je kompleksni broj $z = r e^{i\varphi}$; tada je $z^3 = r^3 e^{3i\varphi}$. Prelaz od z na z^3 izvest ćemo u dva koraka.

Prvi korak: rotacija radijus-vektora $\overrightarrow{Oz}$ oko O *za* $+2\varphi$; time z prelazi u $|z| e^{3i\varphi} = z'$.

Drugi korak: prelaz od z' na z^3, a odvija se tako da se z' pomnoži sa $|z|^2$; uistinu:

$$z' \cdot |z| = |z| e^{3i\varphi} \cdot |z|^2 = |z|^3 e^{i3\varphi} = (|z| e^{i\varphi})^3 = z^3.$$

Vidimo da se na taj način pojavljuje ova geometrijska operacija:

5.2. Svakoj tački T odredimo tačku $3 \cup T$ kojoj je argument tri put veći nego Arg T, a leži na kružnici $k(O; T)$, kojoj je O središte, a OT poluprečnik.

Dakle je Arg $(3 \cup T) = 3$ Arg T.

Jasno je da je tačka $3 \cup T$ potpuno određena tačkom T, i to za svako T.

5.3. Ako je tačka T na zraci Ox, tada je $3 \cup T = T$. Nastaje pitanje: da li iz $A \neq B$ izlazi $3 \cup A \neq 3 \cup B$? Ne mora! I u tome je baš čitav interes preslikavanja $T \to 3 \cup T$. Vidi se, naime, da vrijedi ovo: ako su T_0, T_1, T_2 vrhovi pravilna trokuta kojemu je O središte, tada se tačke $3 \cup T_0$, $3 \cup T_1$, $3 \cup T_2$ poklapaju!

Drugim riječima, ako operaciju obrnutu od operacije $3 \cup$ koja prevodi T na $3 \cup T$ označimo sa $\frac{1}{3} \cup$, tada vidimo da postoje 3 tačke oblika $\frac{1}{3} \cup T$ za svako $T \neq 0$, a vrhovi su pravilnog trokuta upisanog u kružnicu $k(O; T)$.

Jedan od tih vrhova ima svoj argument $= \frac{1}{3} arg\ T$.

5.4. Ako u gornjim razmatranjima umjesto broja 3 uzmemo bilo koji prirodni broj n, tada dolazimo do pridruživanja $V = n \cup T$ i protivnog pridruživanja: $T = n^{-1} \cup V$. Zaključak je analogan:

5.5. *Ako su* $T_0, T_1, \cdots, T_{n-1}$ *vrhovi pravilnog n-kuta s O kao središtem, tada se tačke* $n \cup T_0, n \cup T_1, \cdots, n \cup T_{n-1}$ poklapaju.

Obrnuto, ako je zadana tačka V, tada se može pitati za tačke T za koje je $n \cup T = V$. Takvih tačaka imamo upravo n; a vrhovi su pravilnog n-kuta upisanog u kružnicu $k(O; V)$.

Zanimljivo je da jedan vrh toga n-kuta ima svoj argumenat $= n^{-1}. arg\ V$.

5.6. Analogno se za svaki realni broj λ može iz tačke T preći na skup svih tačaka $\lambda \cup T$ sa svojstvom:

$$\mathrm{Arg}\,(\lambda \cup T) = \lambda\,\mathrm{Arg}\,T.$$

Ako je λ cio broj, onda je tačka $\lambda \cup T$ jednoznačno određena; ako je $\lambda = n^{-1}$, gdje je $n = 2, 3, \cdots$, tada ima upravo n različitih tačaka oblika $n^{-1} \cup T$; one su vrhovi pravilnog n-kuta upisanog u kružnici $k(O; T)$. Ako je λ iracionalan broj, tada je građa skupnosti tačaka $\lambda \cup T$ prilično zamršena; ta je skupnost svuda gusta na kružnici $k(O; T)$.

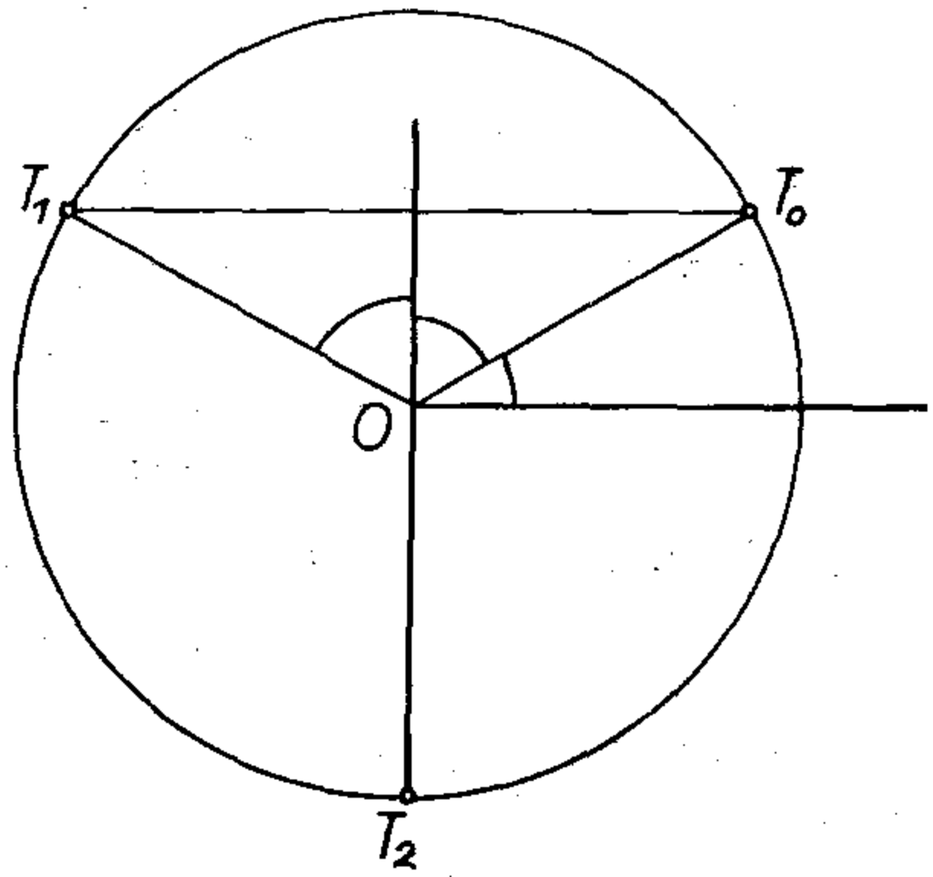
5.7. Antikubiranje. *Antikubirati* zadani broj c ili naći treći korijen iz broja c znači odrediti sve brojeve x za koje je

$$x^3 = c; \tag{1}$$

pri tome c može biti realan ili uopće kompleksan broj.

Ako je $c = 0$, tada je, naravno, 0 jedino rješenje jednadžbe (1); 0 je tada *trostruko* rješenje.

Ako je c oblika $c = e^{i\varphi} = \cos\varphi + i \sin\varphi$, tada je broj $e^{i\varphi/3}$ jedan antikub od c; rotiramo li taj broj $e^{i\varphi/3}$ za $2\pi/3$ i $4\pi/3$, dobiju se još ove dvije vrijednosti antikuba: $e^{i\frac{\varphi+2\pi}{3}}$, $e^{i\frac{\varphi+4\pi}{3}}$; te tri vrijednosti $e^{i\varphi/3}$, $e^{i(\varphi+2\pi)/3}$, $e^{i(\varphi+4\pi)/3}$ određuju vrhove pravilnog 3-kuta; označujemo ih sa $c^{1/3}$; specijalno, $+c^{1/3}$ označuje broj, odnosno onaj vrh 3-kuta (č. trokuta) kojemu je *argument najmanji* ali svakako ≥ 0.



Sl. 5.5.7.

Dakle je $+(e^{i\varphi})^{1/3} = e^{i\varphi/3}$.

Sličan je i opći slučaj $c \neq 0$.

Ako je $c \neq 0$, tada prema prethodnom imamo 3 broja x_0, x_1, x_2 koji zadovoljavaju jednadžbu (1); geometrijski oni predstavljaju vrhove pravilnog trokuta koji je upisan u kružnicu $k(O; +|c|^{1/3})$. Prema tome, ako kut xOc razdijelimo na 3 jednaka dijela, tada na zraci iz O koja s početnom zrakom Ox čini kut $1/3\ arg\ c$, u udaljenosti $+|c|^{1/3}$, leži prvo rješenje; označuje se sa $+c^{1/3}$; preostala dva rješenja proizlaze iz $+c^{1/3}$ rotacijom oko O za $2\pi/3$, odnosno $4\pi/3$ u pozitivnom ili negativnom smislu rotacije. No, to znači da su brojevi

$$+c^{1/3},\quad +c^{1/3} \cdot e^{i2\pi/3},\quad +c^{1/3} \cdot e^{i4\pi/3} \tag{2}$$

tražena tri rješenja jednadžbe (1).

5.8. Zadaci o kubiranju i antikubiranju.

1. Kubiraj brojeve i izraze: 1) 3,4; 2) 0,034 3) 0,00034; 4) 3400; 5) $2{,}8\,a^3\,b^{-2}\,c^{1/2}$; 6) $4\,a^2\,b-4\,ab^2$; 7) $2+5\,i$; 8) $2-5\,i$; 9) $-2+5\,i$; 10) $-2-5\,i$; 11) $4{,}5+6\,i$; 12) $\cos 30^0+i\sin 30^0$; 13) $3\,(\cos 60^0+i\sin 60^0)$; 14) $[(3-5\,i)^2+6\,i]^3$.
2. Antikubiraj brojeve i izraze iz zadatka 1.
3. Promatraj jednadžbu $x^3=y^2$; nađi joj nekoliko rješenja (x, y), specijalno ona rješenja koja su oblika: 1) $(x, 1)$; 2) $(1, y)$.
4. U koordinatnoj ravnini zadana je proizvoljna krivulja k (npr. $x^2+y^2=1$ ili $x^3=y^2$ itd.) i neka tačka t_0; presijeci k s paralelom s x-osi kroz t_0; kroz svako dobiveno sjecište povuci paralelu s y-osi i presijeci k; kroz svako to sjecište povuci paralelu s x-osi i tom paralelom presijeci krivulju k itd. Da li se tim procesom naiđe ponovo na zadanu polaznu tačku t_0?
5. Sličan zadatak, ali tako da prva paralela kroz t_0 bude paralela ne s x-osi nego s y-osi.
6. Zadatak 4 provedi na analitički način za krivulju:

   1) $x^2+y^2=1$; 2) $x^3=y^2$ i tačku t_0 kojoj je apscisa $x_0=0{,}5$.

6. ALGEBARSKE JEDNADŽBE TREĆEG STUPNJA

6.0. Ideja. Linearnu jednadžbu s nepoznanicom x možemo pisati $a_0+a_1\,x=0$ uz zahtjev $a_1\neq 0$; rješenje joj je $x=-a_1^{-1}\,a_0$.

6.0.0. Za kvadratnu jednadžbu $a_0+a_1\,x+a_2\,x^2=0$, $a_2\neq 0$ izlazi

$$x=\frac{-a_1+\sqrt{D}}{2\,a_2},\quad D=a_1{}^2-4\,a_0\,a_2.$$

Naredni stupanj, treći, dovodi nas do opće kubne jednadžbe:

(1) $$a_0+a_1\,x+a_2\,x^2+a_3\,x^3=0,\quad a_3\neq 0.$$

6.0.1. I iz nje se može izvući x u svojoj zavisnosti od koeficijenata a_0, a_1, a_2, a_3; u svakom slučaju, time što zadamo jednadžbu (1) zadan je i skup svih rješenja jednadžbe (1). Tako npr. za jednadžbu $x^3=1$ pripadni skup rješenja glasi $\{1, -1/2+i/2\sqrt{3}, -1/2-i/2\sqrt{3}\}$. Zasluga je talijanskih matematičara 16. stoljeća što su pronašli da iz

(*v*) $$x^3+px+q=0$$

izlazi:

(2) $$x=(-q/2+\sqrt{D/108})^{1/3}+(-q/2-\sqrt{D/108})^{1/3},$$ gdje je

(3) $$D=-4\,p^3-27\,q^2.$$

6.0.2. Tu na „pregledan“ način vidimo kako se x gradi iz koeficijenata p i q.

Naime, prema obrascu (2): *rješavanje normalne kubne jednadžbe* (*v*) *svedeno je na antikvadriranja i antikubiranja izvjesnih izraza koje odmah na pregledan način gradimo iz koeficijenata p, q normalne jednadžbe* (*v*).

Jedina je još poteškoća u tome što — kako znamo — antikvadriranje i antikubiranje nisu jednoznačne operacije.[1)]

6.0.3. Naravno, jednadžba (*v*) je specijalan slučaj opće jednadžbe (1), jer je „najstariji“ koeficijent a_3 iz (1) „normiran“ (postao je 1), a njegov susjed a_2 je uništen ($a_2 = 0$). No, opći slučaj se vrlo lako svodi na „normalni“ slučaj (*v*) (isp. § 6.1.3). Time je, teoretski, problem kubne jednadžbe likvidiran.

6.0.4. No, pri praktičnom rješavanju kubnih jednadžbi dolaze i drugi problemi. Specijalno, ako su koeficijenti kubne jednadžbe realni posebni brojevi, tada je rješenja najzgodnije tražiti ne pomoću (2), nego na trigonometrijski način (§ 6.5. za slučaj $D<0$; § 6.7. za $D>0$). A posebno pitanje: odrediti da li i koliko rješenjâ jednadžbe (1) leži u zadanom intervalu (npr. između -1 i $+1$ ili između 5 i ∞ i sl.) nećemo ni obrađivati još u ovom poglavlju (isp. § 3. za kvadratne jednadžbe i poglavlje 29. za bilo koje jednadžbe).

6.1. Opći oblik kubne jednadžbe i njeno svođenje na normalni oblik.

6.1.0. Definicija. Jednadžba oblika

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 = 0, \quad a_3 \neq 0 \tag{1}$$

u kojoj a-ovi ne zavise od x zove se *kubna jednadžba* ili *jednadžba stupnja* 3 s obzirom na x; a_0, a_1, a_2, a_3 su koeficijenti jednadžbe (1), i to po redu: *prvi, drugi, treći,* i *četvrti koeficijent*. Uloga indeksa 0, 1, 2, 3 sastoji se u tome da na pregledan način vidimo o kojem je koeficijentu riječ. Koeficijent a_3 od x^3 zove se *najstariji* ili *najugledniji* koeficijent jednadžbe (koeficijenti najvišeg ranga ili položaja). Tako npr. imamo ove jednadžbe stupnja 3:

$$x^3 = 0, \; 2 - x^3 = 0, \; 3 + 4x^2 + x^3 = 0, \quad 100 + at + 5t^3 = 0, \text{ itd.}$$

Koeficijenti na najvišem položaju jesu 1, -1, 1 i 5. Ako te 4 kubne jednadžbe usporedimo s općim oblikom, onda vidimo da nijedna od njih nije „*potpuna*“ u smislu da ima 4 koeficijenta $\neq 0$. Prve dvije su „čiste“ (bez koeficijenata uz x i x^2, tj. ti su koeficijenti $= 0$); druga je bez čistog x, a treća je „normalna“ (bez x^2).

6.1.1. *Neravnopravnost koeficijenata u* (1). U sređenoj kubnoj jednadžbi (1) odlučujuću ulogu ima koeficijent uz kubnu nepoznanicu. On je $\neq 0$; naime

---

[1)] Tako npr. $1^{1/3}$ je ne samo $=1$ nego također $-1/2 + i\sqrt{3}/2$ te $-1/2 - i\sqrt{3}/2$; uistinu je npr. $(-1/2 + i\sqrt{3}/2)^3 = -1/8 + \frac{3}{8} i\sqrt{3} + \frac{9}{8} - \frac{i}{8} \cdot \sqrt{3} = 1$.

ako je $a_3 = 0$, tada jednadžba (1) postaje stupnja ≤ 2. Važnu ulogu ima i prvi koeficijent a_0. On može biti $= 0$; jednadžba (1) tada postaje:

$$(a_1 + a_2 x + a_3 x^2)\, x = 0. \tag{2}$$

Kako radimo sa brojevima, izlazi odatle da jednadžba (2) ima rješenja jednadžbe:

$$a_1 + a_2 x + a_3 x^2 = 0 \tag{3}$$

i jednadžbe:

$$x = 0$$

tj. skup rješenja jednadžbe (2) sastoji se od 0 i rješenjâ kvadratne jednadžbe (3).

Zato nam slučaj $a_0 = 0$ ne pravi poteškoća. Ostaje slučaj

$$a_0 \neq 0, \quad a_3 \neq 0.$$

Ako su srednji koeficijenti $= 0$, tada jednadžba (1) postaje:

$$a_0 + a_3 x^3 = 0. \tag{4}$$

To su *čiste kubne jednadžbe*. Njih smo rješavali kad smo se upoznali s antikubiranjem. Iz (4) izlazi:

$$a_3^{-1} a_0 + x^3 = 0$$

$$x = (-a_3^{-1} a_0)^{1/3}.$$

Zato ostaje slučaj da je bar jedan od srednjih koeficijenata $\neq 0$.

6.1.2. Prva redukcija: *normiranje najstarijeg koeficijenta na* 1. To je zaista jednostavna operacija: dovoljno je jednadžbu (1) pomnožiti s inversom od a_3 pa izlazi [1]:

$$a_3^{-1} a_0 + a_3^{-1} a_1 x + a_3^{-1} a_2 x^2 + x^3 = 0. \tag{2}$$

6.1.3. Druga redukcija: *poništenje koeficijenta do najstarijeg*. Pokušajmo — kao što su to radili Viète, Hudde — nepoznato x iz (1), razbiti na dva dijela

$$x = y + z \tag{3}$$

s tim da eventualno jedan od tih dijelova zgodno odredimo.

Unesemo li izraz $y + z$ za x u (1), dobijemo:

$$a_0 + a_1 (y + z) + a_2 (y + z)^2 + a_3 (y + z)^3 = 0,$$

odnosno (poredano po padajućim potencijama od y):

$$a_3 y^3 + (3 a_3 z + a_2) y^2 + (\quad) y + \cdots = 0.$$

---

[1] Kako je lako s brojevima! A da slova u (1) znače matrice!? Ili nešto još zamršenije!

Tu su sada 2 nepoznate: y i z; no koeficijent od y^2 možemo poništiti, tj. staviti:

$$3a_3z+a_2=0$$

i time jednoznačno odrediti z:

$$z=-\frac{a_2}{3a_3}.$$

6.1.3.0. Primjer. Zadana je jednadžba

$$-402+211x+36x^2+2x^3=0;$$

stavimo u nju $x=y+z$; dobijemo:

$$-402+211(y+z)+36(y+z)^2+2(y+z)^3=0;$$

sredimo po padajućim potencijama od y; imamo:

$$2y^3+(6z+36)y^2+(6z^2+72z+211)y+$$

$$+(2z^3+36z^2+211z-402)=0.$$

Na prvi pogled to je zamršen izraz; no slobodno nam je taj izraz pojednostaviti, npr. tako da poništimo koeficijent uz y^2:

$$6z+36=0, \quad \text{tj.} \quad z=-6.$$

Time polazna jednadžba postaje jednostavnijeg oblika: bez koeficijenata uz kvadrat nove nepoznanice y; dobijemo:

$$2y^3-5y+1=0,$$

a veza između stare nepoznanice x i nove y glasi: $x=y-6$.

6.1.3.1. Na isti način vidimo ovo: ako je zadana kubna jednadžba:

$$a_0+a_1x+a_2x^2+a_3x^3=0, \quad a_3\neq 0,$$

tada uvođenjem nove nepoznanice y vezom $x=y-\frac{a_2}{3a_3}$ dolazimo do kubne jednadžbe u kojoj je koeficijent od y^2 jednak 0.

Zato, odsad, možemo pretpostavljati da je već i u zadanoj jednadžbi (1) $a_2=0$.

6.1.4. *Normalni oblik kubne jednadžbe.* To je oblik kod kojeg je najstariji koeficijent jednak 1, a onaj do njega $=0$, tj. $a_3=1$, $a_2=0$. Normalni oblik se obično naznačuje ovako:

$$x^3+px+q=0, \tag{4}$$

tj koeficijent od x se označuje sa p, a konstantni sa q.

Prevedimo npr. jednadžbu

$$-402+211x+36x^2+2x^3=0$$

u normalni oblik.

Najprije normirajmo najstariji koeficijent; dijeleći jednadžbu sa 2, izlazi:

$$-201 + 105{,}5\,x + 18\,x^2 + x^3 = 0.$$

Stavljajući $x = y + z$, odaberimo z tako da koeficijent od y^2 bude $= 0$; izlazi $z = -6$ (isp. § 6.1.3.0); traženi normalni oblik glasi:

$$y^3 - 2{,}5\,y + 0{,}5 = 0.$$

Na isti se način svaka jednadžba stupnja 3 svodi na normalni oblik. Oba koeficijenta p, q u normalnom obliku jednoznačno su određena za svaku kubnu jednadžbu.

6.2. Rješenje normalne kubne jednadžbe. Kardanov obrazac.

6.2.0. Da riješimo jednadžbu (4), najzgodnije je prema Vièteu i Huddeu (1628—1704) prikazati nepoznatu x kao sumu od dvije nepoznate u, v:

$$x = u + v. \tag{5}$$

Time jednadžba (4) prelazi u

$$u^3 + v^3 + (3\,uv + p)(u + v) + q = 0, \tag{6}$$

kojoj će očigledno biti udovoljeno čim je

$$3\,uv + p = 0 \tag{7}$$

$$u^3 + v^3 = -q. \tag{8}$$

No iz (7) izlazi:

$$u^3\,v^3 = -\frac{p^3}{27}. \tag{9}$$

Kako je prema (8) i (9) poznata i suma i produkt brojeva u^3, v^3, moraju prema Vièteovim obrascima za kvadratne jednadžbe ti brojevi u^3, v^3 zadovoljavati kvadratnoj jednadžbi:

$$z^2 + qz - \frac{p^3}{27} = 0. \tag{10}$$

Odatle izlazi:

$$z = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}};$$

dakle:

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \tag{11}$$

$$v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \tag{12}$$

čime prema (5) izlazi:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^2}{27}}}. \tag{13}$$

Stavimo li

$$D = -4p^3 - 27q^2, \tag{14}$$

prelazi (12) u

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{-D}{4 \cdot 27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{-D}{4 \cdot 27}}}. \tag{15}$$

6.2.1. Obrazac (13) za rješenje x zadane kubne jednadžbe (4) zove se *Kardanov obrazac*; taj je obrazac prvi put objavljen u djelu *Hieronymi Cardani artis magnae sive de regulis algebraicis, liber unicus*; Norimbergae 1545 (Knjiga o velikoj vještini ili algebarskim pravilima). Inače je formulu (15) pronašao već god. 1515. *Scipione dal Ferro*, a ponovo god. 1535. *N. Tartaglia* [Tartalja].

6.2.2. Izraz $D = -4p^3 - 27q^2$ u (14) zove se *diskriminanta* kubnog polinoma $x^3 + px + q$, odnosno pripadne jednadžbe (4). Jednadžba (10), tj. jednadžba $z^2 + qz - \frac{p^3}{27} = 0$ zove se *rezolventa*[1] *kubne jednadžbe* $x^3 + px + q = 0$; pomoću nje smo riješili kubnu jednadžbu (4).

Dobili smo, dakle:

6.2.3. Teorem. *Svako rješenje kubne jednadžbe* $x^2 + px + q = 0$ *oblika je* (13), *odnosno* (15), *pri čemu valja imati na umu da prema* (7) *produkt sumanada u* (13) *iznosi* $-p/3$, *a da kubi sumanada u* $(13)_2$, *odnosno* $(15)_2$, *zadovoljavaju kvadratnoj rezolventi* (10).

6.2.4. Drugim riječima: *ako je U jedno rješenje iz* (11), *a V jedno rješenje jednadžbe* (12), *pa ako je* $UV = -p/3$, *tada je*

$$x = U + V$$

jedno rješenje kubne jednadžbe $x^3 + px + q = 0$.

No, ako je U jedno rješenje od (11), tada su preostala dva rješenja jednadžbe (11) brojevi $U\alpha$, $U\alpha^2$, gdje je α primitivni kubni korijen jedinice. Isto tako, brojevi V, $V\alpha^{-1}$, $V\alpha^{-2}$ su sva tri rješenja jednadžbe (12). Odatle proizlazi:

6.2.5. Brojevi

$$\begin{cases} x_0 = U + V \\ x_1 = U\alpha + V\alpha^2 \\ x_2 = U\alpha^2 + V\alpha \end{cases} \tag{5}$$

predstavljaju sva tri rješenja kubne jednadžbe $x^3 + px + p = 0$. Pri tom je U jedno rješenje jednadžbe (11), a V jedino rješenje jadnadžbe (12) uz uslov $UV = -p/3$; broj α zadovoljava $\alpha^3 = 1$, $\alpha \neq 1$.

---

[1] Prema latinskom *resolvo* (resolvi, resolutum) — *riješiti, osloboditi.*

⟶ 6.3. Osnovni teorem o normalnoj kubnoj jednadžbi. Ako je

$$x^3+px+q=0, \text{ onda je } x=u+v, \text{ gdje je}$$

$$u^3=-q/2+\sqrt{-D/108},$$

$$v^3=-q/2-\sqrt{-D/108},\quad D=-4p^3-27q^2,$$

$$uv=-p/3.$$

Neka je U jedna odabrana, inače bilo koja, vrijednost antikuba izraza $-q/2+\sqrt{-D/108}$; stavimo tada $V=-p/(3U)$ (specijalno: $V=0$ za $U=0$); tada se skup rješenja jednadžbe $x^3+px+q=0$ sastoji od izrazâ:

$$U+V,$$

$$(*)\qquad U\alpha+V\alpha^2,$$

$$U\alpha^2+V\alpha.$$

Pri tome je α broj određen pomoću $\alpha^3=1$, $\alpha\neq 1$, dakle ili $\alpha=-1/2+i\sqrt{3}/2$ ili $\alpha=-1/2-i\sqrt{3}/2$ (tu $\sqrt{3}$ odabiremo kao pozitivni antikvadrat broja 3).

6.3.1. Primjedba o izboru u gornjem teoremu. Izlazi na isto da li $\sqrt{3}$ u gornjem teoremu fiksiramo kao pozitivni ili kao negativni antikvadrat broja 3; važno je da u gornjim razmatranjima od više vrijednosti uvijek odaberemo jednu jedinu i da se onda tog izbora pridržavamo. Dakle, za $\sqrt{3}$ odaberemo ili $+\sqrt{3}=1,7\cdots$ ili $-\sqrt{3}=-1,7\cdots$ Ako smo izabrali npr. $\sqrt{3}=1,7\cdots$ (a ne $-1,7\cdots$), tada za α biramo po volji $0,3\cdots$ ili $-1,2\cdots$ No, učinjeni izbor za α dalje nas veže ulazeći u izraze (*); teoremom se onda tvrdi da dobiveni izrazi (*) sačinjavaju skup svih rješenja polazne jednadžbe bez obzira na naše odluke o izboru vrijednostî za $\sqrt{3}$ (dvije mogućnosti izbora), α (dvije mogućnosti izbora), U (tri mogućnosti izbora).

6.4. Kubna jednadžba $x^3+px+q=0$ s realnim koeficijentima. Ispitajmo slučaj kad su koeficijenti p, q realni brojevi. Tada je $D>0$ ili $D=0$ ili $D<0$; tu je $D=-4p^3-27q^2$ (*diskriminanta jednadžbe*).

6.4.1. P r v i s l u č a j: $D<0$. Baza od $(\ )^{1/2}$ u Kardanovu obrascu (15) je >0, pa se može uzeti da su brojevi u, v realni. Prema tome, realno je i rješenje $x_0=U+V$. Preostala dva rješenja x_1, x_2 prema obrascima (*) postaju npr. za $\alpha=(-1+i\sqrt{3})/2$:

$$x_1=\frac{-U-V}{2}+i\frac{U-V}{2}\sqrt{3},$$

$$x_2=\frac{-U-V}{2}-i\frac{U-V}{2}\sqrt{3}.$$

Ako je $D<0$, tada su sva tri korijena različna; dva su korijena međusobno konjugirano povezana.

6.4.2. Drugi slučaj: $D=0$. U tom je slučaju $U=(-q/2)^{1/3}=V$ pa obrasci (15), odnosno (*) postaju:

$$x_0=2U$$

$$x_1=-U$$

$$x_2=-U,\ U=+(-q/2)^{1/3}.$$

Ako je $D=0$, tada su sva tri korijena realna, dva su jednaka, a treći im je protivno jednak.

6.4.3. Treći slučaj: $D>0$ (**casus irreducibilis** — nesvodljiv slučaj). Sva su tri korijena realna (i različita), mada u Kardanovoj formuli dolazi antikvadriranje (traženje drugog korijena iz) negativnog broja.

Da to vidimo, riješimo kubnu jednadžbu **trigonometrijski.**

6.5. Trigonometrijsko rješenje kubne jednadžbe (Viète).

6.5.1. Iz $D>0$ izlazi $-D<0$, pa u^3 ne može biti realan broj. No svaki kompleksni broj je oblika $\rho e^{i\varphi}$, tj. $\rho\cos\varphi+i\rho\sin\varphi$, gdje je $0\leq\rho$, $0\leq\varphi<2\pi$. Stavimo, dakle, da u^3 bude toga oblika, tj.

$$-q/2+(-D/(4\cdot 27))^{1/2}=\rho\cos\varphi+i\rho\sin\varphi,$$

odnosno:

$$-q/2=\rho\cos\varphi$$

$$+(D/108)^{1/2}=\rho\sin\varphi;$$

možemo tražiti da bude također $\rho>0$, $\sin\varphi>0$.

Kvadrirajući te dvije jednadžbe i sabirajući ih, izlazi:

$$-p^3/27=\rho^2,$$

odakle:

$$\rho=+(-p/3)^{3/2}.$$

Naravno, $\rho>0$ jer je $p<0$. Sam broj φ jednoznačno je određen iz $\cos\varphi=-q/2\rho$ uz dodatni zahtjev da bude $\sin\varphi>0$, tj. $0\leq\varphi<\pi$.

Na taj smo način jednoznačno odredili ρ i φ, pa za u imamo ove 3 vrijednosti:

$$(\rho e^{i\varphi})^{1/3}=+\rho^{1/3}\cdot e^{i(\varphi/3+k\cdot 2\pi/3)},\quad (k=0,\ 1,\ 2).$$

Analogno za v imamo ove 3 vrijednosti:

$$(\rho e^{-i\varphi})^{1/3}=+\rho^{1/3}e^{-i(\varphi/3+l\cdot 2\pi/3)},\quad (l=0,\ 1,\ 2).$$

No, kako za rješenja $x=u+v$ vrijednosti u i v treba tako odabrati da bude $uv=-p/3$, dakle realan broj, znači to da u izrazu $x=u+v$, tj.

$$x=+\rho^{1/3}(e^{i(\varphi/3+k\cdot 2\pi/3)}+e^{-i(\varphi/3+l\cdot 2\pi/3)}),\quad (k=0,\ 1,\ 2)\quad (l=0,\ 1,\ 2)$$

treba da bude $k=l$; zato rješenja $x=u+v$ postaju za $k=0,\ 1,\ 2$:

$$x_k = +\rho^{1/3}\cdot\left(e^{i(\varphi/3+k\cdot 2\varphi/3)}+e^{-i(\varphi/3+k\cdot 2\pi/3)}\right)$$

$$(1)\qquad = +\rho^{1/3}\left([\cos(\varphi+2k\pi)\,3^{-1}+i\sin(\varphi+k\cdot 2\pi)\,3^{-1}]\right)+$$

$$+[\cos-(\varphi+k\cdot 2\pi)\cdot 3^{-1}+i\sin-(\varphi+k\cdot 2\pi)\cdot 3^{-1}])\ \text{tj.}$$

$$x_k=2(+\rho^{1/3})\cos(\varphi+k\cdot 2\pi)\,3^{-1},\quad k=0,\ 1,\ 2.$$

A to su tri različna realna broja. Dakle smo dokazali da vrijedi ovaj:

⟶ **6.5.2. Teorem o nesvodljivom slučaju.** *Ako je* $D\equiv -4p^3-27q^2>0$, *tj. ako imamo „nesvodljivi slučaj“* (*casus irreducibilis*), *tada polinom* x^3+px+q *ima sve tri nul-točke realne i različite; to su brojevi* $x_{\dot 3}=2\rho^{1/3}\cos(\varphi/3+2\pi\dot 3/3)$, *pri čemu je* $\dot 3=0,\ 1,\ 2$, zatim je $\rho=+(-p/3)^{3/2}$, $\cos\varphi=-q/(2\rho)$, $0\leq\varphi<\pi$ (svakako je $p\leq 0$).

6.5.3. Napomena. Capelli [Kapeli] i Hölder [Helder] dokazali su god. 1890/91. da se u „nesvodljivom slučaju“ nultačke polinoma x^3+px+q ne mogu dobiti na algebarski način bez antikvadriranja negativnih brojeva.

6.6. Što znači neodrečnost diskriminante? Iz razmatranja prethodnih triju slučajeva izlazi napose:

Teorem. ***Da nul-točke polinoma*** x^3+px+q ***uz realne koeficijente*** p ***i*** q ***budu realne, nužno je i dovoljno da bude:***

$$-4p^3-27q^2\geq 0.$$

F. Viète (Vjet; 1540—1603), francuski matematičar, osnivač algebre općih brojeva.

6.7. Trigonometrijsko rješenje normalne kubne jednadžbe s realnim koeficijentima i s negativnom diskriminantom.

Riješit ćemo kubnu jednadžbu pomoću trigonometrijskih funkcija (Viète).

6.7.0. Neka je $D<0$, tj. $-4p^3-27q^2<0$. U ovom su slučaju dva rješenja nerealna (isp. § 6.4.1). No i ovdje je za *numeričko rješavanje* prikladnija trigonometrijska metoda. Kao i u slučaju $D>0$, stavimo i sada da je

$$\rho=+\left|p/3\right|^{3/2}.$$

6.7.1. Prvi slučaj: $p<0$. Tada je

$$\rho^2=\left(-\frac{p}{3}\right)^3$$

pa iz $D<0$ izlazi

$$\rho^2=(-p/3)^3<q^2/4,\ \text{tj.}\ 0\leq\rho<\frac{|q|}{2};$$

zato se može naći φ tako da vrijedi $2\rho/-q=\sin\varphi$; ako je $q<0$, neka φ bude u prvom kvadrantu, a ako je $q>0$, neka φ bude u trećem kvadrantu. U svakom slučaju je tada: $\operatorname{ctg}\varphi=+(\sin^{-2}\varphi-1)^{1/2}=(4\cdot 27\,\rho)^{-1}.(-D)^{1/2}$,

pa izrazi za u^3, v^3 iz osnovnog obrasca 6.3 postaju

$$u^3 = \rho\,(\sin^{-1}\varphi + \operatorname{ctg}\varphi) = \rho\operatorname{ctg}\varphi/2$$

$$v^3 = \rho\,(\sin^{-1}\varphi - \operatorname{ctg}\varphi) = \rho\operatorname{tg}\varphi/2.$$

Da se nađu brojevi u, v, odredimo ω po formuli:

$$\operatorname{tg}^3\omega = \operatorname{tg}\varphi/2,$$

tako da ω i $\varphi/2$ leže u istom kvadrantu. Izlazi:

$$u = \rho^{1/3}\operatorname{ctg}\omega = (-p/3)^{1/2}\operatorname{ctg}\omega$$

$$v = \rho^{1/3}\operatorname{tg}\omega = (-p/3)^{1/2}\operatorname{tg}\omega.$$

Time izlazi i jedno traženo rješenje:

$$x_0 = u + v = (-p/3)^{1/2}(\operatorname{ctg}\omega + \operatorname{tg}\omega) = 2\,(-p/3)^{1/2}\sin^{-1} 2\,\omega.$$

Ostala dva rješenja su

$$x_1 = u\,\alpha + v\,\alpha^2, \quad x_2 = u\,\alpha^2 + v\,\alpha, \quad \text{gdje je}$$

$$\alpha = (-1 + 3^{1/2} i)/2, \quad \alpha^2 = (-1 - 3^{1/2} i)/2.$$

Nakon izračunavanja dobivamo sva tri rješenja, i to u ovom obliku:

⟶ **6.7.1.1.** Teorem. *Ako je* $p<0$, $D\equiv -4p^3-27q^2<0$, *tada jednadžba* $x^3+px+q=0$ (p, q *realno*) *ima upravo ova* 3 *rješenja*:

$$x_0 = 2\,(-p/3)^{1/2}\sin^{-1} 2\,\omega$$

$$x_{1,2} = (-p/3)^{1/2}(-\sin^{-1} 2\,\omega \pm i\,3^{1/2}\operatorname{ctg} 2\,\omega), \quad \text{gdje je}$$

$$\rho = +(-p/3)^{3/2}, \ \sin\varphi = -2\,\rho/q, \ \operatorname{tg}^3\omega = \operatorname{tg}\varphi/2.$$

6.7.2. Drugi slučaj: $p>0$. Odredimo φ iz $-q/(2\,\rho) = \operatorname{ctg}\varphi$ tako da bude $\sin\varphi>0$, i to:

$$\sin\varphi = +(1+\operatorname{ctg}^2\varphi)^{-1/2} = \rho\,((q/2)^2 + (p/3)^3)^{-1/2}.$$

Zato za u^3, v^3 imamo ove izraze:

$$u^3 = \rho\operatorname{ctg}\varphi/2, \quad v^3 = -\rho\operatorname{tg}\varphi/2, \quad \rho = +(p/3)^{3/2}.$$

Ako kao u prethodnom slučaju odredimo

$$\omega\in[0,\pi/2] \quad \text{iz} \quad \operatorname{tg}^3\omega = \operatorname{tg}\varphi/2,$$

tada izlazi

$$u = (p/3)^{1/2}\operatorname{ctg}\omega, \ v = -(p/3)^{1/2}\operatorname{tg}\omega;$$

nakon kraćeg računanja izlazi ovaj rezultat:

6.7.2.1. Teorem. *Sva tri rješenja kubne jednadžbe* $x^3+px+q=0$ *s realnim koeficijentima, za slučaj* $D\equiv -4p^3-27q^2<0$ *i* $p>0$ *glase*:

$$x_0 = 3\,(p/3)^{1/2}\operatorname{ctg} 2\,\omega$$

$$x_{1,2} = (p/3)^{1/2}(-\operatorname{ctg} 2\,\omega \pm\ i\,3^{1/2}\sin^{-1} 2\,\omega)$$

Pritom je

$$tg^3\omega = tg\,\varphi/2, \quad ctg\,\varphi = -q/2\rho, \quad \rho = +(p/3)^{3/2} \quad i$$

$$0 \leq \omega,\ \varphi/2 \leq \pi/2.$$

6.7.3. S l u č a j $p=0$ ne predstavlja nikakve teškoće, jer se takva jednadžba tada reducira na čistu kubnu jednadžbu.

6.8. Numerički primjer kubne jednadžbe.

P r i m j e r. Riješi jednadžbu

$$f(x) \equiv x^3 + 1647{,}773\,x - 23290 = 0.$$

Uslovi teorema 6.7.2.1 su zadovoljeni, pa ćemo zato jednadžbu riješiti tako da primjenimo taj teorem.

1. *Broj* ρ.

$$\rho = \left(\frac{p}{3}\right)^{3/2} = \left(\frac{1647{,}773}{3}\right)^{3/2} = 549{,}258^{3/2}$$

$$\log\rho = \frac{3}{2}\cdot 2{,}73978$$

$$\log\rho = 3\cdot 1{,}36989$$
$$\log\rho = \quad 4{,}10967$$
$$\rho = 12872,$$
$$\ldots\ldots$$

2. *Broj* φ.

$$\operatorname{ctg}\varphi = -\frac{q}{2\rho} = \frac{23290}{2\cdot 12872} = \frac{11645}{12872}$$

$$\overset{+10}{\log\operatorname{ctg}\rho} = 4{,}06614 \overset{-10}{-} 41{,}10967$$
$$\log\operatorname{ctg}\varphi = 9{,}95647 - 10$$
$$\varphi = 47^0\,52'$$
$$\frac{\varphi}{2} = 23^0\,56'$$

3. *Broj* ω.

$$tg^3\omega = tg\frac{\varphi}{2} = tg\,23^0\,56'$$

$$\overset{+20}{3\log tg\,\omega} = 9{,}64722 \overset{-20}{-} 10$$
$$\log tg\,\omega = 9{,}882406 - 10$$
$$\omega = 37^0\,20'\,10''$$
$$2\omega = 74^0\,40'\,20''.$$

4. *Rješenje* x_0.

$$x_0 = 2\left(\frac{p}{3}\right)^{3/2}\operatorname{ctg}2\omega = 2\cdot\left(\frac{1647{,}773}{2}\right)^{1/2}\operatorname{ctg}74^0\,40'\,20''$$

$$\log x_0 = 0{,}30103 + \frac{1}{2}\cdot 2{,}73978 + 9{,}43789 - 10$$
$$\log x_0 = 9{,}73892 + 1{,}36989 - 10$$
$$\log x_0 = 1{,}10881$$
$$x_0 = 12{,}8473$$

5. Rješenja x_1, x_2:

$$x_{1,2} = -\left(\frac{p}{3}\right)^{1/2}\operatorname{ctg}2\omega \pm \frac{ip^{1/2}}{\sin 2\omega}$$

$$x_{1,2} = -c \pm id$$

$$c = \left(\frac{p}{3}\right)^{1/2}\operatorname{ctg}2\omega, \qquad d \mp \frac{p^{1/2}}{\sin 2\omega}$$

$$\log c = \tfrac{1}{2} \cdot 2{,}73978 + 9{,}43789 - 10$$
$$\log c = 0{,}80778$$
$$c = 6{,}4236.$$

$$\log d = \tfrac{1}{2} \log 1647{,}773 - \log \sin 74^0\, 40'\, 20''$$
$$\log d = \tfrac{1}{2} \cdot 3{,}21690 - 9{,}98427 + 10$$
$$\log d = 1{,}60845 - 9{,}98427 + 10$$
$$\log d = 1{,}62418$$
$$d = 42{,}09$$
$$x_{1,2} = -c \pm id = -6{,}4236 \pm i \cdot 42{,}09$$

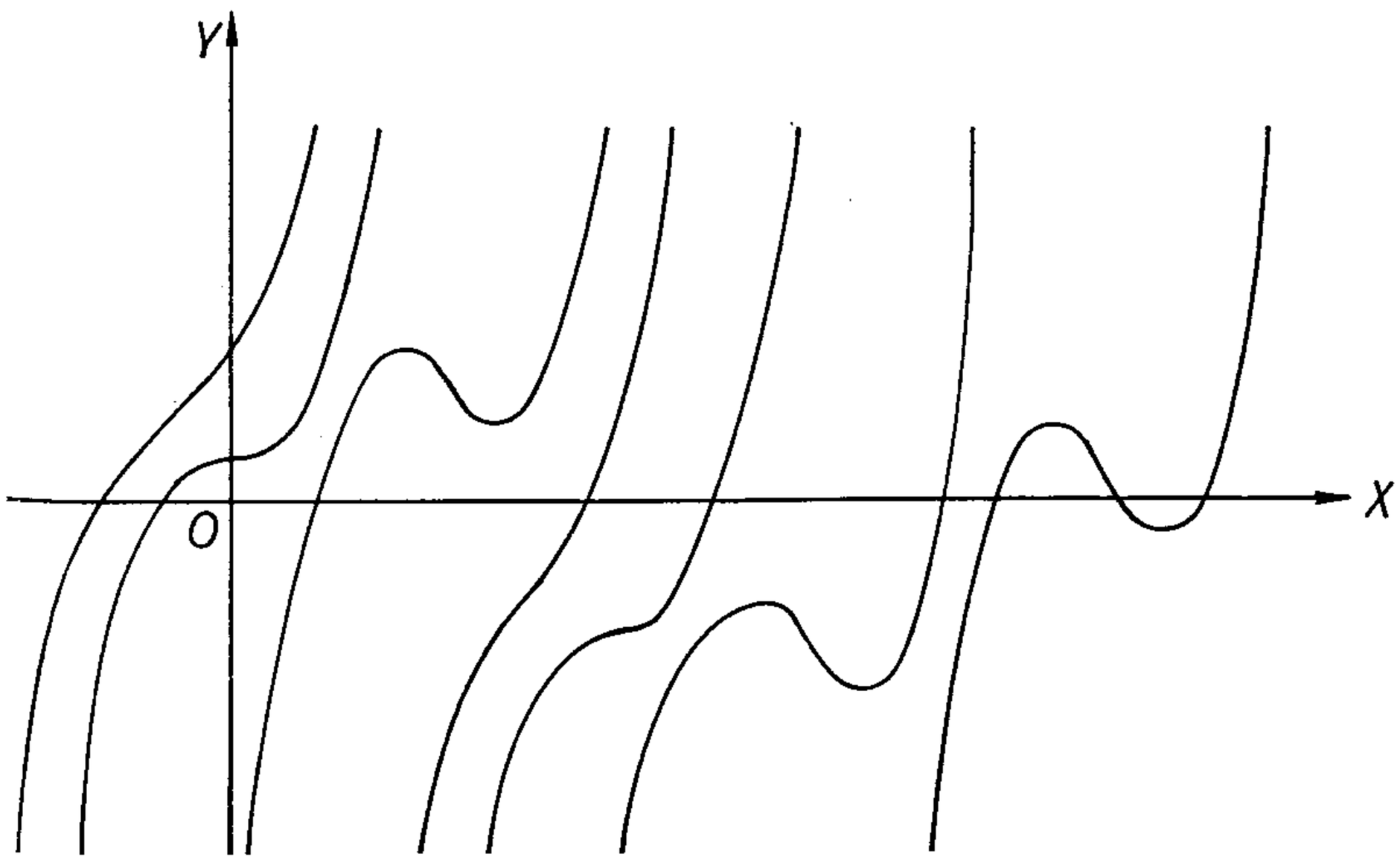
6. Odgovor: Jednadžba (1) ima ova rješenja
$$x_0 = 12{,}8473 \qquad x_{1,2} = -6{,}4236 \pm i \cdot 42{,}09.$$

7. Pokus: $f(x_0) = ?$
$$f(x_0) = 12{,}8472^3 + 1647{,}773 \cdot 12{,}8473 - 23290$$
$$a = 12{,}8473^3 \qquad b = 1647{,}773 \cdot 12{,}8473$$
$$\log a = 3 \cdot 1{,}10881 \qquad \log b = 3{,}21690 + 1{,}10881$$
$$\log a = 3{,}32643 \qquad \log b = 4{,}32571$$
$$a = 2120{,}45 \qquad b = 21169{,}5$$
$$\ldots\ldots \qquad \ldots\ldots$$
$$a + b = 23289{,}95.$$
$$f(x_0) = 23289{,}95 - 23290 = 0{,}05.$$

Prema tome, x_0 je dobra približna vrijednost za rješenje jednadžbe $f(x) = 0$.

6.9. Zadaci o kubnoj jednadžbi.

1. Opiši riječima tok (kubne) funkcije predstavljene jednim od ovih 7 grafova:



Sl. 5.6.9.

2. Prikaži grafički ove funkcije: 1) x^3+1; 2) $2x^3$; 3) $2x^3+1$; 4) $2(x-3)^3$; 5) $2(x-3)^3+1$; 6) $(x-1)\cdot(x+2)\cdot(x+3)$; 7) $(x-1)(x^2+5x-6)$; 7) x^3-6x-1; 9) x^3+3x-2; 10) $(x-1)^3+3(x+1)$; 11) $3x^3-2(x+3)^2-(x+5)$.

3. Svedi na oblik $a_0+a_1x+a_2x^2+a_3x^3$ izraze iz prethodnog zadatka, odredi koeficijente a_0, a_1, a_2, a_3 i diskriminantu dobivenog izraza.

4. Ako je $x^3+px+q=(x-x_1)(x-x_2)(x-x_3)$, dokaži da je diskriminanta izraza x^3+px+q jednaka $(x_1-x_2)^2)(x_1-x_3)^2(x_2-x_3)^2$.

5. 1) Koliko ima različnih polinoma oblika $\pm 2x^3\pm 3x^2\pm 4x\pm 5$?
   2) Uredi ih abecedno prema uređenju nizova njihovih koeficijenata.
   3) Koliko realnih nultačaka ima svaki od tih polinoma?

6. Riješi jednadžbu:
   1) $x^3+9x^2+18x+28=0$; 2) $x^3-3x^2-2x+6=0$.
   $4x^3+2x^2+6x+3=0$, 4) $2x^3+3x^2+6x-4=0$.

7. Kako glasi kubna normirana jednadžba kojoj potpun niz x_1, x_2, x_3 rješenjâ glasi: 1) 1, 2, 3; 2) 1, 1, 0; 3) −2, −2, −2; 4) 2, 5, 9; 5) 2, 5, −9; 6) 2, −5, 9; 7) −2, 5, 9; 8) 2, −5, −9; 9) −2, 5, −9; 10) −2, −5, 9; 11) −2, −5, −9; 12) $x_1^2+x_1+1$, $x_2^2+x_2+1$, $x_3^2+x_3+1$ ako x_1, x_2, x_3 zadovoljavaju $x^3-3x^2-2x+6=0$.

8. Riješi ove jednadžbe:
   1) $x^3-6x+9=0$; 2) $x^3+12x+63=0$;
   3) $x^3+9x^2+18x-28=0$; 4) $x^3+6x^2+30x+25=0$;
   5) $x^3-6x+4=0$; 6) $x^3+6x+2=0$;
   7) $x^3+18x+15=0$; 8) $x^3-3x^2-3x+11=0$;
   9) $x^3+3x^2-6x+4=0$; 10) $x^3+9x-26=0$;
   11) $x^3+24x-56=0$; 12) $x^3+45x-98=0$;
   13) $x^3+3x^2-3x-1=0$; 14) $x^3-6x^2+57x-196=0$;
   15) $x^3+3x-2i=0$; 16) $x^3-6ix+4(1-i)=0$;
   17) $x^3-3abx+a^3+b^3=0$; 18) $x^3-3abfgx+f^2ga^3+fg^2b^3=0$;
   19) $x^3-4x-1=0$; 20) $x^3-4x+2=0$.

9. Zadana je jednadžba $x^3-2mx^2+m^2x-1=0$; riješi je za ove vrijednosti broja m: 1) 0; 2) 3; 3) 5.

10. Riješi pomoću kružnih funkcija i tablicâ ove jednadžbe:
    1) $x^3-5x^2+6x-3=0$; 2) $2t^3+10t^2-28t+16=0$;
    3) $0{,}01y^3+0{,}3y-2{,}5=0$.

11. Neka je $n(a)$ broj realnih nulabrojeva funkcije x^3-3x^2+5x+a; odredi $n(a)$ za za svaki realni broj a.

12. Odredi parametar m tako da slijedeća jednadžba ima bar jedno nejednostruko rješenje: 1) $x^3+m=0$, 2) $x^3+2x+m=0$; 3) $x^3+3x^2+m=0$; 4) $x^3+3x^2+2x+m=0$; 5) $x^3+3x^2+2mx+1=0$; 6) $x^3+3mx^2+2x+1=0$; 7) $x^3+m(3x^2+2x)+1=0$; 8) $x^3+3x^2+m(2x+1)=0$, 9) $x^3-2x+m=0$; 10) $x^3-3x^2+m=0$;

11) $x^3-3x^2+2x+m=0$; 12) $x^3+3x^2-2x+m=0$;

13) $x^3-3x^2+2mx+1=0$; 14) $x^3+3mx^2-2x+1=0$;

15) $x^3-3x^2+m(2x+1)=0$; 16) $x^3-3x^2-2x+m=0$.

13. Kod uspravnog stošca zadan je plašt P i volumen V; nađi r (npr. $P=60\pi\,cm^2$, $V=96\pi\,cm^3$).

14. Nađi visinu kuglina odsječka kojemu je 1) ploština; 2) zapremina jednaka n-tom dijelu a) ploštine, b) zapremine kugle.

15. Kako visoko u kugli polupročnika $r=10$ cm stoji 1 kg vode?

16. Homogena kugla prečnika $2r$ i specifične težine s pliva u vodi; odredi dubinu x uronjenja kugle; npr. za $r=1$, $s=0{,}5$.

17. Paralelnim ravninama razdijeli kuglu na 3), 4) jednaka dijela.

18. Zadana je jednadžba $a(x+c)^{-1}+kx^{-1}+b(x-c)^{-1}=0$; a, b, c su zadani brojevi; odredi k tako da jednadžba ima dvostruko rješenje; nađi to rješenje.

19. Riješi nejednadžbu $p(x)>0$, gdje je $p(x)$ polinom na lijevoj strani jednadžbe u zadatku 6.

20. Isto pitanje za zadatak 7.

21. Riješi ove nejednadžbe:

1) $2x-1<x^3+1$; 2) $2x^2+5>3(x-1)^3$;

3) $\dfrac{x^2-1}{x^3+x+1}>1$; 4) $\dfrac{5x^3-2x+5}{3x^3-1}\leq 4$.

22. Promatraj vezu $2xy^2-3x^3y+4x-5=0$; 1) odredi x_1, x_2, x_3 što odgovaraju broju $y=2$; 2) za svako to x_i iz 1) odredi eventualno pripadno $y\neq 1$; 3) nađi sve vrijednosti x kojima odgovara jedno jedino y; 4) nađi sve vrijednosti y kojima odgovara jedno jedino x.

23. Neka rješenja x_1, x_2, x_3 jednadžbe $x^3+px^2+qx+r=0$ budu pozitivna i <1; odredimo u trokutu ABC tačke P, Q, R tako da bude $\overrightarrow{AP}=\overrightarrow{AB}\cdot x_1$, $\overrightarrow{BQ}=\overrightarrow{BC}\cdot x_2$, $\overrightarrow{CR}=\overrightarrow{CA}\cdot x_3$; dokaži da je omjer ploštine $\triangle PQR$ i $\triangle ABC$ jednak $1+p+q$.

7. ALGEBARSKA JEDNADŽBA 4 STUPNJA

7.0. Opći oblik. Opći oblik algebarske jednadžbe 4. stupnja glasi:

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 = 0, \quad a_4 \neq 0. \tag{1}$$

Pri tom veličine $a_0, a_1, \cdots a_4$ ne zavise od x. Te se veličine zovu *koeficijenti* jednadžbe (1), i to: *prvi koeficijent* a_0, *drugi koeficijent* $a_1, \cdots$, *peti koeficijent* a_4 [1].

Uvijek možemo pretpostaviti da je jednadžba (1) *normirana*, tj. da je $a_4 = 1$: dovoljno je jednadžbu (1) podijeliti sa a_4 pa nove koeficijente opet označiti slovima $a_0, a_1, \cdots$

Također možemo pretpostaviti da nema kubnog člana, tj. da je četvrti koeficijent $= 0$, tj. $a_3 = 0$. Naime, ako je $a_3 \neq 0$, tada možemo umjesto nepoznanice x uvesti novu nepoznanicu y pomoću veze $x = y + z$ i odrediti z tako da novi četvrti koeficijent bude $= 0$; stavimo li $x = y + z$ u (1), tada koeficijent od y^3 glasi:

$$a_3 + 4 a_4 z.$$

Njegovo poništenje je posljedica izbora

$$z = -a_3/(4 a_4).$$

Ako je npr. riječ o jednadžbi

$$8 t^4 - t + 12 t^2 + 19 t^3 + 1 = 0, \text{ tada je dovoljno staviti}$$

$$t = u - 19/(4 \cdot 8) = u - 0{,}59 \cdots$$

pa da novi oblik jednadžbe, sa u kao nepoznanicom, bude bez kubnog člana (tj. da je novi četvrti koeficijent $= 0$).

7.1. Ferrarijevo rješenje. Neka je

$$x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 = 0 \tag{2}$$

normirana jednadžba stupnja 4. Ferrari [Ferari] oko god. 1540. nastoji tu jednadžbu pocijepati na dvije jednadžbe stupnja 2. Iz (2) izlazi:

$$x^4 + a_3 x^3 = -a_2 x^2 - a_1 x - a_0$$

$$\Downarrow$$

$$(x^2 + 2^{-1} a_3 x)^2 = (a_3^2 2^{-2} - a_2) x^2 - a_1 x - a_0. \tag{3}$$

Tu je lijeva strana potpun kvadrat. Nastojmo da i na desnoj strani dobijemo potpun kvadrat L^2, jer bi tada iz (3) proizlazilo:

$$x^2 + 2^{-1} a_3 x = \pm L(x). \tag{4}$$

Uvedimo nepoznat izraz $y/2$ u zagradu izraza $(3)_1$; dobijemo:

$$(x^2 + 2^{-1} a_3 x + 2^{-1} y)^2 = (2^{-2} a_3^2 - a_2 + y) x^2 + (2^{-1} a_3 y - a_1) x + (2^{-2} y^2 - a_0). \tag{5}$$

---

[1]) Kao indeksi služe redni brojevi: 0, 1, 2, 3, 4, odnosno cifre 0, 1, ... Treba se dobro naviknuti na to da je 0 (a ne 1) prvi redni broj, odnosno prva cifra.

No da kvadratna funkcija po x, što se nalazi tu na desnoj strani, bude potpun kvadrat $L(x)^2$, treba da diskriminanta po x bude $=0$, tj. da vrijedi:

$$(6) \qquad (2^{-1} a_3 y - a_1)^2 - 4 (2^{-2} a_3^2 - a_2 + y) (2^{-2} y^2 - a_0) = 0.$$

A to je za y određena jednadžba stupnja 3, koju znamo riješiti. Jednadžba (6) zove se *Ferrarijeva rezolventa* što pripada jednadžbi (2). Ukratko, stvar izgleda ovako:

Iz Ferrarijeve rezolvente (6) *nađe se y; za to y desna strana u* (5) *postaje kvadrat* $(L(x))^2$, *pa iz* (5) *zaključujemo da vrijedi* (4); *no kvadratnu jednadžbu* (4) *znamo riješiti.*

Na taj način, rješavanje jednadžbe 4. stupnja (2) svodi se na rješavanje kubne jednadžbe (6) po pomoćnoj nepoznanici y i kvadratne jednadžbe (4) po traženoj nepoznanici x.

7.2. Kako je Euler riješio jednadžbu 4. stupnja? Euler je god. 1738. riješio jednadžbu 4. stupnja metodom sličnom metodi kojom je Hudde god. 1639. riješio kubnu jednadžbu.

Polazimo od normirane jednadžbe i bez kubnog člana:

$$(1) \qquad a_0 + a_1 x + a_2 x^2 + x^4 = 0.$$

Euler (1738) stavlja:

$$(2) \qquad x = u + v + z;$$

time (1) postaje ekvivalentna s ovom jednadžbom:

$$(u^2 + v^2 + z^2)^2 + 4 (u^2 v^2 + u^2 z^2 + v^2 z^2) + a_2 (u^2 + v^2 + z^2) +$$

$$(3) \qquad + [2 a_2 + 4 (u^2 + v^2 + z^2)] (uv + uz + vz) + (u + v + z)$$

$$(8 uvz + a_1) + a_0 = 0.$$

Ta se jednadžba znatno pojednostavnjuje ako je

$$(4) \qquad 8 uvz + a_1 = 0 \qquad \text{tj.} \qquad uvz = -8^{-1} a_1,$$

$$(5) \qquad 2 a_2 + 4 (u^2 + v^2 + z^2) = 0, \qquad \text{tj.} \qquad u^2 + v^2 + z^2 = -a_2/2.$$

Naime, tada (3) postaje:

$$(6) \qquad u^2 v^2 + u^2 z^2 + v^2 z^2 = 16^{-1} (a_2^2 - 4 a_0).$$

Jednadžbe (5) i (6) odnose se na veličine u^2, v^2, z^2; iz (4) dobijemo i ovu jednadžbu:

$$(7) \qquad u^2 v^2 z^2 = 8^{-2} a_1^2.$$

Na osnovu relacija (4), (5), (7) možemo odmah sagraditi jednadžbu:

$$(y - u^2) (y - v^2) (y - z^2) = 0,$$

kojoj su u^2, v^2, z^2 rješenja; izmnožimo li ta tri izraza, postaje prethodna jednadžba:

$$y^3 - 2^{-1} a_2 y^2 + 4^{-2} (a_2^2 - 4 a_0) y - 8^{-2} a_1^2 = 0. \tag{8}$$

Jednadžba (8) zove se *kubna rezolventa jednadžbe* (2), jer nam (8) daje

$$y_1 = u^2,\ y_2 = v^2,\ y_3 = z^2,$$

a time i samo x u obliku

$$x = y_1^{1/2} + y_2^{1/2} + y_3^{1/2} \tag{9}$$

uz uslov:

$$y_1^{1/2} \cdot y_2^{1/2} \cdot y_3^{1/2} = -8^{-1} a_1. \tag{10}$$

Naime, u (9) ne smiju sva tri y biti s proizvoljnim značenjem, jer mora vrijediti (10). No, ako su u, v, z dobro izabrana značenja za $y_1^{1/2}$, $y_2^{1/2}$, i $y_3^{1/2}$, tj ako je zaista $u+v+z$ jedno traženo rješenje, tada su sva 4 rješenja ovog oblika:

$$\begin{aligned} x_1 &= \ \ u+v+z \\ x_2 &= \ \ u-v-z \\ x_3 &= -u+v-z \\ x_4 &= -u-v+z. \end{aligned}$$

Kao dokaz da su time dobivena sva 4 rješenja, nužno je i dovoljno pokazati da je

$$(x-x_1)\ (x-x_2)\ (x-x_3)\ (x-x_4) = a_0 + a_1 x + a_2 x^2 + x^4, \tag{12}$$

tj. da je

$$\begin{aligned} x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4 &= a_2 \\ -x_1 x_2 x_3 - x_1 x_2 x_4 - x_1 x_3 x_4 - x_2 x_3 x_4 &= a_1 \\ x_1 x_2 x_3 x_4 &= a_0. \end{aligned} \tag{13}$$

Te se nejednakosti mogu direktno provjeriti!

7.3. Zadaci o jednadžbama stupnja 4.

1. Riješi ove relacije:

1) $x^4 - 1 = 0$; 2) $x^4 - 1 > 0$ 3) $x^4 - 1 < 0$; 4) $x^4 - 1 \leq 0$;
5) $x^4 - 1 \geq 0$; 6) $x^4 - 1 \neq 0$.

2, Kojoj normiranoj jednadžbi stepena 4 rješenja glase:
1) $1, -1, 2, -2$; 2) $1, 1, 2, 2$; 3) $1, 1, 1, 2$; 5) $-2, 3, 4, 5$;
6) $2+3i,\ 2-3i,\ -5+i,\ -5-i$; 7) $2+3i,\ -2+3i,\ 4-5i,\ -4+5i$?

3. Riješi $x^4 + 2x^3 - 2x - 1 = 0$.

4) Riješi jednadžbe koje se iz jednadžbi § 6.9.8 dobiju tako da se umjesto člana x^3 piše član x^4; ispiši svih 20 tako nastalih jednadžbi.

5. Sličnih 20 pitanja ako se umjesto člana x^3 piše x^4+2x^3. Ispiši svih 20 tako nastalih jednadžbi.

6. Napiši kubnu rezolventu svake od jednadžbi zadatka 4.

7. Riješi $3x^4-4x^3+1=0$.

8. KONSTRUKCIJE LINEALOM I ŠESTAROM

8.0. Postavlja se pitanje da se zadana jednadžba riješi *grafički, crtanjem*. Naime, ako je riječ npr. o jednadžbi $f(x)=0$, gdje je

$$f(x)=a_0+a_1x+a_2x^2+a_3x^3,$$

tada je dovoljno nacrtati krivulju $y=fx$, potražiti njena sjecišta s x-osi i odrediti apscise tih sjecišta. Te apscise su rješenja jednadžbe $fx=0$.

Specijalno se postavlja pitanje o **elementarnoj konstrukciji krivulje** $y=fx$, tj. o konstrukciji pri kojoj se smijemo služiti *linealom i šestarom kao jedinim pomagalima* (pri tom se predmnijeva da su koeficijenti $a_0, a_1, \cdots$ zadani i numerički i grafički). Tako npr. svaku kvadratnu jednadžbu možemo elementarno riješiti grafički. Kod kubnih to nije moguće već ni za jednadžbe $x^3=2$, $x^3=5$.

8.1. *Konstrukcijama linealom i šestarom odgovaraju racionalne operacije i antikvadriranja.* Pomoću lineala crtamo dûži, odnosno „pravulje“, a pomoću šestara crtamo kružnice. U običnom koordinatnom sistemu pravulja je predočena linearnom jednadžbom a kružnica kvadratnom jednadžbom sa dvije nepoznanice. No pri rješavanju takvih jednadžba vršimo na koeficijentima *racionalne* operacije i *antikvadriranje*.

8.2. Vrijedi i obrat. *Svaki izraz koji se iz zadanih veličina V može dobiti racionalnim operacijama i antikvadriranjima može se iz veličinâ V konstruirati elementarno*, tj. pomoću lineala i šestara.

To je posljedica činjenice da se rješenja kvadratne jednadžbe mogu nacrtati pomoću te dvije sprave ukoliko su već nacrtani koeficijenti jednadžbe.

8.3. Kubna jednadžba ne može se riješiti elementarno. Već najjednostavniji slučaj antikubiranja: naći x iz $x^3=2$ (*duplikacija* ili *udvostručenje kuba*) ne može se riješiti konstruktivno pomoću ravnala i šestara. To i mnogo više odmah ćemo pokazati (isp. i 32 § 4.6.5.2.).

⟶ **8.4.** Teorem. *Ako kubna jednadžba s racionalnim koeficijentima nema nikojeg rješenja u tijelu Q racionalnih brojeva, onda se ona ne može riješiti elementarno, tj. rješenja te jednadžbe ne mogu se dobiti kao rezultat konačnog broja racionalnih operacija i antikvadriranja, odnosno crtajući ravnalom i šestarom.*

Dokaz. Najprije je jasno da zadanu kubnu jednadžbu možemo pretpostaviti u normalnom obliku:

(1) $$x^3+px+q=0.$$

Pretpostavimo, naprotiv, da se jedno rješenje x_0 jednadžbe (1) može dobiti i elementarno; to znači da bi u nizu antikvadriranjâ bilo jedno i *posljednje* pomoću kojeg bi se dobilo x_0; recimo neka je

$$x_0 = A + BY^{1/2}; \tag{2}$$

pri tom se veličine A, B, Y dobiju elementarno iz p, q bez antikvadriranja broja Y, dok se $Y^{1/2}$ ne bi moglo izrazit kao *racionalna funkcija* od A, B, p, q, Y sa racionalnim koeficijentima. Stavimo li (2) u (1), izlazi:

$$P + QY^{1/2} = 0, \tag{3}$$

gdje je

$$P = A^3 + 3AB^2Y + Ap + q$$

$$Q = 3A^2B + B^3Y + Bp.$$

Prema tome P i Q bi se moglo elementarno proizvesti pomoću veličina koje elementarno ne mogu proizvesti broj $Y^{1/2}$; na osnovu (3) znači to da je $P = 0$, $Q = 0$ (jer kad bi bilo $Q \neq 0$, bilo bi $Y^{1/2} = -PQ^{-1}$, tj. $Y^{1/2}$ bi se elementarno izrazilo). No iz $P = 0 = Q$ proizlazi da je i $P - QY^{1/2} = 0$, a to znači da i broj

$$x_1 = A - BY^{1/2} \tag{4}$$

zadovoljava (1). K tome je $B \neq 0$, jer bi inače, protivno gornjoj pretpostavci, i rješenje $x_0 = A$ bilo izražljivo elementarno bez $Y^{1/2}$. Na taj način imamo dva različita rješenja x_0, x_1, pa bi za treće rješenje x_2 iz relacije prema (2) i (3) izlazilo:

$$x_0 + x_1 + x_2 = 0$$ [1]

$$x_2 = -2A;$$

tj. x_2 bi bilo izrazivo i bez $Y^{1/2}$.

No, x_2 prema pretpostavci nije racionalan broj; pa neka je $t^{1/2}$ posljednje antikvadriranje, tako da bude $x_2 = a + bt^{1/2}$, $b \neq 0$, a da se $t^{1/2}$ ne može dobiti kao *racionalna* funkcija od a, b, p, q, t sa racionalnim koeficijentima. Radeći sada sa x_2 kao malo prije sa $x_0 = A + BY^{1/2}$, zaključili bismo da je i $a - bt^{1/2}$ jedno rješenje, a da bi treće rješenje glasilo $-2a$; no to treće rješenje bilo bi x_0 ili x_1, tj. $A + BY^{1/2}$, ili $A - BY^{1/2}$ pa bi se kao i izraz $-2a$ moglo dobiti i bez pojave $Y^{1/2}$ — protivno pretpostavci. Time smo došli do proturječja, a to znači da je teorem dokazan.

8.5. Na sasvim sličan način dokazuje se ovo poopćenje gornjeg teorema:

⟶ Teorem. *Ako kubni polinom nema nijedne nula-tačke u tijelu brojeva* [2] *koje proizvode njegovi koeficijenti, tada se nula-tačke polinoma ne mogu prikazati (računski ili crtanjem) na elementaran način pomoću koeficijenata.*

8.6. Pravilni sedmerokut ne može se nacrtati pomoću šestara i ravnala. Stvarno, ako vrh sedmerokuta uzmemo u tački 1, a središte u 0, tada su svi vrhovi nula-tačke binoma $x^7 - 1$; prema tome, ostali vrhovi $\neq 1$ zadovoljavaju jednadžbi $(x^7 - 1)(x - 1)^{-1} = 0$, tj.

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0.$$

---

[1] Suma $x_0 + x_1 + x_2$ je protivno jednaka koeficijentu od x^2 u (1); a taj je $= 0$.

[2] Tijelo brojeva koje proizvodi (rađa) zadani skup S brojeva je *najmanji skup* Z brojeva u kojem možemo vršiti sve 4 elementarne operacije (tj. rezultati moraju ostati u zajednici Z odakle se uzimaju i podaci) k tome treba biti $Z \supset S$.

No iz $x^7 = 1$ izlazi:

$$x^6 = x^{-1},\ x^5 = x^{-2},\ x^4 = x^{-3},$$

pa prethodna jednadžba za vrhove glasi:

$$x^{-1} + x^{-2} + x^{-3} + x^3 + x^2 + x + 1 = 0,$$

odnosno:

$$(x + x^{-1}) + (x^2 + x^{-2}) + (x^3 + x^{-3}) + 1 = 0. \tag{1}$$

Stavimo li

$$x + x^{-1} = y, \tag{2}$$

izlazi:

$$x^2 + x^{-2} = y^2 - 2$$

$$x^3 + x^{-3} = y^3 - 3y,$$

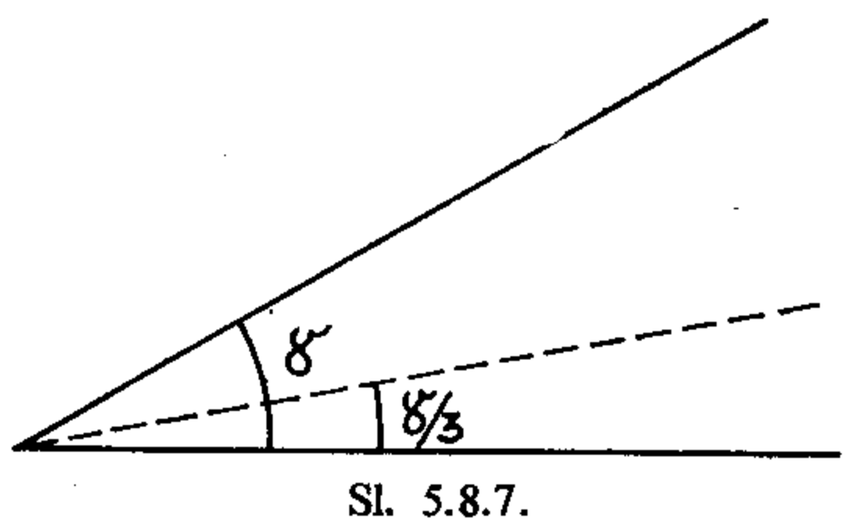
pa jednadžba (1) postaje:

$$y^3 + y^2 - 2y - 1 = 0. \tag{3}$$

To je kubna jednadžba s cijelim racionalnim koeficijentima. Lako se može pokazati da bi svako njeno *racionalno* rješenje moralo biti divizor broja -1 kao koeficijenta najnižeg ranga. No, divizori od -1 jesu 1 i -1, a oni očigledno nisu rješenja od (2). Prema tome, oslanjajući se na teorem 8.4, zaključujemo da se rješenja jednadžbe (3) ne mogu dobiti elementarno. To isto vrijedi i za jednadžbu (1) jer su na osnovu elementarne veze (2) rješenja od (3) izvediva elementarno iz rješenja jednadžbe (1). Time je uistinu dokazano da se pravilni sedmerokut ne može elementarno nacrtati (vidi poglavlje 18, § 6 kako se elementarno crta pravilni 17-kut!).

8.7. Trisekcija (trodioba) kuta. *Riječ je o problemu da se zadani kut* α *podijeli na* 3 *jednaka dijela, svaki veličine* $\alpha/3$.

Ako je kut prav, ispružen, pun, stvar je jednostavna. No već npr. za kut u istostraničnom trokutu stvar nije moguća: *kut od* $20°$ *ne možemo nacrtati elementarno*, tj. služeći se jedino šestarom i ravnalom kao pomoćnim sredstvima.



Sl. 5.8.7.

Radimo *analitički*. Iz

$$\cos(\alpha + \beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta$$

lako se vidi da je

$$\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi, \text{ tj. (umjesto } \varphi \text{ piši } \varphi/3\text{):}$$

$$\cos\varphi = 4\cos^3\varphi/3 - 3\cos\varphi/3. \tag{1}$$

Stavljajući $x = \cos\varphi/3,\ c = \cos\varphi,$

jednadžba (1) postaje:

$$4x^3 - 3x - c = 0.$$

Međutim, može se pokazati da ta jednadžba nema nikakva rješenja koje se *racionalno* izražava pomoću koeficijenata 4, 3 i *c*.

Zato prema teoremu 8.4. nije u općem slučaju moguće svaki kut podijeliti elementarno na tri jednaka dijela. (P. L. Wanzel, 1837).

Trodiobu kuta izvodio je Arhimed (* oko —287—212) uklapanjem, a Hipija (r. oko —460) i Papo (4. st) pomoću krivuljâ.

9. ALGEBARSKA JEDNADŽBA STUPNJA 5. OSVRT NA ALGEBARSKE JEDNADŽBE STUPNJA <5

I d e j a. Dosadašnja simbolika o jednadžbama stupnja <5 prenosi se automatski na jednadžbe stupnja 5, 6, . . . Tako je jasno da će algebarska jednadžba stupnja 5 sa x kao nepoznatom imati ovaj *ništični oblik* ili *nul-oblik*:

$$(1) \qquad a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 = 0, \ a_5 \neq 0.$$

Najjednostavniji je oblik kad su svi srednji koeficijenti $=0$; tada jednadžba postaje $a_0 = -a_5 x^5$ pa se odatle lako nalazi

$$x = (-a_5^{-1} a_0)^{1/5}.$$

Tu se pojavljuje potenciranje sa 1/5.

Nastaje problem: da li se svako rješenje jednadžbe (1) svodi na nizanje konačno mnogo racionalnih operacija i potenciranja sa 1/2, 1/3, 1/5? *Tek je u prošlom stoljeću dokazano da to nije moguće* (Abel, Ruffini). Da nam stvar bude psihološki bliža, vratimo se na jednadžbe stupnja <5.

Već jednadžba $2x = 1$ pokazuje da linearna jednadžba „*nad skupom D*“ cijelih brojeva ne mora „*u tom kolu*“ (skupu) biti rješiva. To znači: ako koeficijenti i jesu u D, rješenje ne mora biti u D.

No svaka linearna jednadžba nad skupom Q *racionalnih* brojeva rješiva je u Q, tj. ako je $ax = b$, $a \neq 0$ i $a, b \in Q$, onda je $x \in Q$.

No, već jednostavna *kvadratna* jednadžba $x^2 = 2$ nad skupom Q nije *u njemu* rješiva! Stvarno, kao što su već Grci pokazali, rješenje $2^{1/2}$ nije racionalan broj, nego leži izvan Q, u skupu iracionalnih brojeva.

Pogotovu opća kvadratna jednadžba $ax^2 + bx + c = 0$, $a \neq 0$ nad tijelom Q racionalnih brojeva ne mora imati rješenja u Q, pa čak ni u tijelu R svih realnih brojeva (kao što pokazuje jednadžba $x^2 + 2 = 0$). No, postoji ipak uska povezanost između *zadanih* koeficijenata i *traženog* rješenja: *rješenje se dobije pomoću prve* 4 *računske operacije i pomoću antikvadriranja izraza* $D = b^2 - 4ac$ (isto se to iskazuje i ovako: *rješenje svake kvadratne jednadžbe leži u tijelu što ga rađaju* (*generiraju*) *koeficijenti i diskriminanta jednadžbe*).

I kod kubnih jednadžbi pojavljuje se opet nova operacija: *antikubiranje* (potenciranje sa 3^{-1}). Kao što se antikvadriranje ne može svesti na elementarnije operacije — racionalne — tako se ni potenciranje sa 1/3 ne može svesti na racionalne operacije i antikvadriranje. No, *rješenje opće kubne jednadžbe svodi se na nizanje: racionalnih operacija, antikvadriranja i antikubiranja u konačnom broju.*

Isto to vrijedi i za jednadžbe stupnja 4.

Dugo se *tragalo i nastojalo pokazati* da se, analogno, i rješenje opće jednadžbe (1) stupnja 5 može izvesti iz koeficijenata jednadžbe (1) slaganjem racionalnih operacija i potenciranja sa 1/2, 1/3, 1/5. *Ruffini* (1813) i naročito *Abel* (1826) *najzad su pokazali da to nije moguće.* (v. 32, § 5.5.3.).

N. H. Abel (1802—1829), veliki norveški matematičar

Zanimljivo je napomenuti ovo: svaka zadana jednadžba (1) petog stupnja može se svesti na pripadni *Bring-Jerrardov* [Džerard] normalni oblik $y^5 - by - 1 = 0$ i da pri tom novi koeficijent b leži u onom tijelu brojeva koje proizvode koeficijenti zadane jednadžbe (drugim riječima: b se može iz koeficijenata a_0, a_1, a_1, a_3, a_4, a_5 dobiti vršeći s njima *konačan broj racionalnih* operacija).

10. HISTORIJAT JEDNADŽBI 3. I 4. STUPNJA

Opća algebarska jednadžba $p(x) = 0$ stupnja 3. i 4. riješena je u 16. st., i to u Italiji. Scipione dal Ferro (1465—1526) riješio je god. 1515. jednadžbu (1) $x^3 + ax = b$ i rješenje saopćio svojem učeniku Fioru; nezavisno od toga, nekoliko godina kasnije, N. Tartaglia je riješio jednadžbu (2) $x^3 + px^2 = q$. Fior je izazvao Tartagliu na takmičenje; Tartaglia je riješio i jednadžbu tipa (1); naprotiv, Fior nije umio da riješi jednadžbe oblika (2). Tartaglia je svoje rješenje saopćio Kardanu, koji ga je god. 1545. u djelu *Ars magna* saopćio kao vlastito rješenje. Doduše, Kardan je tu dao i *djelomičnu diskusiju* kubne jednadžbe, spoznao je da ona ima 3 rješenja, i naišao je na *nesvodljivi* (*ireducibilni*) *slučaj* kad se pojavljuje antikvadriranje negativnog broja. Tek god. 1572. je R. Bombelli riješio nesvodljivi slučaj. Bombelli je također uklonio koeficijent uz x^2. Jednadžbu stupnja 4 riješio je oko god. 1540. Ferrari (1522—1565).

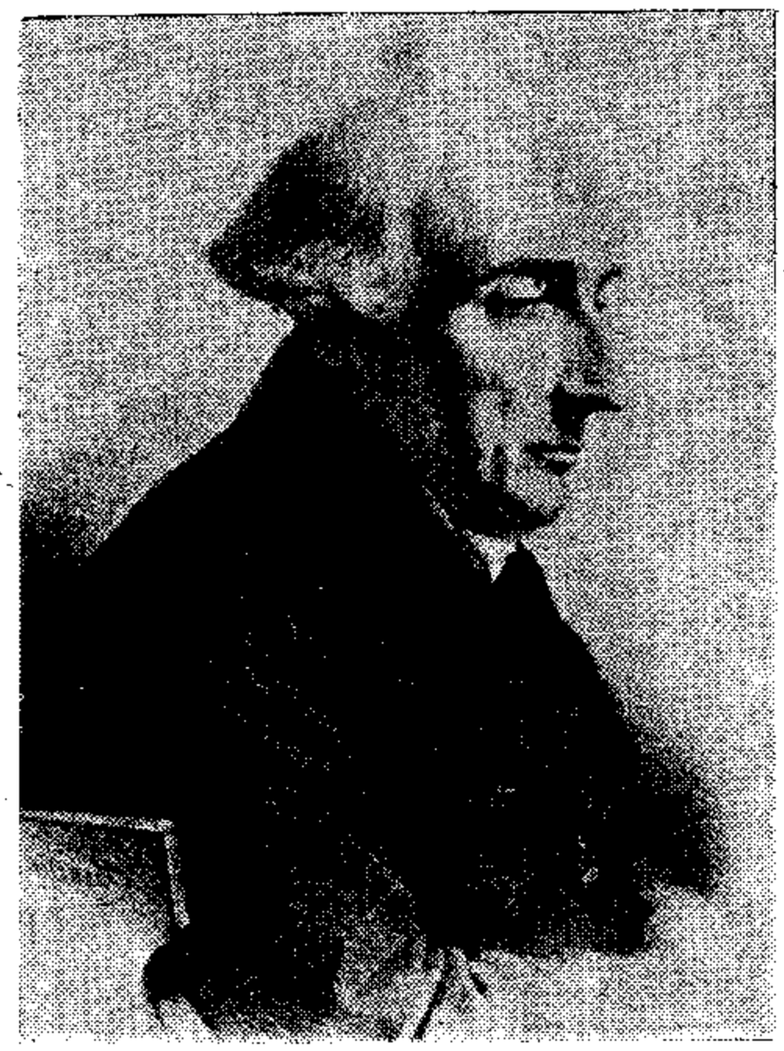
Time je Italija dala velik prilog matematici: uz jednadžbe stupnja 1 i 2, koje su prije toga bile riješene, došlo je do rješenja i jednadžba stupnja 3 i 4, i to na *sličnim principima*: *rješenja se iz koeficijenata izražavaju pomoću konačnog broja algebarskih operacija.* Tek kasnije se saznalo (Ruffini, 1813. nepotpuno, i Abel, 1826) da se time došlo i do *kraja jedne metode*, jer se već *jednadžbe stupnja 5 ne mogu na tom principu riješiti.*

U historiji kubne jednadžbe treba istaknuti rješenje što ga je god. 1770. i 1771. dao J. L. Lagrange [Lagranž][1] (1736—1813); ono je osnovano na sasvim drugim gledištima.

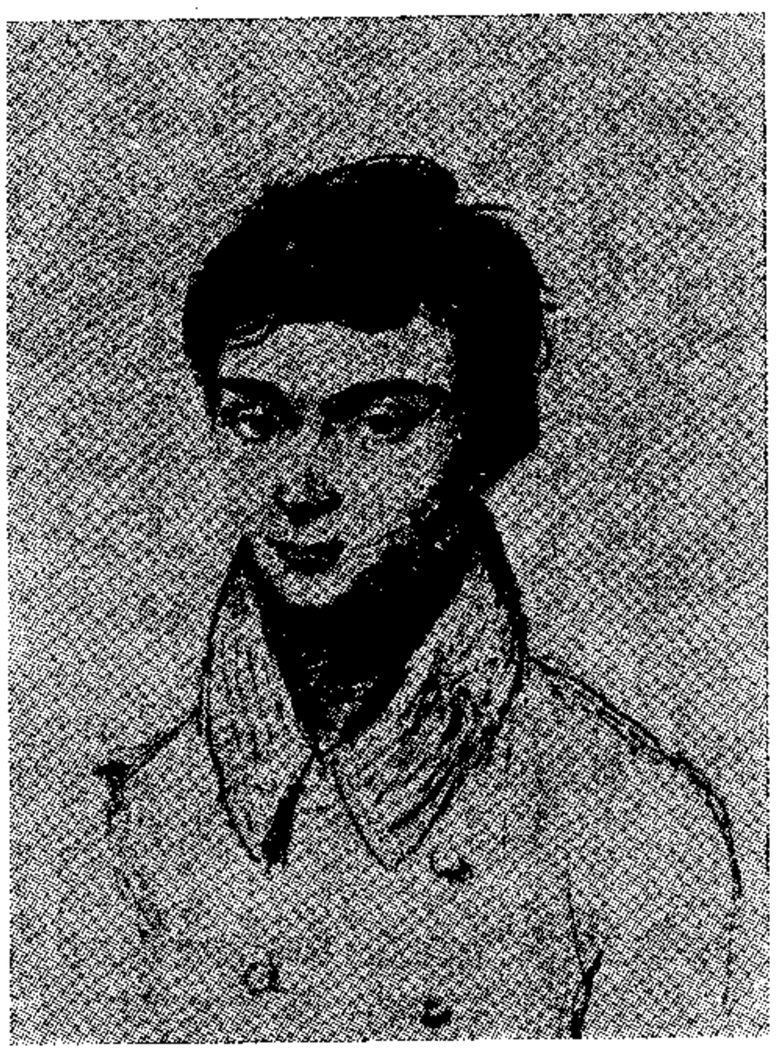
Posebno mjesto u historijatu (kubnih) jednadžbi zauzima pitanje da li se zadana (kubna) jednadžba može riješiti „*elementarno*“, i to računom ili crtnjom. Već najjednostavniji slučaj koji nije trivijalan: $x^3 = 2$ poznat je od davnina. Riječ je o tome da se konstruira kocka koja je po sadržini dvaput veća od

[1] L. Lagrange: *Reflexion sur la résolution algébrique des équations* (*Razmišljanja o algebarskom rješenju jednadžbâ*).

zadane kocke (*delhijski problem*). Iz dokazanog teorema 8.5 lako proizlazi da se pomoću lineala i šestara, a bez upotrebe drugih instrumenata, ne može kocka podvostručiti. To je historijski zanimljiv slučaj: dokazati da nešto nije moguće![1)]



J. L. Lagrange (Lagranž), (1736—1813), slavni francuski matematičar.



Evariste Galois (Galoa), (1811—1832), jedan od najdarovitijih matematičara uopće.

Svojim putem udario je mlađahni Galois[2)]. On je utro put novoj metodi i novoj nauci: *teoriji grupa* pa je na tom općem jeziku i širokom *novom području* lako riješio i stari problem o rješavanju algebarskih jednadžbâ (v. 32 § 5.4.2.). Galoisove ideje vanredno su proširile okvire matematike i njenih primjena!

11. EKVIVALENTNOST ILI RAVNOVALJANOST JEDNADŽBI

11.1. D e f i n i c i j a. Dvije jednadžbe su ekvivalentne ili ravnovaljane, ako su ispunjena ova dva uslova:

1) obje jednadžbe imaju ista rješenja tj. svaki izraz koji zadovoljava jednu jednadžbu zadovoljava i drugu jednadžbu;
2) kolika je kratnost jednog rješenja u jednoj jednadžbi isto je tolika kratnost toga rješenja u preostaloj jednadžbi.

[1)] S toga gledišta spominjemo ove dvije osnovne matematičke tekovine: a) Starogrčku spoznaju da ima dužinâ (npr. stranica i dijagonala kvadrata) bez ikoje zajedničke mjere (otkriće nesumjerljivih—inkomenzurabilnih—veličinâ i iracionalnih brojeva!).—b) Svijesno saznanje: Dokazati da se Euklidov postulat o paralelama ne može dokazati (Lobačevski, 1829) i da zato postoji bar jedna geometrija različna od Euklidove.

[2)] Evariste Galois [Evarist Galoa] (1811—1832), francuski matematičar, poginuo je u dvoboju; jedna od najblistavijih figura u matematici!

Isto tako se definira ekvivalentnost jednog sistema jednadžbi s drugim sistemom jednadžbi.

Specijalno, svaka jednadžba koja nema rješenja ekvivalentna je sa svakom drugom jednadžbom koja ne dopušta rješenja.

Npr. jednadžba $(x-2)\ (x+3)^2=0$ nije ekvivalentna s jednadžbom $(x-2)^2\ (x+3)=0$, premda obje jednadžbe imaju ista rješenja: brojevi $2, -3$ zadovoljavaju obje jednadžbe; međutim, kratnost rješenja nije ista; kratnost od 2 je 1 u prvoj jednadžbi a 2 u drugoj jednadžbi; kratnost broja -3 u prvoj jednadžbi je 2, a u drugoj 1.

11.2. Relacija ekvivalentnosti među jednadžbama odnosno među sistemima je: refleksivna, simetrična i tranzitivna.

11.3. T e o r e m. Jednadžba prelazi u ravnopravnu jednadžbu ako na obje strane jednadžbe pribrojimo jedan te isti broj ili brojevni izraz.

11.4. T e o r e m. Ako se jednadžba pomnoži sa brojem $\neq 0$ ili brojevnim izrazom koji ne može biti 0, prelazi jednadžba u ekvivalentnu jednadžbu.

11.5. T e o r e m. *Neka je* (1) $J_1=J_2$ *jednadžba a f izraz kojeg ne poništava nikoje rješenje jednadžbe* (2) $f\cdot J_1=f\cdot J_2$; *tad su jednadžbe* (1) *i* (2) *međusobno ravnovaljane.*

D o k a z. Jasno je da svako eventualno rješenje jednadžbe (1) zadovoljava jednadžbu (2) i to ne s manjom kratnosti. U drugu ruku, iz (2) proizlazi $f\cdot(J_1-J_2)=0$; no prema pretpostavci prvi faktor f ne može postati 0; zato je drugi faktor $=0$ tj. $J_1-J_2=0$ što znači da vrijedi (1).

Primjer.

$$\frac{1}{a}+\frac{1}{a+x}+\frac{1}{a+2x}=0; \quad x=?$$

Naravno da se ne dopušta da ikoji od izrazâ a, $a+x$, $a+2x$ bude $=0$. Zato je i produkt f tih izraza $\neq 0$ pa se množenjem zadane jednadžbe sa f dobije ravnovaljana jednadžba

$$(a+x)\ (a+2x)+a(a+2x)+a(a+x)=0.$$

Odatle

$$2x^2+6ax+3a^2=0$$

te najzad

$$x_1=\frac{a}{2}(\sqrt{3}-3), \qquad x_2=-\frac{a}{2}(\sqrt{3}+3).$$

Prema tome, zadana jednadžba ima gornja dva rješenja.

11.6. T e o r e m. *Ako je S sistem jednadžbi, P njegov dio sastavljen od jedne ili više jednadžbi sistema S; ako se P zamijeni ekvivalentnim sistemom P', prelazi time i čitav sistem S u ekvivalentan sistem S'.*

11.7. T e o r e m. Ako jednadžba S ili sistem S jednadžbi nema rješenja, tad je bez rješenja i svaki sistem S' u kojem se S nalazi kao sastavni dio.

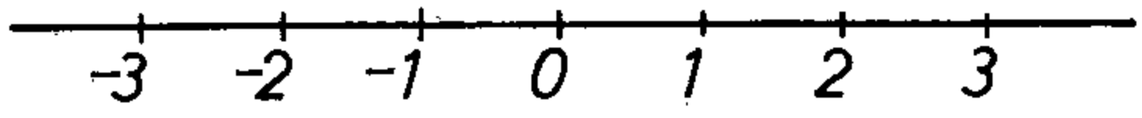
POGLAVLJE 6.

KOLO ILI PRSTEN CIJELIH RACIONALNIH BROJEVA

Riječ je o skupu D svih cijelih racionalnih brojeva[1] koji — uređeni po veličini — glase: ... —2, —1, 0, 1, 2, 3, 4, ...

1. SMJEŠTAVANJE KOLA D NA BROJEVNOJ PRAVULJI I BROJEVNOM n-VRHU

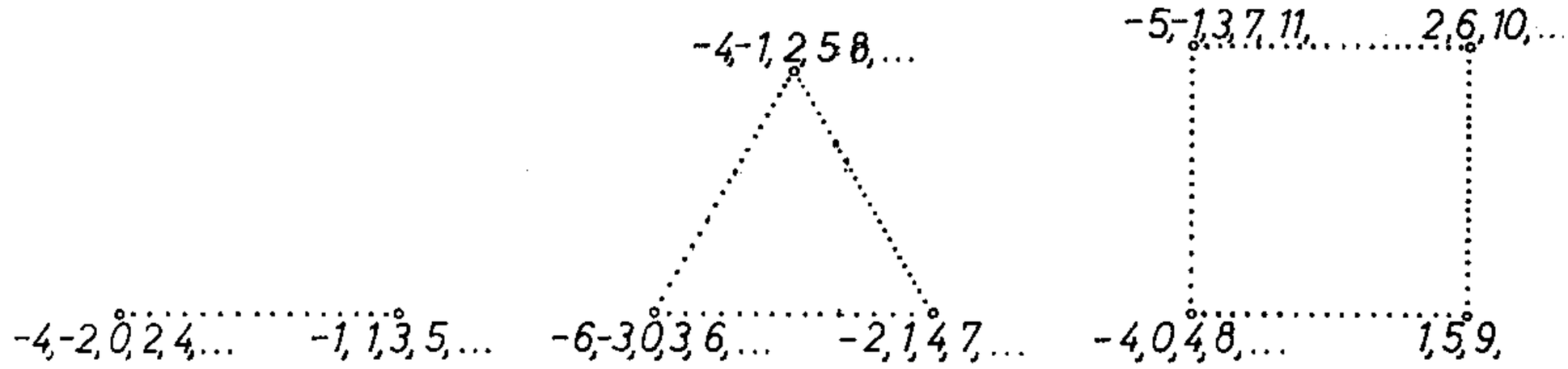
Članove kola D možemo smjestiti na *brojevnoj pravulji*



Sl. 6.1.

ili na proizvoljnom pravilnom n-vrhu ($n = 2, 3, 4, \ldots$) tj. na skupu vrhova pravilnog n-terokuta.

Smjestiti D na n-vrhu znači da sve članove množine D stavljamo u zadanih n tačaka, vrhova, i to ovako: u dva susjedna vrha stave se brojevi 0 i 1, a zatim se idući od 0 preko 1 do narednog vrha stavi 2, pa dalje 3, pa 4, itd. Idući obrnutim smjerom po obodu od 1 do 0, stavi se na svaki vrh na koji naiđemo svaki put naredni broj.



Sl. 6.2.

Na slici je pokazano kako stvar izgleda za 2-vrh (dvovrh), 3-vrh (trovrh), i 4-vrh (četverovrh). Tako vidimo da kod 2-vrha svi parni cijeli brojevi

---

[1] Oznaka D ima nas podsjetiti da je riječ o skupu *diferencija* svih parova prirodnih brojeva. Slična je oznaka N za skup svih prirodnih ili naturalnih brojeva. Kod skupa Q svih *racionalnih* brojeva bit će riječ o kvocijentima (*quotiens*) cijelih brojeva. Zato je lako upamtiti oznake N, D, Q. Neka In označuje početni ili *inicijalni* interval svih brojeva 0, 1, 2, ... koji su $< n$. Npr. $I\,2 = \{0, 1\}$, $I\,10 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, In se zove »*cifarski skup za bazu n*«.

dolaze na isti vrh, svi neparni brojevi zauzimaju preostali vrh. Kod 3-vrha dolaze brojevi 0, 1, 2 na različite vrhove; zajedno s 0 leže svi ovi brojevi:

$$\ldots,\ 3\cdot -3,\ 3\cdot -2,\ 3\cdot -1,\ 0,\ 3\cdot 1,\ 3\cdot 2,\ 3\cdot 3,\ 3\cdot 4,\ \ldots$$

Skup svih tih brojeva možemo označiti sa $3D$. Zajedno s brojem 1 leže brojevi

$$4=3+1,\ 7=3\cdot 2+1,\ 10=3\cdot 3+1,\ 13=4\cdot 3+1,\ \ldots$$

i brojevi

$$-2=3\cdot -1+1,\quad -5=3\cdot -2+1,\ \ldots$$

Sam taj skup možemo označiti sa $3D+1$. Treći vrh brojevnog 3-vrha zauzimaju brojevi množine

$$3D+2;$$

pri tom $3D+2$ znači skup svih brojeva oblika $3\cdot x+2$, pri čemu je x iz D.

Ukratko, u vrhovima brojevnog 3-vrha nalaze se skupovi

$$3D,\quad 3D+1,\quad 3D+2$$

cijelih brojeva; oni zajedno iscrpljuju kolo D:

$$3D\cup(3D+1)\cup(3D+2)=D.$$

Naravno, ti su skupovi bez zajedničkog člana, jer je svaki član iz D smješten na posve određen jedan jedini vrh.

2. RAZREDI ILI KLASE CIJELIH BROJEVA

2.0. Kao što smo skup D razdijelili u razred $2D$ svih parnih brojeva i razred $2D+1$ svih neparnih brojeva, tako sada vidimo da skup D možemo razdijeliti u tri razreda:

razred $3D$ svih brojeva $3\cdot x$, gdje je $x\in D$

razred $3D+1$ svih brojeva $3\cdot x+1$, gdje je $x\in D$

razred $3D+2$ svih brojeva $3\cdot x+2$, gdje je $x\in D$.

Govorimo o *tri razreda cijelih brojeva prema modulu* 3, misleći pri tom na ulogu broja 3, odnosno 3-vrha pri toj podjeli.

2.1. Zato bismo analogno mogli govoriti o dva razreda brojeva prema modulu 2, no u tom slučaju imamo i jednostavniji način izražavanja: *parni* i *neparni* brojevi.

2.2. Primijetimo da svi brojevi istog razreda padaju zajedno — podudarni su (kongruentni su) — i nalaze se na jednom te istom mjestu 2-vrha, odnosno 3-vrha.

2.3. Sasvim je slična situacija s brojevnim 4-vrhom; njegove vrhove zauzimaju skupovi:

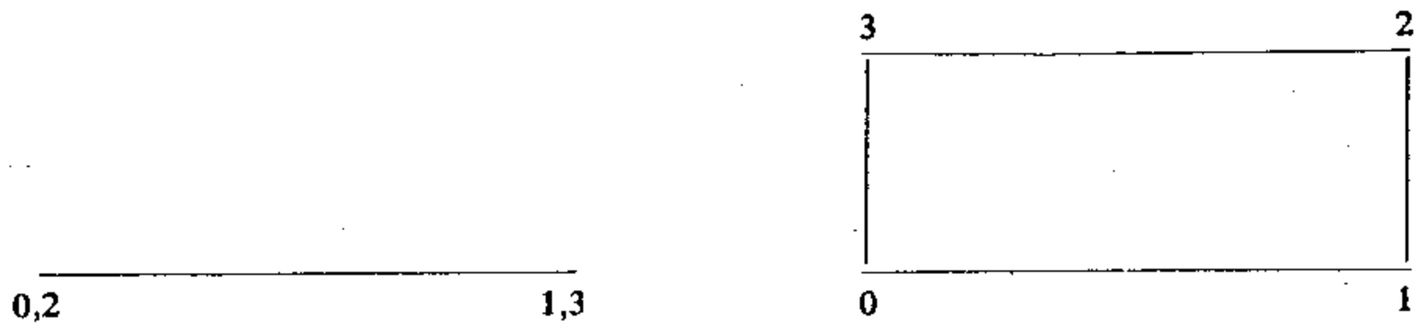
$4D$ $=\{\ldots, 4\cdot(-2), 4\cdot(-1), 0, 4\cdot 1, 4\cdot 2, \ldots\}$

$4D+1=$ skup svih brojeva $4\dot{D}+1$

$4D+2=$ skup svih brojeva $4\dot{D}+2$

$4D+3=$ skup svih brojeva $4\dot{D}+3$; pri tom $\dot{D}$ prolazi kroz D.

Ujedno vidimo da sadržaj od po dvije tačke 4-vrha dolazi u 2-vrhu zajedno:



Npr. brojevi 0, 2 ne padaju zajedno u 4-vrhu, ali padaju zajedno u 2-vrhu.

2.4. Za vježbu promatraj brojevni 6-vrh i 8-vrh te porazmjesti na njegovim vrhovima skup D i formiraj pripadne razrede cijelih brojeva prema modulu 8.

2.5. Slikovita definicija razredâ ili klasâ prema zadanom modulu *m*. Definicija. Neka je m prirodni broj >2; tada pod razredima ili klasama cijelih brojeva prema modulu m razumijevamo svih m množina cijelih brojeva što padaju u vrhove brojevnog m-vrha; svi parni brojevi i svi neparni brojevi čine po jedan razred prema modulu 2; kaže se također da skup D svih cijelih brojeva čini razred prema modulu 1. Nadalje se kaže da jednočlani skup $\{0\}$ čini razred prema modulu 0.

Važno je uočiti, prvo, da svih m razredâ prema modulu m iscrpljuje čitavo kolo D i drugo, da dva takva razreda prema *istom modulu* nemaju ni jednoga zajedničkog člana.

3. KAKO IZGLEDAJU RAZREDI CIJELIH BROJEVA?

3.1. Razred parnih brojeva je skup $2D$ svih cijelih brojeva oblika $2\dot{D}$ (razumijeva se da $\dot{D}$ prolazi čitavim skupom D, da je $\dot{D}=0, \pm 1, \pm 2, \ldots$). Razred neparnih cijelih brojeva je skup $2D+1$ svih cijelih brojeva $2\dot{D}+1$. Drugim riječima, razredi cijelih brojeva prema modulu 2 jesu skupovi:

$$2D, \quad 2D+1.$$

I svaki cio broj je unutra: on je *ili paran* (dakle u $2\dot{D}$) *ili neparan* (tj. u $2D+1$).

3.2. Razredi cijelih brojeva prema modulo 3 jesu ova tri skupa:

skup $3D$ svih 3-kratnika $3\dot{D}$ cijelih brojeva

skup $3D+1$ svih brojeva $3\dot{D}+1$

skup $3D+2$ svih brojeva $3\dot{D}+2$.

Dalje nema smisla ići jer je skup $3D+3$ svih brojeva $3\dot{D}+3$ upravo $3D$ (kad se na brojevnom trokutu učine 3 koraka, dolazi se natrag). Isto tako

$$3D+4=3D+1, \quad 3D+5=3D+2, \text{ itd.}$$

Tako vidimo da se za svaki cijeli broj x množina $3D+x$ svih brojeva $3\dot{D}+x$ podudara s jednim od tri razreda:

(1) $$3D, \quad 3D+1, \quad 3D+2.$$

3.3. Time smo otkrili zaista zanimljivu činjenicu: preslikavanje

(2) $$x \to 3D+x$$

kola D cijelih brojeva u sama sebe ima za vrijednosti uvijek jedan od tri razreda i pri tom je, naravno, x u $3D+x$ jer za $\dot{D}=0$ imamo $x=3\cdot 0+x$. Drugim riječima, pridružimo li broju x razred $3D+x$, znači to upravo naći onaj „razred prema modulu 3“ (zapravo onaj vrh 3-vrha) u kojem je smješteno x.

Pri tom preslikavanju ne mijenja se $3D$, pa preslikavanje ima oblik:

$$x \to \text{„konstanta“} + x$$

(samo je ta »*konstanta*« skup $3D$ svih trokratnika cijelih brojeva).

3.4. Protuoblast funkcije (2) je tročlan skup (1) ili geometrijski: ono što je na vrhovima 3-vrha!

3.5. Slična je situacija s pridruživanjem:

$$\dot{D} \to 4D+\dot{D}$$

i uopće:

$$\dot{D} \to mD+\dot{D}.$$

Tu će svakom $\dot{D}$ ($\dot{D}$ je svaki cijeli broj) biti pridružen sadržaj na onom vrhu m-vrha na kojem je smješteno i $m+\dot{D}$.

3.6. Kongruentni brojevi. Ako su brojevi a, b smješteni na istom vrhu m-vrha, kaže se da su *podudarni* (*kongruentni*) *prema modulu m* i piše:

$$a \equiv b \pmod{m}.$$

(Zamršen način pisanja, bar na prvi pogled; no vrlo je praktičan, kao što ćemo se uvjeriti. Pojam i oznaku kongruencije brojeva uveo je K. F. Gauss, njem. matematičar 18/19. st.)

3.7. Aritmetičke biprogresije. Ako pogledamo razrede prema modulu 2, dobivamo dvije „aritmetičke biprogresije “[1]) s razlikom 2:

$$\ldots, -6, -4, -2, 0, 2, 4, 6, 8, \ldots$$
$$\ldots, -3, -1, 1, 3, 5, 7, \ldots$$

---

[1]) Svaku funkciju kojoj je oblast skup D cijelih brojeva zovemo *biprogresija*. Biprogresija je *aritmetička* (*geometrijska*) ako je diferencija (kvocijent) svakog člana i člana pred njim ista. Ta se konstanta zove *diferencija* (*kvocijent*) biprogresije.

Isto je s razredima „modulo 3“: dobivamo 3 aritmetičke beskonačne biprogresije diferencije 3 (susjedni se članovi razlikuju za 3). Evo tih biprogresija (svaku biprogresiju počni s 0, odnosno s najmanjim brojem ≥ 0):

$$\ldots, \ -6, \ -3, \ 0, \ 3, \ 6, \ldots$$

$$\ldots, \ -5, \ -2, \ 1, \ 4, \ 7, \ldots$$

$$\ldots, \ -4, \ -1, \ 2, \ 5, \ 8, \ldots$$

Dalje ništa, jer su svi brojevi iscrpeni!

Slika je analogna za „module“ 4, 5, ...

Svi članovi klase tvore beskonačnu biprogresiju kojoj je razlika upravo „modul“ *m*. To znači da se svaka dva člana biprogresije razlikuju za kratnik modula *m*. Drugim riječima, razlika bilo kojih članova iz iste klase djeljiva je sa *m*.

Geometrijski je stvar jasna: na *m*-vrhu smješteni su upravo brojevi kojima je razlika djeljiva sa *m*.

3.8. Sad možemo najzad zapisati pravu definiciju, koja će vrijediti i u slučajevima kad je situacija zamršenija (npr. s polinomima).

3.9. Definicija kongruentnosti. *Kaže se da je a podudarno ili kongruentno sa b prema modulu m i piše*:

$$a \equiv b \pmod{m} \tag{3}$$

ako je razlika a—b djeljiva sa m, tj. ako je

$$a = b + m\,\dot{D} \tag{3'}$$

($\dot{D}$ označuje neki cio broj).

Ako a nije kongruentno sa b prema modulu m, kaže se da je a inkongruentno (*nepodudarno*) *sa b modulo m i piše*

$$a \ non \equiv b \pmod{m}. \tag{4}$$

Specijalno, $a \equiv 0 \pmod{m}$ znači da je *a djeljivo sa m*,

$a \ non \equiv 0 \pmod{m}$ znači da *a nije djeljivo sa m*.

Prema tome, treba imati na umu da relacija (3) znači isto što (3'), s tom razlikom što u (3') ipak još ulazi u račun i (poznat ili nepoznat) određen cio broj $\dot{D}$. To treba uvijek imati na umu. Tako npr. sada znamo da „Gaussova rečenica“ $13 \equiv 3 \pmod{5}$ iskazuje jednu istinu, naime činjenicu da je $13-3$ djeljivo sa 5, odnosno $13 = 3 + 5\,\dot{D}$. Naprotiv, rečenica (relacija) $13 \equiv 0 \pmod{5}$ nije istinita jer razlika $13-0$ nije djeljiva sa 5.

Također stoji $x^2 \equiv 1$ (*modul* $x-1$) jer je algebarski polinom x^2-1 djeljiv s $x-1$: kvocijent je polinom $x+1$, itd.

⟶ **3.10.** Osnovna definicija: **klasa ili razred prema zadanom modulu *m*.** Razred ili klasa zadanog skupa *S* prema zadanom modulu *m* jest skup svih članova iz *S* kojima je razlika djeljiva sa *m*.

Prema tome, ako je A razred množine S u odnosu na modul m, onda iz $x\in A$, $y\in A$ izlazi da je $x-y$ djeljivo sa m; obrnuto: ako za x, $y\in S$ znamo da je razlika $x-y$ djeljiva sa m, onda x, y leže u istom razredu.

Tako npr. brojevi $2\dot{D}+1/2$ čine određen razred skupa R realnih brojeva; označuje se sa $2D+1/2$; $2D+1/3$ je jedan drugi razred; $2D+2/3$ je opet jedan razred disjunktan od prethodnih. Svi međusobno različiti razredi množine R u odnosu na broj 2 kao modul jesu skupovi $2D+x$, pri čemu je $x\in R[0, 2)$, tj. x je bilo koji realan broj za koji je $0\leq x<2$.

Napose često imamo posla s razredima mod 2π, mod 360, mod 24 i mod 12.

To su osnovne definicije. Vrijedit će i u mnogo zamršenijim „kolima“, a ne samo u kolu D cijelih brojeva. Brojevi

$$\ldots,\ -7,\ -1,\ 5,\ 11,\ 17,\ 23,\ \ldots$$

čine jedan razred cijelih brojeva za 6 kao modul. Isto to čine, naravno, brojevi

$$\ldots,\ -3,\ 3,\ 9,\ 15,\ \ldots$$

Naime, razlika bilo kojih dvaju od tih brojeva djeljiva je sa 6, a za svakog od njih oduzimanje ili dodavanje modula 6 daje opet određen član zadane skupine.

Od naročite su važnosti razredi oblika $mD=$ skup svih $m\dot{D}$, tj. u tim se razredima nalazi broj 0.

3.11. Kako izgleda razred? — 3.11.0. Recimo da radimo s modulom 6 (skiciraj 6-vrh). Kako izgleda razred u kojem leži neki zadani broj, npr. 17? U isti razred spadaju brojevi $\pm 6+17$, $2\cdot 6+17$, ..., jer ako od tih brojeva oduzmemo 17, diferencija je oblika ± 6, $\pm 2\cdot 6$, $\pm 3\cdot 6$, ..., a to je sve djeljivo sa 6. Dakle, razred u kojem je 17 sadržava sve brojeve $6\dot{D}+17$; međutim, drugih članova u razredu i nema.

Naime, ako je x podudarno sa 17, tj. ako je $x-17$ djeljivo sa 6, dakle $x-17=6q$, onda to znači da je $x=6q+17$, tj. x je oblika $6\dot{D}+17$.

Zaključak je općenit, pa ga možemo napisati:

—→ **3.11.1.** Teorem. *Neka za brojeve m, a oznaka $mD+a$ služi za skup svih vrijednosti $m\dot{D}+a$ (to znači da $\dot{D}$ prolazi skupom D cijelih brojeva), tada je $mD+a$ upravo onaj razred za modul m u kojem leži broj a (drugim riječima, u onoj tački m-vrha u kojoj je broj a smješten, smješten je upravo skup $mD+a$).*

Tako i imamo razrede:

$2D$, $2D+1$ za modul 2

$3D$, $3D+1$, $3D+2$ za modul 3

$4D$, $4D+1$, $4D+2$, $4D+3$ za modul 4, itd.

Govorit ćemo naprosto o razredima; a koeficijent od D ukazuje na „modul“ prema kojem se razred tako imenuje.

3.11.2. Zanimljivo je uočiti, npr., da razredi $4D$, $4D+2$ daju zajedno upravo razred $2D$ parnih brojeva; isto je tako razred $2D+1$ neparnih bro-

jeva sastavljen od dva dijela: $4D+1$, $4D+3$. To se može i formalno zapisati:

$$2D = 4D \cup (4D+2)$$

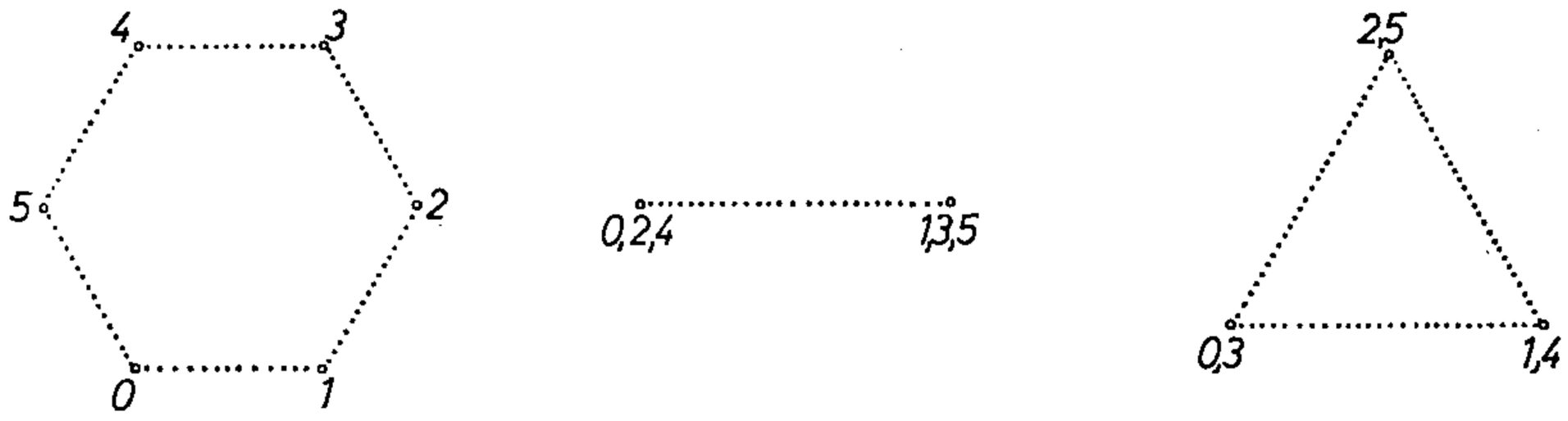
$$2D+1 = (4D+1) \cup (4D+3); \quad \cup \text{ je znak za uniju.}$$

Također uoči da se brojevi 0, 1, 2, 3, 4, 5 s različitih tačaka 6-vrha raspoređuju u tačke 2-vrha ovako: brojevi 0, 2, 4 dolaze u jednu tačku, a brojevi 1, 3, 5 u drugu tačku 2-vrha.

Isti ti brojevi raspoređuju se u tačkama 3-vrha ovako:

0,3; pa 1,4; pa 2,5.

Slikovito to odmah vidimo:



Sl. 6.3.11.2

Ta jednostavna stvar, prenesena na razrede, iskazuje se ovako:

Tri razreda $6D$, $6D+2$, $6D+4$ za modul 6 daju zajedno jedan razred, i to $2D$ za modul 2; preostala 3 razreda prema modulu 6, tj. skupovi $6D+1$, $6D+3$, $6D+5$, daju drugi razred za modul 2; ili ovako: svaki razred za modul 2 *cijepa se* u 3 razreda za modul 6.

Slično je s vezama između razreda za modul 6; npr., razred $3D$ se cijepa u $6D$ i $6D+3$, tj. $3D = 6D \cup (6D+3)$; isto tako (vidi sliku 6.3.11.2) $3D+1 = (6D+1) \cup (6D+4)$, $3D+2 = (6D+2) \cup (6D+5)$.

3.12. Prva svojstva relacije kongruentnosti. — **3.12.0.** Formalno, relacija kongruentnosti podsjeća nas na relaciju jednakosti, specijalno, ako ne gledamo dodatak „mod m“. Pa ako se modul m u toku nekih razmatranja ne mijenja, može ga se i ispustiti, tj. ne treba ga svaki put ispisivati. U tom slučaju relacija kongruencije (3) postaje nam znatno „bliža“ pa očekujemo da će vrijediti analogni zaključci kao kod jednakosti. Npr., ako je $845 \equiv 2 \pmod 3$, $2 \equiv 17 \pmod 3$, izlazi li odatle da je $845 \equiv 17 \pmod 3$? Diferencija je $845 - 17 = 828 = 3 \cdot 276$, tj. $845 \equiv 17 \pmod 3$.

3.12.1. Teorem.

(1) $a \equiv a \pmod m$ (refleksivnost ili povratnost)

(2) $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$ (simetrija)

(3) $a \equiv b \pmod m$, $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$ (tranzitivnost ili prelaznost).

D o k a z. Oznaka $a \equiv a$ (zapravo $a \equiv a \pmod{m}$) kaže da je $a-a$ djeljivo sa m; a to je istinito jer je 0 djeljiva svakim brojem $m \neq 0$.

Druga je relacija također ispravna: ako je $a-b$ djeljivo sa m, tj. ako je $a-b = m \cdot q$, gdje je q cio broj, onda je i $b-a$ djeljivo sa m jer je $b-a = m \cdot (-q)$; kako je q cio broj, cio je i kvocijent $-q$.

Treće svojstvo (tranzitivnost) dokazuje se na sličan način: $a \equiv b$ znači da je razlika $a-b$ djeljiva sa m, tj. $a-b = m \cdot q$ (q cio broj); $b \equiv c$ znači da je $b-c = m \cdot r$ (r cio broj); nađimo $a-c = (b+mq)-(b-mr) = m(q-r)$, tj. $a-c = m(q-r)$, tj. kvocijent od $a-c$ i m je zaista cio broj. A to znači da je $a \equiv c \pmod{m}$.

No, kongruencije s istim modulom zbrajaju se i množe kao jednakosti:

3.12.2. T e o r e m. Iz

(1) $$a \equiv b \pmod{m}$$

(2) $$a' \equiv b' \pmod{m}$$

izlazi:

(3) $$a + a' \equiv b + b' \pmod{m}$$

(4) $$aa' \equiv bb' \pmod{m}.$$

Stvar se svodi na jednakosti. Prva relacija kaže da je

(5) $$a = b + mq;$$

druga kaže da je

(5′) $$a' = b' + mq',$$

gdje su q, q' određeni cijeli brojevi; a treća tvrdi da je

$$a + a' = (b + b') + mr \quad \text{sa} \quad r \in D.$$

No, ta je tvrdnja očigledna: dovoljno je zbrojiti prethodne dvije jednadžbe (5), (5′). Isto tako, pomnožimo li međusobno jednadžbe (5), (5′), izlazi:

$$aa' = (b + mq)(b' + mq') = bb' + m(bq' + qb' + mqq'),$$

tj.

$$aa' = bb' + m\,\dot{D},$$

gdje $\dot{D}$ označuje cijeli broj iz prethodne zagrade. Dakle je relacija (4) o množenju kongruencija zaista ispravna.

Tako je npr. očigledno

$$10 \equiv -1 \pmod{11}.$$

Odatle kvadriranjem:

$$10^2 \equiv 1 \pmod{11};$$

pomnožimo li to s prvom kongruencijom, izlazi:

$$10^3 \equiv -1 \pmod{11} \text{ itd.}$$

$$10^n \equiv (-1)^n \pmod{11}.$$

Naravno da iskazi analogni onima iz § 3.12.2. za 3,4, ... kongruencija također vrijede. Specijalno, odatle izlazi da se kongruencije smiju množiti cijelim brojem i potencirati cijelim brojem:

3.12.3. Teorem. Iz

(6) $a \equiv b$, *izlazi*:

(7) $ak \equiv bk$ *za svaki cijeli broj* k

(8) $a^k \equiv b^k$ *za svaki cijeli broj* $k \geq 0$.

Važna primjedba. Pri gornjim razmatranjima o kongruencijama nismo dirali u modul m. Kod jednadžbi se ne samo iz (6) prelazi na (7), nego i obratno: za svako $k \neq 0$ dolazi se iz (7) na (6) dijeljenjem sa $k \neq 0$. Za kongruencije to ne vrijedi; npr., $24 \cdot 3 \equiv 12 \pmod{12}$ vrijedi, ali ne vrijedi $24 \equiv 4 \pmod{12}$.

Jedan od osnovnih teorema o cijelim brojevima kaže da se iz (7) dolazi na (6) ako su k i m cijeli brojevi bez ikakva zajedničkog djelioca $\neq 1$ (osnovni teorem o djeljivosti produkta, § 11.5).

3.13. O predstavnicima razreda za zadan modul *m*.

1. Brojevi

(1) $$0, 1, 2, \ldots, m-1$$

imaju ova tri svojstva: 1) brojevi (1) međusobno su nekongruentni, 2) svaki cio broj kongruentan je s nekim članom iz (1), 3) svaki broj iz (1) je najmanji neodrečni član razreda modulo m u kojem taj član dolazi.

Kraće se kaže: brojevi (1) čine *potpun skup najmanjih predstavnika* (*ostataka*) *modulo m.*

2. Definicija. *Svaki skup od m nekongruentnih brojeva modulo m zove se potpun skup predstavnika modulo m.* Prvih m članova niza $0, 1, -1, 2, -2 \ldots$ zove se *potpun skup po modulu najmanjih predstavnika modulo m.*

Tako npr. brojevi 1, 3, 5 su tri najmanja predstavnika mod 6; no oni ne čine *potpun* skup predstavnika; potpun skup najmanjih predstavnika po modulu glasi: $0, 1, -1, 2, -2, 3$. Brojevi 2, 9, 13 18, 28, 35 čine potpun skup predstavnika mod 6.

⟶ 3. Teorem. *Zadani skup S prirodnih brojeva je potpun skup predstavnika modulo m onda i samo onda ako su ispunjena ova dva svojstva:*

Prvo svojstvo: *S ima jedan jedini član iz svakog razreda mod m;*

Drugo svojstvo: *Drugih članova S nema.*

Može se reći da S nastaje *odabiranjem*, skupljanjem po jednog člana iz **svakog** razreda modulo m.

3.14. Zadaci o cijelim brojevima i o razredima ili klasama.

1. Šta znači: 1) $2D$; 2) $2D+4$; 3) $2D+5$; 4) $3D$; 5) $3D-5$; 6) $3D+100$?

2. Da li je 1) $3D \supset 6D$; 2) $3D+1 \supset 6D$; 3) $3D+2 \supset D+4$; 4) $3D+2 \supset 6D+5$?

3. Koji su članovi niza $2D$; $2D+1$; $3D$; $3D+1$; $3D+2$; $4D$; $4D+1$; $4D+2$; $4D+3$ međusobno disjunktni a koji nisu?

4. Da li iz $x, y \in 6D$ slijedi $x \equiv y \pmod 6$? Vrijedi li obrat?

5. Odredi članove ovog niza u kojima leži broj 100: $2D$; $3D+1$; $10D+9$; $20D-50$; $300D+200$.

6. Koje su od ovih kongruencija ispravne a koje nijesu? 1) $15 \equiv 3 \pmod 4$; 2) $35 \equiv -18 \pmod 7$; 3) $3^6 \equiv 1 \pmod 2$; 4) $10x \equiv 20 \pmod{10}$; 5) $x^2 - y^2 \equiv 0 \pmod{x+y}$; 6) $x^3 - 1 \equiv 0 \pmod{x-1}$?

7. Kako glase svi razredi množine D s obzirom na modul: 1) 2; 2) 4; 3) 5; 4) 10; 5) 8; 6) 12?

8. Promatraj svih 10 razreda mod 10; u kojem razredu leži pojedini član 10-članog niza 1) $10^0, 10, 10^2, 10^3, \ldots 10^9$; 2) $2^0, 2, 2^2, \ldots, 2^9$; 3) $18, 18^2, 18^3, \ldots, 18^{10}$?

9. Odredi: 1) $D \setminus 2D$; 2) $2D \setminus 4D$; 3) $4D \cup (4D+2)$; 4) $(4D+1) \cup (4D+3)$; 5) $(2D+1) \cup 4D$.

10. Odredi: 1) $2D \cap 4D$; 2) $2D \cap 4D+2$; 3) $3D+1 \cap 4D$; 4) $3D+1 \cap 4D+1$.

11. Dokaži $D^2 \subset 4D \cup (8D+1)$ tj. kvadrat svakog cijelog broja ili je oblika $4D$ ili je oblika $8D+1$.

12. Promatraj svih 5 razreda mod 5; koji su od ovih skupova potpuni predstavnici modulo 5: 1) $\{0, 1, 2, 3, 4\} = S_1$; 2) $S_2 = \{0, -1, -2, -3, -4\}$; 3) $S_3 = \{6, 7, 8, 9, 10\}$; 4) $S_4 = \{n, n+1, n+2, n+3, n+4\}$, 5) $S_5 = \{2, 2^2, 2^3, 2^4, 2^5\}$; 6) $S_6 = \{-2, 2^2, -2^3, 2^4, -2^5\}$; 7) $S_7 = \{5, 8, 15, 23, 1\}$; 8) $S_8 = \{3n, 3(n+1), 3(n+2), 3(n+3), 3 \cdot (n+4)\}$; 9) $S_9 = \{5n, 5(n+1), 5(n+2), 5(n+3), 5(n+4)\}$.

13. Odredi najmanji neodrečni i najveći odrečni broj u ovim razredima: 1) $15D+38$; 2) $18D-100$; 3) $360D+1000$; 4) $360D-1000$.

14. 1) Za koje $n \in N$ racionalni brojevi oblika $\frac{2\dot{D}}{n}+1$ čine razred množine Q prema 2 kao modulu? Kako bismo označili taj razred? 2) Da li je $2D+3/4$ razred u Q? 3) Šta je $\left(2D+\frac{1}{2}\right)+\left(2D+\frac{1}{3}\right)$? 4) Ako je $x, y \in Q[0, 2)$ i $x \neq y$ dokaži da su skupovi $2D+x$, $2D+y$ bez zajedničkog člana; 5) Da li je svaki razred mod 2 množine Q oblika $2D+x$ s određenim x iz $Q[0, 2)$? 6) Pokušaj odrediti po jednog predstavnika iz svakog razreda množine Q za modul 2.

15. Isto pitanje za module: 1) 360; 2) 24; 3) 2π; 4) 1; 5) proizvoljan član $m \in Q$.

16. Isto pitanje za skup R svih realnih brojeva.

4. SVOJSTVA KOLA ILI PRSTENA CIJELIH BROJEVA

Ovdje se ne upuštamo u definiciju cijelih brojeva: uzimamo ih kao već poznate[1]; ipak istaknimo neka svojstva množine D cijelih brojeva da se na njih možemo lakše pozvati.

4.0. Prvo svojstvo ili svojstvo $D_g(+)$: *Iz* $x, y \in D$ *izlazi* $x+y \in D$ (*uslov grupoidnosti ili zatvorenja*).

To znači dvije stvari: prvo, da je za *svako* x, y iz D rezultat $x+y$ *definiran*; drugo, da je taj rezultat opet član u D.

Oznaka D_g s indeksom g ukazuje baš na to da se govori o grupoidnosti i zatvorenosti, tj. o egzistenciji rezultata u skupu D, o kojem je riječ.

Sad je jasno npr. da vrijedi i svojstvo $D_g(-)$, koje se odnosi na diferenciju $x-y$ članova iz D: Iz $x, y \in D$ izlazi $x-y \in D$. No, već za zkup N svih prirodnih brojeva ne vrijedi $N_g(-)$, mada vrijedi $N_g(+)$. Dobro se naučimo na to da $N_g(-)$ izlazi iz $D_g(+)$ tako da umjesto D dolazi N, a umjesto $+$ dolazi $-$; drugim riječima, $N_g(-)$ je oznaka za ovu rečenicu:

$$\text{»}Iz\ x, y \in N\ izlazi\ x-y \in N.\text{«}$$

A jasno je da ta rečenica nije ispravna, jer je npr. $1, 2 \in N$, ali nije $1-2 \in N$ (pazi na redoslijed!).

4.1. Drugo svojstvo ili svojstvo $D_a(+)$. *Iz* $x, y, z \in D$ *izlazi*:

$$(x+y)+z = x+(y+z)\ (\textit{zakon asocijacije ili združivanja}).$$

4.2. Treće svojstvo ili svojstvo $D_n(+)$. *U D se nalazi neutrum, tj. član n sa svojstvom $x+n=x=n+x$ za svako $x \in D$*[2].

4.3. Četvrto svojstvo ili svojstvo $D_i(+)$. *Svakom članu $a \in D$ pripada određen član x iz D za koji je $a+x=n=$ neutrum $=x+a$ (zakon inverzije).*[3]

Time smo nabrojali četiri osnovna svojstva množine D cijelih brojeva, i to svojstva u odnosu na zbrajanje. Slična svojstva za oduzimanje ne vrijede; tako npr. oduzimanje nije asocijativno, tj. ne vrijedi:

$$(x-y)-z = x-(y-z).$$

4.4. Peto svojstvo ili svojstvo $D_k(+)$. *Iz* $x, y \in D$ *izlazi*: $x+y=y+x$ (*zakon komutacije za* $+$).

4.5. Šesto svojstvo ili svojstvo $D_g(\cdot)$. *Iz* $x, y \in D$ *izlazi* $x \cdot y \in D$.

4.6. Sedmo svojstvo ili svojstvo $D_a(\cdot)$. *Iz* $x, y, z \in D$ *izlazi*: $(xy)z = x(yz)$.

4.7. Osmo svojstvo ili svojstvo $D_d(+, \cdot)$. *Iz* $x, y, z \in D$ *izlazi*:

$$x(y+z) = xy + xz$$

---

[1]) Vidi npr. Đ. Kurepa, *Teorija skupova*, Zagreb 1951.

[2]) Naravno da je taj neutrum u D upravo broj 0.

[3]) Naravno, kako je $n=0$, to iz $a+x=0$ izlazi: $x=-a$ u skupu D.

(*zakon desne distribucije operacije* · *prema operaciji* +);

$$(y+z)\,x = yx + zx$$

(*zakon lijeve distribucije operacije* · *prema operaciji* +).

Kraće se kaže ovako: *u D je množenje distributivno ili razdjelno prema zbrajanju.* Npr.

$$3\,(2+5) = (3\cdot 2) + (3\cdot 5) = 6 + 15 = 21.$$

»*Dualna*« izreka: »*Zbrajanje je distributivno prema množenju*« nije istinita. Naime, kad bi npr. u D zbrajanje bilo razdjelno prema množenju, moralo bi biti $3+(2\cdot 5)=(3+2)\,(3+5)$. A to nije ispravno!

Drugim riječima:

$D_d(+,\cdot)$ vrijedi

$D_d(\cdot,\ +)$ ne vrijedi (pripazi na redoslijed operacija $+,\cdot$).

4.8. Na taj smo način naveli devet svagdašnjih svojstava množine D cijelih brojeva. Naravno skup D ima i raznih drugih svojstava, npr. ovo: svaki član x iz D ima svoja dva određena susjeda, i to $x-1$ i $x+1$; ili npr. ovo svojstvo: skup D može se svrstati u jedan niz, npr. ovako:

$$0,\ -1,\ 1;\quad -2,\ 2;\quad -3,\ 3,\ \ldots$$

I to su korisna svojstva množine D; međutim, imajući na umu specijalno gornjih 9 svojstava u $4.9 = 4.0,\ 4.1,\ 4.2,\ \ldots,\ 4.8$, i to kao cjelinu, govori se naprosto ovako: *skup D je kolo ili prsten u odnosu na operacije* $+,\cdot$; *ili još kraće*: $(D+,\cdot)$ *je kolo ili prsten.*[1)]

4.9. Definicija kola. Izreka »*D je kolo ili prsten u odnosu na operacije* $+,\cdot$« odnosno izreka: »*Tročlani niz* $(D,\ +,\cdot)$ *je kolo ili prsten*« znači upravo to da vrijedi:

$$D_g(+),\ D_a(+),\ D_n(+),\ D_i(+),\ D_k(+)$$

$$D_g(\cdot),\ D_a(\cdot)$$

$$D_d(+,\cdot).$$

Prema tome, svih prethodnih 8 svojstava mora biti na snazi pa da kažemo: $(D,\ +,\cdot)$ je kolo. Ako bar jedno svojstvo nije na snazi, tada nije riječ o kolu! A inače, uz gornjih 8 svojstava može biti i drugih, no ona su dodatak svojstvima kola: glavno je upravo 8 navedenih svojstava.

4.9.1. Kolo $I3$. Računanje na brojevnom 3-vrhu. Za nas će biti od interesa npr. da vidimo da „računajući slikovito“ na brojevnom 3-vrhu onako kako se slikovito računa na brojevnoj pravulji vidimo da je skup $I3 \equiv \{0,\ 1,\ 2\}$ jedno kolo u odnosu na to slikovito zbrajanje i pripadno množenje.

Računanje na 3-vrhu izvodi se ovako (slično kao na beskonačnoj brojevnoj pravulji; ali rezultati su sasvim drukčiji!): Zada se pravilan 3-vrh i pozitivan smjer kretanja po njegovu rubu. Zatim se u jedan vrh stavi 0; onda

---

[1)] кольцо (r.), ring (engl.), anneau (fr.), Ring (nj.).

se od 0 pođe za 1 korak u pozitivnom smjeru i u vrh stavi rezultat $0+1=1$. Nastavi se za 1 korak i u dostignut vrh stavi rezultat $1+1=2$; nastavi se za 1 korak pa se rezultat $2+1$ ima staviti $=0$ jer smo u tom vrhu naišli na 0. Dakle je $2+1=0$. Pri tom „zbrajanju" na 3-vrhu ne izlazimo iz skupnosti $I3=\{0, 1, 2\}$: rezultat je uvijek opet u $I3$. Isto je s množenjem (koje svodimo na zbrajanje). Npr., $4\cdot 1$ znači $1+1+1+1$; to znači da od 1 treba u pozitivnom smislu napraviti 3 koraka — dolazimo natrag u 1; dakle je $4\cdot 1=1$. Dobro je umjesto znaka $+$ i $\cdot$ za te operacije zbrajanja i množenja pisati znak $+_3, \cdot_3$ da se podsjetimo da smo na brojevnom 3-vrhu i govoriti *o računanju prema modulu* 3. Zanimljivo je da već 3 broja cifarskog skupa $I3=\{0, 1, 2\}$ čine kolo ili prsten u odnosu na operacije $+_3, \cdot_3$.

Naravno, to kolo $(I3; +_3, \cdot_3)$ mnogo je jednostavnije od kola $(D, +, \cdot)$. Isto vrijedi za računanje na kolu $(I10; +_{10}, \cdot_{10})$. Ali, što je najzanimljivije: ta *aritmetika prema modulu* 10 *zapravo je baza za naše svagdašnje računanje u decimalnom brojevnom sistemu* (isp. 6, § 15).

4.9.2. Analogno se definira kolo $(In, +_n, \cdot_n)$ za svaki prirodni broj $n>1$, pa i $n=1$; to kolo $(I1, +_1, \cdot_1)$ zapravo je kolo $(\{0\}, +, \cdot)$ u odnosu na naše obično zbrajanje i oduzimanje.

4.9.3. Specijalno je važno kolo $(I2, +_2, \cdot_2)$: primjenjuje se u matematičkoj logici i za računske strojeve. No računanje u svakom kolu $(Im, +, \cdot)$ baza je za računanje u m-sistemu brojeva (Poglavlje 6, § 15).

4.9.4. Za nas će biti važno da poslije vidimo da je množina svih polinoma s koeficijentima u skupu realnih (kompleksnih) brojeva u odnosu na varijablu x određeno kolo ili prsten.

4.10. Pitanje: Je li trojka $(D, \cdot, +)$ kolo? Nije! Već smo napomenuli da operacija $\cdot$ nije razdjelna prema operaciji $+$. Pogledajmo koji su uslovi ispunjeni, a koji nisu ispunjeni za uređenu trojku $(D, \cdot, +)$. Uslovi $D_g(\cdot)$, $D_a(\cdot)$ su ispunjeni. $D_n(\cdot)$ također. Naime, $D_n(\cdot)$ glasi: U D se nalazi neutrum, tj. član n sa svojstvom $xn=x$ za svako $x\in D$. Odatle izlazi $n=1$. Naravno, to n za operaciju $\cdot$ je član 1 iz D. Tako vidimo da broj 1 ima prema množenju istu „*neutralnu* ulogu" koju broj 0 ima prema zbrajanju.

Dolazi na red sud $D_i(\cdot)$ o inverziji operacije $\cdot$; ta operacija nije obrtljiva u D, jer npr. jednadžba $2x=1$ nema rješenja u skupu D, mada su koeficijenti 2 i 1 iz D.

Zatim dolazi sud $S_k(\cdot)$: komutativnost množenja. To vrijedi, pa se zato i kaže: *kolo* $(D, +, \cdot)$ *je komutativno*, znajući pri tom da je riječ o svojstvu komutacije druge „više" operacije. Na taj način vidimo da trojka $(D, \cdot, +)$ nije kolo jer nije ispunjeno odgovarajućih 8 svojstava za kolo; specijalno nisu ispunjeni zahtjevi $D_i(\cdot)$, $D_d(\cdot, +)$.

4.11. Ako Q znači skup svih racionalnih brojeva, onda se lako provjeri da je Q kolo, tj. $Q(+, \cdot)$ je kolo; skup R realnih brojeva i skup $R(i)$ kompleksnih brojeva također su kola.

4.12. Ako pogledamo gornja svojstva kola, onda vidimo da se pojavljuju dva analogna svojstva:

$$D_g(+) \qquad D_g(\cdot)$$

i

$$D_a(+) \qquad D_a(\cdot),$$

tj. da u D imamo dvije operacije $+$ i $\cdot$, koje su obje asocijativne. Kraće se kaže da je skup D *polugrupa*, i to i u odnosu na operaciju $+$ i u odnosu na operaciju $\cdot$; no prva operacija je i obratljiva u D: za svako a iz D jednadžba $a+x=0$ ima rješenje u D, označujemo ga $-a$; isto tako tj. za svako $a, b \in D$ jednadžba

$$a+x=b$$

može se riješiti u D; rješenje je $-a+b$; ono je u D.

4.13. Umjesto nabrajanja svih četiriju prvih svojstava: $D_g(+)$, $D_a(+)$, $D_n(+)$, $D_i(+)$ kraće se kaže: *D je grupa u odnosu na operaciju* $+$; naprotiv, *D nije grupa u odnosu na* $\cdot$ jer množenje u D nema obrata. Doduše, ni u širem skupu Q racionalnih brojeva nije množenje obratljivo bez izuzetka; doduše, jednadžba $2x=1$ rješiva je u Q kao i $3x=1$, pa $\frac{5}{2}x=1$ itd. Ali obrat od 0 ne postoji: jednadžba $0x=1$ nema rješenja u Q.

4.14. Ukloni li se 0 iz Q, preostaje skup $Q \setminus \{0\}$ „topova“ ili „tvrđava“ iz Q, tj. skup svih članova iz Q koji su $\neq 0$; taj je skup grupa u odnosu na operaciju množenja.

Slično vrijedi za množinu R svih realnih brojeva, odnosno množinu $R(i)$ svih kompleksnih brojeva.

4.15. Na taj način vidimo da imamo posla s 2 operacije $+$ i $\cdot$, povezane zakonom raspodjele druge operacije $\cdot$ nad prvom $+$; to vrijedi i za skup D i za skup Q i skup R brojeva. No, u posljednja dva slučaja, izuzevši invers od 0, svaki drugi član ima invers. Skup topova u Q, R, $R(i)$ čine tri određene grupe u odnosu na množenje. Na taj način u tim skupovima neograničeno su izvedive operacije $+$, $\cdot$ i njihove inverzne operacije — izuzetak je jedino zabrana i nemogućnost da se dijeli nulom. Kraće se kaže: *Q je tijelo*; R isto tako; $R(i)$ također.

4.16. Imamo ovaj način izražavanja:

$(D, +, \cdot)$ je kolo, ali nije tijelo. Uređena trojka $(Q, +, \cdot)$ je tijelo, dakle je kolo. Isto to vrijedi za $(R, +, \cdot)$, $(R(i), +, \cdot)$.

5. DEFINICIJA POLUGRUPE, GRUPE, KOLA I TIJELA[1)]

5.0. Definicija polugrupe. Zadan je neprazan skup S i neki postupak ili operacija $\circ$ koji svakom uređenom paru x, y iz S pridjeljuje neku stvar $x \circ y$[2)]; kaže se da je S *polugrupa* u odnosu na postupak $\circ$ ili da je $S(\circ)$ *polugrupa* ako su ispunjena oba zahtjeva $S_g(\circ)$ i $S_a(\circ)$:

$S_g(\circ)$: *Iz* $x, y \in S$ *izlazi* $x \circ y \in S$.

$S_a(\circ)$: *Iz* $x, y, z \in S$ *izlazi* $(x \circ y) \circ z = x \circ (y \circ z)$.

[1)] Čitalac ne treba da sada čita ovaj §; neka u ovom § pročita ono na što ćemo ga uputiti u izlaganju; detaljniji opis ovog § nalazi se u poglavlju 17. o grupama.

[2)] To znači da je o neko preslikavanje Descartesova kvadrata S^{I^2}; S^{I^2} je množina svih uređenih parova (x, y) s $x \in S$ i $y \in S$; znači; za svako $(x, y) \in S^{I^2}$ određeno je $x \circ y$; specijalno je određeno $x \circ x$.

5.0.1. P r i m j e r i. Jednočlani skup $\{0\}$, kojemu je 0 jedini član, jest određena polugrupa u odnosu na zbrajanje:

$$(\{0\}, +) \quad \text{je polugrupa.}$$

Skup N prirodnih brojeva je polugrupa u odnosu na zbrajanje.

5.0.2. P r i m j e d b a. Rečenica $S_g(\circ)$ izlazi iz $D_g(+)$ u § 4.0. zamjenjujući D sa S i $+$ sa $\circ$.

Slično vrijedi i za ostale rečenice: $S_n(\circ)$, $S_i(\circ)$, $S_k(\circ)$, pa zato te rečenice ne moramo ovdje posebno ispisivati.

5.1. Definicija grupe (S, o). Neprazan skup S je grupa prema operaciji $\circ$, koja svakom uređenom paru $x, y \in S$ pridjeljuje proizvod $x \circ y$, onda i samo onda ako su ispunjena sva četiri zahtjeva $S_g(\circ)$, $S_a(\circ)$, $S_n(\circ)$, $S_i(\circ)$ prema §§ 4.0—4.3. Tada se govori o uređenom paru $(S, \circ)$ kao o grupi.

5.1.1. D e f i n i c i j a. *Grupa* $(S, \circ)$ *je komutativna ako vrijedi* $S_k(\circ)$ *tj.* $x \circ y = y \circ x$ *za svako* $x, y \in S$.

5.1.2. P r i m j e r. $(\{0\}, +)$ je komutativna grupa; $(N, +)$ uopće nije grupa (isp. § 4.0.1).

5.2. Definicija kola ili prstena. Zadan je neprazan skup S; neka su $+$ i $\cdot$ preslikavanja Descartesova kvadrata S^{I_2}; kaže se da je *uređena trojka* $(S, +, \cdot)$ *kolo ili prsten* ako je S komutativna grupa prema prvoj operaciji, polugrupa prema drugoj operaciji i ako je pri tom druga operacija distributivna (razdjelna) prema prvoj operaciji. Drugim riječima, izreka: $(S, +, \cdot)$ *je kolo ili prsten* znači upravo da su ispunjeni zahtjevi $S_g(+)$, $S_a(+)$, $S_n(+)$, $S_i(+)$, $S_k(+)$, te $S_g(\cdot)$, $S_a(\cdot)$ i, najzad, $S_d(+, \cdot)$ prema §§ 4.$\dot{8}$. ($\dot{8}$ znači: 0, 1, 2, ... 7).

5.2.1. D e f i n i c i j a. Kolo je *komutativno* ako je i druga operacija komutativna.

5.2.2. Jednočlani skup $\{0\}$ je kolo u odnosu na $+$ i $\cdot$; drugim riječima, $(\{0\}, +, \cdot)$ je kolo, i to komutativno kolo! Koliko je vremena trebalo proteći pa da čovjek svjesno vidi da je $(\{0\}, +, \cdot)$ kolo! Pri tom, 0 može biti ne samo 0 (nula) nego bilo koji predmet!

5.3. Definicija tijela ili polja. Svako kolo $(S, +, \cdot)$, u kojem je i dvojka $(S \setminus \{0\}, \cdot)$ grupa, zove se *tijelo ili polje*.

5.3.1. D e f i n i c i j a. Tijelo je *komutativno* ako je komutativna i druga operacija.

Prema tome, svako tijelo ili korporacija ima bar 2 člana.

6. KOLO SVIH KRATNIKA ZADANE VELIČINE. RELACIJA DJELJIVOSTI I KONGRUENTNOSTI

6.0. Nekoliko naziva: kratnik (multiplum) — mjera (faktor). Produkt zadane veličine m i bilo kojeg cijela c zove se *kratnik* ili *multiplum* od m, i to *c-kratno m*. Npr., svi kratnici broja 2 čine skup $2D$ brojeva $2\dot{D}$; to su ujedno *dvokratnici* svih cijelih brojeva. Umjesto da se govori: *k je kratnik od m*, kaže se također: *k je djeljivo sa m* ili *k je kongruentno* 0 *prema modulu m* i piše $k \equiv 0 \pmod{m}$ (isp. definiciju u § 3.9). Svi kratnici binoma $x+1$ su oblika $(x+1)\cdot$polinom.

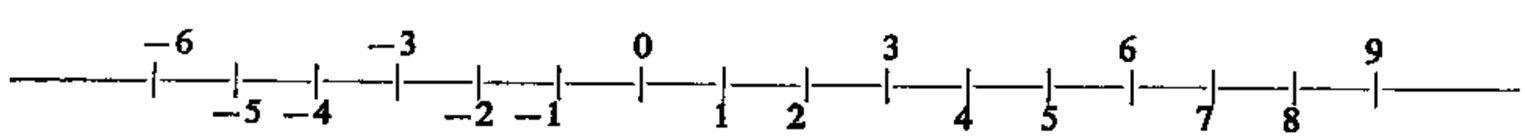
Ako je k kratnik od m, kaže se također da je *m faktor* (*mjera*, *djelilac*) od k piše:

$$m \mid k$$

(čitaj: *m dijeli k* ili *m je faktor, mjera od k*). Npr. $3 \mid 6$, ali je 3 non $\mid$ 4, 3 nije mjera od 4.

6.1. Znamo za osnovno kolo D cijelih brojeva (riječ „kolo" znači da su zadovoljena uobičajena svojstva za zbrajanje i množenje cijelih brojeva; riječ je o svojstvima iz §§ $4.\dot{8}. = 4.0,\ 4.1,\ 4.2, \ldots,\ 4.7$).

Promatrajmo, npr. skup 3-kratnika svih cijelih brojeva; označima ga sa $3D$; to je jedan podskup kola D (članovi su mu *iznad* linije; preostali članovi kola D su ispod pravulje).



Ako zbrajamo i množimo sa članovima iz $3D$, rezultat je opet u $3D$. Npr., $3\cdot 6 + 3\cdot 14 =$ (slovom zakona distribucije $D_d(+, \cdot) = 3\cdot 20 \in 3D$.

Na taj način vidimo da se zakon grupoidnosti $(3D)_g(+)$ za skup $3D$ svodi na oba zakona grupoidnosti u $(D, +, \cdot)$ i na zakon distribucije

$$D_d(+, \cdot) \text{ u } D.$$

Analogno se dokazuje da je i produkt trokratnika opet trokratnik.

6.2. Definicija. Za svaku veličinu m neka mD označuje množinu svih mx, pri čemu x prolazi kroz D, tj.

$$mD = \{m\cdot 0,\ m\cdot 1,\ m\cdot -1,\ m\cdot 2,\ m\cdot -2, \ldots\}.$$

Npr.,

$3^{1/2}D$ je skup svih brojeva $3^{1/2}\dot{D}$

πD je skup svih brojeva $\pi\dot{D}$

iD je skup svih brojeva $i\dot{D}$, tj. $iD = \{i0 = 0,\ i1 = i,\ i2, \ldots\}$

$(1, 2, 3, -2)D$ je skup svih nizova oblika $(x, 2x, 3x, -2x)$, pri tom x prolazi kroz D.

Za funkciju $y = x^2$ znači x^2D skup svih parabola $y = x^2\dot{D}$ itd.

Kao što smo vidjeli da je $(D, +, \cdot)$ kolo, tako se lako vidi da vrijedi:

6.3. Teorem. *Za svaki broj* m[1] *množina* $m\,D$ *svih* $m\,\dot{D}$ (*pri čemu* $\dot{D}$ *prolazi kroz* D) *je kolo u odnosu na* $+$, $\cdot$, *tj.* $(m\,D, +, \cdot)$ *je kolo, i to komutativno kolo.*

Napose $(m\,D, +)$ je komutativna grupa. Na taj način vidimo da u kolu $(m\,D, +, \cdot)$ možemo provoditi prve tri računske operacije i da ne izlazimo van njega!

6.4. Specijalno će nam biti potrebno spomenuto svojstvo množine $m\,D$ da u njoj neograničeno možemo vršiti prve dvije operacije; u tom se i sastoji smisao izreke: $m\,D$ *je aditivna grupa*, i to dio grupe D za svako cijelo m iz D.

6.5. Grupe $m_0\,D + m_1\,D$. Međutim, i s izrazima $m_0\,x + m_1\,y$ znamo računati (m_0, m_1 su zadani, a x, y prolaze kroz D); očigledno je da, vršeći s njima prve dvije operacije $+$, $-$, nećemo izaći napolje: opet smo u jednoj grupi; označimo je sa

$$m_0\,D + m_1\,D. \tag{1}$$

Prema tome, $m_0\,D + m_1\,D$ označuje skup svih izraza $m_0\,x + m_1\,y$ kad x, y prolaze kroz D. Nije baš jednostavno izračunati tu grupu. Inače, njeno određivanje je upravo *problem*: *koja je najmanja količina* >0 *koju možemo izmjeriti cjelobrojnim kombiniranjem mjerâ veličine* m_0 *i* m_1 (pretakanja posuda, mjerenje dužina, itd). Ako je, npr., jedna mjera 5, a druga 3, onda jednakost $5 \cdot 2 - 3 \cdot 3 = 1$ pokazuje da se čak i najmanje cijelo, 1, može dobiti. Da su polazne veličine bile npr. 4, 6, onda bi se njihovim kombiniranjem moglo dobiti 2 (npr. $4 \cdot -4 + 3 \cdot 6 = 2$), a time i čitava grupa $2\,D$, jer je

$$4 \cdot (-4\,\dot{D}) + 3\,(6 \cdot \dot{D}) = 2\,\dot{D}.$$

6.6. Jedna od vrlo dubokih istina sastoji se u tome da je općenito na snazi: *Za svaku dvojku cijelih brojeva* m_0, m_1 *potpuno je određen cijeli broj* c *sa svojstvom*:

$$m_0\,D + m_1\,D = c\,D.$$

To je upravo »*najveća zajednička mjera*« od m_0, m_1, tj. najveći broj $m_0\,\mathrm{M}\,m_1$ kojim su djeljivi m_0, m_1 (izuzetno se nekad stavlja $0\,\mathrm{M}\,0 = 0$). Slično za trojku brojeva m_0, m_1, m_2, pa za niz od 4 člana m_0, m_1, m_2, m_3, itd. Međutim, već sada možemo uočiti ovu istinu:

6.7. Teorem. *Za svaki zadan konačan niz* m_0, m_1, m_2, $\ldots$, m_k *cijelih brojeva skup svih »skalarnih produkata«*

$$m_0\,x_0 + m_1\,x_1 + m_2\,x_2 + \cdots + m_k\,x_k$$

je aditivna grupa, i to aditivna podgrupa grupe $(D, +)$; *pri tom* x_0, $x_1 \cdots x_k$ *prolaze, svi, skupom* D, *nezavisno jedan od drugog.*

---

[1]) Teorem je istinit i za razne veličine m koje nisu brojevi; npr. za nizove i druge funkcije s vrijednostima u množini brojeva; itd., itd.

Sadržaj teorema je svakdašnje baratanje sa sumama i diferencijama cijelih brojeva.

6.8. Svojstvo prelaznosti mjere i kratnika. Ako je x mjera od y, a y mjera od z, onda je x mjera od z; simbolički: $x \mid y$ i $y \mid z \Rightarrow x \mid z$; i dualno (permutacija: faktor $\Leftrightarrow$ multiplum): ako je x multiplum od y i y multiplum od z, onda je x multiplum od z; simbolički:

Ako je

$$x \equiv 0 \pmod{y}$$

$$y \equiv 0 \pmod{z},$$

onda je

$$x \equiv 0 \pmod{z}.$$

Dokaz je trivijalan: treba samo napisati i vidjeti šta je zadano, a što se traži. Dokažimo, npr., prelaznost relacije $\mid$:

$$x \mid y, \quad y \mid z \Rightarrow x \mid z.$$

No, $x \mid y$ znači da je x faktor od y, dakle je

$$xx' = y \tag{1}$$

za neko cijelo x', tj. $x' \in D$; isto tako $y \mid z$ znači da je

$$yy' = z \tag{2}$$

za neko $y' \in D$. Unesemo li (1) u (2), izlazi $(xx')y' = z$, odnosno — zbog zakona asocijacije za množenje u D (zakon $D_a(\cdot)$ iz § 4.7) — imamo:

$$x(x'y') = z. \tag{3}$$

Međutim, po zakonu $D_g(\cdot)$ iz § 4.5. produkt $x' \cdot y'$ cijelih brojeva opet je cio broj. A to znači upravo da je x faktor od z, tj. $x \mid z$, za čim se i ide.

6.9. Očigledno je da su relacije $\mid$ i $\equiv$ povratne ili refleksivne: $x \mid x$, $x \equiv 0 \pmod{x}$ za svako cijelo x (čak i $0 \mid 0$ jer je $0 = 0 \cdot 0$).

6.10. Ako je $x \mid y$ i $y \mid x$, onda je $x = \pm y$; specijalno, za prirodne brojeve vrijedi ovo:

$$x \mid y \text{ i } y \mid x \Rightarrow x = y.$$

6.11. Na taj način vidimo da u množini N svih prirodnih brojeva relacija $\mid$ (biti divizor od) ima sva tri karakteristična svojstva relacija $\leq$ za poredak:

1) refleksivnost: $x \leq x$:

2) antisimetrija : $x \leq y$ i $y \leq x \Rightarrow x = y$; odnosno

3) tranzitivnost: $x \leq y, \quad y \leq z \Rightarrow x \leq z$ (isp. pogl. 2 § 13).

Ta tri svojstva su definiciona svojstva za relaciju poretka (v. 3, § 13.1.1)

6.12. Zadaci.

1. Da li izrazi oblika $a_0+a_1 x+a_2 x^2$, pri čemu su a_0, a_1, $a_2\in D$ čine određenu grupu prema zbrajanju?

2. Navedi nekoliko članova skupnosti: 1) $\frac{3}{2}D$, 2) $\sqrt{2}\,D$, 3) $i\,D$, 4) $D+i\,D=D[i]$, 5) $2\,D+3\,D$.

3. Ako je $x,\ y\in D$ te $x\,|\,y$ i $y\,|\,x$, onda je $x=\pm y$, $xy\neq 0$. Dokaz.

4. Provjeri da je skup $D[i]=D+i\,D$ određeno kolo (to je tzv. Gaussovo kolo).

5. Ako je $(A,\ +,\ \cdot)$ bilo kakav komutativan prsten, pa ako je $a=bc$ te $a, b, c\in A$, kaže se da je a djeljivo sa b i piše $a\equiv 0 \pmod b$ ili $b\,|\,a$. Dokaži da je i tu relacija djeljivosti prelazna. Promatraj specijalno slučaj da se radi o tzv. Gaussovu kolu $D[i]=D+i\,D$.

6. Da li je koji od skupova $4D+\dot{4}$ grupoid u odnosu na 1) zbrajanje; 2) množenje?

7. Isto pitanje pišući umjesto 4 svuda 1) 5, 2) 10, 3) n.

8. P r o b l e m. Postoje li dva brojevna različna razreda A, B koja su u međusobnom aditivnom srodstvu tj. da bude $A+A\subset B$ i $B+B\subset A$?

9. P r o b l e m. Slično pitanje za množidbeno srodstvo: postoje li dva različna razreda A, B cijelih racionalnih brojeva za koje je $AA\subset B$ i $BB\subset A$?

7. DVA PORETKA U SKUPU N PRIRODNIH BROJEVA

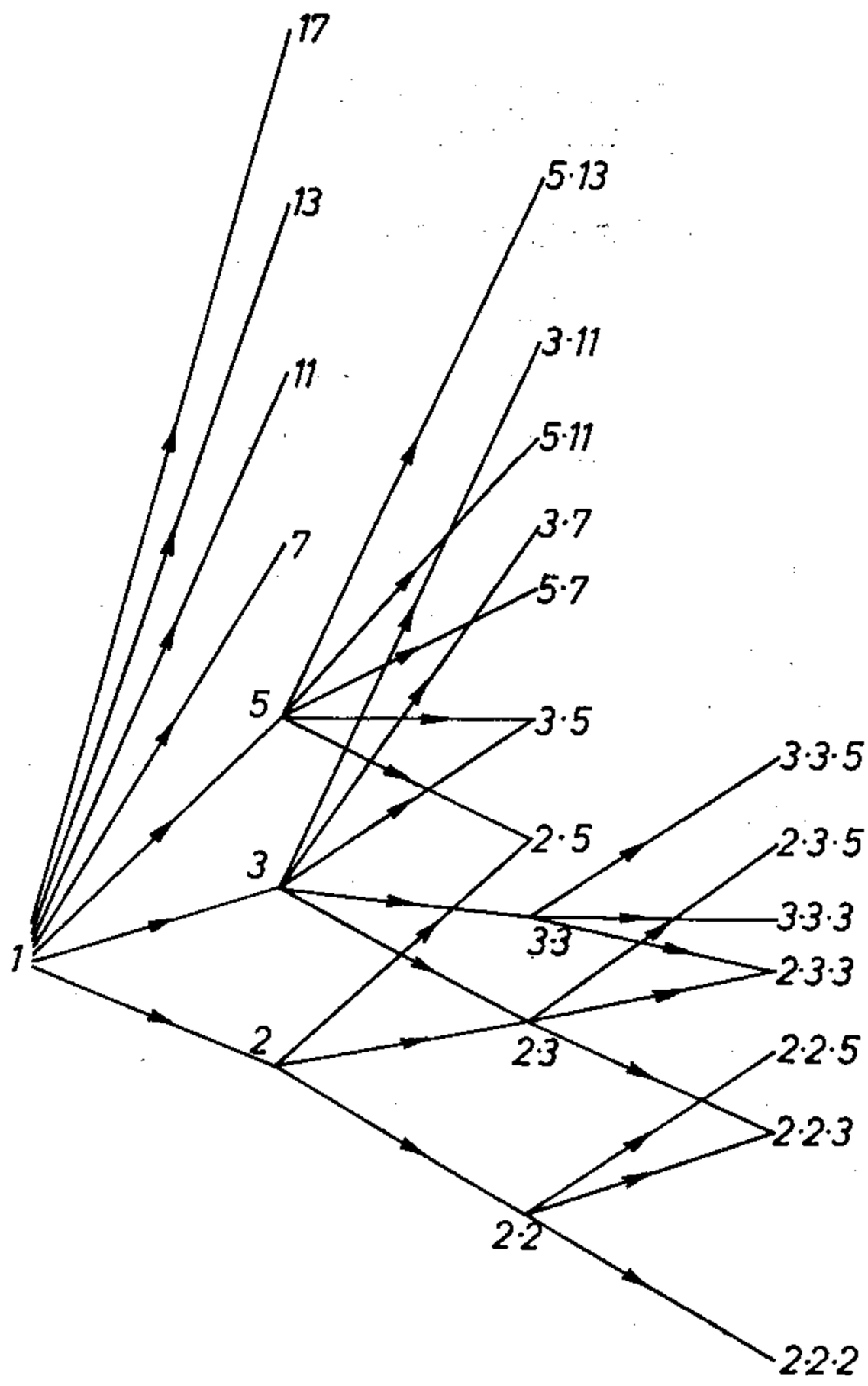
7.1. Prim-brojevi. U skupu N prirodnih brojeva osim prirodnog poretka po veličini relacijom $\leq$ imamo i prirodni poredak po relaciji $|$ djeljivosti ($a\,|\,b$ znači da a dijeli b, odnosno da je a faktor od b). Prvi poredak $(N,\ \leq)$ je potpun, drugi je djelomičan jer, npr., niti je 3 djeljivo sa 2 niti 2 sa 3. Prvom relacijom brojevi se nižu linearno po veličini:

$$1\leq 2\leq 3\cdots$$

(svaki broj je posredno ili neposredno vezan crticama sa svakim drugim članom).

Drugom relacijom, relacijom djeljivosti $|$, skup N se prepliće u mrežu (vidi sliku 6.7.2). Tu su posredno ili neposredno vezani (spojeni) samo oni $\neq$ brojevi x, y za koje je $x\,|\,y$ („veza“ se vrši slomljenim crticama idući od lijeva nadesno). Tako npr. za prvih 25 prirodnih brojeva ispiši kao vježbu „$|$ uređenje“ (neka u svakom stupcu brojevi rastu po veličini!).

7.2. Kod prirodnog poretka $(N,\ \leq)$ poslije broja 1 dolazi broj $1+1$ kao neposredni sljedbenik; u prirodnoj mreži $(N,\ |)$ neposredno poslije broja 1



Sl, 6.7.2.

dolazi čitav niz neposrednih sljedbenika, i to brojevi: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ... zovu se prim-brojevi (prosti brojevi ili prabrojevi).

7.3. Definicija prostih i složenih brojeva. Svaki prirodni broj koji je djeljiv jedino sa 1 i sa samim sobom zove se *prost* ili *prim-broj*. Svaki prirodni broj koji je produkt od dva prirodna jednaka ili nejednaka broja >1 zove se *složen prirodni broj*. Broj 1 ne ubrajamo niti u proste niti u složene brojeve.

Npr., broj 6 je složen jer je $6=2\cdot 3$, a 2 i 3 su >1; broj 5 je prost.

7.4. Skup P. Neka je P skup svih prostih brojeva; dakle je

$$P=\{2,\ 3,\ 5,\ 7,\ 11,\ \ldots\}.$$

7.5. Problem blizanaca. Ni do danas nije ljudima pošlo za rukom da izuče narav množine P svih tih neposrednih sljedbenika broja 1. Ne zna se,

npr., da li među tim sljedbenicima ima beskonačno mnogo »*blizanaca*«! (tj. takvih parova koji se razlikuju za 2; blizanci su, npr., 3, 5, pa 5, 7, pa 11, 13, pa 17, 19; ...; 8999, 9001; 9719, 9721; 9929, 9931, 10005629, 10005631; 10006427, 10006429, ovaj broj je po redu 663983. prosti broj); itd.

No lako vidimo ova tri rezultata iz starogrčke matematike (§ 7.6—§ 7.8.)

7.6. Eratostenovo sito[1]**.** Polazimo od skupa M_0 svih prirodnih brojeva >1:

(1) 2, 3, 4, 5, ...

Prosijavanje se sastoji u tome da se iz tog niza *uklone* svi složeni brojevi. Promatramo prvi broj 2 i skup $2M_0$ svih njegovih kratnika >2; ovaj skup izbacimo iz (1); dobije se određen skup M_1; u preostatku M_1 promatramo *prvi* broj >2 (dakle 3), njega zadržimo, a izbacimo čitavi skup $3M_1$ njegovih trokratnika u M_1; u preostatku M_2 radimo slično: zadržimo *prvi* broj >3 (to će biti 5) i izbacimo $5M_2$, itd.

Neizbačeni brojevi skupa (1) *čine upravo skup P svih prostih brojeva.*

Primijetimo ovo: Za svaki prost broj p *prvi* broj u nizu (1) koji uklanjamo u vezi s promatranjem broja p jest njegov kvadrat p^2; naime, svaki manji kratnik kp bio je izbačen u toku čišćenja u vezi s najmanjim prim-divizorom d faktora k: ako je

$$k = dq \ (d \text{ prost}), \quad \text{tada je } kp = d(qp),$$

dakle je taj broj zaista ranije uočen kao složen.

Zato je jasno da *za svaki prirodni broj* $n>1$ *imamo pred sobom sve proste brojeve* $\leq n$ *nakon što su uklonjeni svi složeni brojevi djeljivi prostim brojem* $\leq n^{1/2}$.

Npr. izbacujući sve složene brojeve ≤ 25 djeljive jednim od prostih brojeva $\leq 25^{1/2} = 5$, preostaju upravo svi prim-brojevi ≤ 25:

2,	3,	4,	5,	6,	7,	8,	9,	10,	11,	12,	13,	14,	15,	16,	17,	18,	19,	20,	21,	22,	23,	24,	25.
		2		2		2	3	2		2		2	3	2		2		2	3	2		2	5

Ispod broja a prvog niza napisan je prost broj p, kojom prilikom je a izbačeno. Oni brojevi iz prvog niza ispod kojih nema ništa napisano jesu prosti.

Vidimo kako se Eratostenovim sijanjem dosta brzo dolazi do svih prostih brojeva $\leq n$.

Nastaje pitanje: Hoće li se proces prosijavanja prema Eratostenu završiti nakon promatranja konačnog broja čišćenja? Drugim riječima, da li je skup P konačan?

Na to pitanje daje odgovor ovaj Euklidov rezultat:

7.7. Euklidov[2] **teorem o prostim brojevima. Prostih brojeva ima beskonačno mnogo.**

---

[1] Prema grčkom matematičaru i geografu Eratostenu (—276? do —195?) Arhimedovu savremeniku.

[2] Euklid (—365? do —275?), veliki grčki matematičar, poznat naročito po »*Euklidovu postulatu o paralelama*«.

Naime, ako već odredismo kakav konačan niz prostih brojeva

$$(*) \qquad n_0,\ n_1,\ n_2,\ \ldots,$$

onda je suma

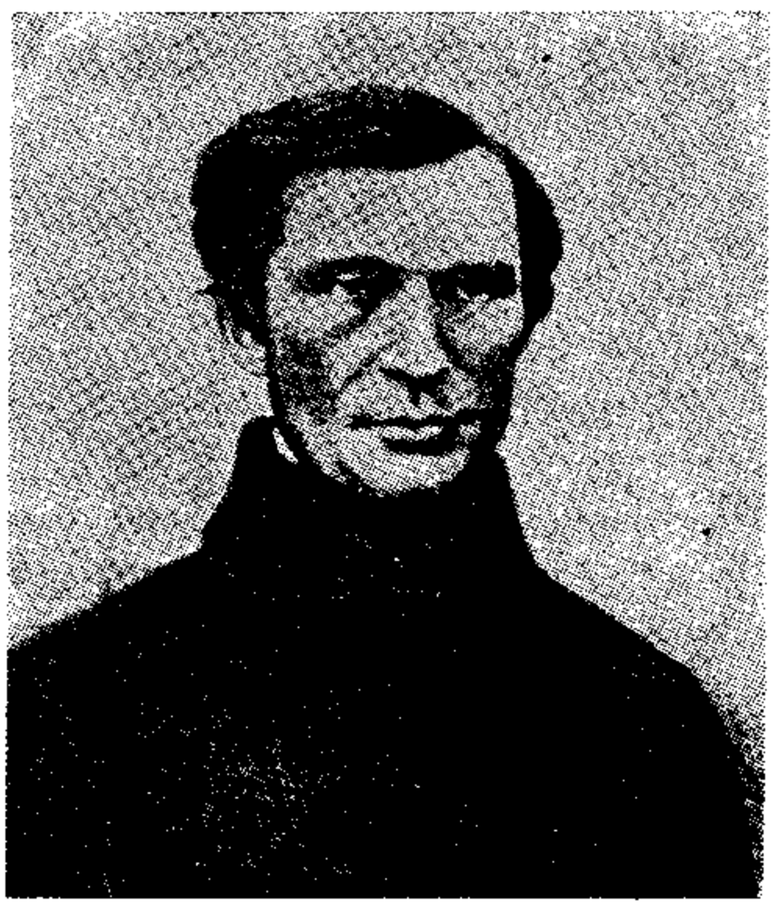
$$n_0 \cdot n_1 \cdot n_2 \cdots + 1$$

određen prirodan broj n; svaki *prost* faktor p tog broja n je različit od svakog prostog broja n_k iz (*), tj. $p \neq n_k$, i to zato jer je $p \mid n$ (p je čak prost faktor od n, tj. prim-broj p dijeli n); naprotiv, n_k ne dijeli n — podijelimo li n sa n_k, prvi član je djeljiv, a drugi daje ostatak $1/n_k$.

Dakle je p nov prim-broj, izvan niza (*), pa tako niz (*) možemo produžiti i produživati sve novim i novim prim-brojevima.

A postoji li prim-faktor od n? Očigledno je da postoji. Prvi član $p(n)$ prirodnog niza 2, 3, 4, 5, ... koji dijeli n je prost broj! Naime, u obrnutom bi slučaju $p(n)$ bio složen broj, dakle produkt ab prirodnih brojeva >1; oni su nužno $<p(n)$, pa bi tako faktor b od faktora $p(n)$ od faktora n bio faktor od n, i to manji od manjeg $p(n)$ — besmisao. Dakle je Euklidov teorem dokazan.

Euklid (—365? do —275?)



P. L. Čebišev
(26. 5. 1821 — 8. 12. 1894),
veliki ruski matematičar

Upravo, misaono, svakom prirodnom broju $n>1$ pridružismo određen prim-broj $p(n)$ — prvi njegov prim-faktor. Time smo odmah na tragu drugom starogrčkom rezultatu: ponovimo proces na *kofaktoru* $f_1 = n/p(n)$ (koji pomnožen sa $p(n)$ daje n) — dolazimo do prim-broja $p(f_1)$ pa je

$$n = p(n) \cdot \frac{n}{p(n)} = p(n) \cdot p(f_1) \cdot \frac{f_1}{p(f_1)} \text{ itd.}$$

Proces se mora prekinuti jer su $p(n)$, $p(f_1)$, $p(f_2)$, ... prosti brojevi pa nakon konačno mnogo koračaja njihov produkt dostiže broj n:

7.8. Teorem (Euklid) *Svaki prirodni broj* >1 *ili je prost ili je produkt niza prostih brojeva* (jednakih ili $\neq$).

Zanimljivo je da je tek Gauss (18/19 st.) upotpunio taj Euklidov *teorem o faktorizaciji* prirodnih brojeva dokazavši da je faktorizacija *jednoznačna* u tom smislu da se pri svakoj faktorizaciji pojavljuju isti prim-faktori s istom kratnosti, iako eventualno u drukčijem redoslijedu. Dokaz se provodi Euklidovim sredstvima (isp. § 14).

7.9. Eto, to su tri rezultata o prostim brojevima iz grčkog doba: teoremi 7.6—7.8. Novi rezultati počeli su se dodavati istom u prošlom stoljeću, npr.:

7.9.1. *Za svaki prirodni broj* $n>1$ *postoji bar jedan prost broj između* n i $2n$ (Bertrand-Čebišev).

7.9.2. *Za svaki par relativno prostih prirodnih brojeva* a, b *sadrži skup* $aN+b$ *beskonačno mnogo prostih brojeva* (Lejeune-Dirichlet; slučaj $a=b=1$ je gornji Euklidov teorem 7.6).

7.9.3. Funkcija $\pi(x)$. *Ako* $\pi(x)$ *kazuje koliko ima prostih brojeva* $\leq x$, *tada vrijedi:*

$$\lim_{x\to\infty} \pi(x) : \frac{x}{lx} = 1, \tag{1}$$

$$\pi(x) : \int_2^x \frac{dx}{lx} \to 1 \text{ sa } x \to \infty. \tag{2}$$

Na tim dvama osnovnim teoremima o *»raspodjeli prostih brojeva«* sudjelovao je čitav niz matematičara: Legendre, Gauss, Čebišev, Hadamard, de la Vallée Poussin. Potpun dokaz izvela su posljednja dvojica god 1898. istodobno i nezavisno.

S matematičkog i spoznajnog gledišta zanimljivo je ovo: Čebišev je dokazao relaciju (1) uz pretpostavku da limes na lijevoj strani postoji, tj. egzistencija toga limesa određuje, dokazao je Čebišev, i svoju vrijednost — upravo 1.

7.10. Koliko ima Fermatovih prostih brojeva? Fermatovi prosti brojevi su prosti brojevi oblika $F_n = 2^{2^n}+1$. Dosad se zna samo ovih 5 Fermatovih prostih brojeva — i on sâm ih je znao:

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 66\,537.$$

Već naredni Fermatov broj nije prost, nego je složen:

$$F_5 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417 \text{ (Euler)}.$$

Neka je p prost broj; vrlo je zanimljivo da se pravilan p-vrh može nacrtati služeći se linealom i šestarom jedino onda ako je p Fermatov prim-broj (Gauss). Zato npr. takva konstrukcija pravilna 7-vrha nije moguća.

Ne zna se da li je F_{13} prost ili složen broj; inače F_{13} ima 2467 cifara. Brojevi F_7, F_8 su složeni, no ne znamo im nijednog prostog faktora. Zna se, npr., da je broj F_{1945} složen: pomoću električnih strojeva nađen je najmanji djelitelj, i to broj $2^{1947}+1$ (on ima 587 cifara; broj F_{1945} ima preko 10^{580} cifara).

P. Fermat (č. Ferma)
(1601—1665),
veliki franc. matematičar

7.11. Veliki Fermatov problem. Fermat je napisao da misli da je F_n prost broj za svako n, no da mu dokaz nije potpuno uspio. To je napisao u obliku napomene zajedno s još nekoliko drugih napomena, od kojih su sve dosad dokazane osim slijedeće izreke, za koju je *tvrdio da ju je dokazao*: *Ne postoje prirodni brojevi* x, y, z, n *za koje bi bilo*:

$$x^n + y^n = z^n, \quad n > 2.$$

To je tzv. *veliki Fermatov problem*, koji ni do danas nije riješen. U poznatim slučajevima $n = 3, 4, 5, \ldots$, npr. do 100, Fermatova je tvrdnja istinita.

7.11.1. Oko pajvećega poznatog prostog broja. Zanimljivo je spomenuti ovo. Prostih brojeva ima beskonačno mnogo; no najveći prosti broj, koji je do god. 1960. bio određen je ovaj treći:

(1) $\qquad 2^n - 1$ za $n = 521, 607, 3217, 4253, 4423;$

u decimalnomu sistemu ima taj broj 969 cifara; odredili su ga u Švedskoj god. 1957. pomoću elektronskih računskih strojeva a na osnovu ovog teorema (Lucas-Lehmer): Neka je p prost broj >2; broj $M_p = 2^p - 1$ je prost onda i samo onda ako M_p dijeli s_{p-1} gdje je $s_1 = 4$ i $s_n = s^2_{n-1} - 2$ za $n = 2, 3, \ldots$

(Za dokaz toga teorema v. W. Sierpiński, Teoria liczb, II, Warszawa 1959, 486. str., napose str. 381—385.)

Provjeravanje na stroju da je broj (1) prost trajalo je oko $5^1/_2$ časova (pripreme tu nisu uračunate!).

U (1) su naznačeni jedini novi prosti brojevi M_n pri $n < 5000$ (v. A. Hurwitz, *New Mersenne primes*, Math. Computation 16 (1962) 249—251; R. M. Robinson, *A report on primes of the form* $k \cdot 2^n + 1$ *and on factors of Fermat numbers* (Proc. Amer. Math. Soc. 9 (1958) 673—681).

7.12. Savršeni (perfektni) brojevi. Sva tri napisana prosta broja (1) daju velike savršene brojeve[1], jer se može pokazati ovo: ako je $2^n - 1$ prost, tada je $2^{n-1}(2^n - 1)$ savršen.

---

[1] Prirodni broj n je *savršen* ili *perfektan* ako je jednak sumi svih svojih divizora $< n$. Takav je broj 6 $(6 = 1 + 2 + 3)$.

Od brojeva oblika $2^{n-1}(2^n-1)$ danas se zna da su savršeni oni za koje je $n=2$, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217; za druge se ne zna; ujedno su svi ti nabrojeni 2^n-1 prosti ($n=31$: Euler, 127: Lucas). Ne zna se da li postoji ikoji *neparan* savršen broj.

7.13. Oko najvećega efektivnog prirodnog broja. S tim u vezi spomenimo i ovo: prirodnih brojeva ima beskonačno; no najveći prirodni broj koji je do danas pronađen i došao do nekoga stvarnog izražaja kreće se „negdje“ oko „četverospratnog“ broja

$$x_0 = e^{e^{e^{79}}} = (\text{približno}) = 10^{10^{10^{34}}},$$

je se tu negdje nalazi prvi broj x za koji Čebiševljeva funkcija

$$\frac{\pi(n)}{n} - \frac{0{,}43429}{ln}$$

postaje i negativnom (Littlewood je god 1914. dokazao da ta razlika nije uvijek ≥ 0, a S. Skewes je god. 1933. odredio približno prvi gornji „izuzetak“ — Skewesov broj x_0).

7.14. Zadaci o prostim i složenim brojevima.

1. Ispiši proste brojeve koji su manji od broja x i odredi $\pi(x)$ za ove vrijednosti x: 1) 20; 2) 100; 3) 1000.

2. 1) Odredi pomoću Eratostenova sata sve proste brojeve koji su <500 (isp. pogl. 6, § 7.6); 2) U ravnini kompleksnih brojeva promatraj čisto imaginarne brojeve $i(1+k^{-1})$ i kompleksne brojeve $n+1+i$; realni broj koji leži na istoj pravulji na kojoj leži broj $i(1+k^{-1})$ te broj $n+1+i$ je složen prirodni broj; kad k, n prolaze skupom N, dobije se tako *svaki* složen prirodni broj. Crtaj!

3. *Eulerov tročlan izraz* je $f(x)=x^2+x+41$. Taj izraz pri $x \in I\,40 = \{0, 1, \ldots, 39\}$ uzima proste vrijednosti. Ne zna se da li je skup $P \cap f\,N$ beskonačan. Ne zna se da li postoji ikoji tročlan izraz $b(x) \equiv ax^2+bx+c$ odnosno algebarski polinom $b(x)$ s cijelim koeficijentima i sa svojstvom da skup $b(N)$ sadržava beskonačno mnogo prostih brojeva.

4. U kojima od razreda 1) $4D+\dot{4}$; 2) $6D+\dot{6}$ ima neparnih prostih brojeva?

5. Ako je p, $q \in P \cap (4D+1)$, da li je $4pq-1 \in 4D+1$?

6. 1) Dokaži da ima beskonačno mnogo prostih brojeva u razredu $4D+3$. Uputa: promatraj broj $a=4p_1 \cdot \cdot \cdot p_k-1$ za $p_k \in 6P \cap (4D+3)$.

   2) Dokaži da je skup $P \cap (6D+5)$ beskonačan. Uputa: promatraj pomoćni broj $6p_1p_2 \cdot \cdot \cdot p_k-1$ za $p_k \in 6D+5$ jer on ima sigurno prost faktor iz $6D+5$.

   3) Prethodne dvije činjenice su specijalni slučajevi ovog teorema (Lejeune-Dirichlet, 1837): Ako prirodni brojevi m, n nemaju nikakvog

zajedničkog djelioca >1, tada je skup $P\cap(m\,N+n)$ beskonačan tj. ima beskonačno mnogo prostih brojeva u aritmetičkoj progresiji $m\,N+n$.

7. Navedi bar jedan član iz $P(n,\ 2\,n)$ za $n=3,\ 6,\ 10,\ 100,\ 10000$ (isp. Pogl. 6, § 7.9.1).

8. Dokaži da su ovi brojevi složeni: 1) n^4+4 za $n>1$; 2) $2^{4n+2}+1$ za $n\geq 1$; 3) $2^{m(2n+1)}+1$ za bilo koje $m,\ n\in N$.

9. **Oko velikih prostih brojeva.** 1) Na poč. 19. vijeka najveće poznato p bio je broj $2^{31}-1=2147483647$ (našao ga je još Euler); 2) do 1951. najveće p bilo je $2^{127}-1$ (ima 39 cifara; našao ga Lucas); 3) 1952. god. na elektronskom računskom stroju SWAC dokazalo se da je $2^{1279}-1$ prost broj (ima 386 cifara); iste godine na tom stroju je dokazano da su i brojevi 2^n-1 za $n=2203,\ 2281$ prosti (imaju 634 odn. 687 cifara); do 1960. zna se za $2^{2317}-1$ kao najveći poznat prost broj; ima 969 cifara. 4) Do 1960. znalo se za 20 prostih brojeva s preko 100 cifara; svi su određeni pomoću elektronskih računskih strojeva.

10. Svih 12 članova aritmetičke progresije $23143,\ 23143+30030,\ \ldots$ su prosti brojevi (Golubijev); to je najduža aritmetička progresija s takvim svojstvom što je poznamo do 1960. godine.

11. Ne zna se da li u nizu $p_1,\ p_2,\ p_3,\ \ldots$ prostih brojeva ima beskonačno mnogo *tročlanih aritmetičkih progresija* građenih od po tri uzastopna prosta broja (stvar je potvrdna, ako se tu briše riječ „uzastopna“).

12. *Cullenovi brojevi* oblika su $n.\ 2^n+1=C_n$. Uvjeri se da su brojevi $C_3,\ C_4,\ C_{10}$ složeni. Pokazano je da je C_{141} prost Cullenov broj; ne zna se da li ih ima većih.

13. Mersenne-ovi brojevi[1] $M_n=2^n-1$. 1) Odredi nekoliko tih brojeva M_n. U god. 1960. znalo se 18 brojeva M_n koji su prosti, a odgovaraju vrijednostima: $n=2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 61,\ 89,\ 107,\ 127,\ 521,\ 617,\ 1279,\ 2203,\ 2281,\ 3217$; od tih 18 brojeva M_n najveći je M_{3217}; najmanji su $M_2=3,\ M_3=7,\ M_5=31,\ M_7=127,\ M_{13}=8191$. 2) Dokaži da vrijedi: $M_1=1,\ M_2=3,\ M_{n+2}=3\,M_{n+1}-2\,M_n$ za $n\in N$; 3) Dokaži:

$$|x|<1/2 \Rightarrow \frac{1}{(1-x)(1-2x)}=\sum_{n=1}^{\infty} M_n\,x^{n-1},\ \text{stavljajući}\ x^0=1.$$

4) Mislilo se dosta dugo da iz $M_n\in P$ slijedi $M_{M_n}\in P$; međutim god. 1935. D. J. Wheeler je to mišljenje opovrgao dokazavši da je broj $M_{M_{13}}=2^{8191}-1$ složen (taj broj ima 2466 cifara). 5) Dokaži da je $M_{23}=47178481\in P$; 6) M_n je suma geometrijskog niza 2^n; nekoji Mersenovi brojevi su sume i aritmetičkih nizova koji počinju sa 1, 2; npr. $M_2=1+2$, $M_4=1+2+3+4+5$, $M_{12}=1+2+\cdots+90$; drugih slučajeva nema (Browkin-Schinzel, 1956). 7) Ne zna se ni za koji prost broj p sa svojstvom da M_p bude djeljivo kvadratom.

---

[1] M. Mersenne [č. Mersen] (1588—1638), francuski matematičar.

14. Promatraj niz $f_n = n! + 1$; u tom nizu ima beskonačno mnogo složenih brojeva, ali se ne zna da li taj niz f_n sadrži beskonačno mnogo prostih brojeva. Dokaži da su brojevi $n! + k$, za $k = 2, \ldots, n$ složeni.

15. *Kineska hipoteza* (oko — 4. vijeka) glasila je: *broj* $k_n = 2^n - 2$ *djeljiv je sa n onda i samo onda ako je n prost broj.* I Leibniz je mislio da je kineska pretpostavka istinita. 1) Međutim, ona nije istinita jer je broj k_{341} djeljiv složenim brojem $341 = 11 \cdot 31$. 2) Dokaži ovo: ako prirodni broj m dijeli prirodni broj n, onda $2^m - 1$ dijeli $2^n - 1$; na osnovu toga dokaži: ako broj m opovrgava kinesku hipotezu, onda je opovrgava i broj $2^m - 1$; 3) Istom je u 1950 (D. H. Lehmer) nađen paran broj n (i to $161038 = l$) koji dijeli $k_n = 2^n - 2$; pokušaj dokazati da je $l \mid (2^l - 2)$ znajući da je $l = 161038 = 2 \cdot 73 \cdot 1103$, $3^2 \cdot 29 \cdot 617 = 161037$, $2^9 - 1 = 7 \cdot 73$, $2^{29} - 1 = 1103 \cdot 486 \cdot 486737$; 3) Ima beskonačno mnogo parnih brojeva n koji dijele k_n (N. G. W. H. Beeger, 1951).

16. *Apsolutno pseudoprosti brojevi.* To su brojevi n za koje je $n \mid (a^n - a)$ za svako $a \in N$. Najmanji takav broj je $561 = 3 \cdot 11 \cdot 17$; ima i drugih; ne zna se da li ih ima beskonačno mnogo.

17. *Hipoteza* (Giuga 1950): $n > 1 \wedge n \in P \Leftrightarrow n \mid (1 + \Sigma \dot{n}^{(n-1)}$. Ta je pretpostavka provjerena za $n < 10^{1000}$.

18. Problem. Ima li beskonačno mnogo prostih brojeva kojima su cifre 1, 2?

19. Problem. Ima li beskonačno mnogo prostih brojeva oblika $n^2 + 1$?

20. Problem. Ima li između $\dot{D}$ i $\dot{D}^2$ bar jedan prost broj?

21. Problem. Je li skup $P(n^2, n^2 + n)$ neprazan?

22. Problem. Je li $P(n^2, (n+1)^2)$ neprazno?

23. Hipoteza (Sierpiński) Da li za $n = 2, 3, \ldots$ svaki od n redića

$$\begin{aligned} &1, 2, 3, \ldots n \\ &n+1, n+2, \ldots, 2n \\ &2n+1, \ldots \quad , 3n \\ &\ldots\ldots\ldots\ldots\ldots \\ &(n-1)n, n(n-1)n+1, \ldots, n^2 \end{aligned}$$

sadržava bar jedan prost broj?

Ako je $n \leq 9$ tada svaki od prvih n redića sadržava neki prost broj.

24. Za skoro svako n skup $P(n^3, (n+1)^3)$ je neprazan (W. H. Mills, 1947).

25. Hipoteza (Schinzel): Ako je x realan broj i $x \geq 117$, tad je $P(x, x + \sqrt{x})$ neprazno; to je ispravno najmanje za $117 \leq x < 10^7$ (Schinzel).

26. Hipoteza. Svakom realnom broju $x \geq 8$ pridružen je bar jedan prost broj smješten između x, $x + (\log x)^4$.

27. **Stroga hipoteza** (Bunjakovski: $s=1$, Schinzel: $s>1$): Neka je s prirodan broj, a $f_1(x)$, $f_2(x)$, ..., $f_s(x)$ niz od s polinoma s cijelim koeficijentima s ovim svojstvima: α) koeficijent najvišeg člana u svakom od s polinoma jednak je 1; β) nijedan od tih polinoma nije produkt od 2 polinoma stupnja >0; γ) ne postoji cio broj >1 koji bi za svako $x\in D$ dijelio produkt $f_1(x)\cdot f_2(x)\cdot\cdot\cdot f_s(x)$. Tada ima beskonačno mnogo prirodnih brojeva n sa svojstvom da su svi brojevi $f_1(n)$, ..., $f_s(n)$ prosti.

Posljedice prethodne hipoteze su vrlo brojne; evo ih nekoliko; nijednu od njih ne umijemo ni dokazati ni opovrgnuti: 1) ima beskonačno mnogo prostih brojeva-blizanaca: 2) Za svako n (specijalno za $n=1$, problem blizanaca!) ima jednadžba $p-q=2n$ beskonačno mnogo rješenjâ; pri tom $p, q\in P$; 3) Skup $P\cap(N^2+1)$ je beskonačan; 4) ima ∞ prostih brojeva oblika x^2+y^2+1 (inače se može dokazati da ima beskonačno prostih brojeva oblika $x^2+y^2+z^2+1$; dokaz je zamršen!); 5) Postoje proizvoljno brojni *aritmetički* nizovi koji se sastoje od uzastopnih prostih brojeva (takav je npr. 4-član niz 251, 257, 263, 269, s razlikom $d=6$); 6) Ima beskonačno mnogo prostih brojeva koji su zbroj od kvadratâ dvaju prostih brojeva (npr. $13=2^2+3^2$, $29=2^2+5^2$); 7) Ima beskonačno mnogo $p\in P$ za koje je 2^p-1 *non* $\in P$; 8) Ima beskonačno mnogo apsolutno pseudoprostih brojeva.

I. M. Vinogradov (* 1891), savremeni ruski matematičar

28. Goldbachova hipoteza (1742)[1]: *Svaki neparan broj* ≥ 9 *može se prikazati kao zbroj od* 3 *prosta broja.* Ta hipoteza još nije provjerena; no Vinogradov ju je 1937. dokazao za skoro svaki neparan broj, tj. skup $(2N+1)\setminus(P+P+P)$ je konačan.

K. G. Borozdkin (Trudí Svesojuznogo matem. s'jezda, 1956, Moskva, T. 1 str. 3) dokazao je da je $\log\log C_0\leq 16{,}038$ pri čemu C_0 (konstanta Vinogradova) označuje prvi broj iznad kojega gornji iskaz vrijedi.

29. Ne zna se da li je skoro svaki parni broj suma od dva prosta broja.

30. Funkcija $P(x)=\pi(x)-\int_2^x \frac{dt}{lnt}$. Mislilo se da je $P(x)\leq 0$ za $x>0$; no, Litllewood je 1914. dokazao da ta funkcija uzima i pozitivnih i negativnih vrijednosti; nula-tačke funkcije P su strahovito velike, naj-

[1]) C. Goldbach [č. Goldbah] (1690—1764), ruski matematičar.

manja je reda veličine $10^{10^{10^{34}}} = s$ u smislu da za neko $x \leq s$ vrijedi $P(x) > 0$ (Skewes, 1933); to je ujedno najveći prirodni broj koji se dosad pojavio u konkretnim problemima.

31. *Malo o. Simbol* $\ll$. Neka su f, g realne funkcije koje su definirane bar za sve realne brojeve $> a$, gdje je a neki realan broj; neka je $gx > 0$; iskazuje se u obliku jednakosti $f = o(g)$ činjenica da je $\lim \frac{fx}{gx} = 0$. $x \to \infty$

Piše se $f = O(g)$ (prema Landau-u) ili $f \ll g$ (prema Vinogradovu), ako postoje brojevi $c > 0$, $x_0 > 0$ sa svojstvom $|fx| \leq cgx$ za svako $x > x_0$. Tako npr. nije $\pi(x) = O(1)$, jer bi $\pi x = O(1)$ značilo da je funkcija πx omeđena.

Tako npr. Čebišev je dokazao da između n i $2n$ postoji bar jedan prost broj; dakle je $p_n < p_{n+1} < 2p_n$ tj. $p_{n+1} - p_n < p_n$; odatle $p_{n+1} - p_n = O(p_n)$. Međutim, vrijedi $p_{n+1} - p_n = O(p_n^{3/4+\varepsilon})$ za svaki realan broj $\varepsilon > 0$ (Čudakov).

32. *Funkcija Čebiševa* glasi $\vartheta(x) = \sum_{p \leq x} ln(p)$ za svako $x \geq 2$; nacrtaj tu funkciju za $x \leq 100$. Može se pokazati da je

$$\vartheta x \, ln \, x + \sum_{p \leq x} \vartheta\left(\frac{x}{p}\right) ln \, p = 2 x \, ln \, x + o(x \, ln \, x).$$

Ta relacija izlazi iz slijedećeg osnovnog teorema tzv. analitičke teorije brojeva: Funkcije

$$\pi(x), \frac{x}{ln \, x} \text{ asimptotski su jednake, tj. } \lim_{x \to \infty} \frac{\pi x}{x/ln \, x} = 1.$$

33. 1) Stavi li se $\zeta(s) = \sum_{n=i}^{\infty} n^{-s}$ te $\zeta(s) = \frac{1}{s-1} + \sum \frac{(-1)^n \gamma_n}{n!} \cdot (s-1)^n$, tada se dobije niz brojeva $\gamma_0, \gamma_1, \gamma_2, \ldots$; ne zna se ni za koji od njih da li je racionalan ili nije (γ_0 je Eulerov broj $= \lim_{k \to \infty} \left(-ln \, k + 1 + \frac{1}{2} + \frac{1}{3} + \right.$ $\left. + \cdots + \frac{1}{k}\right)$. 2) Među brojevima γ_k za $k \in 2N$ (odn. $k \in 2N-1$) ima beskonačno mnogo pozitivnih i beskonačno mnogo negativnih (D. Mitrović, 1957); 3) Problem. Da li za svaki prirodan broj $m > 1$ i svaki razred $mN - m' = K$ postoji beskonačno mnogo pozitivnih i beskonačno mnogo negativnih brojeva γ_n s indeksima n u promatranom razredu K?

34. Problem. Neka $p(n_1, n_2, \ldots, n_k)$ znači prvi prost djelilac broja $n_1 \cdot n_2 \cdot \cdots \cdot n_k + 1$; promatraj niz 2, $p_2 = 3$, $p(2, 3) = 7$, $p(2, 3, 7) = 43$, $p(2, 3, 7, 43) = 13, \ldots$ Koliko ima prostih brojeva koji ne pripadaju tako obrazovanom nizu?

35. Problem: Ne zna se da li u nizu

$$1,\quad 11,\quad 111,\quad 1111,\ldots$$

ima beskonačno mnogo prostih brojeva; opći član toga niza glasi $a_n = 9^{-1}(10^n - 1)$. Prema Kraičiku broj a_{23} je prost; odredi nekoliko drugih prostih članova.

36. Neka je $q_1 = 2$, $q_2 = 5$; neka q_n označuje najmanji prosti broj $> q_{n-1}$ sa svojstvom $(q_n - 1) \mid 2\,q_1\,q_2 \cdot \cdots \cdot q_{n-1}$; odredi još koji član niz q_n. Ne zna se da li je taj niz beskonačan.

37. Dokazati: $n^4 + 4 \in P \Leftrightarrow M(3n + 8,\ 2n^2 + 9n + 7) = 1$ (dostavio Šami Zoran).

8. PROBLEM NAJBLIŽEG SRODSTVA U SKUPU *N* PRIRODNIH BROJEVA

8.1. U prirodnom poretku po veličini samo su dva najbliža prava srodnika svakoga prirodnog broja $n > 1$ i to: $n - 1$ (neposredni pravi predak)[1] i $n + 1$ (neposredni pravi potomak). To je tako formalno. Međutim, stvarno, mi nismo u stanju zamisliti konstrukciju tih brojeva $n - 1$ i $n + 1$ niti ih predstaviti (isp. § 7.12).

8.2. U prirodnom poretku $(N; \mid)$ po djeljivosti problem najbližih pravih srodnika među prirodnim brojevima je još teži nego u poretku $(N, \leq)$ po veličini. Doduše, za svaki prirodni broj n neposredni pravi potomci čine beskonačnu obitelj nP svih brojeva $n\dot{P}$ ($\dot{P}$ prolazi beskonačnim skupom P prostih brojeva 2, 3, 5, 7, 11, ...). No, odrediti sve te potomke ne umijemo ni formalno jer ne znamo kako se stvarno nižu svi prosti brojevi. A kako izgledaju neposredni pravi *preci* prirodnog broja $n > 2$ u mreži $(N; \mid)$ (v. sliku u pogl. 6. § 7)? Oni čine porodicu sa članovima n/p, pri čemu p prolazi skup prostih faktora broja n; ako je n prost broj, onda je, naravno, broj 1 njegov jedini neposredni predak!

8.3. Problem zajedničkih najbližih srodnika.[2] Najveća zajednička mjera i najmanji zajednički kratnik. Najbliži zajednički prethodnik (potomak) dvaju prirodnih brojeva a, b u djelidbenoj strukturi je najveći (najmanji) njihov zajednički divizor (dividend). Za brojeve 4, 6 takvi su srodnici 2 kao preteča i 12 kao zajednički nasljednik. Za brojeve 5, 15 bili bi to 5 i 15.

Uopće, ako su a i b u srodstvu po liniji djeljivosti, onda je preteča manji od njih, a potomak veći od njih.

Najbližeg preteču brojeva a i b u srodstvu po liniji djeljivosti označivat ćemo sa $\mathrm{M}(a, b)$ ili $a\,\mathrm{M}\,b$ i zvati: »*najveći zajednički divizor*« brojeva a i b; dualno, imamo $\mathrm{W}(a, b)$ ili $a\,\mathrm{W}\,b$ (*najmanji zajednički kratnik*).

8.4. Pojava problema: naći najveći zajednički faktor, odnosno najmanji zajednički kratnik zadanih prirodnih brojeva. U uređenju $(N, \leq)$ po veličini svaki je par brojeva x, y uporedljiv: vrijedi $x \leqq y$ ili $y < x$.

---

[1]) Pod dodatkom „pravi" misli se na to da ne bude n uključeno kao svoj vlastiti predak, odnosno potomak.

[2]) Tu se i svaki član smatra svojim vlastitim najbližim pretkom i nasljednikom.

Za uređenja po mjernosti ili djeljivosti to ne vrijedi, npr., niti je $4 \mid 6$ niti $6 \mid 4$. Zato se nameće pitanje kako za dva proizvoljna prirodna broja odrediti u mreži $(N, \mid)$ *najvećega* zajedničkog prethodnika i *najmanjega* zajedničkog potomka! Zovemo ih „najveća zajednička mjera" i „najmanji zajednički kratnik" brojeva a, b; označit ćemo ih sa $x \,\mathrm{M}\, y$, odnosno sa $x \,\mathrm{W}\, y$.

Stvar je, naravno, jednostavna ako je x mjera od y; tada je

$$x = x \,\mathrm{M}\, y \quad \text{i} \quad y = x \,\mathrm{W}\, y;$$

naime, jasno je da mjera (kratnik) nekog broja n iz N ne može biti veća (manja) od n.

Zanimljivo je da se na taj vrlo specijalni slučaj svodi i opći slučaj! To ćemo dokazati u § 10 pomoću tzv. Euklidovog algoritma o dijeljenju.

9. OSNOVNI TEOREM O DIJELJENJU

9.0. Ideja. Riječ je o problemu da nađemo koliko se *cijelo puta* zadani broj m nalazi u zadanom broju a. Rezultat dijeljenja jednoznačno je određen. Razapnimo skup $m\,D$ po liniji i nađimo gdje je a. Iskaz teorema je u § 9.5. i 9.6.

9.1. Zadajmo neki cijeli broj m; pridružimo svakom cijelom broju $\dot{D}$ produkt $m\,\dot{D}$. Imamo preslikavanje $\dot{D} \to m\,\dot{D}$. Skup $m\,D$ svih vrijednosti tog preslikavanja sastavljen je od članova ove aritmetičke biprogresije s diferencijom m:

$$\ldots,\ m\cdot -2,\ m\cdot -1,\ 0,\ m,\ m\cdot 2,\ m\cdot 3,\ \ldots$$

I svaki cijeli broj a ili je u $m\,D$, tj. jedno $m\,\dot{D}$, ili u toj biprogresiji leži između dva **susjedna** člana. Označimo sa mq najveći član iz $m\,D$ koji je $\leq a$;

Sl. 6.9.1.

naravno da je mq potpuno određeno i da već naredni veći članu $m\,D$ premašuje a. Dakle, višak $a-mq$ (označimo ga sa r) broja a nad mq takav je da je ≥ 0 i $< |m|$ ($|m|$ znači m ako je $m>0$; ako je $m<0$, onda $|m|$ znači $-m$).

Imamo, dakle,

$$r = a - mq, \quad 0 \leq r < |m|, \quad \text{odnosno}$$

$$a = mq + r, \quad 0 \leq r < |m|, \quad q, r \in D. \tag{1}$$

Npr., za $a = 28$, $m = 3$ imamo $28 = 3 \cdot 9 + 1$.

Isto za $a = -28$, $m = 3$ imamo $-28 = 3 \cdot -10 + 2$.

9.2. Rezultati q i r pri gornjem omjerivanju broja a sa m zove se *cijelo kvocijenta* i *ostatak dijeljenja* a sa m.

9.3. Jednoznačnost. Dobiveni brojevi q i r u (1) potpuno su određeni. Naime, kad bi stvarno uz (1) postojale još slične relacije

$$a = mQ + R, \quad 0 \leq R < |m|, \quad Q, R \in D, \tag{2}$$

onda oduzimanjem druge jednadžbe od prve izlazi:

$$a - a = (mq + r) - (mQ + R)$$

$$0 = m(q - Q) + (r - R)$$

$$|m| \; |q - Q| = |r - R|. \tag{3}$$

No, oba broja r, R smještena su u poluintervalu $[0, |m|)$ (desni kraj ključen); zato je razmak $|r - R|$ tih brojeva r, R manji od $|m|$, tj.

$$|r - R| < |m|,$$

pa bi iz (3) izašlo:

$$|m| \cdot |q - Q| < |m|.$$

Kako su sva slova ovdje cijeli brojevi, izlazi odatle nužno da je lijeva strana $= 0$, tj. $|q - Q| = 0$, tj. $q - Q = 0$, tj.

$$q = Q. \tag{4}$$

No zbog (4) postaje (3):

$$|m| \; 0 = |r - R|, \quad \text{tj.} \quad 0 = |r - R| \quad \text{i odatle} \quad r = R.$$

Ovo sa (4) dokazuje da su kvocijent q i ostatak r u (1) jednoznačno određeni.

9.4. Isto bi takav dokaz bio da smo radili s racionalnim ili realnim brojevima. Na taj način došli smo do rezultatâ, koje ćemo ispisati da se na njih možemo pozvati: oni su od osnovne važnosti.

⟶ 9.5. Osnovni teorem o dijeljenju u kolu *D*. *Ako je* (a, m) *bilo kakav uređen par članova iz D uz jedino ograničenje* $m \neq 0$ (*divizija sa* 0 *isključena*!), *tada postoji jedan jedini uređen par* (q, r) *članova iz D za koje je*

$$a = mq + r,$$

$$0 \leq r < |m|,$$

r je najmanji broj ≥ 0 *tako da diferencija* $a - r$ *bude djeljiva sa m, tj. da bude* $a \equiv r \pmod{m}$.

Pri tom modul $|m|$ *od m znači m ako je* $m \geq 0$; *ako je* $m < 0$ *tada* $|m|$ *znači* $-m$. *Broj q zove se cijelo kvocijenta brojeva a i b*; *r se zove ostatak pri diobi broja a brojem m.*

Uređen par (q, r) može se označiti funkcionalno sa $E(a, m)$[1]; time se hoće naznačiti da on zavisi od polaznog para (a, m). To bi onda značilo da bismo sa $E_1(a, m)$ mogli označiti cijelo kvocijenta, a sa $E_2(a, m)$ ostatak pri diobi a sa m.

---

[1]) Oznaka E dolazi u vezi s označivanjem *najvećeg cijela* broja $\leq x$: označuje se sa Ex li $E(x)$: npr., $E(5^1/_3) = 5$, $E(-5^1/_3) = -6$ (jer je $-5^1/_3 < -5$).

Npr., cijelo kvocijenta broja -1059 i broja 48 dobije se tako da se podijeli $|-1059|$ sa 48, količniku doda 1, promijeni znak; ostatak je 48—3; izlazi $-1059 = 48 \cdot -23 + 45$, tj. $E(-1059,48) = (-23,45)$.

Teorem 9.5 možemo simbolikom kongruencija izraziti i ovako:

9.5.1. Za svako cijelo a i svako cijelo $m \neq 0$, broj r iz teorema 9.5 je najmanji neodrečni cijeli broj x za koji je razlika $a-x$ djeljiva sa m, tj. za koji je $a \equiv x \pmod{m}$.

⟶ **9.6. Osnovni teorem o dijeljenju u kolu Q racionalnih, odnosno kolu R realnih brojeva.** *Ako je* (a, m) *bilo koji uređen par članova iz* Q (*odnosno iz* R) *uz jedino ograničenje da je* $m \neq 0$, *tada postoji jedan jedini cio* q *i* r *za koji je*

$$a = mq + r$$

$$0 \leq r < |m|.$$

Nužno je $r \in Q$, *odnosno* $r \in R$.

9.7. U praksi specijalno često dolazi $m \in \{10^n, 12, 24, 30, 60, 360, 365, 2\pi\}$. Tako npr. za svaki broj a imamo:

$$\cos a = \cos r, \text{ gdje je } a = 2\pi D + r,\ 0 \leq r < 2\pi, \text{ tj.}$$

$\cos a = \cos E_2(a, 2\pi)$. Isto tako $\operatorname{tg} a = \operatorname{tg} E_2(a, \pi)$, itd.

Bitno će biti da analogan teorem dokažemo u kolu polinomâ; samo će onda umjesto $|b|$ stajati stupanj polinoma b; nešto slično vrijedi u kolima $D + iD$, $Q + iQ$, $R + iR$ kompleksnih brojeva.

9.8. Primjedba. Od interesa je funkcionalno sagledati da se teoremom 9.5. iskazuje određeno jednoznačno preslikavanje Descartesova produkta

$$D \times (D \setminus \{0\}) \quad \text{na Descartesov produkt} \quad D \times D.$$

Isto tako teorem 9.6. iskazuje određeno preslikavanje Descartesova produkta

$$R \times (R \setminus \{0\}) \quad \text{u Descartesov produkt} \quad R \times R,$$

pa čak i u

$$D \times R[0, \infty); \quad \text{pri tom} \quad R[0, \infty)$$

označuje množinu svih neodrečnih realnih brojeva.

Rjeđe se nailazi na tako važne funkcije sa 2 varijable kojima i vrijednost ima 2 varijable! Funkcija

$$(x, y) \to E(x, y)$$

je u tom pogledu zaista prekrasan, prirodan i važan primjer![1)]

[1)] Naravno, moglo bi se uređenoj dvojki brojeva x, y pridružiti u isti mah npr. $x+y$, $x-y$, xy, $x:y$ te dobiti preslikavanje $(x, y) \to (x+y, x-y, xy, x:y)$. Međutim to je preslikavanje ipak izvještačeno!

9.9. Zadaci o dijeljenju

1. Odredi $E(x, y)$ za ove dvojke (x, y): 1) (27, 4); 2) (27, —4); 3) (—27, 4); 4) (—27, —4); 5) (1040, 315); 6) (38, 1/2); 7) $\left(3/4, 1\frac{2}{3}\right)$; 8) (1448, 12); 9) (365, 24); 10) (—2048, 30); 11) (7777, 60); 12) (4444, 360); 13) $(1000, 2\pi)$.
2. U kojem kvadrantu leži veličina kuta: 1) 45^0; 2) 145^0; 3) 1145^0; 4) 11145^0.
3. Odredi $\cos x$ ako je x jednako: 1) 5630^0; 2) 5630; 3) —5630.
4. U kojim razredima mod 4 ima prostih brojeva; u kojima ih nema?
5. Odredi najveće cijelo Ex za brojeve x: 1) 7; 2) 7 1/2; 3) —7; 4) —7 1/2; 5) $7^{1/2}$; 6) $\log 7^{1/2}$; 7) $7 \cdot 71/2$; 8) $(7^{1/2})^7$; 9) e; 10) π; 11) π/n za $n = 2, 3, 4, 5, 6$.
6) Promatraj i nacrtaj funkcije: 1) Ex; dokaži da je $E(x+n) = Ex + En$, ako je $n \in D$; 2) $Ex + E(-x)$; 3) $Ex \cdot Ex^{-1}$.
7. Nađi $s = \sum_{n=1}^{\infty} E\left[\frac{100}{2^n}\right]$ i dokaži da $2^s \mid 100$ ali nije $2^{s+1} \mid 100$. Uzmi umjesto uređenog para (100, 2) kakav drugi par (a, b) prirodnih brojeva i dokaži sličan obrazac (Legendre).
8. Ako je n prirodan broj, onda je:

   1) $E(nx) = \sum E\left(\frac{\dot{n}}{(n+x)}\right)$, 2) $E\,\frac{Ex}{n} = E\,\frac{x}{n}$.
9. Dokaži da je E superaditivna funkcija: $E(x+y) \geq Ex + Ey$ i da je $E(2x + 2y) \geq E\,2x + E\,2y \geq Ex + E(x+y) + Ey$.
10. Za svaki par prirodnih brojeva d, n ima u nizu $1, 2, \ldots, n$ upravo $E\left(\frac{n}{d}\right)$ članova koji su djeljivi sa d.
11. Za koje kompleksne brojeve $x + iy$ izraz $Ex + Ey$ je;

    1) $= 0$; 2) $= 1$; 3) $= 10$; 4) ≤ 10; 5) $\in \{2, 3, 4, 5\}$?
12. Za zadan pozitivan broj a promatraj niz $E(a\dot{N})$; pri tom $\dot{N}$ prolazi skupom prirodnih brojeva; može li se desiti da se taj niz podudara s nizom svih prirodnih brojeva?
13. Neka su a, b pozitivni realni brojevi. Ako su a, b iracionalni brojevi i $a + b = ab$, tad je svaki prirodni broj predstavljiv na jedan jedini način: $E(a\dot{N})$ ili $E(b\dot{N})$. Vrijedi i obrat.
14. Ako je $n > 1$ neparan cio broj, tad je $n(n^2 - 1)$ djeljivo sa 2^3, 3 i sa 24. Dokaži.

15. Dokaži da se razred $12D+1$ ne podudara sa skupom svih cijelih brojeva koji nisu djeljivi ni sa 2 ni sa 3; vredi

$$12D+1 \subsetneq (D \setminus 2D) \cap (D \setminus 3D).$$

16. Dokaži: Produkt od svakih n uzastopnih prirodnih brojeva djeljiv je sa $n!$

17. Nizu brojeva (1) 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, pridruži niz najmanjih neodrečnih ostataka brojeva $2M+E\frac{3M-2}{5}$, pri čemu M prolazi članovima niza (1).

18. Kad A prolazi nizom 1, 2, 3, ... prirodnih brojeva, kako glasi niz

1) $7-E_2(\sigma, 7)$; 2) $9-2E_2(\sigma, 4)$, pri čemu je $\sigma=E\frac{A}{100}$?

19. *Ime dana kojemu je zadan datum.* 1) *Julijanski kalendar* — uveo ga je Julije Cezar 45. godine prije naše ere — uzima da građanska godina traje 365 dana a svaka 4. godina da traje 366 dana kako bi se trajanje građanske godine što bolje približilo trajanju 365,2422... dana tropske godine (trajanje u danima između dva uzastopna sunčeva položaja u proljetnoj tački, kad su dan i noć međusobno jednaki). 2) Kako je prva Nova godina naše ere bila subotom tj. kako je datum $01\cdot01\cdot01$ godine pao subotom, dokaži da julijanskom datumu $d\cdot m\cdot A$ odgovara ovaj dan sedmice:

$$(J) \qquad S(d\cdot m\cdot A)=E_2(d+s+J(A)+a';\ 7);$$

to znači da sumu $d+s+J(A)+a'$ treba podijeliti sa 7 i odrediti pripadni ostatak u skupu $I7=\{0, 1, 2, 3, 4, 5, 6\}$; ime dana određuje se po ključu: 0 (nedjelja), 1 (ponedjeljak), 2 (utorak), 3 (srijeda), 4 (četvrtak), 5 (petak), 6 (subota); pri tome stavljamo: $m=1$ (januar), 2 (februar), ..., 12 (decembar) te $M=m+1$ za $m=1$ i 2 te $M=m$ za $m>2$; $s=2M+E\frac{3M-2}{5}$, $J(A)=7-E_2(\sigma, 7)$, $a'=a+E\frac{a}{4}$, $a=A-100\sigma$, $\sigma=E\frac{A}{100}$. 3) Kojeg je dana u sedmici otkrivena Amerika? (datum: 12. 10. 1492). 4) *Gregorijanski kalendar.* Julijanska godina je duža od tropske godine pa je zato kalendarski 21. mart zaostajao za danom proljetne ravnodnevnice toliko da je u 16. stoljeću ravnodnevnica nosila datum 11.3. (umjesto 21. 3.). Zato je papa Gregorije XIII naredio ovo: (I) Petak što dolazi na četvrtak 04. 10. 1582. ima da nosi datum 15. 10. 1582; (II) godina rednog broja A (sa $A>1582$) bit će prestupna (tj. imati 366 dana) onda i samo onda ako je broj A djeljiv sa 4 uz dodatni zahtjev da A mora biti djeljivo sa 400 ukoliko je A djeljivo sa 100 (zato npr. stoljetne prestupne godine jesu: 1600, 2000, 2400; ... a nijesu 1700, 1800, 1900, 2100, 2200, 2300, 2500, ...). To zapravo znači da Gregorijanska građanska godina traje prosječno 365,2425 dana pa i u tom našem današnjem

računanju s vremenom imamo zaostajanje datuma; po jedan dan na svakih 3550 godina. 5) Dokaži da datum $d \cdot m \cdot A$ po Gregorijanskom kalendaru odgovara sedmični dan

$$S(d \cdot m \cdot A) = E_2(d + s + G(A) + a',\ 7), \tag{G}$$

$$G(A) = 9 - 2\,E_2(\sigma,\ 4)$$

i gdje A znači prirodni broj ≥ 1582; $E_2(\sigma, 4)$ je ostatak djeljenja sa 4 broja σ. 6) Odredi S za ove datume: 05. 01. 1622 (Newtonov rođendan), 31. 3. 1727 (umro Newton), 30. 4. 1777 (rodio se Gauss), 23. 02. 1855 (umro Gauss), 25. 10. 1917 po julijanskom odnosno 07. 11. 1917 po gregorijanskom kalendaru (dan Oktobarske revolucije u Rusiji).

10. NAJVEĆI ZAJEDNIČKI FAKTOR ILI NAJVEĆA ZAJEDNIČKA MJERA ZADANOG NIZA CIJELIH BROJEVA

10.0. Definicija. *Najveća zajednička mjera zadane uređene dvojke* $(a, b) \neq (0, 0)$ *cijelih brojeva je najveći prirodni broj kojim je djeljiv svaki član zadane dvojke* (a, b). Najveća mjera dvojke (a, b) označuje se sa $\mathrm{M}(a, b)$ ili $a\,\mathrm{M}\,b$ (čitaj a mjera b). Najveća zajednička mjera zadanog niza f cijelih brojeva, koji nisu svi $= 0$, jest najveći prirodni broj kojim je djeljiv svaki član zadanog niza f. Označuje se sa $\mathrm{M}\,f$ ili $\mathrm{M}(f_1, f_2, \ldots)$ ili $f_1\,\mathrm{M}\,f_2\,\mathrm{M}\ldots$, npr. $4\,\mathrm{M}\,6 = 2$, $10\,\mathrm{M}\,8 = 2$, $\mathrm{M}(0, 4, 8, 12, \ldots) = 4$, $3\,\mathrm{M}\,3 = 3$, $n\,\mathrm{M}\,n\,\mathrm{M}\,n \cdot \cdot \cdot = n$.

10.0.1. Primjedba. Najveća zajednička mjera *konstantnih nizova nula* obično nije definirana; prema tome, $\mathrm{M}(0, 0)$, $\mathrm{M}(0, 0, 0), \ldots$ obično nije definirano.

10.1. Relativno prosti brojevi. Kaže se da je broj a (*relativno*) *prost prema* b ako im je $\mathrm{M} = 1$, tj. ako $a\,\mathrm{M}\,b = 1$.

Ako je $\mathrm{M}\,f = 1$ za niz f, kaže se da su članovi niza međusobno prosti (inače 2 po 2 ne moraju biti međusobno prosta).

Npr., članovi niza $(4, 3, 6, 16) = f$ su međusobno prosti:

$\mathrm{M}\,f = 1$, mada je npr., $\mathrm{M}(4, 6) = 2$, $\mathrm{M}(4, 8, 16) = 4$, $\mathrm{M}(8, 16) = 8$.

10.2. Osnovna lema o najvećoj zajedničkoj mjeri. *Ako su* a, b, p, r *cijeli brojevi ne svi* 0, *tada iz jednakosti*

$$a = bq + r \qquad \text{izlazi:} \tag{1}$$

$$a\,\mathrm{M}\,b = b\,\mathrm{M}\,r. \tag{2}$$

Dokaz. Najprije iz oblika (1) za broj a izlazi da je svaki zajednički faktor od b i r ujedno faktor i od a („izlučivanje zajedničkog faktora“!); specijalno to vrijedi za faktor $b\,\mathrm{M}\,r$; no taj je broj faktor i od b, tj. $b\,\mathrm{M}\,r$ je zajednički faktor od a i od b pa je zato $\leq$ od najvećega zajedničkog faktora $a\,\mathrm{M}\,b$ tih brojeva a, b. Dakle vrijedi:

$$b\,\mathrm{M}\,r \leq a\,\mathrm{M}\,b. \tag{3}$$

Na isti se način iz relacije $r=a-bq$ zaključuje da je

$$b \,\mathrm{M}\, r \geq a \,\mathrm{M}\, b. \tag{4}$$

Dokazane relacije (3) i (4) kazuju da je relacija (2) ispravna.

10.3. Euklidov algoritam za određivanje broja $a\,\mathrm{M}\,b$.

P r o b l e m. *Zadano je* a, b; *nađi* $a\,\mathrm{M}\,b$.

P r i p r e m n i k o r a k. Ako je jedan od brojeva a, b djeljiv drugim, stvar je gotova jer je $a\,\mathrm{M}\,b=\inf\{|a|, |b|\}$, tj. $a\,\mathrm{M}\,b$ je manji od brojeva $|a|$, $|b|$.

Ako veći od brojeva, recimo $|a|$, nije djeljiv manjim brojem b, onda dolazi naredni:

P r v i k o r a k. Podijelimo a sa b i nađimo najveće cijelo q razlomka a/b i pripadni ostatak r:

$$a=bq+r, \quad 0\leq r<|b|.$$

Prema osnovnom teoremu o diobi, cijeli brojevi q, r potpuno su određeni. Prema osnovnoj lemi o M, imamo jednakost:

$$a\,\mathrm{M}\,b=b\,\mathrm{M}\,r. \tag{5}$$

Time je polazni zadatak: naći $a\,\mathrm{M}\,b$ *sveden na jednostavniji slučaj*: naći $b\,\mathrm{M}\,r$ (jednostavniji zato jer su brojevi b, r jednostavniji od brojeva a, b; bilo je, naime, $|a|>|b|$, a sada je $|b|>r$).

D r u g i k o r a k. Ponavlja se sve što je rečeno, lanac se nastavlja s tim što bivši divizor b sada postaje dividend, a ostatak r postaje divizor. Ako je r mjera ili djelilac od $|b|$, tada je $\mathrm{M}(b, r)=|r|$; ako r nije mjera od b, onda se potraže diobom cijeli brojevi q_1, r_1, za koje je

$$b=rq_1+r_1, \quad 0\leq r_1<r. \tag{6}$$

Opet je

$$b\,\mathrm{M}\,r=r\,\mathrm{M}\,r_1. \tag{7}$$

Zatim bi, ako nije r djeljivo sa r_1, došlo traženje rastava

$$r=r_1 q_2+r_2, \quad 0\leq r_2<r_1$$

itd. dok se proces ne zaustavi. *Proces se mora zaustaviti* jer ostaci r, r_1, r_2 naredni ostaci, koje bismo dobili, bivaju sve manji:

$$r>r_1>r_2>\cdots \tag{8}$$

No, svi su ti brojevi u (8) *redni* brojevi i $<|b|$; zato je niz u (8) nužno *konačan*: dolazi se do prvoga rednog broja 0.

Neka je, npr., $r_{s+1}=0$; to znači da bismo dobili ovakav niz:

$$a, b, r, r_1 r_2 \cdots r_s, 0\,(=r_{s+1}). \tag{9}$$

10.4. Prvi rezultat Euklidova postupka. T e o r e m. *Posljednji divizor pr nizu dijeljenjâ u Euklidovu algoritmu u vezi sa zadanim brojevima* a, b *je upravo najveći zajednički djelilac* $a\,\mathrm{M}\,b$ *tih brojeva.*

Naime, prema onom što smo rekli, imamo ovaj lanac jednakosti:

$$a \,\mathrm{M}\, b = b \,\mathrm{M}\, r = r \,\mathrm{M}\, r_1 = r_1 \,\mathrm{M}\, r_2 = \cdots = r_{s-1} \,\mathrm{M}\, r_s = r_s \,\mathrm{M}\, 0 = r_s, \quad \text{tj.} \tag{10}$$

$$a \,\mathrm{M}\, b = r_s. \tag{11}$$

10.5. Još jedan rijetko dalekosežan zaključak. Pogledajmo niz (9) i njegove članove i sjetimo se kako su ostaci r, r_1, ... dobiveni. Imamo po redu činjenice da je

$$\begin{aligned} r &= a - qb \\ r_1 &= b - q_1 r \\ r_2 &= r - q_2 r_1 \\ &\cdots\cdots\cdots \\ r_s &= r_{s-2} - q_s r_{s-1}, \end{aligned} \tag{12}$$

tako da se počev od trećega svaki član u nizu (9) izražava pomoću svoja dva prethodnika kao *cjelobrojan spoj*. Ako sada idemo natrag u nizu (9) — od posljednjeg člana prema prvom, onda zaključujemo da se r_s *izražava kao cjelobrojan spoj brojeva* a i b; naime, uvrstimo li u (12) pretposljednji izraz u posljednji, izlazi:

$$r_s = r_{s-2} - q_s (r_{s-3} - q_{s-1} r_{s-1} r_{s-2}) = \text{cijelo} \cdot r_{s-3} + \text{cijelo} \cdot r_{s-2}; \tag{13}$$

ako nadalje r_{s-2} izrazimo pomoću svoja dva prethodnika r_{s-3} i r_{s-4}, prelazi (13) u oblik $r_s = \text{cio broj} \cdot r_{s-4} + \text{cio broj} \cdot r_{s-3}$, itd. dok u nizu (10) ne dođemo do kraja: r_s *je linearan homogen izraz od brojeva* a *i* b *s cjelobrojnim koeficijentima*:

$$r_s = xa + yb, \quad \text{gdje je} \quad x \in D,\ y \in D. \tag{14}$$

Tako smo dokazali ovaj važni rezultat:

⟶ **10.6.** Teorem. *U prstenu ili kolu* D *cijelih brojeva ima jednadžba*

$$ax + by = a \,\mathrm{M}\, b \tag{15}$$

bar jedno rješenje; pri tom su a, b *članovi u* D, *ne oba* 0.

Pogledajmo osnovnu vezu (15). Ako je f neki zajednički faktor od a i b, onda su $\frac{a}{f}$, $\frac{b}{f}$ cijeli brojevi, pa iz (15) izlazi:

$$\frac{a}{f} x + \frac{b}{f} y = \frac{a \,\mathrm{M}\, b}{f}. \tag{16}$$

Lijevo je cijelo, dakle je i desno cijelo.

⟶ **10.7.** Teorem. *Svaki zajednički faktor dvaju brojeva faktor je najvećega zajedničkog faktora. Najveći zajednički faktor dvaju brojeva djeljiv je svakim drugim zajedničkim faktorom tih brojeva.*

To je osnovno svojstvo od $a \,\mathrm{M}\, b$ pa se tako $a \,\mathrm{M}\, b$ i *definira* u zamršenijim kolima (npr. u kolu polinomâ). Na taj način rezultate iz 10.4—10.6 možemo oglasiti kao:

⟶ **10.8.** ***Osnovni teorem o najvećem zajedničkom divizoru.*** (I) *Neka je* (a, b) *uređena dvojka članova prstena* D *cijelih racionalnih brojeva; neka je* $b \neq 0$. *Tada se najveći zajednički divizor* $a \,\mathrm{M}\, b$ *od* a i b *dobije kao posljednji divizor u Euklidovu lancu divizija koji se započinje divizijom* a *sa* b. *Veličina* $a \,\mathrm{M}\, b$ *zavisi od* a *i* b *i ne zavisi ni od kakvih drugih veličina; iz* a *i* b *se dobije kao rezultat niza racionalnih operacija zbrajanja, oduzimanja, množenja i dijeljenja.*

(II) *Jednadžba* $ax + by = (a \,\mathrm{M}\, b)$ *dopušta bar jedno rješenje u prstenu* D, *pa je* $a D + b D = (a \,\mathrm{M}\, b) D$.

(III) *Svaki zajednički djelilac djelitelj je najvećeg.*

10.9. Primjer. Nađi najveći zajednički divizor brojeva 4752, 624. Lančasta Euklidova dijeljenja vide se iz ove sheme:

$$4762 : 624 = 7$$

$$384$$

$$624 : 384 = 1$$

$$240$$

$$384 : 240 = 1$$

$$144$$

$$240 : 144 = 1$$

$$96$$

$$144 : \ 96 = 1$$

$$48$$

$$92 : \ \boxed{48} = 2$$

$$0$$

Čitav postupak može se ovako iskazati pomoću 3 rubrike:

$$\begin{array}{rcrl} 4752 & \longrightarrow & 624 & 7 \\ & \swarrow & & \\ 384 & \longrightarrow & 240 & 1 \\ & \swarrow & & \\ 144 & \longrightarrow & 96 & 1 \\ & \swarrow & & \\ \boxed{48} & \longrightarrow & 0 & 1 \end{array}$$

Znak $x \to y$ tu znači: naći najveće cijelo i ostatak pri diobi x sa y. Strelica dalje od y ukazuje na ostatak. Desno se po redu pišu najveća cijela. Ono

što je sa 0 povezano strelicom jest traženo M. (tj. najveća zajednička mjera). Iz prednje sheme može se brzo naći cjelobrojno rješenje jednadžbe

$$4752\,x + 624\,y = 48.$$

Treba početi straga i 48 izražavati pomoću njegova dva prethodnika služeći se pretposljednjim kvocijentom (zato je posljednji kvocijent 2 precrtan). Ide se po redu:

$$\begin{aligned} 48 &= 144 - 96 \cdot 1 = 144 - (240 - 144 \cdot 1) = 2 \cdot 144 - 240 = \\ &= 2 \cdot (384 - 240 \cdot 1) - 240 = 2 \cdot 384 - 3 \cdot 240 = \\ &= 2 \cdot 384 - 3 \cdot (624 - 384 \cdot 1) = 5 \cdot 384 - 3 \cdot 624 = \\ &= 5 \cdot (4752 - 624 \cdot 7) - 3 \cdot 624 \\ &= 5 \cdot 4752 - 38 \cdot 624, \quad \text{tj.} \\ 48 &= 5 \cdot 4752 - 38 \cdot 624. \end{aligned}$$

Rješenje je $x = 5$, $y = -38$.

10.10. Zadaci o najvećem zajedničkom djeliocu (v. § 11.8).

11. NAJMANJI ZAJEDNIČKI KRATNIK

Razmatranja o najmanjem zajedničkom kratniku (djeljeniku, multiplumu) zadanih veličina provode se *dualno* razmatranjima o najvećem zajedničkom faktoru (djeliocu, mjeri); treba permutirati riječi i pojmove: najmanji — najveći djelitelj — djeljenik. I oznaka će biti dualna:[1)]

M, W.

Osnovni teorem će biti $(a\,\mathrm{M}\,b)\cdot(a\,\mathrm{W}\,b) = ab$, odnosno teorem 11.7.

11.1. D e f i n i c i j a. *Najmanji zajednički kratnik uređene dvojke* $(a, b) \neq (0, 0)$ cijelih brojeva a, b koji su $\neq 0$ jest *najmanji* prirodni broj koji je djeljiv sa a i b. Označićemo ga sa $a\,\mathrm{W}\,b$. Za niz $f = (f_0, f_1 \cdots)$, kojemu su članovi iz kola D cijelih brojeva i $\neq 0$, definira se višekratnik $\mathrm{W}\,f = \mathrm{W}\,(f_0, f_1, \ldots)$ ili $f_0\,\mathrm{W}\,f_1\,\mathrm{W}\cdots$ kao *najmanji* prirodni broj koji je djeljiv svakim članom niza f. Npr. $6\,\mathrm{W}\,9 = 18$.

11.2. Naravno, zadani brojevi a, b koji su $\neq 0$, imaju beskonačno mnogo zajedničkih kratnika, npr. produkt ab i brojeve $ab\,D$, koji čine čitavu grupu $(ab)\,D$. Također je jasno da je suma (diferencija) od proizvoljna dva kratnika zadanih brojeva opet njihov kratnik. To znači da svi kratnici obrazuju grupu; pa ako je $v = a\,\mathrm{W}\,b$ *najmanji* pozitivni kratnik, slutimo da je svaki drugi

---

[1)] Da izbjegnemo brkanje operatora M, W, možemo naznačiti ovo mnemotehničko pomagalo: W je u vezi s unijom $\cup$, a M u vezi s presjekom $\cap$ skupova; specijalno će se vidjeti ovo: skup prostih djelilaca od $a\,\mathrm{M}\,b$ (odnosno $a\,\mathrm{W}\,b$) je presjek (unija) množine svih prostih djelilaca od a i one od b (v. § 14.4; 14.5). Nadalje, W kao dvostruko V podsjeća da je riječ o višekratniku! Bolja je oznaka W od v jer je izrazitija veza M, W nego veza M, v.

kratnik V kratnik od toga najmanjeg v. To je očigledno jer, vršeći s v zbrajanja i oduzimanja, ne možemo dobiti nešto >0 i $<v$. Formalno to potvrđujemo i zakonom o dijeljenju: neka je $V=vq+r$, $0\leq r<v$. To znači da bi r kao razlika $V-vq$ dvaju kratnika brojeva a, b bilo također kratnik; zbog $r<v$ moguće je to samo ako je $r=0$ (inače bi r bio manji pozitivni kratnik od najmanjega, što je besmisao).

Tako smo dokazali:

11.3. Teorem. *Svaki kratnik brojeva a, b kratnik je istaknutoga najmanjeg $a\,\mathrm{W}\,b$ koji je $\gtrless 0$ i koji generira grupu $(a\,\mathrm{W}\,b)\,D$ svih kratnika.*[1)]

11.4. O kratniku $V=\frac{ab}{m}$, gdje je $m=a\,\mathrm{M}\,b$.

Očigledno je V kratnik i od a i od b.

Naime, $V/a=b/m$, $V/b=a/m$; no b/m i a/m su cijeli brojevi jer je $m=a\,\mathrm{M}\,b$ zajednička mjera tih brojeva. Dakle je broj V jedan zajednički kratnik brojeva a i b. Da slučajno V nije upravo *najmanji* kratnik! Tako je bar kod jednostavnih primjera! No, prema 11.3. vrijedi ovo:

11.4.1. Broj $V=\frac{ab}{m}$, gdje je $m=a\,\mathrm{M}\,b$, djeljiv je brojem

$$v=a\,\mathrm{W}\,b.$$

11.4.2. Ako dokažemo i obrnuto: $v=a\,\mathrm{W}\,b$ je kratnik od $V=(ab)/m$, dokazali bismo time važnu jednadžbu:

$$\frac{|ab|}{a\,\mathrm{M}\,b}=a\,\mathrm{W}\,b.$$

⟶ **11.4.3.** Teorem $\mathrm{M}(a,b)\ \mathrm{W}(a,b)=ab$.

Dokaz. Stavimo $\mathrm{M}=\mathrm{M}(a,b)$, $\mathrm{w}=\mathrm{W}(a,b)$. Kako w dijeli ab, broj

$$d\overset{\text{def}}{=}\frac{ab}{\mathrm{w}}\in N \tag{1}$$

je cio.

Broj d dijeli i a i b; zato je $d\leq M$. Tvrdimo da je $d=M$. No, broj

$$\mathrm{W}\overset{\text{def}}{=}\frac{ab}{M} \tag{2}$$

je zajednički kratnik od a i b, pa je zato oblika

$$\mathrm{W}=\mathrm{w}\cdot k \tag{3}$$

pri nekom $k\in N$. Na osnovu $\mathrm{w}=\mathrm{W}\,k^{-1}$ daje (1)

$$d=\frac{kab}{\mathrm{W}}=(\text{radi (2)})=k\,M. \tag{4}$$

[1)] Ta je grupa i ideal u kolu D jer je produkt svakog $\dot{D}$ i svakog kratnika (kao kratnik) opet u $(a\,\mathrm{W}\,b)\,D$.

Drugim riječima, broj d je djeljiv sa M. Kako je $d \leq M$ (M je najveća zajednička mjera) znači to da je $k=1$, tj. $d=M$. Zato relacija (3) daje $W=w$; to sa (2) daje

$$w=\frac{ab}{M}$$

dakle $M\,w=ab$, što se i tvrdi teoremom.

11.5. Teorem. Ako je umnožak ab cijelih brojeva a, b djeljiv cijelim brojem c te ako su brojevi a, c međusobno prosti, onda je b djeljivo sa c; simbolički:

$$c \mid ab \wedge a\,\mathrm{M}\,c=1 \Rightarrow c \mid b.$$

11.5.1. Prvi dokaz. Po prethodnom teoremu je

$$a\,\mathrm{W}\,c=ac.$$

No, po pretpostavci c dijeli ab pa je dakle ab djeljivo sa a i sa c, dakle je ab zajednički kratnik od a, c i prema tome djeljiv sa $a\,\mathrm{W}\,c$, tj. sa ac; dakle je $\frac{ab}{ac}\in D$, tj. $\frac{b}{c}\in D$, što smo i htjeli dokazati.

Drugi dokaz. Prema pretpostavci a i c su relativno prosti: $a\,\mathrm{M}\,c=1$. Zato, prema osnovnom teoremu o ekstremalnom faktoru (§ 10.8. (II)), znamo da jednadžba

$$ax+cy=1 \quad (=a\,\mathrm{M}\,c) \tag{5}$$

ima u prstenu D bar jedno rješenje: $x\in D$, $y\in D$. Na desnoj strani u (5) pojavljuje se broj 1; zato množenjem te jednadžbe (5) ispitivanim brojem $\frac{b}{c}$ dobijemo zgodan prikaz tog broja $\frac{b}{c}$:

$$ax\cdot\frac{b}{c}+by=\frac{b}{c}, \quad \text{tj.}$$

$$\frac{ab}{cb}x+by=\frac{b}{c}. \tag{6}$$

No, prema (4), $\frac{ab}{c}\in D$; također je $b\in D$ kao i x i y prema (5); to znači da je čitava prva strana u (6) cio broj, a to znači da je zaista b/c cio broj. Time je i teorem 11.5. dokazan. Prema 11.4.2. dokazan je time i teorem 11.4.3.

11.5.1. Primijetimo odmah kako smo na prirodan način (nastojeći da dokažemo da je $\frac{ab}{m}$ ekstremalan kratnik) došli do teorema **11.5!**

On će nam poslužiti kao ključni položaj za razne dokaze: teorem 11.5. pokazat će se fundamentalnim (isp. § 13).

11.6. Skup svih kratnika broja a je aD; *skup svih kratnika broja* b *je* bD = skup svih bx kad x prolazi kroz D. Skup svih kratnika od a i b je naravno, zajednički dio ili presjek tih skupova aD, bD; taj se presjek označuje:

$$aD \cap bD.$$

No, prema 11.3, svaki je zajednički kratnik od a i b kratnik broja $a \,\mathrm{W}\, b$, dakle leži u množini $(a \,\mathrm{W}\, b)D$ svih kratnika od $a \,\mathrm{W}\, b$; time dolazimo do veze:

$$aD \cap bD = (a \,\mathrm{W}\, b)D. \tag{7}$$

11.6.1. Slična relacija vrijedi i za više brojeva: *za svaki konačan niz cijelih brojeva* $a_0, a_1, \ldots$ *vrijedi relacija:*

$$a_0 D \cap a_1 D \cdots = (a_0 \,\mathrm{W}\, a_1 \,\mathrm{W}\, a_2 \,\mathrm{W} \cdots) D.$$

Skupljajući rezultate 11.4.3, 11.6, 11,6.1 dolazimo najzad do ovoga osnovnog rezultata:

11.7. Osnovni teorem o kratniku dvaju brojeva. *Za svaki par cijelih brojeva* a, b *vrijedi:*

$$(a \,\mathrm{W}\, b) \cdot (a \,\mathrm{M}\, b) = ab \qquad \text{(isp. 11.8.9);}$$

$$aD \cap bD = (a \,\mathrm{W}\, b)D.$$

Za svaki konačan niz cijelih brojeva $a_0, a_1, \ldots . a_k$ *vrijedi:*

$$a_0 D \cap a_1 D \cap \cdots a_k) = (a_0 \,\mathrm{W}\, a_1 \,\mathrm{W} \cdots \mathrm{W}\, a_k) D.$$

Svaki kratnik brojeva $a_0, a_1, \ldots$ *kratnik je od* $a_0 \,\mathrm{W}\, a_1 \,\mathrm{W} \ldots$

11.8. Zadaci o najvećem zajedničkom djeliocu i najmanjem zajedničkom kratniku:

1. Nađi najveći zajednički djelilac M i najmanji zajednički kratnik W ovih brojeva: 1) 24, 42; 2) 24, —42; 3) —24, —42; 4) 18, 50, 80; 5) 73044, 4368; 6) 43726, 24400; 7) 2^5-1, 2^5+1; 8) 3953, 7571.

2. Euklidovim postupkom odredi najveći zajednički djelilac ovih brojeva: 1) 6188, 4709; 2) 81719, 52003, 33649, 30107.

3. Nađi neko cjelobrojno rješenje jednadžbe: 1) $5x+6y=1$; 2) $105x-1000y = 105 \,\mathrm{M}\, 1000$; 3) $347x+100y=1$.

4. Odredi: 1) $2D \cup 3D$; 2) $2D \cup 4D \cup 5D$; 3) $2D \cap 3D$; 4) $15D \cap 20D$; 5) $15D \cap 20D$; 6) $3D \cap (2D+1)$; 7) $3D \cup (2D+1)$; 8) $2D \cup 3D \cup 5D$; 9) $(4D \cup 5D) \cap 3D$.

5. Pitanje kao u zad. 4 pišući svuda $+$ odn. $\cdot$ umjesto $\cup$ odn. $\cap$.

6. Dokaži: $n \,\mathrm{M}\, (n+1) = 1$, $n \,\mathrm{W}\, (n+1) = n(n+1)$.

7. Dokaži: $(n_1 \,\mathrm{M}\, n_2 \,\mathrm{M} \cdots \mathrm{M}\, n_k)^s = n_1^s \,\mathrm{M}\, n_2^s \cdots \mathrm{M}\, n_k^s$ i dualno.

8. Ako su brojevi $n_1, n_2, \ldots, n_k$ dva po dva međusobno prosta, pa ako je $n_1 n_2 \cdots n_k = x^s$, tad su i faktori $n_1, n_2, \ldots, n_k$ s-ti stepeni prirodnih brojeva.

9. Za svaki konačni niz $n_1, \ldots, n_k$ od $k>2$ prirodnih brojeva bez ponavljanja jednakost $\mathrm{M}(n_1, n_2, \ldots, n_k) \cdot \mathrm{W}(n_1, n_2, \ldots, n_k) = n_1 n_2 \cdot \cdot \cdot n_k$ vrijedi onda i samo onda, ako su brojevi $n_1, \ldots n_k$ međusobno dva po dva prosta (o slučaju $k=2$ isp. § 11.7).

10. Dokaži $(a \mathrm{W} b) \mathrm{M} c = (a \mathrm{M} c) \mathrm{W} (b \mathrm{M} c)$;

i dualno $(a \mathrm{M} b) \mathrm{W} c = (a \mathrm{W} c) \mathrm{M} (b \mathrm{W} c)$.

11. Dokaži $(a \mathrm{M} b)\,(c \mathrm{M} d) = ac \mathrm{M} ad \mathrm{M} bc \mathrm{M} bd$; i dualno.

12. Dokaži: 1) $\mathrm{M}(a, b) = 1 \Leftrightarrow \mathrm{M}(a+b, ab) = 1$; 2) $ad - bc = 1 \Rightarrow (a + +b) \mathrm{M} (c+d) = 1$.

13. Ako je $\frac{m}{n} = \frac{m'}{n'}$, $m' \mathrm{M} n' = 1$, tad je $m = km'$, $n = kn'$ za posve određeno cijelo k.

14. Dokaži $(n_0 \mathrm{M} n_1 \mathrm{M} n_2)\,(n_0 n_1 \mathrm{W} n_1 n_2 \mathrm{W} n_2 n_0) = n_0 n_1 n_2$ ili simbolički: $\left(\underset{i}{\mathrm{M}}\, n_i\right) \cdot \left(\underset{i}{\mathrm{W}}\, \frac{c}{n_i}\right) = c$; tu je $c = \underset{i}{\Pi}\, n_i$; $i = \dot{3} = 0, 1, 2$; dokaži da slična formula vrijedi za n_0, n_1, n_2, n_3 i u opće za r prirodnih brojeva $n_r = n_1, \ldots, n_r$ (Le Besgue).

15. Objasni na primjeru i dokaži $\mathrm{W}(2n)' = \mathrm{W}(n+n')$; kao i obično r' prolazi $1, 2, \ldots, r$.

16. Neka je (a, b) određen par prirodnih brojeva sa svojstvom $a \mid b$; odredi sve prirodne brojeve x, y za koje je $x \mathrm{M} y = a$, $x \mathrm{W} y = b$.

17. Problem. Za svaki prirodan broj n stavimo $!n = 1 + 1! + 2! + \cdots + +(n-1)!$ i $M_n = M(!n, n!)$. Da li $n>1 \Rightarrow M_n = 2$?

12. JEDNOSTAVNA INTERVENCIJA POJMA GRUPE. OPET O EKSTREMALNOM ZAJEDNIČKOM FAKTORU (KRATNIKU) ZADANIH BROJEVA

12.0. Maloprije smo (u § 10) dokazali da je najveći zajednički faktor $a \mathrm{M} b$ brojeva a, b oblika $ax + by$ za neke cijele brojeve x, y i da je svaki drugi zajednički faktor od a, b ujedno i faktor od $a \mathrm{M} b$. Analogno svojstvo vrijedi za 3, 4, ... zadana broja. To se može izvesti potpuno iz gornjega osnovnog teoiema o M. Međutim, evo drugog dokaza da se vidi kako se, baratajući direktno s *pojmom grupe*, može doći odmah do dubokih rezultata. To činimo tim radije što smo, eto upravo, dokazali da se grupe javljaju promatrajući i kratnike proizvoljnog broja a, ali isto tako i sve kratnike bilo koja dva zadana broja (§ 11.3).

12.1. Kako izgledaju **zatvoreni okviri za prve dvije računske operacije** u skupu D cijelih brojeva?

Ili tehnički prevedeno: *kako izgledaju aditivne podgrupe u kolu cijelih brojeva*? Jasno je da, polazeći od kakvoga droja m iz D pa vršeći s njim zbrajanja i oduzimanja, dolazimo i do $m+m=2m$, $m-m=0$, $m+m+m=3m \ldots$, tj. dolazi se do množine mD i ništa dalje: *mD je aditivna grupa*. A sada se pita za obrat!

Je li svaka aditivna podgrupa G iz D nužno oblika mD za neko $m \in D$? Naravno, ako se G sastoji jedino od 0, stvar je trivijalna — odgovor je: *da*, jer je $\{0\} = 0 \cdot D$. Ali, ako G ima nešto i osim 0, recimo neki član g, onda je u G i $-g$ (ta nije li G grupa, pa ne sadrži li uz g, 0 također $0 - g$, tj. $-g$). Znači da je zbilja g i $-g$ u G; znači da G sadrži i jedan *pozitivan broj*; pa neka je m *najistaknutiji* među njima: *minimalni pozitivni* član u G (maksimalnog nema!) Je li možda taj član m sposoban da generira čitavo G, tj. da je svako $g \in D$ djeljivo sa m? Pa podijelimo g sa m:

$$g = mq + r, \quad 0 \leq r < m \tag{1}$$

(osnovni teorem o diobi iz § 9). Tu se pojavljuje $r = g - mq$. Naravno, r je u grupi G jer je rezultat od g i m pomoću + i —; no ne može biti $0 < r$ zbog $r < m$ iz (1), jer bi $r > 0$ značilo da je r *pozitivan* član u grupi G manji od najmanjeg m — apsurd. Dakle, u (1) znak $\leq$ znači $=$, tj. $0 = r$ pa (1) daje $g = mq$, tj. $g \in mD$, tj. $G \in mD$, tj. $G \subset mD$, što s očiglednom relacijom $mD \subset G$ daje naslućivanu jednakost $G = mD$. Tako smo došli do ovog:

⟶ **12.2.** Teorem. *Svaka aditivna grupa $(G, +)$ u kolu $(D, +, \cdot)$ cijelih brojeva nužno je oblika mD sa $m \in D$ i $m \geq 0$*[1]*;*

12.2.1. Primijenimo sada teorem 12.2. na specijalne podgrupe u D. Pa neka je

$$(m_1, m_2, \ldots, m_s) \tag{2}$$

bilo kakav niz od s cijelih brojeva, ne svi 0; tada imamo podgrupe:

$$m_1 D,\ m_2 D,\ \ldots,\ m_s D. \tag{3}$$

Njihov je presjek isto grupa, koja se odmah nameće; suzdržimo se časak pa, gledajući skup $aD + bD$ iz teorema 10.8, promatrajmo i ovdje odgovarajuću sumu:

$$m_1 D + m_2 D + \cdots + m_s D, \tag{4}$$

tj. množinu svih vrijednosti

$$m_1 x_1 + m_2 x_2 + \cdots, \text{ gdje su } x_1, x_2, \ldots, m_s \in D. \tag{5}$$

Očigledno je (4) grupa u odnosu na adiciju. Dakle, po teoremu 12.2. jednadžba

$$m_1 D + m_2 D + \cdots + m_s D = yD \tag{6}$$

ima bar jedno rješenje y u D. A za tim smo i išli, jer tu je sve sadržano. Prvo, y je faktor od svakog m_i. Naime, ako u (5) stavimo $x_i = 1$ i $x_k = 0$ za sve druge indekse, dobije se upravo m_i kao član u (4), dakle (zbog (6)), $m_i \in yD$, tj. $y \mid m_i$.

Dakle je zaista y faktor svih članova m_i.

---

[1]) Zato je G i *ideal u tom kolu* (ideal kola D je svaka aditivna grupa G sa svojstvom $GD \subset G$ i $DG \subset G$, tj. množenje iz kola s članovima iz grupe ne vodi van grupe). Naime, u gornjem primjeru $GD = mD \cdot D = m(D \cdot D) = mD = G$.

Sa druge strane, $y \in y\,D$ (zbog $y = y \cdot 1$), dakle zbog (6), vrijedi $y \in (6)_2$; to znači da je y oblika (5), dakle:

$$m_1 x_1 + m_2 x_2 + \cdots = y \text{ za jedan niz } x_1, x_2, \ldots, \in D. \tag{7}$$

Odatle za *svaki* zajednički faktor f od svih m_i izlazi:

$$\frac{m_i}{f} x_1 + \frac{m_2}{f} x_2 + \cdots = \frac{y}{f}. \tag{8}$$

Lijevo su cijeli brojevi $\frac{m_i}{f}$. Odgovarajući umnošci također; znači, lijeva strana u (8) je cio broj, dakle i desna, tj. $f \mid y$.

Time smo druga dva dijela osnovnog teorema o M dokazali za proizvoljno dug konačan niz cijelih brojeva.

12.3. ***Osnovni teorem o najvećem zajedničkom faktoru.*** (I) *Za svaki konačan niz* $m = (m_1, m_2, \ldots, m_s)$ *cijelih brojeva jednoznačno je određen redni broj* x, *za koji je*

$$m_1 D + m_2 D + \cdots + m_s D = x D;$$

x je najveća zajednička mjera brojeva $m_1, m_2, \ldots, m_s$:

$$x = \mathrm{M}(m_1, m_2, \ldots, m_s)$$

$$m_1 D + m_2 D + \cdots = \mathrm{M}(m_1, m_2, \ldots, m_s) D.$$

(II) *x je skalaran produkt zadanog niza $m_1, m_2, \ldots, m_s$ i bar jednog, iste dužine, niza članova iz D:*

$$x = m_1 x_1 + m_2 x_2 + \cdots \text{ sa } x_1, x_2, \ldots \in D.$$

(III) *Svaki zajednički divizor brojeva $m_1, m_2, \ldots$* divizor je i od $\mathrm{M}(m_1, m_2, \ldots)$.

Na sličan način, promatrajući umjesto zamršenije grupe (6) ponovno jednostavniju grupu

$$m_1 D \cap m_2 D \cap \cdots \cap m_s D, \tag{9}$$

dolazimo do

12.4. ***Teorema o najmanjem zajedničkom kratniku.*** *Ako je $m_1, m_2, \ldots, m_s$ konačan niz sa članovima iz kola D cijelih brojeva, tada u D postoji jedan jedini član $x \geq 0$ za koji je*

$$m_1 D \cap m_2 D \cap \cdots = x D; \tag{10}$$

x je najmanji zajednički kratnik članova $m_1, m_2, \ldots$ i označuje se sa

$$m_1 \mathrm{W}\, m_2 \mathrm{W} \cdots \text{ili } \mathrm{W}(m_1, m_2, \ldots).$$

Svaki zajednički kratnik svih $m_1, m_2, \ldots, m_s$ kratnik je najmanjega.

Dokaz. Najprije, skup (9) je grupa za adiciju; naime, uzmemo li neke podatke p u (9), znači to da su oni u svim „faktorima“ $m_i D$ presjeka (9); kako je svaki od njih grupa, znači da će i rezultat dobiven iz podataka p zbrajanjem i oduzimanjem biti u svakom od njih, dakle i u njihovu presjeku (9).

A to stvarno znači da je (9) zbilja podgrupa u D. Zato, prema teoremu 12.2, postoji neodrečno rješenje x u D za jednadžbu (10). Dokažimo da je svaki zajednički kratnik V brojeva $m_1, m_2, \ldots, m_s$ kratnik od broja x. No, po definiciji, svaki zajednički kratnik V je u $(10)_1$, dakle zbog (10) i u $(10)_2$, tj. $V \in xD$, tj. $V = xD$, što upravo znači da je V kratnik od x. Dokažimo, obrnuto, da je x zajednički kratnik od $m_1, m_2, \ldots, m_s$. Pa to je trivijalno jer, zbog $x = x \cdot 1$, $1 \in D$ imamo $x \in xD$, tj. $x \in (10)_2$, pa dakle i $x \in (10)_1$, tj. x je zajednički kratnik svih m_i.

Teorem je dokazan.

13. OSNOVNA SVOJSTVA O DJELJIVOSTI. RELATIVNO PROSTI BROJEVI[1)]

Sad smo u stanju da na malom prostoru iznesemo osnovne stvari o relaciji djeljivosti. *Središnju ulogu ima činjenica da se najveći zajednički djelilac* $a \,\mathrm{M}\, b$ *brojeva* a, b *izražava homogeno pomoću* a *i* b, tj. da jednadžba

$$ax + by = a \,\mathrm{M}\, b$$

ima bar jedno rješenje u kolu D cijelih: $x, y \in D$ (osnovni teorem 10.7. i 12.3). Odatle odmah izlazi ovo svojstvo:

13.1. Teorem. *Ako su* a i b *relativno prosti, tj.* $a \,\mathrm{M}\, b = 1$, *tada jednadžba* $ax + by = 1$ *ima bar jedno rješenje u kolu* D *cijelih; i obrnuto: ako je ta jednadžba u* D *rješiva, tada je* $a \,\mathrm{M}\, b = 1$.

⟶ **13.2.** Teorem (Euklid). (I) *Ako su* a, b *relativno prosti prema* c, *onda je i njihov produkt relativno prost prema* c; *simbolički*

$$\text{(II)} \qquad a \,\mathrm{M}\, c = 1, \quad b \,\mathrm{M}\, c = 1 \;\Rightarrow\; (ab) \,\mathrm{M}\, c = 1.$$

Ako je

$$\text{(1)} \qquad B \,\mathrm{M}\, C = 1, \qquad \textit{tada je}$$

$$\text{(2)} \qquad (AB) \,\mathrm{M}\, C = A \,\mathrm{M}\, C$$

za bilo kakve cijele brojeve A, B, C.

Dokaz. Relativna prostost od a i c znači da postoje cijeli brojevi x, y za koje je

$$\text{(3)} \qquad ax + cy = 1.$$

Isto tako, iz $b \,\mathrm{M}\, c = 1$ izlazi da postoje cijeli brojevi x', y' za koje je

$$\text{(4)} \qquad bx' + cy' = 1.$$

Množenjem jednadžbi (3) i (4) dobijemo:

$$(ab)(xx') + c \cdot \text{cijelo} = 1.$$

To, prema (3), znači da je $(ab) \,\mathrm{M}\, c = 1$.

[1)] Treba napomenuti da mi dosad radimo s cijelim brojevima bez obzira na njihovo predstavljanje u numeričkim sistemima.

Još preostaje da dokažemo drugi dio teorema. Najprije, jasno je da desna strana u (2) ne može biti veća od lijeve strane: $(2)_1 \geq (2)_2$. Treba pokazati i dualno da je $(2)_1 \leq (2)_2$, tj. da je svaki zajednički divizor d produkta AB i broja C divizor i broja A. No, međusobna prostost od B i C (relacija (1)) ima za posljedicu da jednadžba

$$Bx + Cy = 1$$

ima neko $x, y \in D$. Odatle, množeći sa A:

$$(AB)\,x + C\,(Ay) = A$$

i dijeleći sa d:

$$\frac{AB}{d}\,x + \frac{C}{d}\,(Ay) = \frac{A}{d}\,.$$

Kako je tu svaki član na lijevoj strani cio broj, znači da je lijeva strana cio broj, dakle je d divizor od A, za čime se i ide.

Time je važni Euklidov teorem 13.2. dokazan.

13.3. Teorem. **Poopćenje prvog dijela Euklidova teorema.** *Ako je svaki član a_i jednoga konačnog niza od cijelih brojeva $a_1, a_2, \ldots, a_r$ relativno prost prema svakom članu $c_1, c_2, \ldots, c_s$ drugog niza cijelih brojeva, tada je produkt $A = a_1 \cdot a_2 \cdot \ldots \cdot a_r$ članova prvog niza relativno prost prema produktu $C = c_1 \cdot c_2 \cdot \ldots \cdot c_s$ članova drugog niza.*

Simbolički: *neka je dan niz od r brojeva a_i i niz od s cijelih brojeva c_j sa svojstvom $a_i \,\mathrm{M}\, c_j = 1$; tada je* $\left(\prod_{k=1}^{r} a_i\right) \mathrm{M} \left(\prod_{j=1}^{s} c_j\right) = 1$.

Dokaz se vodi postepeno na osnovu prethodnog teorema 13.2. (I), koji je zapravo identičan sa slučajem $r = 2$, $s = 1$ u teoremu 13.3. Prema 13.2. (I), $a_1\, a_2$ je relativno prost prema prvom broju c_1; iz istog razloga (piši u 13.2. (I) $a_1\, a_2 = a$, $a_2 = b$; $c_1 = c$) je $a_1\, a_2\, a_3 \,\mathrm{M}\, c_1 = 1$, pa $a_1\, a_2\, a_3\, a_4 \,\mathrm{M}\, c_1 = 1 \cdot \cdot \cdot$ i, najzad, $A \,\mathrm{M}\, c_1 = 1$, gdje je $A = a_1\, a_2 \cdot \cdot \cdot a_r$. Isto tako je $A \,\mathrm{M}\, c_j = 1$. No, iz $A \,\mathrm{M}\, c_1 = 1$, $A \,\mathrm{M}\, c_2 = 1$ izlazi opet, prema teoremu 13.2, da je $A \,\mathrm{M}\, c_1\, c_2 = 1$. Odatle i iz $A \,\mathrm{M}\, c_3 = 1$, izlazi $A \,\mathrm{M}\, c_1\, c_2\, c_3 = 1$, itd., dok se ne dođe do $A \,\mathrm{M}\, C = 1$, gdje je C produkt svih $c_1, c_2, \ldots, c_s$. Time je teorem dokazan.

13.3.1. Korolar. *Ako su dva broja međusobno prosta, onda su sve prirodne potencije jednoga relativno proste prema svim prirodnim potencijama drugoga*: simbolički: ako je $a \,\mathrm{M}\, b = 1$, tada je $a^r \,\mathrm{M}\, b^s = 1$ za bilo koje redne prirodne brojeve r, s. *Specijalno, bilo koja potencija jednog prostog broja prosta je prema svakoj potenciji svakoga drugog prostog broja.*

13.3.2. Korolar. *Ako je* $a^n \,\mathrm{M}\, b^s > 1$, *tada je* $a \,\mathrm{M}\, b > 1$.

⟶ **13.4.** Teorem.[1] *Ako je broj a djeljiv sa dva međusobno prosta broja b, c, onda je on djeljiv i njihovim produktom*: *simbolički*: *ako je* $a \equiv 0 \pmod{b}$ *i* $a \equiv 0 \pmod{c}$ *te* $b \,\mathrm{M}\, c = 1$, *onda je* $a \equiv 0 \pmod{bc}$. Ili ovako: *iz* $b \mid a$, $c \mid a$, $b \,\mathrm{M}\, c = 1$ *izlazi* $(bc) \mid a$.

---

[1]) U praksi se služimo npr. pravilom o djeljivosti broja a sa 6 na osnovu svojstva da je a djeljivo sa 2 i 3.

D o k a z. Kako je a djeljivo sa b, kvocijent q je cio broj: $a = bq$. Dovoljno je dokazati da je taj kvocijent q djeljiv sa c, jer ako je $q = cq'$ znači da je $a = bq = bcq'$, tj. a je djeljiv sa bc. No, prema pretpostavci, a, dakle produkt bq, djeljiv je sa c; također prema pretpostavci, faktor b je prost prema c; onda, prema teoremu 11.5. o djeljivosti produkta, znamo da je preostali faktor, kofaktor, djeljiv sa c. Time je dokaz izveden. Navedimo ipak i ovdje spomenuti:

—→ **13.5.** T e o r e m. **O djeljivosti produkta.** *Ako je produkt bq djeljiv sa c,* tj. $(bq)\,\mathrm{M}\,c = c$; *ako je, nadalje, prvi faktor relativno prost prema divizoru c* (*tj.* $b\,\mathrm{M}\,c = 1$), *tada je drugi faktor q djeljiv sa c, tj.* $q\,\mathrm{M}\,c = c$.

Dokažimo opet taj teorem, svodeći ga ovaj put na Euklidov teorem 13.2. (II). Naime, po ovom teoremu, zbog pretpostavke $b\,\mathrm{M}\,c = 1$, izlazi da za svaki broj q imamo:

$$(*) \qquad q\,\mathrm{M}\,c = (bq)\,\mathrm{M}\,c.$$

Ako je specijalno bq djeljivo sa c, tj. $bq\,\mathrm{M}\,c = c$, znači to, prema (*), da je $q\,\mathrm{M}\,c = c$, tj. da je zaista q djeljivo sa c.

—→ **13.6.** T e o r e m. (I) *Ako je produkt djeljiv prim-brojem, mora mu neki faktor biti djeljiv tim prim-brojem.*

(II) *Ako je broj djeljiv sa dva ili više različitih prim-brojeva, djeljiv je on i njihovim produktom.*

Teorem (II) je poseban slučaj teorema 13.4. jer je svaki prost broj prost prema svakom drugom prostom broju. Teorem (I) izlazi neposredno iz teorema 13.5. o djeljivosti produkta. Neka je, naime, produkt fg djeljiv nekim prim-brojem p; ako f nije djeljivo sa p, onda to znači da su f i p međusobno prosti; zbog $p \mid fg$, mora prema teoremu 13.5. o djeljivosti, biti $p \mid g$.

14. O FAKTORIZACIJI PRIRODNIH BROJEVA. VEZA S NAJVEĆOM ZAJEDNIČKOM MJEROM I S NAJMANJIM ZAJEDNIČKIM KRATNIKOM

Podsjetimo se da se pod prostim brojem razumijeva svaki prirodni broj > 1 koji nema nikojeg divizora > 1 osim sama sebe. U § 7. dokazano je da svih prostih brojeva ima beskonačno mnogo, pa ih možemo ponizati *uzlazno* ovako:

$$(1) \qquad p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ \ldots,\ p_n,\ \ldots$$

Također je dokazano da se svaki prirodni broj > 1 koji nije prost može prikazati kao produkt jednakih ili nejednakih prostih brojeva. Sada ćemo dokazati *jednoznačnost* tog razvoja.

—→ **14.1.** T e o r e m. *Svaki složen prirodni broj* $n > 1$ *može se predstaviti kao produkt jednakih ili nejednakih prirodnih prostih brojeva; ne obaziruć se na redoslijed faktora, taj je rastav broja n jednoznačan* (prvi dio teorema potječe od Euklida, a drugi od Gaussa).

Možemo pisati:

$$n = \prod p, \quad \text{pri čemu} \quad p \in P \text{ i } p \mid n.$$

Postojanje bar jednog niza

(2) $$N_1, \ldots, N_r$$

prostih brojeva tako da bude

(3) $$n = N_1 N_2 \cdot \cdot \cdot N_r$$

gotovo je očigledno. Dovoljno je sa N_1 označiti bilo koji prost broj kojem je n kratnik (n je složen), pa sa N_2 prost faktor od n/N_1 (ukoliko nije već n/N_1 prost broj itd.). Pa neka je za isti složeni prirodni broj n također

(4) $$n = M_1 \cdot \cdot \cdot M_s \qquad \text{za niz}$$

(5) $$M_1, M_2, \ldots, M_s \qquad \textit{prostih} \text{ brojeva.}$$

Iz (3) i (4) izlazi:

(6) $$N_1 \cdot \cdot \cdot N_r = M_1 \cdot \cdot \cdot M_s .$$

Svaki član niza (2) član je u nizu (5), i obrnuto: svaki član niza (5) član je u nizu (2), mada eventualno zauzima neki drukčiji položaj. Stvarno, *svaki* od tih članova N_i u (2) divizor je broja n, tj. produkta članova iz (5). Kad se prim-broj N_i ne bi pojavljivao i u nizu (5) kao član, bio bi on prost prema svakom članu tog niza, pa dakle (v. teorem 13.3) i prema njihovu produktu, tj. prema samom broju n. No, to je apsurd jer je N_i prim-divizor od n. Slično, svako M_i član je u nizu (2). Kad je sve tako ustanovljeno, prelazimo sada na zaključak.

P r v i k o r a k. I u prvom nizu (2) i u drugom nizu (5) precrtajmo po jedan član (recimo N_1 u (2) i jedan član u (5) koji mu je jednak; on može u (5) biti i stoti po redu!).

D r u g i k o r a k. Ponavljanje prvog koraka na preostatku od niza (2) i na preostatku od niza (5), itd., sve dok u jednom od nizova (2), (5) ne preostane jedan jedini član, recimo neka je to član x u nizu (5). No, taj se član pojavljuje i u konačnom preostatku onoga drugog niza (2), jer je pri svakom koraku produkt članova preostatka niza (2) jednak umnošku članova preostatka niza (5). Dakle je i na drugoj strani preostao jedan jedini član i on je $= x$. Dakle je bilo jednako mnogo članova: bilo ih je $r = s$, i jedan niz je permutacija drugoga. Specijalno, dakle, svaki prim-divizor broja n koji se pojavljuje u jednoj faktorizaciji (3), pojavljuje se i u drugoj faktorizaciji (4), i to jednak broj puta.

Time je teorem potpuno dokazan.

14.2. Skup prim-divizora zadanoga prirodnoga broja $n > 1$. Posebno, pri *svakoj* faktorizaciji broja n pojavljuju se svi njegovi prim-faktori. Zato je

prirodno za svaki broj $n>1$ promatrati skup $P(n)$ svih prostih djelilaca broja n[1].

Npr. $P(2)=\{2\}$, $P(8)=\{2\}$, $P(6)=\{2, 3\}$.

Tada teorem o faktorizaciji možemo izreći u ovoj finoj formi: Postoji jedno jedino preslikavanje $x \to \nu(x)$ množine $P(n)$ u skup rednih brojeva $<n$ sa svojstvom $n = \prod_{x \in P(n)} x^{\nu(x)}$. Npr., za broj 100 imamo $P(m)=\{2, 5\}$ pa je riječ o pridruživanju $2 \to 2$, $5 \to 2$ i faktorizaciji $100 = 2^2 \cdot 5^2$. Time dolazimo na tzv.:

—→ **14.3. Normalni oblik faktorizacije.** Ako u faktorizaciji prirodnog broja $n>1$ skupimo jednake prim-faktore i njihov udio označimo u obliku stepena (potencije), pa ako još prim-faktore poredamo po veličini, dobijemo *normalni uzlazni oblik faktorizacije broja n.*

Npr. faktorizacija $5 \cdot 3 \cdot 2 \cdot 2 \cdot 5 \cdot 3 \cdot 7 \cdot 5$ ima ovaj uređeni uzlazni oblik $2^2 \cdot 3^2 \cdot 5^3 \cdot 7$. Silazni bi oblik bio $7 \cdot 5^3 \cdot 3^2 \cdot 2^2$.

14.4. Najveći zajednički divizor i najmanji zajednički kratnik parova prirodnih brojeva. Očigledno je, npr. $2 \cdot 3^2 \cdot 5^2 \,\mathrm{M}\, 2^2 \cdot 5^3 \cdot 13 = 2 \cdot 5^2$; u rezultat ulaze prim-brojevi koji su i u jednom i u drugom broju.

14.4.1. Teorem. *Svaki prim-divizor od najvećeg zajedničkog divizora* $m \,\mathrm{M}\, n$ *je prim-divizor i od m i od n; pripadni eksponent u* $m \,\mathrm{M}\, n$ *je infimum od pripadnih eksponenata u m, n. Time je* $m \,\mathrm{M}\, n$ *određeno kao produkt takvih potencija zajedničkih prim-divizora. Specijalno,* $P(m \,\mathrm{M}\, n) = P(m) \cap P(n)$, *gdje* $P(x)$ *označuje skup prim-divizora od x* (v. § 14.2).

Najprije, ne može $m \,\mathrm{M}\, n$ sadržavati nikoji divizor osim onih koji su i u $P(m)$ i $P(n)$; dakle je

$$(*) \qquad P(m \,\mathrm{M}\, n) \subset P(m) \cap P(n);$$

nadalje, svaki zajednički prim-divizor p od m i n mora ući i u $m \,\mathrm{M}\, n$ jer je $m \,\mathrm{M}\, n$ najveći *zajednički* divizor od m i n. To upravo znači da je $P(m \,\mathrm{M}\, n) \supset \supset P(m) \cap P(n)$. To sa (*) daje traženu jednakost u teoremu.

Još ostaje ona stvar o veličini eksponenta u p^x koji ulazi u $m \,\mathrm{M}\, n$; očigledno je da je za svaki zajednički divizor p broj $x \leq$ od odgovarajućih eksponenata za p u m i n.

Ipak, ako su dva broja a, b zadani u svojem običnom pozicionom obliku (npr. decimalnom sistemu), obično je Euklidova verižna dioba najbrži put da se nađe $a \,\mathrm{M}\, b$.

14.5. Najmanji zajednički kratnik i prim-brojevi. Odredimo npr., najmanji zajednički kratnik brojeva iz 14.4.

Imamo $2 \cdot 3^2 \cdot 5^2 \cdot 7 \,\mathrm{W}\, 2^2 \cdot 5^3 \cdot 13 = 2^2 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 13$.

U rezultat ulazi svaki prim-divizor svakog od zadanih brojeva, i to s eksponentom, koji je *supremum* od odgovarajućih eksponenata u zadanim brojevima. Specijalno, $P(m \,\mathrm{W}\, n) = P(m) \cup P(n)$.

---

[1]) Od interesa je, kao što ćemo pokazati, da je

$$P(a \,\mathrm{M}\, b) = P(a) \cap P(b)$$

$$P(a \,\mathrm{W}\, b) = P(a) \cup P(b).$$

Razmatranja i dokaz su dualni onima iz § 14.4.

P r i m j e d b a. *Sada vidimo opravdanost oznaka* $m \,\mathrm{W}\, n$, $m \,\mathrm{M}\, n$; one su u vezi s unijom i presjekom! Kod $m \,\mathrm{W}\, n$ (odnosno $m \,\mathrm{M}\, n$) imamo uniju (odnosno presjek) množina pripadnih prim-divizora; znak M podsjeća nas na znak $\cap$, a znak W podsjeća nas na znak $\cup$ za uniju; osim toga i sam znak W je „kratnik" — dvostruko V.

14.6. Faktorizacija u obliku beskonačnog produkta. Radi kratkoće možemo iz normalnog oblika faktorizacije napisati malo promijenjeni oblik dovodeći u igru svaki prim-broj po redu, i to s eksponentom 0, ukoliko se taj prim-broj nije pojavljivao u normalnom obliku faktorizacije.

Radi lakšeg načina izražavanja možemo pisati, npr.:

$$3 \cdot 5^2 \cdot 11 = 2^0 \cdot 3 \cdot 5^2 \cdot 7^0 \cdot 11 \cdot 13^0 \cdot 17^0 \cdot \ldots$$

Tako dobijemo, formalno, produkt od beskonačno mnogo članova; no oni su gotovo svi $= 1$, pa se takvi produkti vladaju kao produkti s konačnim brojem faktora.

Tako bismo, npr., za broj 45 imali:

$$45 = 3^2 \cdot 5 = 2^0 \cdot 3^2 \cdot 5 \cdot 7^0 \cdot 11^0 \cdot \ldots; \qquad \text{slično:}$$

—→ **14.6.1.** *Za svaki prirodni n:*

$$n = 2^{N_1} \cdot 5^{N_2} \cdot 7^{N_3} \cdot \ldots p_k^{Nk} \cdot \ldots;$$

pri tom, za svaki prosti broj p_k, označuje N_k *najveći* cijeli broj ≥ 0 sa svojstvom da je p_k^{Nk} *divizor broja n, tj.*

$$n = p_1^{N_1}\, p_2^{N_2}\, p_3^{N_3} \cdot \ldots; \quad \textit{pri tom je}$$

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ \ldots$$

uzlazni niz svih prostih brojeva.

Niz $N_1, N_2, N_3, \ldots$ *je jednoznačno određen. Piše se simbolički:*

$$n = \prod_{k=1}^{\infty} p_k^{Nk}.$$

Tako npr. imamo $45_1 = 0$; $45_2 = 2$; $45_3 = 1$; $45_{4+\dot{\omega}} = 0$; pri tom ω označuje svaki broj ≥ 0 (sa $\mathrm{I}\,\omega$ označujemo skup svih cijelih brojeva ≥ 0).

U toj simbolici imamo:

—→ **14.6.2.** T e o r e m. *Za prirodne brojeve a, b vrijedi:*

(I) $$a \,\mathrm{W}\, b = \prod_{n=1}^{\infty} p_n^{Sup\ \{A_n,\ B_n\}}$$

(II) $$a \,\mathrm{M}\, b = \prod_{n=1}^{\infty} p_n^{Inf\ \{A_n,\ B_n\}}.$$

14.7. Još jedan oblik faktorizacije.[1] — **14.7.1.** Ako za niz eksponenata $N_1, N_2, \ldots$ svakoga prirodnog broja n promatramo *najveći* zajednički divizor n_e tog niza, onda očekujemo da se niz $N_1, N_2, \ldots$ može pisati kao produkt niza $\frac{N_1}{n_e} = n_1, \frac{N_2}{n_e} = n_2, \ldots$ i broja n_e i da se taj eksponent n_e može staviti van znaka Π. Zaključak je ispravan, pa imamo:

14.7.2. T e o r e m. *Svakom prirodnom broju* $n>1$ *pripada jedan jedini prirodni broj* n_e *i jedno jedino preslikavanje* $p \to n(p)$ *množine* P *svih prim-brojeva u skup* $I\omega = \{0, 1, 2, \ldots\}$ sa svojstvom da bude:

$$n = \left(\prod_p p^{n(p)}\right)^{n_e}, \quad \mathop{\mathrm{M}}_p n(p) = 1.$$

Tako npr. za $n = 18^2$ imamo $18^2 = 2^2 \cdot 3^4 \cdot 5^0 \cdot 7^0 \cdot \ldots = (2 \cdot 3^2 \cdot 5^0 \cdot \ldots)^2$, tj. $18^2{}_e = 2$, $18^2(2) = 1$, $18^2(3) = 2$ i $18^2(p_{3+\dot{\omega}}) = 0$.

D o k a z. Neka je

$$n = \left(\prod_p p^{n(p)}\right)^{n_e}, \qquad \mathop{\mathrm{M}}_p n(p) = 1,$$

$$n = \left(\prod_p p^{n(p)'}\right)^{n_e'}, \qquad \mathop{\mathrm{M}}_p n(p)' = 1.$$

Dakle je

$$\left(\prod_p p^{n(p)}\right)^{n_e} = \left(\prod_p p^{n(p)'}\right)^{n'_e} \qquad \text{i dalje:}$$

$$\prod_p p^{n(p) n_e} = \prod_p p^{n(p)' n'_e}.$$

Prema Euklid-Gaussovu teoremu o faktorizaciji izlazi odatle:

$$n(p)\, n_e = n(p)'\, n_e' \quad (p \in P). \tag{1}$$

Na taj način dobijemo skup jednadžbi (1), pri čemu je

$$\mathop{\mathrm{M}}_p n(p) = 1 = \mathop{\mathrm{M}}_p n(p)'. \tag{1'}$$

Treba zaključiti da je

$$n(p) = n(p)', \quad n_e = n_e'. \tag{1''}$$

Najprije je jasno da u (1) ima svega konačan broj jednadžbi koje nisu oblika $0 = 0$. Zato je od interesa da promatramo odmah i slučaj jednadžbi analognog tipa u kojem ih može biti i beskonačno.

---

[1]) Teorem je dokazan u članku D. Đoković — Đ. Kurepa (Vesnik Društva matematičara i fizičara Srbije, 10 (1958), 35—42) kako bi se dokazali obrasci

$$\sum_{x,\, y=1}^{\infty} (1+x)^{-(1+x)} = 1 \quad \text{i} \quad \sum_m (m-1)^{-1} = 1,$$

pri čemu m prolazi skupom prirodnih brojeva oblika x^y $(x>1,\ y>1)$.

14.7.3. Teorem. *Neka je zadan (konačan ili beskonačan) niz jednadžbi*

(2) $$r_i x = r_i' x' \quad (i = 0,\ 1,\ 2,\ \ldots),$$

pri čemu su svi koeficijenti prirodni brojevi. Ako je

(3) $$\mathrm{M}(r_0,\ r_1,\ \ldots) = 1,$$

tada je sistem (2) *ekvivalentan sa*

(4) $$r_i y = r_i', \quad \textit{gdje je} \quad y = x/\mu, \quad \mu = x\,\mathrm{M}\,x'$$

i pri tom y prirodan broj.

Logički se mogu zamisliti samo ova dva slučaja:

Prvi slučaj. $\mu = 1$. Kako je produkt $r_i x$ djeljiv sa x', to, prema osnovnom teoremu 13.5, pretpostavka $x\,\mathrm{M}\,x' = 1$ ima za posljedicu $x' \mid r_i$; to znači da je x' zajednički djelilac brojeva $r_0, r_1, \ldots$; po pretpostavci (3) znači to da je $x' = 1$ pa (2) postaje $r_i x = r_i'$, tj. dobije se traženi oblik (4).

Drugi slučaj. $\mu > 1$. Neka je tada $x = \mu y$, $x' = \mu y'$; naravno, $x'\,\mathrm{M}\,y' = 1$. Uvrstimo li te izraze za x i x' u (2) i podijelimo sve jednadžbe sa μ, dobije se ekvivalentan sistem

(5) $$r_i y = r_i' y',$$

za koji je zadovoljen uslov prvog slučaja; izlazi $y' = 1$; tj. (5) postaje traženog oblika (4). Teorem je dokazan.

14.7.4. Teorem. *Ako za (konačan ili beskonačan) skup relacijâ oblika*

$$r_i x = r_i' x'$$

vrijedi $$\mathrm{M}\,r_i = 1 = \mathrm{M}\,r_i',$$

pri čemu su brojevi r_i prirodni, onda je nužno $r_i = r_i'$, $x = x'$.

Naime, prema teoremu 14.7.3. zbog $\mathrm{M}\,r_i = 1$ izlazi da je $r_i \mid r_i'$; iz istog razloga zbog $\mathrm{M}\,r_i' = 1$ izlazi $r_i' \mid r_i$; kako su r_i, r_i' prirodni brojevi, znači da je $r_i = r_i'$, a time i $x = x'$.

Time je teorem dokazan.

Specijalno, promatrajući u sistemu (1) one jednadžbe za koje je $n(p) \neq 0$, dakle i $n(p)' \neq 0$, dobijemo zbog (1′) jednadžbe kakve smo riješili u teoremu 14.7.4; to znači da je zaista ispunjeno (1″), a time je dokazan i teorem 14.7.2.

14.8. Stvarna faktorizacija zadanog broja. Danas brojeve zadajemo obično u *pozicionom* (mjestovnom) decimalnom brojevnom sistemu (ili sistemu s kojom drugom bazom $m \neq 10$, recimo $m = 2$). Problem je da se broj n rastavi u *proste* djelitelje ako je zadano

(1) $$n = n_0 + n_1\,10 + n_2\,10^2 + \cdots + n_k\,10^k = (n_k\,n_{k-1} \cdots n_1\,n_0)_{10}.$$

Pogleda se da li je broj djeljiv sa 2. To se ocjenjuje po posljednjoj cifri; ako je cifra jedinica u broju n djeljiva sa 2, tada je $2 \mid n$. Onda se napiše $n = 2 \cdot n'$. Sa n' radimo isto, itd.

Navedimo ova praktična pravila o djeljivosti brojeva u *decimalnom* obliku.

14.8.1. *Broj n u decimalnom obliku* (1) *djeljiv je sa* 2 (odnosno 5, odnosno 10) *ako i samo ako mu je cifra jedinica* n_0 *djeljiva sa* 2 (odnosno sa 5, odnosno sa 10).

Stvar je jasna jer iz (1) izlazi, npr. $\frac{n}{2} = \frac{n_0}{2} + \text{cijelo}$, tj. $2 \mid n \Leftrightarrow 2 \mid n_0$.

14.8.2. *Broj u decimalnu obliku djeljiv je sa* 3 (odnosno sa 9) *ako i samo ako mu je suma cifara djeljiva sa* 3 (odnosno 9).

Naime, iz (1) izlazi:

$$\frac{n}{3} = \frac{n_0 + n_1 + \cdots}{3} + \text{cijelo, tj.}$$

$$3 \mid n \Leftrightarrow 3 \mid (n_0 + n_1 + \cdots).$$

14.8.3. Za broj 11 vrijedi pravilo:

$$11 \mid n \Leftrightarrow n \mid (n_0 + n_2 + \cdots) - (n_1 + n_3 + \cdots).$$

Naime, iz (1), dijeljeći sa 11, izlazi:

$$\frac{n}{11} = \frac{n_0 - n_1 + n_2 - + \cdots}{11} + \text{cijelo}.$$

Naime, vidimo da je

$$10 = 11 - 1$$

$$10^2 = 11 \cdot 9 + 1$$

$$10^m = 11 \cdot \text{cijelo} + (-1)^m.$$

14.9. Zadaci o faktorizaciji brojeva.

1. Odredi skup $P(n)$ svih prostih faktora broja n za $n =$ 1) 100; 2) 1000; 3) 10^n; 4) $10^5 - 1$; 5) $10^5 + 1$.

2. Rastavi na proste faktore broj: 1) 10000; 2) 35000; 3) $(10^5 - 1)(10^3 - 1)$; 4) 6!; 5) 25!; 6) 100!; 7) 200!; 8) Vrijedi $2^{183} - 1 = 7 \cdot 367 \cdot 55633 \cdot 2305843009213693951 \cdot 372017086253051463039733520041$; ovi su faktori prosti brojevi (Gabard, 1954).

3. Izračunaj: 1) $2 \cdot 5 \cdot 7$ M $2 \cdot 3 \cdot 7$; 2) $5 \cdot 7$ M $2 \cdot 7^2 \cdot 11$ M 7^3 M 11; 3) 5! M 4! M 3!

4. Zamijeni M sa W u zad. 3.

5. Izračunaj (20 W 25) M 15 i njegov dual (20 M 25) W 15.

6. Da li je operator M distributivan (razdjelan) prema W?

7. Dualno od zadatka 6.

8. Ako je S konačan skup prirodnih brojeva koji su udvoje međusobno prosti, onda je W $\dot{S} = \Pi \dot{S}$. Dokaz!

9. Dokaži: ako su brojevi $\frac{a}{b}$, $\frac{c}{d}$ racionalni i pozitivni, tada je $+\left(\frac{a}{b}\right)^{\frac{c}{d}}$ ili prirodan broj ili iracionalan broj.

10. Dokaži da je broj $e=\sum\frac{1}{\omega!}$ iracionalan.

11. Problem. Ne zna se da li je Eulerov broj $\gamma=\lim_{n\to\infty}\left(\sum_{\nu=0}^{n-1}\frac{1}{1+\nu}-ln\right)=$ $=0{,}5772156649\cdots$ racionalan ili iracionalan.

12. Izvedi pravilo o djeljivosti prirodnog broja $n=\sum_{k}10^k n_k$ brojem:
1) 7; 2) 13; 3) 17; 4) 19.

13. Svaki od brojeva $1, 2, \cdots, n$ dijeli bar jedan od brojeva $r+1, r+2, \cdots, r+n$.

14. Za svaki prost broj p i $n\in N$ vrijedi $p^{\alpha}\mid n$, $p^{\alpha+1}$ non $\mid n$, gdje je $\alpha=\sum_{k=1}^{\infty}E\frac{n}{p^k}$ (Legendre).

15. Ako je $n=2^k-1$, tad su brojevi $\binom{n}{\cdot\,n}$ neparni; i obrnuto.

16. Svakom prirodnom broju n pridijeli uređen par (n_1, n_2) cijelih brojeva tako da bude $n=2^{n_1}(2n_2-1)$; odredi (n_1, n_2) ako n znači:
1) 1, 2, 3, $\cdots$, 20; 2) 100, 1000; 3) ab.

17. Zadan je prirodan broj n; nađi x_0, x_1, x_2 tako da bude

$$x_0 x_1 x_2=n,\ \ x_3.\in 3N-3\cdot;$$

promatraj slučaj $n=10$, 1002, 32469.

18. Prirodnom broju $n>1$ pridruži niz

$$(1)\qquad n=O_1 n,\ O_2 n=O_1(O_1 n),\cdots,\ O_k n=O_1(O_{k-1} n),\cdots$$

pri čem $O_1 n$ znači zbroj od 1 i svih prostih djelilaca broja n; dokaži da je niz (1) periodičan i da mu je perioda ili 3, 4 ili 6 (Oltramare).

15. DIJADSKI BROJNI SISTEM. BROJEVNI SISTEMI SA ZADANOM BAZOM

15.0. Svakodnevno se služimo velikom naučnom tekovinom: *decimalnim* prikazivanjem brojeva. Npr. 222,2 znači $2\cdot 10^2+2\cdot 10+2\cdot 10^0+2\cdot 10^{-1}$; prema tome, *znak* 2 u 222,2 pojavljuje se 4 puta, ali *svaki* put s *drugim značenjem*: idući od desna nalijevo, *vrijednost* se množi svaki put sa 10. U tome je smisao izreke da je naš način prikazivanja brojeva *pozicioni* ili *mjestovan*; k tome se pomoću 10 znakova, cifara $0,1,\cdots,9$, koje čine skup $I10$, prikazuju svi drugi brojevi. Baza sistema je 10. Specijalno se *prirodni* brojevi prikazuju

u *decimalnom* sistemu pomoću 1, 10, 100, 10^3, 10^4, $\cdots$ To je danas i u *pisanom* sistemu, a tako je i u *govoru*, jer se većina brojeva u govoru naziva prema osnovnim brojevima koji predstavljaju cifre i brojeve 10, 10^2, 10^3, $\cdots$ Npr., osamnaest znači *osam na deset*, tj. $10+8$, trideset $=3\cdot 10$, itd.

15.1. Svojstva decimalnog sistema. Možemo reći da *decimalni* sistem prikazivanja brojeva ima ova svojstva:

1. (***Bitno svojstvo***)**:** *Sistem je pozicioni ili mjestovan, tj. vrijednost cifre* (*slova*) *zavisi od mjesta u broju što ga zauzima.*

2. »***Alfabet***« **(*cifarski skup*)** *se sastoji od* 10 *znakova ili slova ili cifara*: 0, 1, $\cdots$, 9. *Ti znakovi služe ujedno za prikazivanje prvih* 10 *rednih brojeva* $\dot{9}=0, 1, 2, \cdots, 9$. *Specijalno je važno da je zastupljena cifra za nulu ili ništicu pa se i cifra i taj broj označuju sa* 0.

3. *Ako se neka cifra u broju pomakne za jedno mjesto ulijevo* (*udesno*), *mjestovna joj se vrijednost pomnoži* (*podijeli*) *sa* 10.

4. *Svaki se broj gradi iz osnovnih brojeva oblika*

$$\cdots,\ 10^{-2},\ 10^{-1},\ 10^{0},\ 10,\ 10^{2},\cdots \tag{1}$$

tako da ove brojeve množimo članovima skupnosti $I10$ *i rezultate zbrajamo. Pri tom se brojevi osnovne biprogresije* (1) *množe svi sa* 0, *počev od nekog mjesta.*

Npr., ako počev od eksponenta 6 množimo sa 0, a prije toga sa 3, onda iz (1) dobijemo ovu „funkciju“ u skupu D svih cijelih brojeva:

$$\cdots,\ 3\cdot 10^{2},\ 3\cdot 10^{4},\ 3\cdot 10^{3},\ 0,\ 0,\cdots$$

Njena se suma označuje kao „decimalni prikaz“

$$333333{,}33\cdots$$

15.2. Sasvim je analogno i za *svaku* drugu bazu $m\in N$, $m>1$, npr. za bazu 2 (*dijadski ili binarni sistem*), bazu 3 itd. Npr., za bazu 2: promatra se skup 2^D svih brojeva $2^{\dot{D}}$ (tj. $\dot{D}$ prolazi kroz skup D svih cijelih brojeva). Skupom 2^D imamo podjelu svih pozitivnih realnih brojeva u potpuno određene intervale, od kojih svaki sadrži jedan jedini broj iz 2^D, i to upravo na svojem lijevom kraju. Tako npr. broj 2^3 iz 2^D leži upravo u intervalu koji počinje sa 2^3, a završava sa 2^4 ispuštajući 2^4 (2^4 pripada narednom intervalu). Skup 2^D određuje *geometrijsku* biprogresiju (za razliku od množine $2D$, koja čini *aritmetičku* biprogresiju). Isto je tako za svaki broj $m\neq 0$.

15.3. *Za svako* $m\neq 0$, $m\neq 1$, *skup* m^D *je bez jednakih članova*: biprogresija je čisto uzlazna ako je $m>1$, a čisto silazna ako je $m<1$; svaki realni pozitivni broj ili je u m^D ili leži između potpuno određena dva susjedna člana iz m^D.

Upravo to što izgovorismo čini osnov za prikazivanje brojeva u bazi m (i to je pandan osnovnog teorema o dijeljenju)[1].

---

[1] Naime, pri dijeljenju smo isključivali 0 kao divizor; za svako $m\neq 0$ ima aritmetička biprogresija mD ovo svojstvo: svaki realni broj (pa bio on pozitivan, negativan ili 0) ili leži u mD ili između *dva susjeda* u mD; to nam je dalo osnovni teorem o dijeljenju brojem m s onoliko posljedica, što smo već dosad izveli!

15.4. Primjer. Odredi onaj interval u 3^D u kojem leži broj 265. To je onaj interval koji *završava* s prvim brojem 3^n koji premašuje 265.

Gledajmo i računajmo!

$$3^0 = 1$$
$$3 = 3$$
$$3^2 = 9$$
$$3^3 = 27$$
$$3^4 = 81$$
$$3^5 = 243.$$

Dakle je $265 = 3^5 + 22$.

S viškom 22 radimo istu stvar:

$$22 = 2 \cdot 3^2 + 4$$
$$4 = 1 \cdot 3^1 + 1.$$

Dakle je $265 = 3^5 + 2 \cdot 3^2 + 1 \cdot 3^1 + 1 \cdot 10^0$, pa se to piše poziciono u bazi 3:

$$= (100211)_3.$$

Isto tako, npr., $(321{,}405)_8$ je prikrata za

$$3 \cdot 8^2 + 2 \cdot 8^2 + 1 \cdot 8^0 + 4 \cdot 8^{-1} + 0 \cdot 8^{-2} + 5 \cdot 8^{-3}.$$

15.5. Zaključak je opći i glasi ovako (ograničimo se na slučaj $m > 1$, pa čak i na slučaj da je m prirodan broj): *Za svaki broj $m > 1$, skup m^D čisto raste i ima svojstvo da je za svaki realni broj $a > 0$* određen onaj broj m^q za koji je $m^q \leq a < m^{q+1}$ (tj. a leži u intervalu u kojem i član m^q iz m^D); izmjeri li se a sa m^q, dobije se kvocijent c, gdje je c ujedno i *cifra* baze m, tj. $c \in Im$; ujedno je, naravno, $c \neq 0$ *i* c će biti *najuglednija* cifra u prikazu broja m; nadalje se dobije višak $r < 10^q$ pa imamo:

$$a = c\,10^q + r, \quad 0 \leq r < 10^q.$$

To je osnov! Sad se s *rezultatom* r postupa kao s *početnim podatkom* a, tj. . . . . (opiši to riječima!).

Tako vidimo ovo:

—→ **15.6.** Teorem. *Za svaki prirodni broj m (baza!) > 1, imamo pripadni skup $Im = \{0, 1, \cdots\}$ od m članova ṁ; svakom prirodnom broju a pripada jedan jedini cifarski niz cifara iz Im:*

$$a_0,\ a_1, \cdots$$

potpuno određene dužine k sa svojstvom da posljednji »najugledniji« član bude $\neq 0$ (tj. $a_{k-1} \neq 0$) i da skalarni produkt

(1) $$a_0 m^0 + a_1 m + a_2 m^2 + \cdots \text{ bude upravo } = a.$$

Tada se simbolički piše:

(2) $$a = (a_{k-1} \cdots a_2 a_1 a_0)_m$$

i kaže da je broj a predstavljen u koordinatnom (brojevnom) sistemu baze m; kaže se da a u tom sistemu ima k cifara; najuglednija je a_{k-1}; *ona je* $\neq 0$; *druge mogu biti i* 0.

15.7. Cifra jedinica. Ukazujemo specijalno na cifru a_0 *na mjestu jedinica.* Možemo je označiti sa $(a_0)_m$, ako bi oznaka a_0 ili $(a)_m$ dovela do zabune.

Jedinična cifra broja a u pozicionom sistemu baze m je ostatak pri dijeljenju broja a s modulom m, tj. $(a_0)_m$ *je onaj jednoznačno određeni broj r iz* Im *za koji je* $a = mq + r$ (*primjena osnovnog teorema o dijeljenju*). *Prelaz* $a \to (a_0)_m$ *je jednoznačan; obrnut prelaz od jedinične cifre r na pripadne brojeve dovodi do razreda ili klase* $mD + r$.

15.8. Slučaj dijadskog sistema. Cifre su 0 i 1; zato ista osnovna jedinica 2^x ne može doći dvaput u prikazivanju cijela broja *a*. Na taj način vidimo da vrijedi ovaj vrlo lijep

⟶ Teorem. *Svaki prirodni broj može se prikazati na jedan jedini način kao suma od konačno brojeva iz osnovne množine* 2^D.

Npr., $19 = 2^4 + 3 = 2^4 + 2^1 + 1 = 2^4 + 2^1 + 2^0$ pa se piše:

$$(19)_{10} = (10011)_2.$$

15.9. Zbrajanje i množenje u zadanom brojevnom sistemu kao odraz računanja na brojevnom *m*-vrhu i računanja prema modulu *m*.

Primjer (baza 10):

Zadano:	489	
	+	
Zadano:	147	
	526	Rezultat bez prenosa
Prenosi:	110	Prenosi
Rezultat:	636.	

Rezultat bez prenosa je upravo kao rezultat zbrajanja odgovarajućih cifara na brojevnom 10-vrhu, odnosno kao rezultat zbrajanja prema 10 kao modulu (isp. pogl. 6, § 4.9). Tako je i u drugim slučajevima. Evo primjera za bazu 3:

Baza 3	Podaci:	1221 · 2
Dobije se:		2112
		+
Prenos:		11
		0212
		+
Prenos:		1
Konačan proizvod:		10212

Pri tom treba imati na umu (u „memoriji“ ili „pamtilu“ — kod računskih strojeva) 3-vrh, odnosno ove tablice za zbrajanje i množenje prema modulu 3 u skupu $I3$:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

15.9.1. Na taj način vidimo kako je računanje prema zadanom modulu m u množini Im (npr. u $I10$) baza za brojevni pozicioni sistem baze m.

15.9.2. Računanje prema zadanom modulu *m*. Ukratko, došli smo do ovog zaključka: Razvitak ljudske kulture doveo nas je do decimalnog brojevnog sistema i drugih sličnih pozicionih sistema. Računanje u pozicionom sistemu baze m vršeno je *nesvjesno* kao računanje na brojevnom m-vrhu ili (kao što se kaže) prema modulu m (isp. pogl. 6, § 4.9). A danas možemo *svjesno* reći: na m-vrhu možemo provoditi prve tri računske operacije uz sva uobičajena pravila o kolu ili prstenu: *cifarska množina Im je kolo ili psten u odnosu na zbrajanje i množenje*.

15.9.3. *Potanje ispitivanje baze računanja u decimalnom sistemu.*

15.9.3.0. Nesvjesno, čitavo računanje u našem uobičajenom računanju bazirano je na ovim dvjema tablicama za zbrajanje i množenje na 10-vrhu, odnosno (to je učenije i tehnički u upotrebi!) — računanje prema 10 kao modulu:

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

·	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Računski strojevi imaju u sebi takve tablice i po njima rade (ako su ustrojeni decimalno!). Vanredno je korisno pogledati gornje dvije tablice. Vjerujemo da će se mnogi iznenaditi gledajući ih!

15.9.3.1. Promatraj još jedanput tablicu računanja (I 10; +), tj. zbrajanje u gornjoj tablici. Gledaj, npr.,

$$7 + 8 = 5.$$

Prstom lijeve ruke markiraj prvi podatak 7, prstom desne ruke markiraj drugi podatak 8; očima markiraj rezultat 5.

15.9.3.2. Ista jednakost $7+8=5$ u računu oduzimanja glasi:

$$7=5-8 \text{ i}$$

$$8=5-7.$$

Opet markiraj lijevim prstom prvi podatak („ubac“) 5 unutar kvadrata, drugi podatak (ubac) 8 gore i očitaj lijevo „izbac“ 8[1)]

15.9.3.3. Posebno se iz tablice vidi za svako $x \in Im$ koliki je protivni član $-x$, tj. $0-x$. Npr., $-2=0-2=8$.[2)]

Tako vidimo za prelaz od x na $-x$ u tablici $(I\,10, +)$ imamo:

$$-0=0,\ -1=9,\ -2=8,\ -3=7,\ -4=6,\ -5=5,$$

$$-6=4,\ -7=3,\ -8=1,\ -9=1,$$

tj. $$-x=10-x$$

ili tabelarno:

x	0,	1,	2,	3,	4,	5,	6,	7,	8,	9
$-x$	0	9	8	7	6	5	4	3	2	1

Odatle se vidi da je

$$-(-x)=x; \quad \text{npr.,}\ -(-3)=-7=3.$$

15.9.3.4. Tako vidimo da tablica $(I\,10, +)$ zbilja predstavlja jedan *okvir računanja*; dovoljno „širok“ okvir da nas prve dvije računske operacije ne izvode iz njeg: „tablica $(I\,10, +)$ predstavlja grupu odnosno jest grupa“ — kaže se u matematici!

15.9.3.5. Kod tablice $(I\,10, \cdot)$ vidimo opet da je proizvod („iznos“) u rezervi $I\,10$, odakle dolaze podaci, i da vrijede uobičajena naučena pravila. Nađimo, npr., $-2\cdot-3$. Treba znati što znači -2, a što -3, tj. $0-2$ i $0-3$. Prema tablici iz § 15.9.3.3. očitavamo: $-2=8$, $-3=7$; dakle je $-2\cdot-3=8\cdot7=$(prema tablici množenja)$=6=$(prema tablici množenja)$=2\cdot3$. Dakle je zaista $-2\cdot-3=6$[3)].

15.9.3.5.1. Međutim, vidimo novu situaciju: tek u *nekim* recima (stupcima) tablice dolazi čitav skup $I\,10$. I to u onim recima (stupcima) gdje nalijevo (odnosno gore) kao unos služi 1, odnosno 3, odnosno 7, odnosno 9[4)].

[1)] Vrlo je sugestivan taj način izražavanja u radu s matematičkim strojevima! Input (s) — output (s) kažu na engleskom; i mi možemo tako govoriti ili: unos — iznos. I američkim studentima u prvi mah djeluje neobično takvo izražavanje. Međutim, ti engleski izrazi prodrli su i u druge jezike.

[2)] Kad se pojavi neka oznaka, uvijek treba znati što ona predstavlja!

[3)] Francuski pisac S t e n d h a l je rekao da ga je relacija $-2\cdot-3=6$ neprestano mučila i uzrujavala. To je tako kad se negdje hoće da vidi više nego ono što stvar znači. Treba uvijek ići na izvor i pitati što zapravo pojedina stvar, simbol, $\cdots$ znači!

[4)] Rješenja su to jednadžbe $x\,\mathrm{M}\,10=1$ u skupu $I\,10$. Slučajnost ili pravilnost!? Pravilnost — odraz Euklidova teorema o djeljivosti produkta (isp. pogl. 6, § 17.4.1).

Zato će obrnuta operacija od množenja — dijeljenje — moći da se „neograničeno“ vrši samo s tim brojevima kao divizorima! Npr., $8:3=$(unutar tablica nađi podatak („unos“) 8 ispod (desno od) podatka („unosa“) 3 i očitaj proizvod $=6$, tj. $8:3=6$, i zbilja je $6\cdot 3=8$. Isto tako $9:7=7$; i zbilja je $7\cdot 7=9$.

Nađimo $8:2$. Na isti način vidimo: $8:2=4$; ali također $8:2=9$, tj. $8:2$ je i 4 i 9. U tablici $(I\,10,\ \cdot)$ dijeljenje sa 2 je *dvoznačna operacija*, naime $x:2$ ima dvije vrijednosti za svako dopušteno $x\in I\,10$, izuzetak je jedino 0; naime, $0:2=0$ i ništa drugo. Ali npr. $1:2$ ne postoji (ispod podatka 2 nema proizvoda 1)[1].

To ne treba da nas čudi jer, napokon, mi radimo s cijelim brojevima, a ne s razlomcima.

15.9.4. Slučaj baze 2. Danas se na strojevima obično računa po bazi 2; tablice „računanja“ glase:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Tablica je zaista jednostavna!

Prednost toga *binarnog* sistema kod strojeva je u tome da se dvije cifre 0 i 1 *lako ostvare* (npr. „0“ kao stanje bez električnih impulsa ili bar ispod određenog napona; cifra 1 ili stanje „1“ znači naprotiv: *struja teče* i *dostigla je određen napon*).

No iz tih tablica ujedno vidimo da su neograničeno izvodljivi ne samo zbrajanje, oduzimanje i množenje nego također i dijeljenje sa 1 (uz isključenje 0).

15.9.5. Baza 3. Pogledajmo tablicu množenja u brojevnom sistemu 3.

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Postoji li tu $1:2$? Iz tablice očitavamo (podaci ili ulazi 1, 2 su uokvireni): $1:2=$(onaj podatak 1 u tablici ispod gornjeg ulaznog podatka 2) nalazi se desno od traženog proizvoda, a vidimo da stoji 2, tj. $1:2=2$. I zaista je $2\cdot 2=1$, kaže tablica.

Vidimo ovo: ako se ne obaziremo na 0 i promatramo preostatak tablice, izlazi tablica:

·	1	2
1	1	2
2	2	1

Tu je i množenje i dijeljenje moguće „neograničeno“, tj. unutar tablice. Ta tablica predstavlja grupu, i to za množenje.

---

[1]) Promatraj analogije između operacije raspolavljanja (dijeljenje sa 2) u I 10 i antikvadriranja u skupu realnih brojeva!

15.9.5.1. Rezimirajući, vidimo ovu iznenadnu pojavu: u cifarskom skupu $I3$ vrijede sva uobičajena pravila o sve 4 prve računske operacije: sve su te operacije neograničeno izvedive unutar okvira $I3$ (jedino, kao i uvijek: 0 kao divizor otpada!) To znači: $(I3; +, \cdot)$ je jedno tijelo ili polje. *I mi već na tako mršavom skupu možemo oprobati i provjeriti sva ona pravila koja su najvažnija za sve* 4 *računske operacije u tijelu racionalnih brojeva, u tijelu realnih bvojeva, u tijelu kompleksnih brojeva.*

15.9.6. Primjedba. Pogledaj tablicu $(\{0, 1\}, +)$ i tablicu $(\{1, 2\}, \cdot)$. Ne vidi li se slična struktura? (Zamjena: $0, 1, +$ / $\downarrow\ \downarrow\ \downarrow$ / $1, 2, \cdot$)

u podacima ima za posljedicu odgovarajuću zamjenu u proizvodima.)

15.10. Zadaci o brojevnim sistemima.

Ovdje će nam značiti $(\cdots a_1 a_0, a_{-1} a_{-2} \cdots)_b = \sum_{k=-\infty}^{\infty} a_k \cdot b^k =$

$$= \cdots + a_1 b^1 + a_0 b^0 + a_{-1} b^{-1} + a_{-2} b^{-2} + \cdots$$

1. Niz rednih brojeva 0, 1, 2, 3, ... pisan u bazi 2 glasi (svaki put pribroji 1): 0, 1, 10, 11, 100, 101, ... Kako glasi 20. član?

2. Ispiši čitavu tablicu o prikazivanju decimalnih cifara $1, \ldots, 9$ te brojeva 10, 100 u brojevnim sistemima s bazom: 2, 3, 4, 5, 6, 7, 8

Baze

10	8	7	6	5	4	3	2
1	1						1
2	2	2	2	2	2	2	
3							
4							
5							
6							
7							
8							
9							
10	12						
100	144						1100100

3. Brojkama 0, 1, 2, 3, . . . , 7 baze 8 pridružimo tročlane nizove baze 2 prema ovoj tablici:

Baza 2	8
0 0 0	0
0 0 1	1
0 1 0	2
0 1 1	3
1 0 0	4
1 0 1	5
1 1 0	6
1 1 1	7

i pišemo $(x)=y$, ako je x kojigod član ispod baze 2, a y odgovarajući član ispod baze 8 (npr. $(100)=4$). Dokaži da je $(1101110,\ 10101)_2=(001)\ (101)\ 110),\ (101)\ (010))_8$ i uopće $(\cdots a_2 a_1 a_0,\ a_{-1} a_{-2} a_{-3} \cdots)_2 = (\cdots(a_2 a_1 a_0),\ (a_{-1} a_{-2} a_{-3})\ (a_{-4} a_{-5} a_{-6})\cdots)_8$. Iz toga jednostavnog prevođenja na bazu 8 iz baze 2, i obrnuto, zaključujemo na veliku važnost baze 8 u računanju pomoću matematičkih strojeva; naime, baza 8 je tako jednostavno vezana s bazom 2 koja ima veliku prednost što se cifre 0, 1 lako i raznovrsno ostvaruju no ima manjak u tom što su dijadski prikazi vrlo dugi; a baza 8 je jednostavna zbog gornje veze sa 2 a opet prikazi u bazi 8 malo su tek duži od prikaza u bazi 10.

4. Osnovne brojeve 10, 10^2, 10^3, 10^4, 10^5, 10^6 prikaži u brojevnom sistemu sa bazom: 1) 2; 2) 3; 3) 5; 4) 7; 5) 8; 6) 12; 7) 60; 8) 360.

5. Napiši broj $(1\ 1\ 1\ 1\ 1\ 1)_2$ iz baze 2 u bazu: 1) 10; 2) 3; 3) 4.

6. Poredaj po veličini brojeve; $a=354$, $b=(100000)_2$, $c=(59)\,0_{60}$, $d=(466)_7$, $e=(1\cdot(12)\,(13))_{15}$.

7. Zadani su brojevi $a=1\,0\,0\,1$, $b=1\,1\,0\,0\,0$, $c=1\,0\,1\,0\,1$; nađi: 1) $a+b+c$; 2) $a+b-c$; 3) $ab+c$; 4) $(a+b)\,(a+c)$, 5) $(a-b)\,(a+b)$. Baza je 2.

8. Odredi kvocijent uzastopnih članova ovoga niza: 1001011101; 100101110,1; 10010111,01; . . . time da se mjestovni zarez („decimalni zarez“) pomiče svaki put za jedno mjesto ulijevo; baza računanja je: 1) 10; 2) 2; 3) 3; 4) 4; 5) 8; 6) 100.

9. Broj 1/3 prikaži u bazi: 1) 3; 2) 2; 3) 5; 4) 9.

10. U bazi 2 prikaži brojeve: 1) 34, 57, 2) 1 0 1, 11; 3) -28, 4; 4) $\frac{5}{3}$; 6) $\pi=3{,}14159\ldots$; 7) $e=2{,}7181\ldots$

11. Broj $\frac{3}{5}=0{,}6$ napiši u bazi 2 time da brojeve 3 i 5 napišeš u bazi 2 i izvršiš dijeljenje, odnosno da 0,6 direktno pišemo u bazi 2.

12. Kako se u bazi 2 1) množi; 2) dijeli s dekadskim jedinicama 10, 10^2, 10^3, . . . odnosno 10^{-1}, 10^{-2}, . . .?

13. S koliko se 0 završava umnožak prvih 100 prirodnih brojeva, ako ga pišemo u bazi 1) 10; 2) 2; 3) 3; 4) 5; 5) 50?

14. Odredi skup realnih brojeva oblika $\sum_{n=1}^{\infty} c_n b^{-n}$; pri tom je $c_n \in I2$. Promatraj slučajeve da je baza b: 1) 2; 2) 10; 3) 2/3; 4) 4; 5) 8.

15. Koliko ima 10-cifrenih prirodnih brojeva u bazi:
1) 2; 2) 3; 3) 4; 4) 8; 5) 10; 6) 60?

16. 1) Odredi najveći od traženih brojeva u zadatku 15; 2) koliko mjestovnih cifara on ima u naznačenim bazama?

17. Neka za n-ti prirodni broj i proizvoljan prirodan broj $b>1$ znak $b(n)$ kazuje koliko cifara u bazi b ima n-ti broj. Odredi 1) $2(100)$; $10(100)$;
2) $\lim_{n\to\infty} \frac{2(n)}{8(n)}$; $\lim_{u\to\infty} \frac{2(n)}{10(n)}$; 3) $\lim \frac{8(n)}{10(n)}$.

18. Za prikazivanje svih cijelih brojeva u bazi b sa n mjestovnih vrijednosti potrebno je u elektronskim računskim strojevima oko $b \cdot n$ elektronskih cijevi; odredi bn za razne baze $b=2, 3, \ldots$ ako se radi o prikazivanju prvih k prirodnih brojeva (npr. $k=1000$).

16. ARITMETIKA PRSTENA *Im*

16.0. Ideja. Imaj na umu skup Im cifara $0, 1, \ldots <m$; npr., konkretno za slučaj $m=10$; gledajmo skup $I10$ naših uobičajenih cifara $0, 1, \ldots, 9$ i na način kako formalno glasi tablica zbrajanja i tablica množenja ne odgovarajućih *brojeva* $0, 1, \ldots, 9$, nego odgovarajućih *cifara* shvatajući ih kao vrijednosti pojedinih mjesta dvaju brojeva. Eto, tako se dobiju zbrajanje i množenje u prstenu $I10$, odnosno Im[1]. To smo objašnjavali u prethodnom paragrafu, no dobro je da se i ovdje naglasi.

16.1. Pogledajmo, npr., izraz $7 \cdot 9$; to je i produkt dvaju brojeva u našem sistemu, ali i „produkt“ dviju cifara u prstenu Im; vrijednost u prvom slučaju je 63, a vrijednost u drugom slučaju je cifra 3 (i to je upravo cifra jedinica za bazu 10 u broju $7 \cdot 9 = 63$).

16.2. Ili ovaj primjer: broj $1 \cdot 2 \cdot 3 \cdot \ldots \cdot 9$, tj. 9! vrlo je velik. Koliki je taj produkt u prstenu cifara? Naravno: 0, jer se pojavljuju faktori 2 i 5, a njihov je produkt 0. Prema tome, 9! je u prstenu $I10$ cifara $=0$; to znači naprosto da broj 9! ima 0 kao cifru za jedinično mjesto, tj. 9! je djeljivo sa 10. Isti je zaključak za svaki *složeni* broj m.

16.2.1. Teorem. *Za svaki prirodni* ***složeni*** *broj m, broj*

$$(m-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (m-1)$$

djeljiv je sa m; drugim riječima, u cifarskom ili brojčanom sistemu Im vrijedi

$$(m-1)! = 0.$$

---

[1] Jedna od najdubljih stvari u matematici sastoji se u ovom: *konkretnu veličinu* shvatiti kao *opću*! Pustiti, npr., 10 u našem slučaju da bude varijabla kroz skup prirodnih brojeva, pa i još dalje.

16.2.2. A ako modul m nije složen broj, nego je prost broj p? Koliko je, npr., 6! u prstenu $I7$? „Računajmo“!

$$6! = 1 \cdot (2 \cdot 3) \cdot 4 \cdot (5 \cdot 6) = 6 \cdot 4 \cdot 2 = 6 \cdot 8 = 6 \cdot 1 = 6, \quad \text{tj.} \quad 6! = 6, \quad \text{odnosno}$$

$$6! = -1 \quad \text{jer je} \quad 6 = -1.$$

Što jednakost $5! = 6$ u prstenu $I7$ znači za prsten D svih cijelih brojeva? Znači naprosto da je razlika $6! - 6$ djeljiva sa 7.

Tj. $$6! \equiv 6 \pmod 7,$$

tj. $$(7-1)! \equiv 7-1 \pmod 7$$

$$(7-1)! \equiv -1 \pmod 7.$$

I zbilja $6! = 720$, pa je razlika $720 - 7$ djeljiva sa 7:

$$720 - 6 = 714 = 7 \cdot 102.$$

Zanimljivo je da se tu 7 može nadomjestiti svakim prostim brojem p (*Wilsonov teorem*; § 17.6.11).

16.3. Veza između cifarskog prstena Im i prstena D cijelih brojeva. Zaključak je ovaj: za svaki prirodni broj $m > 1$ veza između cifarskog prstena Im i prstena D svih cijelih brojeva uspostavljena je ovim prevođenjem:

Cifarski prsten Im	Prsten D svih cijelih brojeva
Cifra c	Broj c; svaki broj klase $mD + c$
Cifarska jednakost $a = b$	Djeljivost diferencije brojeva a i b sa m; formalno[1]: $a \equiv b \pmod m$; $m \mid a-b$; $m \,\mathrm{M}\, (a-b) = m$ (tri načina ispisivanja jedne te iste činjenice!).
Cifarska nejednakost $a \neq b$	Nedeljivost diferencije $a-b$ sa m; formalno: $a \not\equiv b \pmod m$; $m \text{ non} \mid a-b$; $m \,\mathrm{M}\, (a-b) \neq m$

16.4. Intervencija skupova. Razredi cijelih brojeva prema zadanom modulu. — **16.4.1.** Već smo se upoznali s tim da cijeli skup D možemo porazdijeliti na vrhove pravilnog m-vrha. U vrhove dolaze biprogresije

$$mD,\ mD+1,\ mD+2,\ \ldots,\ mD+m-1.$$

---

[1] Kao što znamo, služimo se sa sva ta tri znaka da izrazimo u suštini istu stvar: *$a-b$ je djeljivo sa m*, odnosno *m je divizor od $a-b$*, odnosno *m je najveći zajednički divizor od $a-b$ i m*,

Računanju s brojevima odgovara računanje s tim razredima, i obrnuto. Tako npr., ako radimo s modulom 10, onda je $(10\,D+7)+(10\,D+9)$ upravo $10\,D+6$. Naime, sumu $(10\,D+7)+(10\,D+9)$ definiramo kao množinu svih vrijednosti $x+y$, pri čemu je $x\in 10\,D+7$, $y\in 10\,D+9$, dakle je x oblika $10\,a+7$, $y=10\,b+9$, pa je

$$x+y=(10\,a+7)+(10\,b+9)=10\,(a+b+1)+6.$$

No, kad a, b prođu nezavisno kroz D, onda kroz D prođe i $a+b+1$, i obrnuto. Tako je, dakle, $(10\,D+7)+(10\,D+9)=10\,D+6$.

Tu se opet pojavljuju, formalno, i cifre 7, 9 i njihova suma 6.

Slično definiramo produkt dva razreda A, B kao onaj razred koji obuhvata sve produkte $\dot{A}\,\dot{B}$; pri tom je $\dot{A}\in A$, $\dot{B}\in B$.

16.4.2. Na taj način imamo vrlo prikladnu i lijepu vezu između *računanja u cifarskom prstenu* $I\,10$ i *skupovnom računanju s pripadnim razredima*:

$$10\,D,\ 10\,D+1,\ \ldots,\ 10\,D+9;$$

veza je ova:

Cifra c u $I\,10$	Razred $10\,D+c$
Jednakost $a=b$ u $I\,10$	Jednakost odgovarajućih razreda: $10\,D+a=10\,D+b$
Nejednakost $a\neq b$ cifara	Disjunktnost odgovarajućih razreda: oni su bez ikojega zajedničkog elementa, dakle im je presjek prazan $(10\,D+a)\cap(10\,D+b)=$ prazno

16.4.3. Posve je ista stvar ako umjesto modula (ili baze) 10 uzmemo kao modul bilo koji prirodni broj $m>1$ (formalno: neka 10 bude oznaka za bilo koji prirodni broj >1 itd. $\cdots$; zato je i zgodno uz zadani redni broj x uvesti oznaku $\dot{x}$ ili $x^{\cdot}$ za svaki redni broj $<x$; u tom bi slučaju, dakle,

$$10^{\cdot}\text{ bilo }0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9).$$

16.5. Rezime prethodnih razmatranja.

16.5.1. Ako je m proizvoljan prirodni broj >1, tada su potpuno određeni pripadni razredi cijelih brojeva; to su ovi skupovi — biprogresije:

$$m\,D,\ m\,D+1,\ m\,D+2,\ \ldots$$

Ima ih upravo m; za svaki cijeli broj d skup $m\,D+d$ podudara se s jednim od tih m razreda.

16.5.2. Nadalje se može sagraditi prirodni pozicioni sistem s bazom m i promatrati pripadni cifarski skup od m znakova koji će nam služiti za

označivanje prvih m rednih brojeva $0, 1, 2, \ldots, m-1$; označimo taj skup sa Im.

16.5.3. Zbrajanje i množenje brojeva pisanih sada u odabranom sistemu bazirano je na potpuno određenom zbrajanju i množenju cifara unutar Im, tj. da rezultat tih operacija s ciframa opet ostane u Im i bude „cifra". Na taj način cifarski skup Im postaje kolo ili prsten s obzirom na takvo definirano *interno* zbrajanje i množenje.

16.5.4. Isto tako, *zbrajanje* i *množenje* u skupu pomenutih razreda daje jedan prsten u skupu svih tih razreda[1].

16.5.5. *Na taj način imamo tri prstena*:

Polazni prsten D svih cijelih brojeva sa svojim običnim zbrajanjem i množenjem (i svim posljedicama; npr., oduzimanje, dijeljenje itd.).

Prsten sastavljen od m razredâ prema modulu m; računanje je po principu: svaki sa svakim (tj. razred A + razred B jest razred koji obuhvata $\dot{A}+\dot{B}$ za svako $\dot{A}$ i svako $\dot{B}$; isto tako $A \cdot B \supset \{\dot{A} \cdot \dot{B}\}$, i slično.

Prsten sastavljen od m cifara; računanje u cifarskom prstenu usklađeno je s računanjem u odabranom pozicionom m-sistemu.

16.5.6. *Činjenicama u jednom od triju prstena odgovara određena činjenica i u svakom od preostala dva kola.* Ta se veza uspostavlja ovim „trojezičnim rječnikom" za prevođenje:

Cifarski prsten $Im = \{0, 1, \ldots, m-1\}$	Kolo razredâ cijelih brojeva prema modulu m $D/m\,D$	Kolo D svih cijelih brojeva
1. Cifra c	Razred $m\,D + c$ = skup svih cijelih brojeva oblika $m\,\dot{D} + c$	Broj c i svaki broj iz dotičnog razreda
2. Cifarska jednakost $a = b$	Jednakost pripadnih razreda $m\,D + a = m\,D + b$	Djeljivost razlike brojava $a-b$ modulom m; odnosno djeljivost sa m razlike što se dobije oduzimajući bilo koji član jedne klase od bilo kojeg člana druge klase. Simbolički se to ispisuje: $a \equiv b \pmod{m}$ ili $m \mid a-b$ ili $m\,\mathrm{M}\,(a-b) = m$

[1]) Taj se skup od m razredâ može označiti sa $D/m\,D$.

3. Cifarska nejednakost $a \neq b$	Disjunktnost pripadnih razreda: $m D + a \cap m D + b =$ $=$ prazno	Nedjeljivost sa m broja $a-b$, odnosno razlike $(mx+a)-(my+b)$, gdje $x, y \in D$. Simbolička oznaka: $a \not\equiv b \pmod{d}$ $m \text{ non} \mid a-b$ $m \text{ M } (a-b) \neq m$
4. $a+b$	Razred koji sadrži $(m D + a) + (m D + b)$	Svaki broj oblika $(mx+a)+(my+b)$
5. $a \cdot b$	Razred koji sadrži $(m D + a)(m D + b)$	Svaki broj koji je $\equiv ab \pmod{m}$

To je *trojezični rječnik* $I(m)$, $D/m D$, D.

Analogno bi se sastavio rječnik s kolom D na prvom mjestu. U tom rječniku (to je posljedica gore napisanog rječnika) svakom $\dot{D}$ (tj. svakom članu $\dot{D}$ iz D) odgovara upravo onaj razred u kojom se $\dot{D}$ nalazi, tj. razred (biprogresija) $m D + \dot{D}$; istom broju $\dot{D}$ odgovara u Im upravo ostatak što ga dobijemo na osnovu osnovnog teorema o diobi dijeleći $\dot{D}$ sa m.

16.6. Zadaci o računanju u *Im*.

1. Odredi stepene a^n za $n>1$, specijalno 2^{50} u prstenu 1) $I3$; 2) $I5$; 3) $I10$.

2. 1) Promatraj kvadriranje i antikvadriranje u prstenu $I5$; da li su obje operacije izvedive neograničeno? 2) Da li za svako $a \in I5$, jednadžba $x+y=a$ ima rješenje u $I5$? 3) A jednadžba $x+y=a$?

3. Promatraj samo parne razrede $10 D + 10^{\cdot}$ za $10^{\cdot} = 0, 2, 4, 6, 8$;
   1) mogu li se s njima vršiti sve četiri osnovne računske operacije?
   2) uočavaš li sličnosti u tom računanju i u računanju s razredima $5 D + 5^{\cdot}$ odnosno u cifarskom skupu $I5$?

4. Riješi jednadžbu $x^2+1=0$ u prstenu 1) $I2$; 2) $I3$; 3) $I5$; 4) $I10$.

5. Promatraj prsten $I5$; 1) uvjeri se da je $(a+b)^5 = a^5 + b^5$; 2) nađi $(x+2)\cdot(x+4)$; 3) nađi $(x+1)\cdot(x+2)\ (x+3)\ (x+4)$; 4) $(x-3)\cdot$ $\cdot(x^2+3x+4)$; 5) da li u prstenu $I5$ vrijedi osnovni teorem o diobi? 6) podijeli x^3-2 sa $x-3$; 7) riješi $x^3=2$ pokušavanjem; 8) riješi $x^2+3x+4=0$.

6. Nađi prvi broj x tako da n^x-n bude djeljivo sa 1) 2; 2) 10; 3) 5.

17. LINEARNA DIOFANTSKA JEDNADŽBA S DVIJE NEPOZNANICE. LINEARNA KONGRUENCIJA S JEDNOM NEPOZNANICOM. DIJELJENJE U CIFARSKOM PRSTENU

17.1.—17.1.1. Diofantska jednadžba s dvije nepoznanice x, y je oblika:

$$ax + my = c; \tag{1}$$

a, m, c su poznati članovi prstena D cijelih brojeva. Traže se brojevi $x, y \in D$ za koje vrijedi (1). Jednadžba je *homogena* ako je $c = 0$.

17.1.2. Linearna kongruencija s nepoznanicom x je oblika:

$$ax \equiv c \pmod{m}. \tag{2}$$

Kongruencija je *homogena* ako je $c = 0$. Svako x za koje vrijedi (2) zove se *rješenje kongruencije*. Pri tom se rješenja koja su kongruentna mod m ne smatraju različnim.

Tako npr.

$$4x \equiv 2 \pmod{10} \tag{3}$$

ima rješenje $x = 3$ i 8; to su dva *nepodudarna* rješenja, jer im razlika $3 - 8$ nije djeljiva modulom kongruencije, tj. brojem 10. Sva rješenja x kongruencije (3) kongruentna su sa 3 ili s 8 i ispunjuju razrede $3 + 10D$, $8 + 10D$, tj. svako x oblika $3 + 10\dot{D}$, $8 + 10\dot{D}$ zadovoljava (3); no ne može biti više od dva nepodudarna rješenja.

17.1.3. *Kongruenciji* (3) odgovara u cifarskom prstenu $I\,10$ *jednadžba*:

$$4x = 2. \tag{4}$$

Traži se *svako* $x \in Im$ za koje vrijedi (4), tj. (tako možemo rcći) *traži se znamenka jedinica x cijelih brojeva kojima produkt sa* 4 *završava sa* 2. Očigledno je $x =$ cifra 3 i $x =$ cifra 8. Dakle: u cifarskom prstenu $I\,10$ našega decimalnog brojevnog sistema ima linearna jednadžba (4) dva rješenja, i to 3 i 8 (u *prstenu D* svih cijelih brojeva nema (4) uopće rješenja; ima tek u prstenu Q racionalnih brojeva, i to $x = 2^{-1}$).

17.2. Veza između diofantske jednadžbe, kongruencije i dijeljenja u cifarskom prstenu. Diofanska jednadžba $ax + my = c$ može se pisati, naravno, i u obliku $ax - c = -my$, odakle vidimo da je $ax - c$ djeljivo sa m; to se piše i ovako:

$$ax \equiv c \pmod{m}.$$

I obrnuto. Na taj način vidimo: ako smo odredili x za diofantsku jednadžbu (kongruenciju), onda je isto to x i ono što se traži u kongruenciji (diofantskoj jednadžbi).

Zato vidimo kako se rješavanje diofantskih jednadžbi i kongruencija svodi jedno na drugo.

Kongruenciji

$$ax \equiv c \pmod{m}$$

pripada cifarska jednadžba

$$ax = c,$$

pri čemu treba imati na umu ovo: ako a, c i nisu eventualno na prvi pogled cifre, tj. u *Im*, onda treba znati da su to samo različita *predočenja* odgovarajućih cifara koje se inače dobijaju tražeći najmanji ostatak ≥ 0 pri diobi od a, odnosno c sa m. (Tako npr. ako je riječ o „cifri" — 8 u decimalnom sistemu, onda treba znati da je to 0—8, tj. 2.)

Isto tako 8459 znači u sistemu 12 „cifru" $r = 11$, jer je

$$8459 = 12.704 + \overline{|11|}.$$

Isto je tako s rješenjem x.

17.3. Homogen slučaj. — **17.3.1.** Teorem. *Homogena kongruencija*

$$ax \equiv 0 \pmod{m} \tag{5}$$

ima kao rješenja brojeve

$$x = \frac{m}{d}\dot{D}, \tag{6}$$

gdje je $d = a \,\mathrm{M}\, m$ (najveći zajednički *divizor od* a i m). Svi ti brojevi čine razred $\frac{m}{d}D$, odnosno d različitih razreda $mD + \dot{d}$ ($\dot{d} = 0, 1, 2, \ldots, d-1$). Drugim riječima, kongruencija (5) ima *upravo d inkongruentnih rješenja, i to* 0, 1, ..., $\dot{d}$, ... *ili brojeve koji su ovima kongruentni prema modulu m.*

Naime, neka je $d = a \,\mathrm{M}\, m$; tada dijeleći i kongruenciju i modul sa d, imamo kongruenciju:

$$\frac{a}{d}x = 0 \left(\mathrm{mod}\ \frac{m}{d}\right). \tag{7}$$

U (7) je napisano da je produkt $\frac{a}{d}x$ djeljiv sa $\frac{m}{d}$; no brojevi $\frac{a}{d}$, $\frac{m}{d}$ su relativno prosti $\left(\frac{a}{d} \,\mathrm{M}\, \frac{m}{d} = 1\right)$; to, prema Euklidovu teoremu o djeljivosti produkta, znači da je x *djeljivo sa* $\frac{m}{d}$, tj.

$$x \equiv 0 \left(\mathrm{mod}\ \frac{m}{d}\right), \text{ tj.}$$

$$x = \frac{m}{d}\dot{D}. \tag{8}$$

Sva rješenja polazne kongruencije (5) daju razred

$$\frac{m}{d}D \tag{9}$$

(dakle razred s obzirom na broj $\frac{m}{d}$ kao modul).

Npr., za kongruenciju (10) $4x \equiv 0 \pmod{10}$ daje formula (8)

$$x = \frac{10}{2}\dot{D} = 5\dot{D},$$

tj. sva rješenja kongruencije (10) čine razred

$$5D = \{\cdots, -10, -5, 0, 5, 10, 15, \cdots\}.$$

Nama treba razred prema modulu 10 jer je takva kongruencija (10). No, očigledno, razred (biprogresija) $5D$ cijepa se na dva razreda $10D$, $10D+5$, tj.

$$\{\cdots, -10, -5, 0, 5, 10, \cdots\} = \{\cdots, -10, \quad 0, 10, 20, \cdots\} \cup$$
$$\cup \{\cdots, -15, -5, \quad 5, 15, 25, \cdots\}.$$

Isto tako razred (9) je unija od d razreda $mD+\dot{d}$, gdje je

$$\dot{d} = 0, 1, 2, \cdots, d-1.$$

Vrijedi, naime, ovaj očigledni i zanimljivi rezultat, pri čemu možemo imati na umu sliku da umjesto „jedinice za mjerenje“ a uzimamo k-struko veću jedinicu ka.

17.3.2. Teorem. *Svaki razred prema modulu a raspada se u k razreda prema modulu ka; odnosno ovako: po k razreda s obzirom na modul ka iscrpljuju jedan razred prema modulu a, i to ovako:*

$$aD+\dot{a} = (kaD+\dot{a}) \cup (kaD+\dot{a}+a) \cup \cdots (kaD+\dot{a}+2a) \cup \cdots, \text{ tj.}$$

$$aD+\dot{a} = \bigcup_{\dot{k}} (kaD+\dot{a}+\dot{k}a).$$

Naravno, umjesto a može tu doći proizvoljan broj b.

Geometrijski je stvar očigledna: k uzastopnih vrhova $0, 1, \cdots, k-1$ jednog poligona od ka stranica određuje upravo k upisanih poligona po a stranica, od kojih je prvi s vrhovima

	$0,$	$1,$	$2,$	$\cdots,$	$a-1$
drugi	$a,$	$a+1,$	$a+2,$	$\cdots,$	$2a-1$
treći	$2a,$	$2a+1,$	$2a+2,$	$\cdots,$	$3a-1$
. . . . .					
k-ti	$(k-1)a,$	$(k-1)a+1,$	$(k-1)a+2$	$\cdots$	$ka-1.$

Skiciraj!

Formalno, iz te tablice vidimo da su brojevi iz svakog stupca $\equiv \bmod a$; nadalje, da su iz dva različita stupca $\not\equiv \bmod a$; kako je svih tih k brojeva $\not\equiv \bmod ka$, znači to da oni leže u sve samim $\neq$ razredima mod ka i da se razred $aD+\dot{a} \bmod a$ cijepa u odgovarajućih k razreda mod ka, što odgovaraju stupcu u kojem je $\dot{a}$; dakle je zaista na snazi cijepanje.

⟶ **17.3.3.** Teorem. **Homogena diofantska jednadžba**

$$ax+my=0$$

zadovoljena je ovim i samo ovim vrijednostima:

$$x=\frac{m}{d}\dot{D},\quad y=-\frac{a}{d}\dot{D},\ \text{gdje je}\quad d=a\,\mathrm{M}\,m.$$

Naime, x je nađeno u (8).

17.3.4. Teorem. *Rješenja cifarske jednakosti*

$$ax=0$$

u prstenu $Im=\{0,\ 1,\ \ldots,\ \dot{m},\ \ldots\}$ *glase*:

$x=\frac{m}{d}\dot{d}$; tu $\dot{d}=0,\ 1,\ \ldots,\ d-1$; $d=a\,\mathrm{M}\,m=$ *najveći zajednički djelilac od* a *i* m.

Npr., za prsten $I10$: iz $5x=0$ izlazi $x=0,\ 2$.

17.4. Nehomogen, opći slučaj. — 17.4.0. Egzistencija. Kao što ni obične jednadžbe (npr. $0\cdot x=2$) ne moraju imati rješenja, tako ni kod relacije koje sad promatramo rješenje ne mora postojati. Očigledno je, npr., da jednadžba $4x+6y=1$ nema rješenja u *cijelim* brojevima (lijeva je strana djeljiva sa 2, a desna nije). Iz istog razloga: ako jednadžba $ax+my=c$ ima *cjelobrojno* rješenje, onda $a\,\mathrm{M}\,m$ (najveći zajednički divizor od a, m) mora biti divizor od c. Mnogo je dublje da vrijedi i obrat.

17.4.1. Teorem. *Ako je* $a\,\mathrm{M}\,m$ *djelilac od* c, *onda jednadžba*

$$ax+my=c \tag{1}$$

ima bar jedno cjelobrojno rješenje. Specijalno, ako su a, m *relativno prosti* (tj. $a\,\mathrm{M}\,m=1$), *onda jednadžba* (1) *ima cjelobrojno rješenje.*

Naime, prema osnovnom teoremu o najvećem divizoru, broj se $a\,\mathrm{M}\,m$ cjelobrojno izražava pomoću a i m (§ 10.6):

$$a\,\mathrm{M}\,m=aX+mY, \tag{2}$$

gdje su X i Y cijeli brojevi.

No, ako je c djeljivo sa $d=a\,\mathrm{M}\,m$, onda, množeći (2) cijelim brojem $q=d^{-1}c$, dobijemo:

$$c=a(qX)+m(qY).$$

To znači da je $x=qX$, $y=qY$ rješenje jednadžbe (1).

Kod stvarnih primjera možemo primijeniti formulu (2), tj. osnovni teorem o M, no može se odmah pristupiti rješavanju (ono se u suštini ipak svodi na gornja razmatranja o M).

17.4.2. Primjer. Riješi

$$436x + 12y = 16. \tag{1}$$

Odatle:

$$y = \frac{-436x + 16}{12} = -36x + 1 + \frac{-4x + 4}{12} = -36x + 1 + t$$

$$-4x + 4 = 12t$$

$$x = \frac{12t - 4}{\boxed{|-4|}} = -3t + 1.$$

Za t se može uzeti proizvoljan cio broj; x će biti također cijelo; y isto; rješenje je dakle:

$$x = -3t + 1$$

$$y = -36(-3t + 1) + 1 + t = 109t - 35; \quad t \in D.$$

Traženo rješenje glasi:

$$x = -3\dot{D} + 1, \; y = 109\dot{D} - 35. \tag{2}$$

Npr., za $\dot{D} = 0$ izlazi rješenje:

$$x = 1, \; y = -35. \tag{3}$$

Pokus: $(1)_1 = 436 \cdot 1 + 12 \cdot -35 = 436 - 420 = 16 = (1)_2$. Ispravno!

Postupak kako se rješava je očigledan: *riješi se po jednostavnijoj nepoznanici, podijeli, odredi cio dio, a za ostatak se uvede nova nepoznanica, itd.* Pri tom dijeljenje treba obaviti tako da izađu po apsolutnoj vrijednosti što manji novi brojevi. *Posljednji divizor* — 4 *je uokviren*; on određuje najveći zajednički djelilac koeficijenata: $436 \text{ M } 12 = 4$. On je zbilja djelilac i od trećeg koeficijenta 16.

17.4.3. *Isti primjer pomoću kongruencije.* Zadana jednadžba glasi:

$$12y = -436x + 16. \tag{4}$$

To znači da desna strana mora biti djeljiva sa 12 (ukoliko je jednadžba moguća; jednadžba je moguća jer je $12 \text{ M } 436 = 4 = 4 \text{ M } 16$).

Drugim riječima, imamo:

$$-436x + 16 \equiv 0 \pmod{12}. \tag{5}$$

Sad se umjesto koeficijenata stave što zgodniji *kongruentni* brojevi: po apsolutnoj vrijednosti što manji:

$$-436 = 12 \cdot -36 - 4, \quad \text{tj.} \quad -436 \equiv -4 \pmod{12}$$

$$16 = 12 + 4, \quad \text{tj.} \quad 16 \equiv 4 \pmod{12}.$$

Stavi li se to u (5), izlazi:

$$-4x+4\equiv 0 \pmod{12}. \tag{6}$$

Tu se sada isproba kojih god 12 nekongruentnih brojeva, tj. po jedan sa svakog vrha 12-vrha, odnosno po 1 iz svakog razreda.

Recimo da radimo s apsolutno najmanjim brojevima x:

$$x=0,\ \pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 5,\ 6.$$

Treba vidjeti po redu koji od njih zadovoljava, a koji ne zadovoljava:

0 ne; 1 da; -1 ne; 2 ne; -2 da; 3 ne; -3 ne; 4 da; -4 ne;

5 ne; -5 da; 6 ne.

Kongruenciju (6), odnosno (5) zadovoljavaju četiri broja:

$$x=1,\ -2,\ 4,\ -5.$$

To znači da će i svaki broj iz odgovarajućeg razreda

$$12D+1,\ 12D-2\ (=12D+10),\ 12D+4,\ 12D+7$$

zadovoljavati kongruenciju. No, samo inkongruentna rješenja smatramo različitima; zato, npr., rješenje 1 i rješenje $12+1=13$ ne smatramo različitima. Nađena četiri rješenja su različita: razlika od nikojih dvaju rješenja nije $\equiv 0 \pmod{12}$. Ali su sva četiri $\equiv \bmod 3$. Drugim riječima, sva rješenja x kongruencije (5) ispunjuju ova četiri razreda mod 12:

$$12D+1,\ 12D+10\ (=12D-2),\ 12D+4,\ 12D+7,$$

tj. upravo razred $3D+1 \bmod 3$.

Sa svakim nađenim $x\in 3D+1$, tj. sa svakim $x=3\dot{D}+1$ možemo poći u zadanu diofantsku jednadžbu po pripadno y; izlazi $y=-109\dot{D}-35$.

Tako smo došli do rješenja:

$$x=3\dot{D}+1,\ y=-109\dot{D}-35.$$

A to je očigledno isto što i rješenje (2): dovoljno je umjesto $\dot{D}$ pisati $-t$.

17.4.4. *Isti primjer pomoću cifarskog prstena.* Problem smo sveli na kongruenciju (6), odnosno

$$-4x\equiv -4 \pmod{12}, \text{ odnosno}$$

$$4x\equiv 4 \pmod{12}.$$

Prevedeno na cifarsko množenje u cifarskom prstenu $I\,12$, znači to da je

$$4x=4$$

i da treba odrediti x. No, tablica množenja sa 4 u $I\,12$ glasi:

x	0	1	2	3	4	5	6	7	8	9	10	11
$4x$	0	4	8	0	4	8	0	4	8	0	4	8

Vidimo da se zadani produkt 4 pojavljuje četiri puta, i to ispod 1, 4, 7, 10.

Rezultat: cifarska jednadžba $4x=4$ ima u prstenu $I\,12$ kao rješenja ove četiri „cifre“:

$$x=1,\ 4,\ 7,\ 10;\quad \text{drugih nema.}$$

Pripadni brojevi 1, 4, 7, 10 rješenja su zadane kongruencije; a drugih nekongruentnih nema! Primijetimo da su ta četiri rješenja 1, 4, 7, 10. Onda se dalje ide i u polaznu diofantsku jednadžbu po jedno y da se dobije jedno partikularno rješenje diofantske jednadžbe. Naime, opće rješenje možemo tada odmah napisati, kao što ćemo sada dokazati. Teorem 17.5. kazuje kako izgleda opće rješenje.

17.5. Teorem o općem rješenju. (I) *Diofantska jednadžba*

$$ax+my=c \tag{1}$$

ima cjelobrojno rješenje onda i samo onda ako je c djeljivo najvećim zajedničkim djeliocem $a\,\mathrm{M}\,m=d$ *koeficijenata a, m; tada je ona ekvivalentna s jednadžbom*

$$\frac{a}{d}x+\frac{m}{d}y=\frac{c}{d}\,.$$

Ako je x_0, y_0 *neko partikularno rješenje jednadžbe* (1), *opće rješenje te jednadžbe glasi:*

$$x=x_0+m'\,\dot{D},\qquad m'=m/d \tag{2}$$

$$y=y_0-a'\,\dot{D},\ a'=\frac{a}{d}\ \ (\dot{D}\ \textit{proizvoljan cio broj}). \tag{3}$$

To specijalno znači da svi x-ovi ispunjuju razred $\frac{m}{d}D+x_0$, *a svi y-i razred* $-\frac{a}{d}D+y_0$.

(II) *Da kongruencija*

$$ax\equiv c\ (mod\ m) \tag{4}$$

ima bar jedno rješenje, nužno je i dovoljno da bude

$$c\equiv 0\ (mod\ d=a\,\mathrm{M}\,m). \tag{5}$$

Ako je uslov (5) *ispunjen, tada je polazna kongruencija* (4) *ekvivalentna s kongruencijom*

$$\frac{a}{d}x\equiv\frac{c}{d}\ \left(mod\,\frac{m}{d}\right)\ (\textit{modul drukčiji}). \tag{6}$$

Ako je x_0 *jedno rješenje kongruencije* (4) *odnosno* (6), *tada sva rješenja ispunjuju upravo razred oblika*

$$\frac{m}{d}D+x_0, \tag{7}$$

tj. d razredâ oblika

$$m\,D + x_0 + \dot{d}; \tag{8}$$

pri tom, kao obično, $\dot{d} \in Id = \{0,\ 1,\ \ldots,\ d-1\}$.

(III) *Zadan je prirodni broj m, cifarski prsten* $I\,m$ *i njegov par elemenata oznake a, c (pri tom su a, c bilo kakva dva cijela broja); jednadžba* $ax = c$ *ima u tom* $I\,m$ *bar jedno rješenje onda i samo onda ako je* $a\,\mathrm{M}\,m$ *divizor broja c. Ako je* x_0 *jedno rješenje promatrane jednadžbe, tada je ujedno svako rješenje oblika* $x_0 + \dot{d}$; *pri tom* $\dot{d}$ *znači svaki neodrečni element* $< d = a\,\mathrm{M}\,m$.

Dokaz. Onaj dio teorema koji se odnosi na egzistenciju rješenja bio je dokazan ranije (§ 17.4.1). Dokažimo zato još onaj dio teorema koji se odnosi na izgradnju općeg rješenja pomoću posebnog rješenja; ta je veza tipična!

Pa neka je x_0, y_0 jedno rješenje diofantske jednadžbe (1), tj.

$$ax_0 + my_0 = c. \tag{9}$$

Oduzmemo li tu jednakost od jednakosti (1), izlazi:

$$a(x - x_0) + m(y - y_0) = 0. \tag{10}$$

A to je homogena jednadžba za $x - x_0$, $y - y_0$. Po teoremu 17.3.3. ima (10) kao opće rješenje:

$$\begin{aligned} x - x_0 &= \frac{m}{d}\dot{D} \\ y - y_0 &= -\frac{a}{d}\dot{D}, \text{ gdje je } d = a\,\mathrm{M}\,m. \end{aligned} \tag{11}$$

A to upravo iskazuje teorem o diofantskim jednadžbama. Posebno to znači da polazna kongruencija (4) ima upravo rješenja (11) kao svoja rješenja; sva ta rješenja daju razred $\frac{m}{d}D + x_0$. A taj je razred (7), prema § 17.3.2, unija od d razreda ispisanih u (8).

Time je teorem dokazan.

17.6. Glavni korolar. Osnovni skup $\Phi(m)$. — **17.6.1.** *Glavni korolar.*

(I) *Ako su a, m relativno prosti brojevi* ($a\,\mathrm{M}\,m = 1$), *tada kongruencija* $ax \equiv c \pmod m$ *ima upravo jedan razred rješenja mod m; posebno to vrijedi za svako* $a \in \Phi(m)$.

(II) *U cifarskom kolu* $I\,m$ *ima cifarska jednadžba* $ax = c$ *jedno jedino rješenje za svako* $a \in \Phi(m)$, *tj. za svako* $a \in I\,m$ *sa* $a\,\mathrm{M}\,m = 1$.

17.6.2. Osnovna definicija. Svakom prirodnom broju m pridružit ćemo skup $\Phi(m)$ svih brojeva $0, 1, \ldots < m$ koji su relativno prosti prema m. Drugim riječima, $\Phi(m)$ je skup svih rješenja jednadžbe $x\,\mathrm{M}\,m = 1$ za $x \in I\,m$. Kardinalni broj množine $\Phi(m)$ označivat ćemo sa $\varphi(m)$.

Npr.,

$$\Phi(2)=\{1\},\ \varphi(2)=1,\ \Phi(3)=\{1,\ 2\},\ \varphi(3)=2,$$

$$\Phi(4)=\{1,\ 3\},\ \varphi(4)=2,\ \Phi(5)=\{1,\ 2,\ 3,\ 4\},\ \cdots$$

17.6.2.1. $\Phi(m)$ se zove *sveden potpun skup ostataka ili predstavnikâ modulo m.*

17.6.2.2. Svaki najobuhvatniji skup nekongruentnih brojeva mod m koji su prosti prema m zove se *sveden* (reduciran) *potpun skup predstavnikâ* (reprezentanata) modulo m.

Npr., brojevi 1, 5 čine sveden potpun skup ostataka mod 6; naprotiv, ni 2, 5 ni 3, 19, ni 7, 19 ne čine sveden potpun skup ostataka modulo 6.

17.6.3. *Za svaki prosti broj p vrijedi* $\Phi p=\{1, 2, 3, \ldots, p-1\}$ *i* $\varphi(p)=p-1$.

Naime, svaki od brojeva $p>0$ je prost prema p; a tih brojeva ima $p-1$.

17.6.4. Korolar. *U cifarskom prstenu Im svako* $a\in\Phi(m)$ *ima svoj jednoznačni invers ili reciprok* a^{-1} *sa svojstvom* $aa^{-1}=1=a^{-1}a$.

Naime, a^{-1} je jedino rješenje u Im cifarske jednadžbe $ax\equiv 1$.

17.6.5. *Dijeljenje u prstenu Im izvedivo je jednoznačno jedino sa svakim članom iz* $\Phi(m)$ *kao divizorom.*

U prvom redu, prema prethodnom korolaru, za svako $a\in\Phi(m)$ postoji i a^{-1} u Im sa svojstvom $a^{-1}a=aa^{-1}=1$. Neka je, nadalje, $c\in Im$; riječ je o tome da vidimo možemo li podijeliti c sa a; riječ je o rješavanju jednadžbe

$$ax=c.$$

Pomnožimo je sprijeda sa a^{-1}. Izlazi:

$$(a^{-1}a)\,x=a^{-1}c$$

$$1\,x=a^{-1}c$$

$$x=a^{-1}c.$$

To je traženi kvocijent od c sa a. Taj je kvocijent određen jednoznačno. Stvarno, neka je uz $ax=c$ također $ax'=c$, dakle (oduzimanjem!) $ax-ax'=0$, tj. $a(x-x')=0$. Pomnožimo li to sa a^{-1} sprijeda, izlazi $x-x'=a^{-1}0=0$, tj. $x=x'$. Time ujedno dokazasmo ovo:

17.6.5.1. *U prstenu Im množenje sa svakim* $a\in\Phi(m)$ *je regularna operacija: iz* $x\neq x'$ *mora izlaziti* $ax\neq ax'$.

U drugu ruku, pretpostavimo da je $a\in Im$ takvo da za svako $c\in Im$ jednadžba $ax=c$ bude moguća u Im. Tada je nužno $a\in\Phi(m)$, tj. $a\,\mathrm{M}\,m=1$; naime, kad bi bilo $a\,\mathrm{M}\,m>1$, onda bismo mogli promatrati specijalno jednadžbu $ax=1$; ona, međutim, nije moguća; kad bi ona, naime, imala rješenje (označili bismo ga sa a^{-1}), tada bi i kongruencija $ax\equiv 1 \pmod m$ imala broj a^{-1}

kao rješenje, mada njena desna strana 1 nije djeljiva sa $a \mathrm{M} m$, koji je po pretpostavci >1.

Tako vidimo da se skup $\Phi(m)$ izričito ističe u kolu Im.

Primjer decimalnih cifara: Pogledajmo posebno tablicu množenja za skup $\Phi(10)$ naših običnih decimalnih cifara: $\Phi(10)=\{1, 3, 7, 9\}$:

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Vidi se da cifre iz $\Phi(10)$ obrazuju *grupu za množenje*, tj. čine multiplikativnu grupu. Stvar nije slučajna:

⟶ **17.6.6.** Osnovni teorem o skupu $\Phi(m)$. *Za svaki prirodni broj m skup $\Phi(m)$ svih rednih brojeva $<m$ koji su prosti prema m čini multiplikativnu grupu u cifarskom prstenu $I\,m$. Specijalno, ako je $x, y \in \Phi(m)$, tada je i produkt $xy \in \Phi(m)$. Za svako $a \in \Phi(m)$ predstavlja množenje $x \to ax$ permutaciju množine $\Phi(m)$, pa u $\Phi(m)$ iz $ax = ax'$ izlazi $x = x'$.*

Teorem je drukčiji iskaz raznih prethodnih razmatranja. Specijalno, dokažimo da iz $a, x \in \Phi(m)$ izlazi $ax \in \Phi(m)$. No, a i x su relativno prosti prema m; znači po Euklidu (§ 13.2) i produkt ax brojeva a, x je prost broj prema m. Pa neka je r šifra od ax, tj. onaj broj iz Im koji je $\equiv ax \pmod m$, tj. neka je r ostatak pri dijeljenju broja ax sa m; dakle je $ax = mq + r$; pa jednakost $1 = ax \,\mathrm{M}\, m$ postaje $1 = (mq + r) \,\mathrm{M}\, m$, a ovo je $= r \,\mathrm{M}\, m$ (svaki divizor od m i r divizor je i od $mq + r$). Dakle je zaista $r \,\mathrm{M}\, m = 1$; to znači da je cifarski produkt ax opet relativno prost prema m. Time je „grupoidno“ svojstvo množine $\Phi(m)$ utvrđeno: proizvod je u području podataka.

Nadalje, *ako su x, y dva $\neq$ elementa iz Im, tada su i ax, ay dva različita elementa iz Im.* To smo upravo dokazali u § 17.6.5.1. No svako $c \in \Phi(m)$ je oblika ax sa $x \in \Phi(m)$. Naime, a^{-1} je u Im, dakle je i $a^{-1}c$ u $\Phi(m)$; upravo je $a a^{-1} c = c$. Dakle je zaista c produkt od a i određenog člana $a^{-1}c$ iz $\Phi(m)$. Time je dokazano da je pridruživanje $x \to ax$ u $\Phi(m)$ određena permutacija.

17.6.6.1. Korolar. *Ako je S bilo koji skup od m nekongruentnih brojeva,* mod m, *tada je u njemu potpuno određen podskup S_φ od $\varphi(m)$ brojeva prostih prema m; za svako a za koje je $a \,\mathrm{M}\, m = 1$ skup aS svih ax sa $x \in S$ je opet skup od m nekongruentnih brojeva; svaki član iz $a\,S_\varphi$ je prost prema m.*

17.6.7. Teorem. *Za svaki broj b i svaki broj a za koji je $a \,\mathrm{M}\, m = 1$ i svaki skup S od m brojeva dva po dva $\not\equiv$ mod m, skup $aS + b$ svih $a\dot{S} + b$ predstavlja određenih m brojeva dva po dva $\not\equiv$ mod m. Specijalno, sadrži on određen skup S' od $\varphi(b)$ brojeva prostih prema m; općenito nije $S' = a\,S_\varphi$ skup od svih $\varphi(m)$ brojeva iz S prostih prema m.*

Naime, prelaz od S na $aS + b$ može se izvesti posredno:

$$S \to aS \to aS + b.$$

Govoreći na jeziku prstena Im, vrijedi $S=Im$ (tj. svako $\dot{S}$ je $\equiv \dot{m} \bmod m$). Prema prethodnom teoremu, prelaz $\dot{S} \to a\dot{S}$ je „permutacija" množine S, pri čemu se, prema korolaru, permutira i množina S_φ; isto tako prelaz $a\dot{S} \to a\dot{S}+b$ je permutacija množine aS „$=$" Im.

17.6.8. Teorem. *Ako je modul m prost broj, onda je cifarski prsten Im čak i tijelo (korporacija) ili polje, tj. u njemu se izvode sve četiri elementarne računske operacije uz uobičajena pravila; i obrnuto, ako je cifarsko kolo Im tijelo i* $m>1$, *onda je m prost broj.*

Taj teorem je iskaz — na tehničkom jeziku matematike — onih stvari koje smo rekli ranije. Naime, za svaki prost broj p očigledno je skup $\Phi(p)$ sastavljen od svih brojeva $1, 2, \ldots, p-1$; svaki je od njih prost prema p; to znači, prema § 17.6.3, da je u Ip dijeljenje moguće svakim članom $\neq 0$ koji je u Ip. A to upravo znači da je kolo Ip i tijelo.

Obrat je očigledan: ako je Im tijelo i $m>1$, tada je m prost broj; u obrnutom slučaju, m bi bio složen broj, recimo $m=ab$, gdje su a i b oboje >1 i $<m$; no to znači da je produkt ab djeljiv sa m, tj. $ab=0$ u prstenu Im, pa jednadžba $ax=1$ ne bi mogla postojati. Naime, množeći tu jednadžbu sa b, izašlo bi $abx=b$, tj. (zbog $ab=0$) $0=b$, tj. b bi bilo djeljivo sa m, što je apsurd jer je b pravi djelilac od m.

Za ilustraciju činjenice da je, npr., $I2$ ili $I3$ tijelo, a $I10$ nije tijelo upućujemo na § 15.9.3 — 15.9.5.

17.6.9. Teorem. (Fermat, 1640; i Euler, 1760) ***Za svako*** $a \in \Phi(m)$ ***vrijedi*** $a^{\varphi(m)}=1$. ***Drugim riječima, za svaki broj a koji je relativno prost prema prirodnom broju m vrijedi***

$$a^{\varphi(m)} \equiv 1 \pmod m, \text{ tj. broj } a^{\varphi(m)}-1$$

djeljiv je brojem m. Specijalno, za svaki prost broj p i svako $a=1, 2, \ldots, p-1$ ***vrijedi*** $a^{p-1} \equiv 1$, ***odnosno*** $a^p \equiv 0 \pmod p$; ***ili ovako: ako cio broj a nije djeljiv sa p, onda broj*** a^{p-1} ***podijeljen sa p daje ostatak*** 1.

(Slučaj $m=p$: Fermat, 1640; dokaz: Ivory, 1806; opći slučaj: Euler, 1760). Npr. $m=4$, $a=35$, $\varphi(4)=2$; imamo $35^2 \equiv (3)^2 \equiv 1 \pmod 4$.

Dokaz teorema. Za svako $a \in \Phi(m)$ pridruživanje $x \to ax$ za koje je $ax \equiv 1 \pmod m$ je permutacija mnogosti $\Phi(m)$. To znači da je umnožak svih članova x iz $\Phi(m)$ isto što i produkt svih produkata ax iz $\Phi(m)$, tj.

$$\prod x = \prod_x ax, \quad x \in \Phi(m). \tag{1}$$

No, tu se ax pojavljuje kao faktor $\varphi(m)$ puta ($\varphi(m)$ kazuje koliko $\Phi(m)$ ima članova); zato je $\prod_x ax = a^{\varphi(m)} \prod_{x \in \Phi(m)} x$. Drugim riječima, (1) daje

$$w(m) = a^{\varphi(m)}\, w(m), \quad \text{gdje je} \tag{2}$$

$$w(m) = \prod_{x \in \Phi(m)} x \ . \tag{3}$$

Kao produkt članova iz grupe $\Phi(m)$ vrijedi $w(m) \in \Phi(m)$, pa se sa $w(m)$ u (2) može skratiti i time izlazi tražena relacija $1 = a^{\varphi(m)}$. U posebnom slučaju, kad je m prost broj p, skup $\Phi(p)$ se sastoji od $p-1$ brojeva $1, 2, \ldots, p-1$ (svi su oni, naime, prosti prema p).

Time je važan teorem 17.6.9. dokazan.

P r i m j e r. Odredi koju cifru predstavlja 12^{18} u sistemu baze 5, tj. odredi ostatak mod 5 broja 12^{18}. Najprije je $12 \equiv 2 \bmod 5$, pa je $12^{18} \equiv 2^{18}$. Nadalje je, po Fermatu, $2^{\varphi(5)} = 1$, tj. $2^4 \equiv 1$. Zato eksponent zamijeni ostatkom mod $\varphi(m)$. Izlazi, dakle, $12^{18} \equiv 4 \pmod 5$.

17.6.10. Rješenje linearne kongruencije pomoću Fermat—Eulerova teorema. Linearna kongruencija

$$a x \equiv c \pmod m \tag{1}$$

očigledno je ekvivalentna s kongruencijom

$$\frac{a}{d} x \equiv \frac{c}{d} \left(\bmod \frac{m}{d} \right), \text{ gdje je } d = a \,\mathrm{M}\, m. \tag{2}$$

No, brojevi $\frac{a}{d}$, $\frac{m}{d}$ su relativno prosti; zato, prema Fermat-Eulerovom teoremu, vrijedi:

$$\left(\frac{a}{d} \right)^{\varphi\left(\frac{m}{d}\right)} \equiv 1 \left(\bmod \frac{m}{d} \right). \tag{3}$$

Usporedi li se (2) i (3), nameće se samo po sebi da (3) pomnožimo sa $\frac{c}{d}$; izlazi:

$$\frac{a}{d} \left(\frac{a}{d} \right)^{\varphi\left(\frac{m}{d}\right)-1} \cdot \frac{c}{d} \equiv \frac{c}{d} \left(\bmod \frac{m}{d} \right). \tag{4}$$

Oduzimanjem (4) od (2) izlazi:

$$\frac{a}{d} \left[x - \frac{c}{d} \left(\frac{a}{d} \right)^{\varphi\left(\frac{m}{d}\right)-1} \right] \equiv 0 \left(\bmod \frac{m}{d} \right).$$

Zbog $\frac{a}{d} \,\mathrm{M}\, \frac{m}{d} = 1$ može se tu faktor $\frac{a}{d}$ ispustiti pa izlazi:

$$x \equiv \frac{c}{d} \left(\frac{a}{d} \right)^{\varphi\left(\frac{m}{d}\right)-1}. \tag{5}$$

Specijalno:

$$x \equiv c\, a^{\varphi(m)-1} \quad \text{ako je } d = a \,\mathrm{M}\, m = 1. \tag{6}$$

Time se i na ovaj način pokazalo da kongruencija (1) ima jedan razred rješenja $\bmod \frac{m}{d}$, ako uopće ime rješenja.

Primjer. $3x \equiv 5 \pmod{19}$. Prema (6) je $x \equiv 5 \cdot 3^{\varphi(19)-1} = 5 \cdot 3^{17} = 5 \cdot (3^3)^5 \cdot 3^2 \equiv$ (zbog $3^3 \equiv 8$, $5 \cdot 3^2 \equiv 7$) $\equiv 8^5 \cdot 7 \equiv (8^2)^2 \cdot 8 \cdot 7 \equiv 7^2 \cdot -1 \equiv -11 \equiv 8 \pmod{19}$, tj. $x \equiv 8 \pmod{19}$.

17.6.11. Wilsonov teorem. Gaussovo poopćenje. U dokazu prethodnog teorema javio se produkt svih „regularnih" elemenata cifarskog kola Im[1] — mislimo na broj $w(m)$. Možemo li mu odrediti vrijednost? Npr. u decimalnom prstenu $I10$ skup regularnih elemenata glasi $\Phi(10) = \{1, 3, 7, 9\}$; produkt im je 9, odnosno -1 (drugim riječima, produkt brojeva $1 \cdot 3 \cdot 7 \cdot 9$ ima 9 kao cifru jedinica). U prstenu $I5$ regularni su elementi: 1, 2, 3, 4; cifarski produkt im je 4, tj. -1.

Za cifarski prsten Ip (p prost broj) regularni su elementi:

$$1,\ 2,\ 3,\ \ldots,\ p-1 \qquad \text{ili u drugoj oznaci:}$$

$$1,\ 2,\ \ldots,\ -2,\ -1.$$

Krajnje cifre 1, $p-1$ (tj. -1) imaju produkt -1. Još se radi o preostalim „srednjim" ciframa

$$2,\ 3,\ \ldots,\ p-2. \tag{3}$$

No, promatrajmo za svaku od tih cifara a pripadnu inverznu cifru a^{-1}; ona postoji i zadovoljava jednu jedinu jednadžbu $ax = 1$; nadalje je $a^{-1} \neq a$; kad bi, naime, bilo $a = a^{-1}$, značilo bi to da je $a^2 = 1$, tj. da je broj $a^2 - 1$, tj. $(a-1)(a+1)$ djeljiv brojem p; kako je p prost broj, znači to (§ 11.5) da je jedan od faktora $a-1$, $a+1$ djeljiv sa p; to je moguće ili da je $a-1=0$ ili $a+1=p$, tj. $a=1$, $p-1$, protivno pretpostavci da je a uzeto iz niza (3). Ukratko, nekrajnje cifre u Ip, tj. cifre (3), sparuju se dvije po dvije i daju produkt 1; prema tome, i produkt svih članova u (3) je 1 pa je, znači, produkt svih cifara u Ip jednak produktu krajnjih cifara 1, -1, tj. -1. Tako smo odredili broj $w(p) = -1$. I to je Wilsonov teorem:

17.6.11.1. Teorem (Wilson, 1741—1793). *Za svaki prost broj p produkt svih cifara iz $\Phi(p) = \{1, 2, \ldots, p-1\}$ u prstenu Ip iznosi $p-1$ (tj. -1), tj. $w(p) = -1$. Drugim riječima, produkt brojeva $1, 2, \ldots, p-1$ podijeljen brojem p daje ostatak -1; ili ovako:*

$$(p-1)! \equiv -1 \pmod{p}. \tag{W}$$

Vrijedi i obrat: (W) $\Rightarrow p \in P$ (isp. § 17.7.17.3).

---

[1] Svaki element a kola K za koje je množenje $x \to ax$ jedna permutacija čitava kola zove se regularan element kola. Tako npr. u kolu racionalnih brojeva jedino 0 nije regularna!

Mnogo je teže odrediti broj $w(m)$ za složen broj m. Zanimljivo je da je $w(m)$ ili 1 ili -1 (*Gauss*). Ako pokušamo odrediti član $w(m)$ u prstenu Im kao što smo ga odredili za slučaj $m=p$, tada opet imamo sparivanje $a \to a^{-1}$ kao maloprije; ali je mnogo teže odrediti koliko se puta može pojaviti slučaj da je a samo sa sobom spareno, tj. da bude $a=a^{-1}$, tj. $a^2=1$. Tako se dolazi do kvadratne jednadžbe $x^2=1$ u kolu Im, odnosno do kvadratne kongruencije $x^2 \equiv 1 \pmod{m}$. Gauss je bio veliki izgrađivač toga matematskog područja.

17.6.11.2. Gaussov teorem (1801). *Za svaki prirodni broj m produkt regularnih članova cifarskog prstena Im iznosi* $w(m)=\pm 1$; *ako je* 1) $m=4$ p^n, $2p^a$ (p *prost broj i* >2), *onda je* $w(m)=-1$; *u svim drugim slučajevima* je $w(m)=1$.

Npr., $w(100)=1$.

17.7. Zadaci o linearnim diofantskim jednadžbama i linearnim kongruencijama s jednom nepoznatom veličinom.

1. Da li je ispunjen nuždan i dovoljan uslov pa da ova kongruencija ima bar jedno rješenje: 1) $3x \equiv 5 \pmod{6}$; 2) $4x \equiv 6 \pmod{12}$; 3) $354y \equiv 0 \pmod{199999}$; 4) $at \equiv 0 \pmod{b}$; 5) $8u \equiv 1 \pmod{16}$, 6) $324x \equiv 18 \pmod{500}$; 7) $-1005x \equiv 412 \pmod{1961}$?

2. Nađi rješenja kongruencija iz zad. 1 i to specijalno ona koja su neodrečna i ≤ 100.

3. Napiši kongruencije iz zad. 1 kao diofantske jednadžbe.

4. Riješi ovu diofantsku jednadžbu: 1 *a*) $2x-5y=3$, 1 *b*) $20x-50y=40$; 1 *c*) $100x-500y=400$; 2 *a*) $35x+42y=125$, 2 *b*) $-35x+42y=125$, 2 *c*) $35x-42y=125$, 2 *d*) $-35x-42y=125$, 2 *e*) $-35x+42y=-125$. Kako su povezana rješenja ovih kongruencija s rješenjima kongruencije 2 *a*)? 3) $10!\,x+\binom{10}{4}y=840$.

5. Riješi sve prethodne relacije radeći u brojevnom prstenu Im, gdje je m modul kongruencije, odnosno koeficijent veličine y.

6. 1) Odredi $\Phi(m)$ i $\varphi(m)$ za svako m iz prethodnog zadatka;
   2) Dokaži: Ako su n, m relativno prosti, onda je $\Phi(n)\cdot\Phi(m)=\Phi(nm)$;
   3) Ako je $m \mathrm{M} n=1$, nađi zbroj brojeva iz $\Phi(m\cdot n)$.

7. Zadatke iz 1. riješi služeći se Fermat-Eulerovim teoremom.

8. Dokaži: 1) Ako je p prost broj, tada je svaki prost faktor broja $M_p=2^p-1$ oblika $2kp+1$; 2) Svaki prost faktor broja $F_n=2^{2^n}+1$ oblika je $2^{n+1}k+1$; 3) Ako je p prost broj, svaki prost faktor broja $N_p=2^p+1$ oblika je $2kp+1$.

9. Odredi najmanji pozitivni broj iz 1) $2D\cap(5D+3)$; 2) $(3D+1)\cap\cap(7D+5)$; 3) odredi sve 4-cifrene pozitivne brojeve koji podijeljeni sa 7 odnosno 9 daju ostatak 5 odnosno 8.

10. Promatraj cifarski skup $I5$; odredi 1) $3\cdot I5$; 2) $10\cdot I5$; 3) $17\cdot I5$; 4) $20\cdot I5$; 5) $nI5$, sve računajući u tom cifarskom prstenu.

11. Isto pitanje za operaciju zbrajanja.
12. Promatraj 1) $\Phi(10)$; 2) $\Phi 11$, 3) $\Phi 20$; napiši odgovarajuću tablicu a) zbrajanja, b) oduzimanja, c) množenja, d) dijeljenja, e) kvadriranja, f) antikvadriranja, g) kubiranja, h) antikubiranja.
13. U prstenu $(\Phi(m), +_m, \cdot_m)$ odredi produkt $w(m)$ svih njegovih elemenata za $m =$ 1) 3; 2) 4; 3) 5; 4) 6; 5) 7; 6) 8; 7) 9; 8) 10; 9) 11; 10) 20.
14. Služeći se Fermat-Eulerovim teoremom odredi ostatak pri diobi za ove parove brojeva: 1) 3^{80}, 14; 2) 7^{1000}, 360; 3) 2^{250}, 13; 4) 457^{35983}, 5; 5) 459^{35425}, 7.
15. *Farey-evi nizovi.* Zadan je realan broj $x \geq 1$; odredi uzlazan niz svih pozitivnih racionalnih brojeva u neskrativom obliku $\frac{m}{n}$ za koje je $0 < n \leq x$ kao i broj tx članova toga Farey-eva niza koji odgovara broju x. Promatraj specijalno slučajeve: 1) $x = 1$; 2) $x = 2$; 3) $x = 3$; 4) $x = 5\frac{1}{2}$.
16. Pođimo od razlomaka $\frac{0}{1}, \frac{1}{1}$, pa uklapajmo induktivno između svaka dva susjedna člana $\frac{a}{b}, \frac{c}{d}$ za koje je $b + d \leq x$ član $\frac{a+c}{b+d}$; 1) dokaži da je $ad - bc = -1$ i da se na taj način dobije Fareyev podniz svih brojeva ≤ 1. Neka je $\tau \geq 1$; 2) dokaži da je svaki realan broj x moguće predstaviti u obliku $x = \frac{m}{n} + \frac{\Theta}{n^\tau}$, pri čemu je $m \,\mathrm{M}\, n = 1$, $0 < \Theta < 1$.
17. 1) Provjeriti izravno da je $(p-1)! + 1$ djeljivo sa p za proste brojeve $p = 5, 7, 11$; 2) podijeli $(m-1)! + 1$ sa m za $m = 3, 6, 8$; da li je ostatak $= 0$? 3) dokaži da iz $m \mid (m-1)! + 1$ izlazi da je m prost broj pa je prema tome Wilsonov iskaz (W) karakterističan za proste brojeve.
18. Za svaki $n \in N$, $k \in I_n$ vrijedi ovo:

    n je prost $\Leftrightarrow (n-k-1)!\ k! \equiv (-1)^{k+1} \pmod{n}$ (*Vl. Kirin*[1]).
19. Za svaku $n \in N$, $n > 3$ vrijedi ovo:

    n je prost $\Leftrightarrow 1 \cdot 1! + 2 \cdot 2! + \cdots + (n-3)(n-3)! \equiv 0 \pmod{n}$ (*G. Kalajdžić*).
20. Problem. Ne zna se da li postoji složen prirodni broj n sa svojstvom da $2^n - 1$ bude djeljivo sa n^2.
21. Problem. Ne zna se da li postoji pravokutan paralelepiped sa svojstvom da mjerni brojevi svih njegovih bridova i svih dijagonala (prostornih i plošnih) budu prirodni brojevi.
22. Rešiti jednačinu $(xy + yz + zx)^2 - 9 = (x + y + z)^4$ u skupu celih brojeva (Šami Toran).

---

[1]) Vl. G. Kirin, *A note on Wilson's theorem* (Glasnik Mat. Fiz i Astr., Zagreb, 17 (1962) 181—182).

18. LINEARNE KONGRUENCIJE S VIŠE MODULA

18.0. U prvom stoljeću prije naše ere Kinez *Sun Cu* traži prirodni broj koji — podijeljen sa 3, 5, 7 — daje za ostatak 2, 3, 2.

Znači da treba biti

$$x \equiv 2 \pmod 3$$

$$x \equiv 3 \pmod 5$$

$$x \equiv 2 \pmod 7.$$

Interpretiralo se kao da on promatra broj $W(3, 5, 7) = 3 \cdot 5 \cdot 7$ i da onda određuje kratnike $\alpha_0 = 70$, $\alpha_1 = 21$, $\alpha_2 = 65$ od $5 \cdot 7$ odnosno $3 \cdot 7$, odnosno $5 \cdot 7$ tako da oni budu $\equiv 1$ mod 3, 5, 7 po redu. I tada je $2\alpha_0 + 3\alpha_1 + 2\alpha_2$ jedno rješenje. Izlazi $x \equiv 23 \mod (3 \cdot 5 \cdot 7)$.

Prethodni zadatak je tipičan kao što pokazuje:

18.1. Teorem o simultanim kongruencijama. *Neka je*

$$x \equiv c_1 \pmod{m_1}$$

$$x \equiv c_2 \pmod{m_2} \tag{1}$$

$$\cdots\cdots\cdots$$

$$x \equiv c_s \pmod{m_s}$$

zadan skup od s kongruencija; neka su moduli m_k dva po dva međusobno prosta; tada je ***sistem*** (1) *ekvivalentan s* ***jednom*** *kongruencijom mod m, gdje je $m = \Pi m_k = m_1 \cdots m_s$; specijalno ako je*

$$M_k y_k \equiv 1 \pmod{m_k}, \quad \textit{gdje je} \quad M_k = m/m_k, \tag{2}$$

tada je

$$x \equiv \sum_k c_k M_k y_k \pmod m; \tag{3}$$

i obrnuto: ako je ispunjeno (2), *onda iz* (3) *izlazi* (1).

Primijetimo ovo: ako su svi $c_k = 0$, tada je pomcću (1) iskazano da je x djeljivo relativno prostim brojevima m_k; prema osnovnom teoremu znači to da je x djeljivo produktom Πm_k svih tih modula. Obrat je očigledan.

Dokaz teorema. Zbog pretpostavke da su svi zadani moduli međusobno prosti, izlazi da je $M_k \mathrm{M}\, m_k = 1$; zato za svako $k \in 1(s)$ sve vrijednosti od nepoznanice y_k leže u određenom razredu mod m_k.

Dokaz (1) $\Rightarrow$ (3). Kad su tako brojevi y_k pomoću (2) određeni, pomnožimo svaku kongruenciju iz (1) odgovarajućom kongruencijom iz (2), i to unakrst; izlazi:

$$x \cdot 1 = c_k M_k y_k \pmod{m_k}. \tag{4}$$

Kako je očigledno $M_i \equiv 0 \pmod{m_k}$ za svako $i \neq m_k$, znači da iz (4) izlazi:

$$x \equiv \sum c_k M_k y_k \pmod{m_k}.$$

To znači da je $x-\sum c_k M_k y_k$ djeljivo svakim m_k, dakle i njihovim produktom m, jer su m_k dva po dva međusobno prosta. Dakle, zaista vrijedi (3).

(3) $\Rightarrow$ (1). To je očigledno. Treba, naime, pokazati da vrijedi:

$$\sum c_k M_k y_k \equiv c_k \pmod{m_k}. \tag{5}$$

No, zbog (2) $M_k y_k$ se smije zamijeniti sa 1; a svi drugi M_i su $\equiv 0 \pmod{m_i}$, dakle zbilja (5) postaje $c_k \equiv c_k \pmod{m_k}$, što je očigledno ispunjeno.

Time je teorem dokazan.

18.2. *Tih-Hing* (8. st.) rješava sistem (1) i za slučaj kad moduli nisu relativno prosti svaki sa svakim. Promatra najmanji kratnik W modulâ i prikazuje ga kao produkt faktorâ $\mu_k \mid m_k$, i to tako da su 2 po 2 međusobno prosta. Ako je tada $y_i \equiv 0 \pmod{m/\mu_i}$, gdje je $m = \Pi \mu_k$, te $y_k \equiv 1 \pmod{\mu_k}$, tada je $\sum y_k c_k$ rješenje polaznog sistema.

Tih-Hing specijalno pita da se odredi broj jedinica za posao ako isti broj x jedinica takvog posla urade ekipe od 2, odnosno 3, odnosno 6, odnosno 12 radnika pri čemu se zna da poslije cijeloga dnevnog rada svake od tih ekipa ostane još 1, odnosno 2, 5, 5 jedinica nesvršena posla.

18.3. *Za egzistenciju sistema* (1) *nužno je i dovoljno da bude* $c_i - c_k$ *djeljivo sa* $m_i \,\mathrm{M}\, m_k$ *za svaki par* $\neq$ *indeksa.*

To se vidi unošenjem rješenja x iz i-te jednadžbe u k-tu jednadžbu.

Stvar se dokazuje induktivno.

Tako npr. iz prve jednadžbe izlazi

$$x = c_1 + m_1 y_1,$$

gdje je y_1 neodređen broj. Unesemo sad to x u narednu jednadžbu; izlazi:

$$c_1 + m_1 y_1 \equiv c_2 \pmod{m_2}, \text{ tj.}$$

$$m_1 y_1 \equiv c_2 - c_1 \pmod{m_2}.$$

To je sad već opća linearna kongruencija za y_1; uslov je da bude $c_2 - c_1$ djeljivo sa $m_1 \,\mathrm{M}\, m_2$. Kad se tako nađe y_1, ide se u treću jednadžbu, itd.

18.4. Linearne kongruencije s više modula. Diofantske jednadžbe s više nepoznanica. Zadaci.

1. 1) Riješi
$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod 5$$
$$x \equiv 6 \pmod 7;$$

2) Spoznaj da se tu radi o određivanju skupnosti $(3D+1) \cap (5D+2) \cap (7D+6)$.

3) Odredi najveće negativno rješenje i najmanje pozitivno rješenje.

2. Postoji li 3-cifren broj koji podijeljen sa 5 odnosno sa 8 odnosno sa 9 daje za ostatak: 2 odnosno 7 odnosno 1?

3. Odredi $(8D-1)\cap(11D+3)\cap(15D-5)\cap(49D+8)$.

4. *Magični kvadrati.*

1) Pod magičnim kvadratom razreda $n\times n$ razumijevamo svrstavanje *prvih* n^2 prirodnih brojeva u oblik jedne kvadratne tablice sa svojstvom da je suma S članova svakog retka jednaka sumi članova svakog stupca jednako sumi članova na svakoj od dvije dijagonale.

Npr. evo jednog magičnog kvadrata $n\times n$:

1	12	8	13
14	7	11	2
15	6	10	3
4	9	5	16

Tu ie $S=34$.

2) Dokaži da nema magičnog kvadrata 2×2.

3) Odredi magične kvadrate razreda 3×3.

4) Odredi bar jedan magični kvadrat razreda 5×5 (ima ih oko 60000).

5. Odredi koje rješenje jednadžbe $x!+1=y^2$.

6. Isto pitanje za $x!-1=p$ (p prost broj).

7. Jednadžba $991n^2+1=s^2$ nije moguća za $n=1, 2, 3, \ldots, n_s$
$s=12055\ 735\ 790331\ 359\ 447\ 442\ 538\ 767$ no zadovoljena je za $n=n_s$,
$s=379\ 516\ 400\ 906\ 811\ 930\ 638\ 014\ 896\ 080$ (W. Sierpiński).

8. Da li je ovaj sistem moguć; nađi rješenja:

1) $3x\equiv 5 \pmod 6$
$2x\equiv -1 \pmod 8$
$4x\equiv 7 \pmod 9$;

2) $x\equiv 2 \pmod 3$
$x\equiv 1 \pmod 5$
$x\equiv 71 \pmod{125}$;

3) $x\equiv 5 \pmod 8$
$x\equiv 13 \pmod{16}$
$x\equiv 2 \pmod 3$

4) $2x\equiv 3 \pmod 5$
$x\equiv 1 \pmod 7$
$x\equiv 21 \pmod{25}$
$x\equiv 71 \pmod{125}$
$x\equiv 1 \pmod 5$;

5) Izlazi iz 4) pišući mod 75 umjesto mod 7.

$$3x \equiv 2 \pmod{25}$$

$$7x \equiv 3 \pmod{3};$$

6) $x \equiv 5 \pmod{8}$, $x \equiv 13 \pmod{16}$, $x \equiv 2 \pmod{3}$, $x \equiv 21 \pmod{25}$, $x \equiv 71 \pmod{125}$, $x \equiv 1 \pmod{5}$.

9. Problem. Postoje li dva brojevna razreda A, B koja su u međusobnom aditivnom odnosno multiplikativnom srodstvu tj. da vrijedi

$$A + A \subset B \text{ i } B + B \subset A \qquad \text{odnosno}$$

$$A \cdot A \subset B \text{ i } B \cdot B \subset A?$$

10. Problem. 1) Odredi množinu K svih konačnih dvonizova

$$a_1, a_2, \ldots, a_k$$

$$b_1, b_2, \ldots, b_k$$

sa svojstvom da prvi niz bude strogo uzlazan ($a_1 < a_2 < a_3 < \cdots < a_k$) i da je $\bigcup_{k'} (a_{k'} D + b_{k'}) = D$;

2) Dokaži da je dvoniz $\begin{matrix} 2, & 3, & 4, & 6, & 12 \\ 0 & 0 & 1 & 1 & 11 \end{matrix}$ član u K.

3) Da li postoji i takav slučaj da su svi a-ovi neparni?

4) Može li se a_1 uzeti proizvoljno?

19. O NEKIM FUNKCIJAMA U SKUPU PRIRODNIH, ODNOSNO CIJELIH BROJEVA

19.0. Dosad smo se sreli s nekim funkcijama u skupu N prirodnih brojeva. Tako je, npr., za svako $n > 1$ važno znati koliko n ima prostih djelitelja, odnosno uopće djelitelja. Naročito smo se sreli sa skupom $\Phi(n)$ brojeva $< n$ prostih prema n i vidjeli koliko je taj skup važan, a već smo vidjeli da i broj $\varphi(n)$, koji kazuje koliko $\Phi(n)$ ima brojeva, dolazi na bitan način u vezi s kongruencijama. Sad ćemo ispitati specijalno funkciju φ, dokazati neka njena svojstva i s tim u vezi uvesti *Möbiusovu funkciju*.

19.1. Eulerova funkcija φ ili Eulerov indikator. — 19.1.0. *Eulerova funkcija* (*ili Eulerov indikator*) definirana je u skupu prirodnih brojeva. Stavlja se $\varphi(1) = 1$; za svako $n > 1$, kazuje Eulerov broj $\varphi(n)$ koliko u skupu $In = \{0, 1, \ldots, n-1\}$ ima relativno prostih brojeva prema n. Drugim riječima, kazuje $\varphi(n)$ koliko jednakost $x \,\mathrm{M}\, n = 1$ ima rješenja u In; sva ta rješenja čine skup $\Phi(n)$ (isp. § 17.6.2). Funkcija $n \to \varphi(n)$ javlja se u raznim matematičkim oblastima (teorija grupa, korijeni jedinice, itd.).

Očigledno je da je $\Phi(5) = \{1, 2, 3, 4\}$. Također se vidi da je, npr., $\Phi(5^4)$ sastavljeno od svih brojeva intervala $I5^4$ osim brojeva koji su djeljivi

sa 5, a to su: 0, 5, $5\cdot 2$, $5\cdot 3, \ldots,$ 5^4-5; svi ovi isključeni brojevi čine aritmetičku progresiju, odnosno skup $5\,I(5^3)$, kojem su 0, 5^4-5 krajnji članovi, a diferencija $=5$; članova ima 5^3. Dakle je $\varphi(5^4)=5^4-5^3$. Slično, $\varphi(5^s)=5^s-5^{s-1}$; isto tako, $\varphi(p^s)=p^s-p^{s-1}$ za svaki prost broj p i svaki prirodni broj s.

19.1.1. Također se vidi da se, npr., $\Phi(100)$ dobije iz $I\,100$ kao preostatak uklanjanja iz $I\,100$ svih brojeva koji su djeljivi bar jednim prostim djeliocem $p=2$, 5 broja 100; time se učini da $x\in\Phi\,100$ ne zadovoljava $x\,\mathrm{M}\,p=p$, pa zato sa 100 ne može imati p kao zajednički djelilac.

Zaključak je općenit:

Skup $\Phi(n)$ *dobije se kao ostatak u množini* In *kad iz* In *uklonimo sve brojeve koji sa* n *imaju zajednički bar jedan* n*-ov prost djelilac.*

To je jasno! No mnogo je teže prebrojiti skup $\Phi(n)$, tj. odrediti broj $\varphi(n)$.

Pa neka je p prost djelilac prirodnog broja m i $m=pm'$; svi brojevi iz Im koji su djeljivi sa p čine aritmetičku progresiju

$$p\cdot 0,\ p\cdot 1,\ p\cdot 2, \ldots,\ p\cdot(m'-1);\ \text{ima ih } m'.$$

Skup tih brojeva je produkt $p\cdot I(m')$ od p i svakog broja iz intervala $I(m')$. Preostatak $Im \setminus pIm'$ ima $m-m'$ brojeva. No, $m-m'=m-mp^{-1}=m(1-p^{-1})$ (p non$\mid x$, tj. p ne dijeli x).

Time smo dokazali da vrijedi:

19.1.2. Lema. Ako je m proizvoljan prirodan broj >1, a p njegov prost djelilac i $m=pm'$, tada $Im \setminus pIm'$ predstavlja množinu svih brojeva iz Im koji nisu djeljivi sa p; tih brojeva ima $m(1-p^{-1})$.

Na osnovu te leme dokazat ćemo:

—→ **19.1.3.** Teorem. *Ako je* n *bilo koji prirodan broj* >1, *a*

$$p_0,\ p_1, \ldots,\ p_{s-1},\ p_s \tag{1}$$

bilo kojih njegovih različitih $1+s$ *prostih djelitelja, tada u skupu*

$$In=\{0,\ 1, \ldots,\ n-1\} \qquad \textit{ima upravo}$$

$$n(1-p_0^{-1})(1-p_1^{-1})\cdots(1-p_{s-1}^{-1})(1-p_s^{-1})=n\prod_{k=0}^{s}(1-p_k^{-1}) \tag{2}$$

brojeva koji su prosti prema brojevima (1).

Dokaz ćemo provesti indukcijom prema broju upotrijebljenih prim-faktora. Logički, dokaz je dosta težak!

Prema lemi 19.1.2. teorem je istinit ako se niz (1) sastoji od jednoga jedinog člana $p=p_0$; pretpostavimo sada da je dokazan ovaj izkaz

(H_s): *za zadani broj* $s>0$ *i za svaki broj* m *i svaki podskup* X *od* s *prostih djelilaca broja* m, *pokazuje izraz*

(3) $$m\prod_{x\in X}(1-x^{-1})$$

koliko skup I m sadrži brojeva koji su relativno prosti prema svakom broju iz X.

Traženi skup S svih brojeva iz In prostih prema svima p_s' i p_s dobije se i tako da se iz skupa $M\subset In$ svih brojeva prostih prema svima p_s' odstrani skup Y svih prisutnih kratnika broja p. Uočimo najprije da po hipotezi (H_s') vrijedi:

(4) $$kM=n\prod(1-p_s').$$

Koliko Y ima članova? Svakako je

$$Y\subset p_s\, I\left(\frac{n}{p_s}\right).$$

Međutim, određen podskup od $p_s\, I\, m$, gdje je $m=\dfrac{n}{p_s}$ uklonjen je iz In već u toku procesa u vezi s prethodnim brojevima p_s'; zato sad još preostaje da razmatramo samo ove brojeve

(5) $$p_s\cdot\dot{m},\ \ m=\frac{n}{p_s}\ \text{ iz }\ p_s\, I\, m$$

koji su prosti prema svim p_s', tj. $p_s\,\dot{m}\,\mathrm{M}\,p_s'=1$, dakle i $\dot{m}\,\mathrm{M}\,p_s'=1$; takvih rješenja m prema indukcionoj hipotezi (H_s') i obrascu (3) ima upravo

$$m\prod(1-p_s'^{-1})$$

i to je kY:

(6) $$kY=m\prod\left(1-p_s'^{-1}\right);$$

zato jednakost

$$S=M\setminus Y \qquad \text{daje}$$

$$kS=kM-kY, \qquad \text{odnosno po (4) i (6)}$$

$$kS=n\prod\left(1-p_s'^{-1}\right)-m\prod\left(1-p_s'^{-1}\right).$$

Unese li se tu $m=n/p$ iz (5) i izluči

$$n\prod\left(1-p_s'^{-1}\right)$$

kao faktor, dobije se traženi obrazac (1).

Time je dokazan prelaz od s na $s+1$. Prema principu indukcije dokazan je time i teorem 3.

—→ **19.1.4.** Teorem o φ-funkciji. **(a)** ***Ako sa P (n) označimo skup svih prostih djelitelja prirodnog broja n, tada je***

$$\varphi(n)=n\prod(1-p^{-1}),$$

pri čemu je $p\in P(n)$.

To se kraće može naznačiti sa $n\prod_{P(n)}$, ***znajući da se oznaka*** Π ***za množenje odnosi na izraze*** $1-x^{-1}$, ***pri čemu*** x ***prolazi skupom*** $P(n)$.

(b) $$\varphi(p^m)=p^m-p^{m-1}$$

za prost broj p ***i svaki prirodan broj*** m.

(c) *Za svaki konačan jednolistan (tj. bez = članova) niz prostih brojeva* $p, q\cdots$; *i svaki pripadni niz* $m_p, m_q, \ldots$ *prirodnih brojeva vrijedi:*

$$\varphi(p^{m_p}\cdot q^{m_q}\cdot\ldots)=p^{m_p}\cdot q^{m_q}\cdot\ldots(1-p^{-1})(1-q^{-1})\cdot\ldots=$$

$$=(p^{m_p}-p^{m_p-1})\cdot(q^{m_q}-q^{m_p-1})\cdot\ldots=\varphi(p^{m_p})\varphi(q^{m_q})\cdot\ldots$$

(d) *Ako je* $m\,\mathrm{M}\,n=1$, *tada je* $\varphi(m\cdot n)=\varphi(m)\varphi(n)$[1], *i obratno.*

Teorem (a) je specijalan slučaj prethodnog teorema 3 kad niz (1) obuhvata sve proste brojeve od n. Teorem (b) je specijalan slučaj teorema (a): $P(n)=\{p\}$. Teorem (c) izlazi iz (a) jer je $P(p^{m_p}\cdot q^{m_q}\cdot\ldots)=\{p, q, \ldots\}$. Teorem (d) izlazi iz (a) zbog toga što za relativno proste brojeve m, n vrijedi $P(m)\cap P(n)=$ prazno (inače je $P(m)\cup P(n)=P(m\cdot n)$ bez obzira na to takvi su m i n), pa je prema oznaci iz (a):

$$\varphi(m)\varphi(n)=m\prod_{P(m)}\cdot n\prod_{P(n)}=n\cdot m\prod_{P(m)\cup P(n)}=n\cdot m\prod_{P(n\cdot m)}$$

(ovdje dolazi do izražaja činjenica o ekvivalenciji

$$m\,\mathrm{M}\,n=1\ \Leftrightarrow\ P(m)\cap P(n)=\text{prazno}).$$

Primjeri. $\varphi(100)=\varphi(2^2\cdot 5^2)=(2^2-2^1)(5^2-5)=2\cdot 20=40$. Sam skup $\Phi(100)$ se sastoji od brojeva <100 koji su neparni i prosti prema 5:

$$\Phi(100)=\{1,\ 3,\ 7,\ 9,\ 11,\ \ldots,\ 99\}$$

$$\varphi(2\cdot 3)=\varphi(2)\varphi(3)=1\cdot 2=2.$$

Specijalno ističemo multiplikativni karakter funkcije φ (teorem d).

19.1.5. Drugi dokaz multiplikativnog karaktera Eulerove funkcije. Riječ je o dokazu zaključka:

Ako su a, c *relativno prosti prirodni brojevi, tj.*

(1) $$a\,\mathrm{M}\,c=1,$$

onda je

(2) $$\varphi(ac)=\varphi(a)\varphi(c).$$

Neka je $v=ac$. Kao obično, za redni broj x označujemo sa $\dot{x}$ redne brojeve $<x$. Tada u prvom redu svako $\dot{v}$ na jednoznačan način može se pisati u obliku:

(3) $$\dot{v}=a\dot{c}+\dot{a},$$

(4) $$I\dot{v}=a\,I\dot{c}+I\dot{a}.$$

---

[1]) Kaže se da je φ multiplikativna funkcija, odnosno distributivna prema množenju relativno prostih brojeva.

Dovoljno je $\dot{v}$ podijeliti sa a i odrediti kvocijent c i ostatak a. Zbog (3) očigledno je $\dot{v}\,\mathrm{M}\,a = a\,\mathrm{M}\,a$. Specijalno, za svako $a_1 \in \Phi(a)$, tj. za $a_1\,\mathrm{M}\,a = 1$ imamo:

$$(ac + a_1)\,\mathrm{M}\,a = 1 \qquad (a_1 \in \Phi\, a)); \tag{5}$$

$\Phi(a)$ označuje sva rješenja od $a\,\mathrm{M}\,a = 1$. No, skup

$$a\,I(c) + a_1 \tag{6}$$

svih $ac + a_1$ nastaje iz Ic tako da se interval Ic pomnoži sa a i pomakne za a_1.

Zbog (1) vrijedi $(ac\,\mathrm{M}\,c) = c\,\mathrm{M}\,c$; specijalno, za svako $c_1 \in \Phi(c)$ imamo $c_1\,\mathrm{M}\,c = 1$, pa dakle i

$$ac_1\,\mathrm{M}\,c = 1. \tag{7}$$

Brojevi iz (6) dva po dva su nepodudarna mod c jer bi iz

$$ac + a_1 \equiv ac' + a_1 \pmod{c}$$

izlazilo (ispusti a_1):

$$ac \equiv ac' \pmod{c},$$

što zbog (1) po teoremu 11,5. ima posljedicu $c = c' \pmod{c}$. Kako je, dakle, skup (6) sastavljen od c nepodudarnih brojeva mod c, znači da m sadrži potpuno određen podskup $S(a_1)$ od $\varphi(c)$ brojeva koji su prosti prema c (to su, naime, brojevi koji su podudarni s po jednim brojem iz $\Phi(c)$). No, osim toga, prema (5) svaki broj iz $S(a_1)$ je prost prema a; znači, svaki broj iz $S(a_1)$ je prost i prema c; prema Euklidovu teoremu 13.2, znači to da je svaki broj iz $S(a_1)$ prost i prema produktu $ac = v$.

Na taj način, za svako $a_1 \in \Phi(a)$ pridružen je i potpuno jednoznačno određen skup $S(a_1)$ od $\varphi(c)$ brojeva prostih prema v.

No, skup $S(a_1)$ je dio množine $a\,Ic + a_1$; za različite a_1 ti su skupovi disjunktni — to izlazi iz osnovnog teorema o diobi. Na taj način dobijemo $\varphi(a)$ disjunktnih skupova $S(a_1)$ po $\varphi(c)$ brojeva iz Ic i svi su oni prosti prema v; dakle je broj $\varphi(a)\cdot\varphi(c)$ tako dobivenih brojeva $\leq \varphi(v)$; drugim riječima:

$$\varphi(a)\,\varphi(c) \leq \varphi(a \cdot c). \tag{8}$$

Još treba dokazati da tu ne može biti znak $<$; kad bi, naime, u (8) stajalo $<$ umjesto $\leq$, značilo bi to da postoji bar jedan broj $b \in I(ac)$ sa svojstvom $b\,\mathrm{M}\,ac = 1$ i broj b ne bi ležao ni u kojem skupu $S(a_1)$ sa $a_1 \in \Phi(a)$. No, b je oblika $ax + y$ s određenim $x \in Ia$, $y \in Ic$. Zato bi y bio broj izvan $\Phi(a)$, dakle $y\,\mathrm{M}\,a > 1$; odatle izlazi također $(ax + y)\,\mathrm{M}\,a > 1$, tj. $b\,\mathrm{M}\,a > 1$, pa to prije $b\,\mathrm{M}\,ac > 1$, protivno pretpostavci da je $b\,\mathrm{M}\,ac = 1$,

Time je multiplikativnost Eulerove formule dokazana.

19.1.6. P r i m j e d b a. Ako se u jednu ruku ima na umu da je multiplikativnost funkcije φ jedna posljedica gornjeg teorema 3, na osnovu kojeg smo dokazali Eulerov teorem o φ; ako se u drugu ruku pogleda na prethodni dokaz te posljedice i kako se u njemu pozivamo na prilično toga od ranije, onda nije osobito čudo da je onaj dokaz u § 19.1.3 bio logički težak!

19.1.7. Gaussov teorem o φ-funkciji. — **19.1.7.0.** Ako je $d \mid n$, tada sistem

$$x \,\mathrm{M}\, n = d, \quad x \in In \tag{1}$$

ima $\varphi(m)$ rješenja, gdje je $m = nd^{-1}$.

Stvarno, kratnici djelitelja d od n koji su u In čine skup $d \cdot I\frac{n}{d}$.

Prema tome se za sistem (1) radi da se odrede svi oni brojevi r iz Im za koje je $dr \,\mathrm{M}\, n = d$. tj, $r \,\mathrm{M}\, \frac{n}{d} = 1$, a takvih brojeva po definiciji ima $\varphi\left(\frac{n}{d}\right)$.

19.1.7.1. (Gaussov teorem o φ). $\sum_{d \mid n} \varphi(d) = n$; *pri tom se sumacija odnosi na sve djelitelje broja n* (*brojevi* 1 *i n uključeni*!).

Kaže se: *identična funkcija* $n \to n$ *u N je sumator funkcije* $n \to \varphi(n)$.

Npr., djelitelji broja 24 jesu: 1, 2, 3, 4, 6, 8, 12, 24; dalje je

$$\varphi(1) = 1, \quad \varphi(2) = 1, \quad \varphi(3) = 2, \quad \varphi(4) = 2, \quad \varphi(6) = 2,$$

$$\varphi(8) = 2^3 - 2^2 = 4, \qquad \varphi(12) = \varphi(3)\,\varphi(4) = 2 \cdot 2 = 4,$$

$$\varphi(24) = \varphi(3 \cdot 8) = \varphi(3)\,(8) = 2 \cdot 4 = 8,$$

$$\sum \varphi(d) = 1 + 1 + 2 + 2 + 4 + 2 + 4 + 8 = 24.$$

Dokaz G a u s s o v o g t e o r e m a. Promatrajmo, naime, funkciju f

$$\dot{n} \to \dot{n} \,\mathrm{M}\, n$$

u skupu In. Neka je A skup njenih vrijednosti; znači da je pripadna antifunkcija ^{-}f definirana u A; no za svako $d \in A$, ^{-}fd ima prema gornjoj lemi upravo $\varphi\left(\frac{n}{d}\right)$ vrijednosti (jer ^{-}fd upravo označuje svako rješenje od (1)); no antidomen antifunkcije je domen In; a kako za $d \neq d'$ iz A izlazi $^{-}fd \neq {}^{-}fd'$, znači to da su skupovi $\{^{-}fd\}$ disjunktni kad $d \in A$; to znači da je kardinalni broj n njihove unije jednak sumi kardinalnih brojeva od svih $\{^{-}fd\}$, tj,

$$\sum_{d} \varphi\left(\frac{n}{d}\right), \quad d \in A,$$

A to se i htjelo dokazati.

19.2. Neke definicije o funkcijama u *N* i *D*. U vezi s važnim svojstvima funkcije φ možemo postaviti neke definicije.

19.2.1. Multiplikativnost funkcije. Neka je funkcija f definirana u skupu N prirodnih brojeva (vrijednosti joj mogu biti u N, u $I\omega = \{0\} \cup N$, D, Q, R, ...); kaže se da je funkcija f *multiplikativna ili distributivna prema množenju* ako iz $m \,\mathrm{M}\, n = 1$ izlazi $f(mn) = f(m)\ f(n)$[1],

Osnovna multiplikativna funkcija je funkcija $d_0(n)$, koja kazuje koliko n ima djelitelja ≥ 1; multiplikativne su i funkcije $d_k(n) = \sum_{d|n} d^k(n)$, $k = 0,\ 1,\ \cdots$ Važno je da je φ također multiplikativna.

Suponirat ćemo da je $f(1) \neq 0$ *za svaku multiplikativnu funkciju* f. Bez sumnje, najjednostavnije distributivne funkcije su one koje su izvan jedinice konstantne.

19.2.2. Sumator zadane funkcije. Zadana je funkcija f u N; ako je $g(n) = \sum_{d|n} f(d)$, pri čemu d prolazi skupom $D(n)$ svih djelitelja broja n, tada se kaže da je g *sumator funkcije* f i piše:

$$g = Sf.$$

Također se kaže da je f *antisumator od* g i piše:

$$^{-}Sg = f.$$

Sumator sumatora zove se *sumator drugog reda*. Slično za antisumator. Sumator (antisumator) n-tog reda označavat će se sa S^n (odnosno S^{-n} ili ^{-n}S), Po definiciji: $S^{n+1} f = S(S^n f)$, $S^{-n-1} = {}^{-}S({}^{-n}Sf)$. Stavlja se $S^0 f = f$.

Na taj je način za svaku funkciju f vezan skup $S^D f$ funkcija oblika $S^n f$, gdje je n cio broj.

Vidjeli smo, prema Gaussu, da je identička funkcija j, sumator Eulerove funkcije φ. Sada, formalno, možemo *reći da je* φ *antisumator od identičke funkcije* $\dot{N} \to \dot{N}$. No, je li time φ određeno? I kako (isp. § 19.2.3.1)?

⟶ **19.2.3. Osnovni teorem.** ***Traženje sumatora i antisumatora zadane funkcije jednoznačne su operacije. Pri tom se distributivnost ne gubi: sumator (antisumator) distributivne funkcije opet je distributivna funkcija.***

Po definiciji, veza između bilo koje funkcije f koja je definirana u N i njenog sumatora $F = Sf$ određena je ovim nizom jednakosti:

$$(S) \qquad \begin{aligned} F(1) &= f(1) \\ F(2) &= f(1) + f(2) \\ F(3) &= f(1) + f(3) \\ F(4) &= f(1) + f(2) + f(4) \\ &\cdots\cdots\cdots\cdots \end{aligned}$$

---

[1]) To je analogon aditivnosti: $f(m+n) = f(m) + f(n)$.

. . . . . .

$$F(n)=\sum_{d|n} f(d).$$

Specijalno:

(1) $$F(p^n)=\sum_{d|n} f(d)=f(p^0)+f(p)+f(p^2)+\cdots+f(p^n)=$$
$$=F(p^{n-1})+f(p^n)$$

za svaki broj $p^n \in P^N$, gdje je P skup svih prostih, a N skup svih prirodnih brojeva.

Odatle očigledno možemo, i obrnuto, izraziti f pomoću F, tj. naći ^{-}SF; a to znači da je antisumator jednoznačno određen. Specijalno se vidi da je

(2) $$f(p^n)=F(p^n)-F(^{n-1}).$$

Mnogo je zanimljivije svojstvo distributivnosti (razdjelnosti).

(a) Slučaj sumatora: *f distributivno; dokazati da je i $Sf=F$ distributivno*. Neka su a, b prirodni brojevi i $a \,\mathrm{M}\, b=1$; treba dokazati da je

$$F(ab)=F(a)\,F(b). \quad \text{No,} \quad F(ab)=\sum_{d|c} f(d), \quad c=ab.$$

A svako $d \mid ab$ produkt je jednoga jedinog divizora $d_1 \mid a$ i jednoga jedinog $d_2 \mid b$, jer je $a \,\mathrm{M}\, b=1$; naime, faktorizacija od d je jednoznačna pa u d ulaze potpuno određeni prim-divizori od a i potpuno određeni prosti faktori iz b s potpuno određenim eksponentima. Zato se može pisati $\sum_{d|c} f(d)=\sum f(d_1 \cdot d_2)$, pri čemu je $d_1 \mid a$, $d_2 \mid b$; dakle je $d=d_1 d_2$. Zato je $f(d)=f(d_1 d_2)$; ovo je dalje zbog distributivnosti funkcije: $f(d)=f(d_1)f(d_2)$. Na taj način $F(ab)$ postaje

(3) $$F(ab)=\sum_{d|c} f(d)=\sum_{d_1|a;\ d_2|b} f(d_1)\,f(d_2)=$$ (zakon distribucije množenja prema $+$) $$=\sum_{d_1|a} f(d_1) \sum_{d_2|b} f(d_2)=F(a)\,F(b),$$ tj. $F(ab)=F(a)\,F(b)$.

(b) Dokažimo sada da je *antisumator f distributivne funkcije F distributivan.* Gore je pokazano da je f jednoznačno određeno i da zadovoljava (2) u skupu P^N. U drugu ruku, ako definiramo funkciju g tako da se na P^N podudara sa f i da bude distributivna, onda je, zbog jednoznačnosti faktorizacije prirodnih brojeva, g potpuno određena funkcija. No, sumator G od g podudara se sa zadanom funkcijom F. Naime po definiciji od g, funkcije G i F se zbilja podudaraju na P^N; nadalje, F i G su distributivne funkcije: F zato jer smo tako zadali, a G zato jer je G sumator distributivne funkcije (v. slučaj (a)). Dakle: F i G su dvije distributivne funkcije koje se podudaraju u P^N:

(4) $$F=G \text{ u } P^N;$$

time se one podudaraju i u N zbog jednoznačnosti faktorizacije; naime, za $n = p^\alpha \cdot q^\beta \ldots$ imamo:

$$F(n) = F(p^\alpha \cdot q^\beta \ldots) = (\text{distr.!}) = F(p^\alpha)\, F(q^\beta) = (\text{zbog } (4)) =$$

$$= G(p^\alpha)\, G(p^\beta) \cdot \ldots = (\text{distr. od } G) = G(p^\alpha q^\beta \ldots) = G(n), \text{ tj.}$$

$$F(n) = G(n).$$

Dakle je $F = G$. No, F je sumator od f; G je sumator od g; to zbog $F = G$ znači da je F sumator i od f i od g; drugim riječima, f i g su antisumatori od F; to zbog jednoznačnosti procesa antisumatora znači da je $f = g$; kako je g distributivno, znači da je zaista i f distributivno. Dakle je antisumator distributivne funkcije distributivan. Time je teorem potpuno dokazan.

19.2.3.1. Korolar. Prema Gaussu, identična funkcija $n \to n$ je sumator Eulerove funkcije φ; znači da je φ antisumator od identičnosti; kako je identičnost distributivna, to je distributivan i njen antisumator φ.

Gornji teorem 19.2.3. pokazuje kako je velika korist od lijepo formuliranih općih ideja.

19.2.4. Za svaku funkciju f skup $S^D f$ funkcijâ čini grupu prema operaciji

$$S^a S^b f = S^a (S^b f).$$

Ako je f distributivna funkcija, onda je to i svaki član grupe.

19.2.5. Teorem. *Ako je f multiplikativna funkcija, tada njen sumator ima oblik*:

$$F(n) = \sum_{d|n} f(d) = \prod_{p|n} \sum_{p^\alpha|n} f(p^\alpha) = \prod_{p|n} [1 + f(p) + f(p^2) + \cdots + f(p^\alpha)].$$

Dokaz je jasan: treba izmnožiti zagrade na desnoj strani; svaki član iz svake zagrade množi se svakim članom iz tuđe zagrade; time se dobije parcijalni produkt oblika $f(p^a)\, f(q^b) \ldots$; ovo je dalje, zbog distributivnosti funkcije f, jednako $f(p^a q^b \ldots) = f(d)$, gdje je $d \mid n$. Zbog jednoznačnosti faktorizacije svakog broja d, može se svako $d \mid n$ predočiti na taj način u jednom jedinom obliku.

Time je teorem dokazan.

19.3. Möbiusova funkcija. — 19.3.0. Bez sumnje. najjednostavnija distributivna funkcija je konstanta 1. Pokušajmo naći koji član grupe sumatorâ $S^D 1$.

Sistem (S) gornjih jednadžbi u § 19.2.3. pokazuje da je na desnoj strani (za konstantu $n \to 1$):

$$S\,1\,(n) = \sum_{n|d} 1 = (\text{broj divizora od } n) = d_0(n).$$

Potražimo sada antisumator funkcije $n \to 1$. To znači da su sada u sistemu (S) lijeve strane $= 1$; zato očitavamo po redu da antisumator konstante 1 prima vrijednosti: 1, 0, 0, 0, ...

Time su nađeni članovi $S^{-1}1$, $S^0 1$, $S^1 1$. Što bi bilo: drugi antisumator i drugi sumator? Za drugi antisumator imamo jednadžbe:

$$1 = f(1)$$

$$0 = f(1) + f(2)$$

$$0 = f(1) + f(3) = \sum_{d \mid 3}$$

. . . . . .

Dobije se po redu $1, -1, -1, 0, -1, \ldots$

Ta se funkcija zove *Möbiusova funkcija i označuje sa* μ: $N \to N$. Ipak dajemo uobičajenu definiciju te funkcije.

19.3.1. Definicija Möbiusove[1] **funkcije** μ; područje joj je skup prirodnih brojeva; vrijednosti su: $\mu(n) = 0$, ako je n djeljivo kojim kvadratom prosta broja; za svaki drugi slučaj $\mu(n) = (-1)^{kP(n)}$; pri tom $kP(n)$ označuje glavni (kardinalni) broj množine $P(n)$ svih prostih djelitelja broja n; specijalno, $kP(1) = 0$, dakle $\mu(1) = 1$.

$$\mu(2) = \mu(3) = \mu(p) = -1 \quad \text{za svaki prost broj } p$$

$$\mu(6) = (-1)^{P(6)} = (-1)^{k\{2,\,3\}} = (-1)^2 = 1$$

$$\mu(100) = 0 \quad \text{jer je} \quad 2^2 \mid 100.$$

19.3.2. *Distributivnost funkcije* μ se odmah dokazuje na osnovu obrasca:

$$P(a) \cap P(b) = \text{prazno},$$

za relativno proste brojeve a, b. Naime, neka su a, b relativno prosti; dokažimo da je

$$\mu(ab) = \mu(a)\,\mu(b). \tag{1}$$

Ako je jedan od brojeva a, b djeljiv sa p^2, onda je to i umnožak pa je relacija (1) svakako ispunjena: obje strane su 0. Ostaje slučaj kad ni a ni b nije djeljivo sa p^2; kako su $P(a)$, $P(b)$ disjunktni, to nije ni ab djeljivo sa p^2, pa je po definiciji:

$$\mu(ab) = (-1)^{kP(ab)} = (-1)^{kP(a)+kP(b)}$$

(jer su skupovi $P(a)$, $P(b)$ bez zajedničkog člana); zato je to dalje:

$$= (-1)^{kP(a)}\,(-1)^{kP(b)} = \mu(a)\,\mu(b). \quad Q.\,E.\,D.$$

Isporedi također poglavlje 18. § 5.3.

19.3.3. Teorem. *Ako je* f *distributivno, tada je*

$$\sum_{d \mid n} \mu(d) f(d) = \prod_{p \mid n} [1 - f(p)];$$

pri tom za $n = 1$ *desnu stranu shvatimo kao da je* 1.

---

[1] A. F. Möbius (č. Mebius; 1790—1868), njemački matematičar.

Naime, kako je μ distributivna funkcija, to je i produkt $\mu f = g$ distributivnih funkcija μ, f distributivna funkcija; zato se na g može primijeniti prethodni obrazac 19.2.5, imajući pri tom na umu da je

$$g(p) = \mu(p) f(p) = -f(p), \; g(p^a) = 0 \text{ za } a > 1.$$

Specijalno, stavimo li u gornji obrazac $f(n) = 1$, dobijemo ovaj rezultat kao rješenje nedovršene zadaće iz uvoda:

19.3.4. T e o r e m. $\sum_{d|n} \mu(d) = 1$ za $n = 1$, inače $= 0$, tj. *sumator Möbiusove funkcije je konstanta* 0 *izvan* 1 (*u* 1 *je jednak* 1).

19.3.5. T e o r e m.

$$\sum_{d|n} \frac{\mu(d)}{d} = \prod_{p|n} (1 - p^{-1}), \quad n > 1.$$

To je specijalan slučaj iz tačke 3. za $f(n) = n^{-1}$.

Tu na desnoj strani vidimo kako se pojavljuju karakteristični faktori $1 - p^{-1}$, koje smo vidjeli kod funkcije φ (isp. teorem 19.1.4).

⟶ 19.3.6. Teorem (efektivno izračunavanje funkcije iz svojeg antisumatora). Möbiusova inverzna formula. *Neka je f funkcija definirana u skupu N prirodnih brojeva i neka je*

$$F(n) = \sum_{d|n} f(d) \quad \text{za svako } n \in N;$$

tada je

$$f(n) = \sum_{d|n} \mu(d) \, F\left(\frac{n}{d}\right). \tag{1}$$

D o k a z. Prema definiciji, za svako $d \mid n$ vrijedi:

$$F\left(\frac{n}{d}\right) = \sum_{x \mid \frac{n}{d}} f(x), \; \mu(d) F\left(\frac{n}{d}\right) = \mu(d) \sum_{x \mid \frac{n}{d}} f(x) = \sum_{x \mid \frac{n}{d}} \mu(d) f(x),$$

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \sum_{x \mid \frac{n}{d}} \mu(d) f(x).$$

Tu imamo $x \left| \frac{n}{d} \right.$, dakle i $xd \mid n$, dakle $d \left| \frac{n}{x} \right.$; zato se sumacione varijable d i x mogu permutirati; izlazi:

$$\sum_{n|d} \mu(d) \, F\left(\frac{n}{d}\right) = \sum_{x|n} \sum_{d \mid \frac{n}{x}} \mu(d) f(x) = \sum_{x|n} f(x) \sum_{d \mid \frac{n}{x}} \mu(d), \text{ tj.}$$

$$\sum_{d|n} \mu(d) \, F\left(\frac{n}{d}\right) = \sum_{x|n} f(x) \sum_{d \mid \frac{n}{x}} \mu(d). \tag{2}$$

No, prema 19.3.4, imamo:

$$\sum_{d \mid \frac{n}{x}} \mu(d) = \begin{cases} 1 & \text{za } \frac{n}{x} = 1 \\ 0 & \frac{n}{x} > 1 \end{cases}, \text{ tj. za } \begin{matrix} n = x \\ n > x. \end{matrix}$$

To znači da za svako $n>x$ suma u (1) je $=0$; ostaje samo slučaj $n=x$, kad je ta suma $=1$; no tada je $x=n$ pa prva suma postaje $f(n)\cdot 1 = f(n)$.

Time je upravo izvedena tražena formula Q. E. D.

19.3.7. Primijenimo Möbiusovu inverzionu formulu na Eulerovu funkciju φ; prema Gaussu, njen je sumator identitet:

$\sum_{d \mid n} \varphi(d) = n$; to znači da je odatle prema prethodnom teoremu:

$$\varphi(n) = \sum_{d \mid n} \mu(d) \frac{n}{d}, \quad \varphi(n) = n \sum_{d \mid n} \frac{\mu(d)}{d};$$

odatle prema 19.3,5,:

$$\varphi(n) = n \prod (1 - p^{-1}). \tag{3}$$

A to je osnovna formula za φ iz teorema 19.1.4.

19.3.8. Eulerov dokaz da ima beskonačno mnogo prostih brojeva. Upravo vidjesmo kako se pojavljuje izraz $1-p^{-1}$; Euler se s takvim izrazima sreo kad je dokazao prethodnu formulu (3) za φ. Zato nije nikakvo iznenađenje da je upravo on dao i *prvi analitički* dokaz, baziran na pojmovima o *granici*, jednoga čistog problema iz teorije prirodnih brojeva; naime, da prostih brojeva ima beskonačno mnogo.

Stvarno, kako je $p>1$, može se pisati:

$$(1-p^{-1})^{-1} = 1 + p^{-1} + p^{-2} + \cdots = \sum_{n=0}^{\infty} p^{-n}.$$

Za 2 nejednaka prosta broja p, q bilo bi slično:

$$(1-p^{-1})^{-1}(1-q^{-1})^{-1} = \sum_{n_1=0}^{\infty} p^{-n_1} \sum_{n_2=0}^{\infty} q^{-n_2} = \sum_{n_1, n_2=0}^{\infty} (p^{n_1} q^{n_2})^{-1}. \tag{4}$$

Na taj način u (4) izađu svi brojevi $\frac{1}{n}$ za koje je $P(n) = \{p, q\}$.

Analogno zaključujući, imamo:

$$\prod_{p \in P} (1-p^{-1})^{-1} = \prod_{p \in P} \left(\sum_{m_p=0}^{\infty} p^{-m_p} \right); \tag{5}$$

uzimajući iz svakog

$$\sum_{m_p=0}^{\infty} p^{-m_p}$$

po jedan član, i to gotovo uvijek član 1, dobije se $\sum n^{-1}$.

Naime, za svaki prirodni broj n potpuno je određeno $n_p \in \{0, 1, 2, \ldots\}$ tako da bude $\prod_{p \in P} p^{n_p} = n$; to znači, specijalno, da je (5) dalje jednako:

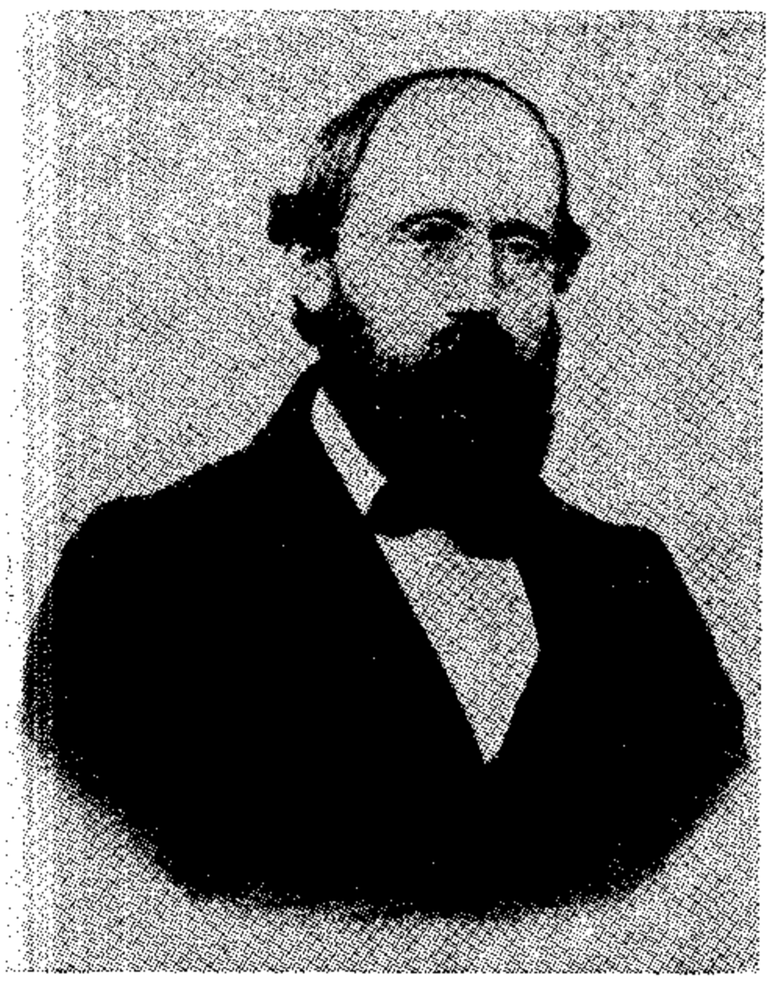
$$\sum_{n=1} n^{-1}.$$

A ovo je beskonačno — to je poznata suma harmonijskoga reda! Znači da u (5) mora biti beskonačno mnogo faktora $(1-p^{-1})^{-1}$, tj. P je beskonačno.

19.3.9. Na sličan se način vidi da vrijedi ovaj Eulerov identitet iz god. 1737:

$$\prod_{p \in P} (1-p^{-s})^{-1} = \sum_{n=0}^{\infty} n^{-s}$$

za svaki kompleksan broj s kojem je realan dio >1.



Bernhard Riemann (č. Riman; 1826—1866) veliki njemački matematičar

Ako ta dva jednaka izraza označimo sa $\zeta(s)$, dobije se tzv. *Riemannova zeta-funkcija.* Ona je usko povezana s funkcijom $\Pi(x)$, koja kazuje koliko ima prostih brojeva $\leq x$.

19.3.10. Glasovita je *Riemannova hipoteza* (Riemann, 1859) da u brojevnoj ravnini kompleksnih brojeva sva rješenja jednadžbe $\zeta(s)=0$ leže na pravulji $x=1/2$; drugim riječima, ako je za kompleksan broj $x+iy$ ispunjeno $\zeta(x+iy)=0$, $x>0$, tada je $x=1/2$.

Ta Riemannova hipoteza nije do danas niti dokazana niti oborena.

19.4. Zadaci o cjelobrojnim funkcijama.

1. Odredi φn za ove vrijednosti broja n: 1) 1, 2, ..., 100; 2) 20!; 3) 100!; 3) 2^m; 5) $2^m 3^n$.

2. Dokaži da je $\varphi n > \frac{n^{1/2}}{4}$, dakle je $\lim_{n\to\infty} \varphi n = \infty$.

3. 1) Pri $n>1$ broj φn je paran; 2) Može se pokazati da je skup $2N \setminus \varphi N$ beskonačan (Schinzel); 3) misli se (R. D. Carmichael) da protivna funkcija $^{-}\varphi n$ nije nigdje jednoznačna; to je provjereno za $n \leq 10^{400}$. 4) Nađi koje rješenje jednadžbe $\varphi n = \varphi(n+1)$; ne zna se da li tih rješenja ima beskonačno.

4. $\varphi n \mid n \Leftrightarrow n = 2^r \cdot 3^s$, pri čemu je $r \in N$, $s \in I\omega = \{0, 1, 2, \ldots\}$.

5. Neka je $d \mid n$; tada relacije $x \leq n$, $x \,\mathrm{M}\, n = d$ imaju upravo $\varphi\left(\frac{n}{d}\right)$ rješenja.

6. Funkcija $d_0 n$ kazuje koliko prirodni broj n ima djelilaca >0. 1) Odredi $d_0 n$ za $n \leq 100$; 2) $d_0 p^a = a+1$; 3) $d_0(p^a q^b) = (a+1)\cdot(b+1)$;

4) da li je funkcija $d_0 n$ distributivna? 5) Odredi bar nekoliko vrijednosti sumatora Sd_0 funkcije d_0; 6) odredi nekoliko vrijednosti antisumatora $S^{-1} d_0$ funkcije d_0.

7. 1) Broj $\sigma n \overset{def}{=} \sum_{d|n} d$ tj. σn označuje zbroj svih pozitivnih djelilaca broja n. 2) Odredi σn za prvih 100 brojeva. 3) Dokaži:

$$\sigma p^a = \frac{p^{a+1}-1}{p-1}, \quad \sigma(p^a q^b \cdot \ldots) = \frac{p^{a+1}-1}{p-1} \cdot \frac{q^{b+1}-1}{q-1} \cdot \ldots$$

4) Ne zna se da li jednadžba $\sigma n = \sigma(n+1)$ ima beskonačno rješenja.

5) $\lim_{n\to\infty} \frac{\sigma(a_n)}{a_n} = 1, \quad a_n = p_1 p_2 \cdot \ldots \cdot p_n + 1; \quad P = \{p_1 = 2, \ p_2 = 3, \ p_3 = 5, \ldots\}$

6) $\sigma(F_n) / F_n \to 1$, kad $n \to \infty$, $F_n = 2^{2^n} + 1$;

7) $p \in P$, $N_p = 2^{p+1}$, $\sigma(N_p) / N_p \to 3/4$ kad $p \to \infty$;

8) $p \in P$, $M_p = 2^p - 1$; $\sigma(M_p) / M_p \to 1$ kad $p \to \infty$,

8. 1) Za prirodni broj r neka $d_r n$ kazuje koliko ima r-članih nizova prirodnih brojeva kojima je produkt $= n$; odredi d_3 (30). 2) Dokaži da je $d_2 n = d_0 n$; 3) funkcija $d_r n$ je multiplikativna funkcija i jednaka je sumatoru funkcije $d_{r-1} n$. 4) Ako su $q_1, q_2, \ldots, q_m$ prosti različni brojevi, tad je $d_r(q_1 q_2 \cdot \ldots \cdot q_m) = r^m$; 5) Za svaki realni broj $\varepsilon > 0$ imamo $\lim_{n\to\infty} \frac{d_r(n)}{n^\varepsilon} = 0$; 6) $\sum_{0<a\leqslant n} d_r(a)$ pokazuje broj rješenja relacije $x_1 x_2 \cdot \ldots \cdot x_r \leq n$ s prirodnim brojevima $x_1, \ldots, x_r$.

9. Dokaži da je $(\zeta(s))^r = \sum_{n=1}^{\infty} \frac{d_r(n)}{n^s}$ za svaki prirodni broj r.

10. Funkcija $\wedge n$ je lnp za $n = p^r$ sa $r \in N$; inače je $\wedge n = 0$. Nađi vrijednosti funkcije $\wedge$ u $N(\cdot, 1000)$. Ako je $Rs > 1$, onda je

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty} \frac{\wedge(n)}{n^s}.$$

11. Za $Rs > 1$ vrijedi $\prod_{p\in P}(1 - p^{-s}) = \sum_{n=1}^{\infty} n^{-s} \mu(n)$. Dokaži!

12. **Savršeni (perfektni) brojevi** su rješenja jednadžbe $\sigma n = 2n$ (isp. zad. 7). 1) Euklid ih je poznavao 4 i to: 6, 28, 496, 8128; dobiju se po obrascu: Ako je $2^n - 1 \in P$, onda je $2^{n-1} + (2^n - 1)$ savršen broj; 2) svaki savršen broj je tog oblika; 3) ne zna se da li ima ikoji neparan savršen broj (isp. pogl. 6. § 7.12); 4) ne zna se da li ima beskonačno mnogo parnih savršenih brojeva.

13. *Sprijateljeni brojevi*; to je svaki par brojeva m, n za koje $\sigma m = n$, $\sigma n = m$. 1) takvi su parovi: (220, 230), $(2^5 \cdot 37, \ 2 \cdot 5 \cdot 11^2)$; 2) ne zna se da li ima beskonačno mnogo sprijateljenih brojeva; 3) ne zna se može li paran broj biti sprijateljen s neparnim brojem.

14. *Waringov problem*[1]. *Broj Gn.* Iz godine 1770. potječe ova hipoteza od Waringa: *svaki redni broj* $n=0, 1, 2, 3, \ldots$ *može se prikazati kao zbroj od r potencija* x^k *pri čemu je* $x \in I\omega$; *pri tom r zavisi samo od k* a ne zavisi od n; neka je $G(k)$ najmanji broj r s gornjim svojstvom. To znači ovo: svaki prirodni broj suma je od $G(k)$ potencijâ x^k rednih brojeva, no postoji bar jedan prirodni broj koji nije suma od $G(k)-1$ potencije x^k, $x \in I\omega$. Tako npr. $G(2)=4$ (Lagrange) tj. svaki prirodni broj suma je od 4 kvadrata, ali postoji bar jedan prirodni broj koji nije suma od 3 kvadrata. Kao rezultat rada od skoro dva stoljeća dokazalo se ovo:

1) $G(2)=4$ (Lagrange); provjeri taj teorem za brojeve ≤ 100.
2) $G(k) \geq k$ za $k \geq n$;
3) $G(k) < \infty$ (Hilbert, 1909);
4) $G(3) \leq 8$ (Landau);
5) $G(4) \leq 17$ (Esterman, Davenport, Heilbronn, 1936)
6) $G(k) \leq 6k(lnk+1)$ za $k \geq 16$ (Vinogradov, 1937);
7) $G(k) < 3k\ lnk + 11k$.

15. Smithov teorem:

$$\begin{vmatrix} 1\,M\,1, & 1\,M\,2, \ldots, & 1\,M\,n \\ 2\,M\,1, & 2\,M\,2, \ldots, & 2\,M\,n \\ \cdots & \cdots & \cdots \\ n\,M\,1, & n\,M\,2, \ldots, & n\,M\,n \end{vmatrix} = \varphi(1)\varphi(2)\cdots\varphi(n);$$

lijeva strana je oznaka za determinantu (vidi poglavlje 11).

Literatura: Bachmann [1], [2], Borevič Šafarevič [1], Buhstab [1], Cahen [1], Dickson [1], [2], Gribanov [1], Hasse [1], [2], Kraitschik [1], Landau [1], Lejeune-Dirichlet [1], Plemelj [1], Prachar [1], Scholz [1], Sierpiński [1], Vinogradov [1].

[1]) E. Waring, (1734—1798), engleski matematičar.

POGLAVLJE 7.

KOLO ILI PRSTEN ALGEBARSKIH POLINOMA

1. OSNOVNE DEFINICIJE

1.1. Pojam polinoma. Pođimo od nekog komutativnog kola ili prstena A[1] s jedinicom 1; A može biti, npr., kolo D cijelih brojeva, razlomljenih brojeva ili koje cifarsko kolo In sastavljeno od cifara $0, 1, \ldots, n-1$.

Neka je x kakva veličina; tada imamo geometrijski niz

(1) $$(1=)\, x^0,\ x=x^1,\ x^2, \ldots,\ x^n \text{ od } 1+n \text{ članova.}$$

Neka je isto tako

(2) $$a_0,\ a_1, \ldots,\ a_n$$

kakav niz od $1+n$ članova iz kola K; tada imamo često posla sa skalarnim produktom nizova (1) i (2), tj s izrazom:

(3) $$a_0 x^0 + a_1 x + a_2 x^2 + \ldots + a_n x^n.$$

Takvi se izrazi zovu *cijele racionalne funkcije* ili *algebarski polinomi* ili naprosto *polinomi u x nad kolom ili prstenom A* (jer su koeficijenti iz A).

1.2. Stepen ili stupanj. Ako je $a_n \neq 0$, kaže se da je stepen ili stupanj polinoma (3) jednak n i pišemo $\operatorname{st} a = n$.

1.3. Polinomi stupnja 0. Polinom 0. Članovi iz A kao polinomi nad A. Slučaj nule. Specijalno svaki element a kola A smatramo polinomom nad A, i to stupnja 0 ako je $a \neq 0$; *stupanj ili stepen elementa* 0 *kao polinoma nije definiran*, no ako u formuli negdje izađe uslov $\operatorname{st} a < 0$, onda treba znati da se time misli da je a nula! To nam je potrebno, npr., zbog formulacije osnovnog teorema o dijeljenju.

Tako. npr. $2-5x$, 3, $5-\frac{2}{3}x^2$ jesu polinomi stepena 1, 0, 2 u kolu racionalnih brojeva (prva dva u kolu cijelih brojeva). Specijalno važan polinom je identiteta: x ili $1 \cdot x$.

1.4. *Na polinom* (3) *gledamo kao na skalarni produkt niza koeficijenata* (2) *i geomotrijskog niza veličine x.* Sâmo to x može biti dvostrukog karaktera: *ili*

---

[1] A je početno slovo latinske riječi *anulus* (prsten).

da x putuje nekom oblašću ili da se uopće ne mijenja. Zato, gledajući na izraz (3), treba imati na umu da tu imamo $1+n$ veličina $a_0, a_1, \ldots, a_n$ te isto toliko veličina $x^0 (= 1), x^1, \ldots, x^n$ koje su vezane uz x. U (3) se mogu mijenjati svi koeficijenti, njih $1+n$ na broju, a x biti čvrsto; a može se mijenjati samo x, a koeficijenti da su čvrsti. Tako npr. ako u $b+c\sqrt{2}$ mijenjamo samo b, c, dobijemo skup izraza koje smo označavali sa $A+A\sqrt{2}$, ako se b, c kreću po A. Međutim, može se također promatrati $b+cx$ kad se x kreće, npr., skupom svih realnih brojeva.

1.5. Jednakost dvaju polinoma. — 1.5.1. Formalna jednakost ili identičnost dvaju polinoma.

Definicija. Polinom $a \ldots a_0 + a_1 x^1 + \ldots + a_n x^n$ jednak je *formalno ili identički* s polinomom $b \ldots b_0 + b_1 x + \ldots b_r x^r$ ako je $st\, a = st\, b$ te ako je $a_k = b_k$ *za svako* $k \leqslant st\, a$. *Pišemo* $a = b$.

1.5.2. Definicija. Polinom a je *funkcionalno jednak* s polinomom b ako oni imaju istu oblast te se u svakoj tački oblasti podudaraju.

1.6. ***Skup A*** **[*x*].** Skup svih polinomskih izraza u x s koeficijentima iz A označit ćemo sa $A[x]$ (čitaj A uglasto x); *pri tom za izjednačivanje vrijedi podudaranje u stepenu i odgovarajućim koeficijentima* (formalna jednakost!)

Oznaka $A[x]$ ima da nas podsjeti na tri stvari: na *neodređenu varijablu ili veličinu* x, *na skup* A *za koeficijente* i na oznaku [ ] za „cijele" (tj. za polinome). Treba *razlikovati* $A[x]$ *od* $A(x)$ (vidi niže, t. 1.8.).

1.7. Formalno računanje sa polinomima vrši se na uobičajeni način, specijalno:

1.7.1. Definicija. Dva se polinoma *zbrajaju, sabiru* tako da se zbroje odgovarajući koeficijenti. Tako se npr. $(1-3x)+(4+4x^2)$ zbraja ovako: $(1+4)-3x+4x^2$ (ako u jednom polinomu nema odgovarajućeg koeficijenta, podrazumijeva se da on postoji i da mu je vrijednost 0).

1.7.2. Definicija. *Množenje* se vrši ovako: Produkt $a \cdot b$ polinomâ a, b jest polinom ab za koji je

$$(a\,b)(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + \ldots$$

$$+ (a_0 b_k + a_1 b_{k-1} + \ldots + a_k b_0) x^k \ldots + a_n b_r \cdot x^n x^r;\ n = \mathrm{st}\, a,\ r = \mathrm{st}\, b.$$

Vidimo da je

$$(a\,b)_k = \sum_{i+j=k} a_i b_j;$$

pri tom su $i \leqq n$, $j \leqq r$ proizvoljni redni brojevi kojima je zbroj (zbir) $= k$.

Drugim riječima:

$$(a\,b)(x) = \sum a_i b_j x^k, \text{ uz uslov } i+j=k,\ i \leqq st\, a,\ j \leqq st\, b.$$

1.7.3. Specijalno treba naglasiti da se svaki elemenat a iz *polaznog* prstena A množi svakim elementom b iz *novog* prstena $A[x]$, tj. polinomom b tako da se a množi *svakim članom od* b, a dobiveni produkti se zbrajaju i daju produkt $a\,b$.

Upotreba *donjih indeksa* kod koeficijenata i *gornjih indeksa* kod veličine x pokazuje kako se množenje vrši pravilno.

1.8. Razlomljene ili racionalne funkcije iznad A s obzirom na x. *Skup* $A(x)$. To su kvocijenti dvaju polinoma iznad A s obzirom na x. Njihov skup označujemo sa $A(x)$ (isp. t. 1.6).

1.8.0. D e f i n i c i j a. Opći oblik razlomljene racionalne funkcije iznad A u odnosu na x (ili racionalnog izraza iznad A) glasi:

$$\frac{a_0 x^0 + a_1 x + a_2 x^2 + \ldots + a_m x^m}{b_0 x^0 + b_1 x + b_2 x^2 + \ldots + a_n x^n};$$

pri tom su svi a_i i svi b_k iz A; *isključuje se slučaj da je nazivnik b konstanta* 0.

1.8.1. Definicija jednakosti u $A(x)$:

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow a\,d \equiv b\,c.$$

1.8.2. Zbrajanje i množenje vrše se po ovim odredbama:

$$\frac{a}{b} + \frac{c}{d} \equiv \frac{a\,d + b\,c}{b\,d}$$

$$\frac{a}{b} \cdot \frac{c}{d} \equiv \frac{a\,c}{b\,d}$$

Eto, to su definicije.

1.9. P r i m j e d b a. Razlikuj $A[x]$ od $A(x)$; $A[x]$ je skup polinomâ nad A s obzirom na x, a $A(x)$ je skup razlomljenih funkcija nad A u odnosu na veličinu x. *Naravno*, $A[x] \subset A(x)$.

1.10. Zadaci o polinomima

1. Promatraj izraz $1 + 2x + 2^{1/2} x^2$; da li je to polinom nad kolom A ako A znači: 1) kolo R realnih brojeva; 2) kolo Q racionalnih brojeva; 3) kolo $I5$ cijelih brojeva modulo 5; 4) Kolo $I7$; 5) kolo $I17$?

2. Promatraj dvočlan $x + x^2$ u prstenu: 1) R; 2) Q; 3) $I2$; 4) $I5$. Da li se on reducira na konstantu u bar jednom slučaju?

3. Koliko ima funkcionalno-različitih algebarskih trinoma nad prstenom: 1) $I2$; 2) $I3$; 3) $I5$; 4) $I6$; 7) D?

4. Promatraj skup S_1 linearnih i skup S_2 kvadratnih polinoma nad prstenom $I2$; ima li koji član u S_1 koji je funkcionalno jednak s kojim članom u S_2? Nađi $S_1 \cap S_2$.

5. Da li su polinomi $x^3 + x$, $x^4 + x$ funkcionalno jednaki u 1) $I2$; 2) $I3$; 3) $I4$?

6. Poređaj po uzlaznim potencijama i reduciraj polinom $x(x+1)(x+2)$, ako se radi o aritmetici 1) modulo 2; 2) mod. 3; 3) mod. 10.

7. Nađi $(x+1)(x+2)(x+3)(x+4)$ i to za 1) kolo cijelih brojeva; 2) kolo $I2$; 3) kolo $I5$.

8. 1) Nađi sve moguće produkte $(a+x)\cdot(b+x)$ kao i sve moguće kvadratne trinome $a_0+a_1x+a_2x^2$ nad prstenom $I2$. 2) Koliko ima ovih koji nisu među prethodnima?

9. (*Izvod ili derivat* $Da(x)$ *polinoma* $a(x)$ definira se ovako:
$Da=D(a_0+a_1x+a_2x^2+\ldots+a_nx^n)=a_1+2a_2x+3a_3x^2+\ldots$
$+na_nx^{n-1}$. Dokaži ove obrasce: 1) $D(a+b)\equiv Da+Db$;
2) $D\lambda a\equiv\lambda Da$ za svaki parametar λ; 3) $D(ab)\equiv Da\cdot b+a\cdot Db$;
4) $D(a^n)\equiv na^{n-1}Da$.

10. Odredi $D^{(n)}a(x)$ za $n=0,\ 1,\ 2,\ldots$ i za svaki polinom $a(x)$; stavljamo $DD^{(n-1)}=D^{(n)}$.

11. Dokaži $D^{(n)}\operatorname{tg}x=(D^{(1)}+D^{(0)})^{n-1}\operatorname{tg}x$ za $n=2,\ 3,\ 4,\ldots$

$=(\text{def})\,(D^{(n-1)}D^{(0)}+(n-1)\,D^{(n-1)}D^{1}+\binom{n-1}{2}D^{(n-2)}D^{(2)}+\ldots)\operatorname{tg}x.$

12. Dokaži da je $(x+\sqrt{x^2-1})^n+(x-\sqrt{x^2-1})^n$ polinom n-og stupnja za svaki prirodni broj; odredi najugledniji koeficijent.

13. 1) Napiši produkt izrazâ a^2-b^2, x^2-y^2 kao razliku dvaju kvadrata.
2) Provjeri $(a^3+b^3+c^3-3abc)(x^3+y^3+z^3-3xy)=(ax+by+cz)^3+$
$+(ay+bz+cx)^3+(az+bx+cy)^3-3(ax+by+cz)(ay+bz+cz)\cdot$
$\cdot(az+by+cz)$.

2. OSNOVNI TEOREM

2.1. Teorem. *Ako je A kakvo kolo, a x kakva neodređena veličina, tada skup $A[x]$ svih polinoma u x s koeficijentima u A čini određeno kolo ili prsten u kojem je polazno kolo A sadržano zajedno sa svojom strukturom, tj. jednakost, suma, produkt itd. iz A prenosi se za elemente iz A i u $A[x]$.*

Tako npr. broj 3 i broj 5 daju kao sumu broj $3+5$, tj. 8; isto to vrijedi za 3 i 5 kao polinome stupnja 0.

2.2. Teorem se dokazuje proveravajući da se formalno u skupu $A[x]$ zaista mogu provoditi prve tri računske operacije i da pri tom važe uobičajena pravila. *Čitav je dokaz prilično dug. Ideja mu je vrlo jednostavna.*

2.3. Dokažimo npr. da za zbrajanje polinomâ vrijedi zakon udruživanja ili asocijacije:

$$(a+b)+c=a+(b+c). \tag{1}$$

Neka su m, n, p stepeni od a, b, c. Dakle:

$$a = a_0 + a_1 x + \ldots + a_m x^m, \quad a_m \neq 0$$
$$b = b_0 + b_1 x + \ldots + b_n x^n, \quad b_n \neq 0$$
$$c = c_0 + c_1 x + \ldots + c_p x^p, \quad c_p \neq 0.$$

Formalno se može pisati $a = \sum_{i=0}^{\infty} a_i x^i$, podrazumijevajući da je $x^0 = 1$, $a_{n+i} = 0$ za svako $i > 0$.

Tada polinom $(a+b)+c$ glasi:

$$\sum_{n=0}^{\infty} [\,(a_n + b_n) + c_n]\, x^n;$$ ovo je dalje formalno:

$$= \sum_{n=0}^{\infty} [a_n + (b_n + c_n)\,]\, x^n$$

(jer u polaznom prstenu A vrijedi $(a_n + b_n) + c_n = a_n + (b_n + c_n)$. No ovo je upravo $a + (b + c)$. Dakle, zaista vrijedi (1).

2.4. Analogno za asocijativni zakon množenja: za a, b, $c \in A[x]$ vrijedi:

$$(a\,b)\,c = a\,(b\,c). \tag{2}$$

Dokaz je idejno prost, ali je formalno prilično zamršen. Bez upotrebe indeksâ dokaz bi pogotovu bio zamršen!

Relacija (2) predstavlja formalnu jednakost polinoma $(2)_1$, na lijevoj strani i polinoma $(2)_2$, tj. $a\,(b\,c)$ na desnoj strani. To znači da su odgovarajući koeficijenti u $(2)_1$ jednaki odgovarajućim koeficijenima u $(2)_2$, i to svi! Dakle, treba pokazati da je

$$((2)_1)_k = ((2)_2)_k \text{ za } k = 0,\ 1,\ 2, \ldots \tag{3}$$

Pogledajmo (3) za $k = 0$; traži se dokaz od

$$((a\,b)\,c)_0 = (a\,(b\,c))_0. \tag{4}$$

No, po definiciji produkta polinomâ imamo:

$$(4)_1 = ((a\,b)\,c)_0 = (a\,b)_0\,c_0 = (\text{po def. od } a \cdot b) = (a_0\,b_0\,c_0) = (\text{po asoc. u ishodnom prstenu } A)$$

$$= a_0\,(b_0\,c_0) = (\text{def. množenja u } A[x]) = a_0\,(b\,c)_0 = (\text{isti razlog}) =$$

$$= (a\,(b\,c))_0 = (4)_2, \text{ tj. } (4)_1 = (4)_2; \text{ to znači da (4) vrijedi.}$$

Dakle (3) vrijedi za $k = 0$; pokušajmo stvar za $k = 1$, tj. treba dokazati:

$$((a\,b)\,c)_1 = (a\,(b\,c))_1. \tag{5}$$

Radi se kao (4):

$$(5)_1 = ((a\,b)\,c)_1 = (a\,b)_0\,c_1 + (a\,b)_1\,c_0 =$$
$$= (a_0\,b_0)\,c_1 + (a_0\,b_1 + a_1\,b_0)\,c_0 = (a_0\,b_0\,c_1 +$$

$$+(a_0 b_1 c_0 + a_1 b_0 c_0) = (a_0 b_0 c_1 + a_0 b_1 c_0) + a_1 b_0 c_0 =$$
$$= a_0 (b_0 c_1 + b_1 c_0) + a_1 (b_0 c_0) = a_0 (bc)_1 + a_1 (b c)_0 =$$
$$= (a (b c))_1 = (5)_2.$$

Dakle je $(5)_1 = (5)_2$, tj. (3) vrijedi i za $k = 1$.

Vidi se koliko treba više pisati da se provjeri (3) za $k = 1$ nego za $k = 0$; još bi više trebalo da se piše za $k = 2, 3, \ldots$

Dokažimo sada jednakost (3) za svako $k = 0, 1, \ldots$

Imamo po redu:

$$(6) \qquad ((a b) c)_k = \sum_{i+\gamma=k} (a b)_i c_\gamma = \sum_{i+\gamma=k} \sum_{\alpha,\beta} a_\alpha b_\beta c_\gamma;$$

$\alpha = 0, 1, \ldots,$ *st a*; $\beta = 0, 1, \ldots,$ *st b*; $\gamma = 0, 1, \ldots,$ *st c*; pri tom je $\alpha + \beta = i$, dakle $\alpha + \beta + \gamma = k$.

No to je dalje $= \sum a_\alpha b_\beta c_\gamma = \sum_\alpha a_\alpha \sum_{\beta,\gamma} (b_\beta c_\gamma) = \sum_{\alpha+l=k} a_\alpha (b c)_l = (a (b c))_k$.

Time je (3) dokazano.

2.5. Jedinični element u prstenu $A(x)$ je broj 1, odnosno jedinični element iz A shvaćen u $A[x]$ kao polinom stupnja 0.

Ipak nećemo izvoditi cio dokaz gornjeg teorema.

2.6. O stupnju produkta. Neka su a, b polinomi; neka je $\mathrm{st}\, a = m$, $\mathrm{st}\, b = n$; dakle:

$$a = \sum_{i=0}^{m} a_i x^i, \quad a_m \neq 0$$

$$b = \sum_{i=0}^{n} b_i x^i, \quad b_n \neq 0.$$

Tada po definiciji produkta $a b$, *svi* koeficijenti reda $r > m + n$ jesu 0, tj. $(a b)_r = 0$ za $r > m + n$. Znači da je

$$(1) \qquad st\,(a b) < st\, a + st\, b.$$

Koeficijent s indeksom $m + n$ jednak je

$$(2) \qquad (a b)_{m+n} = a_m b_n.$$

To znači da je taj koeficijent produkta $a b$ upravo produkt od najuglednijeg koeficijenta u a i najuglednijeg koeficijenta u b; ovi su koeficijenti $\neq 0$. Međutim, *u općem slučaju to još ne osigurava da im i produkt bude* $\neq 0$. Tako npr. da radimo s cifarskim prstenom $I4$ cifara 0, 1, 2, 3 i linearnim polinomima

$$1 + 2x, \quad 1 - 2x,$$

njihov je produkt

$$1 - 2 \cdot 2x^2. \text{ No, u } I4 \text{ vrijedi } 2 \cdot 2 = 0.$$

Prema tome, u prstenu $I4$ imamo:

$$(1+2x)(1-2x)=1.$$

Ali, ako je kolo A *»bez nula-divizora«*, tj. *ako je produkt dvaju članova koji su* $\neq 0$ *opet* $\neq 0$ *onda u prstenu* $A[x]$ *za množenje polinoma vrijedi*:

$$st\,a\,b = st\,a + st\,b.$$

Specijalno, za prstene D, Q, R, $R(i)$ cijelih, racionalnih, realnih, kompleksnih brojeva znamo da su bez nula-divizora; zato će stepen produkta dvaju polinoma biti suma stepena tih polinoma (izuzetak je sa 0 jer produkt polinoma 0 i svakog drugog polinoma je opet 0, pa je stepen produkta neodređen).

3. O TIJELU $A(x)$ RAZLOMLJENIH FUNKCIJA S OBZIROM NA NEODREĐENU VELIČINU x

3.1. Možemo poći, npr., od prstena D cijelih brojeva; on je snabdjeven jedinicom i ima svojstvo da je produkt dvaju topova opet top, tj. produkt dvaju elemenata koji su $\neq 0$ opet je $\neq 0$ (kraće se zato kaže: prsten D je *područje cijelih* ili *D je integritetno područje*). Ili još općenitije, pođimo od nekog prstena A s jedinicom 1 (dakle $1\,x = x\cdot 1 = x$ za svako $x \in A$).

3.2. Tada se odmah vidi da se u skupu razlomljenih funkcija s koeficijentima iz A mogu vršiti ne samo prve tri računske operacije nego i da se može dijeliti (izuzevši 0 kao djelitelj). A to upravo znači da je $A(x)$ jedno tijelo.

3.3. Specijalno za svako $a \in A(x)$ za koje je $a \neq 0$ postoji i recipročno a^{-1} sa svojstvom

$$a\,a^{-1} = 1$$

(1 je jedinica u A; zato i treba suponirati da i A ima jedinicu). Npr., u $D(x)$ imamo elemente — polinome

$$2,\ 1,\ 1-x,\ 0,\ \frac{x+3}{x^2+5x-1};$$

njihovi su reciproci po redu:

$$2^{-1}=\frac{1}{2},\ 1,\ \frac{1}{1-x},\ \text{bez},\ \frac{x^2+5x-1}{x+3}.$$

3.4. Izgradnja tijela Q racionalnih brojeva kao tijela D (1). Kvocijentno tijelo. Posebno, vidimo ovo: u oblasti D cijelih ne može se dijeliti bez ograničenja (npr., $1:2$ ne postoji); u skupu $D(x)$ može se dijeliti bez ograničenja (jedino 0 kao divizor ne dolazi u obzir); **pri tom x može biti bilo što osim 0.** Specijalno, može biti $x=1$ pa dobijemo skup $D(1)$ *»razlomljenih racionalnih funkcija u odnosu na* 1 *s koeficijentima iz D«*. A što to znači? To znači da je

stvarno riječ o racionalnim funkcijama $\frac{a}{b}$ sa $a, b \in D$, $b \neq 0$; naime, svaki je polinom s obzirom na „veličinu 1“ s koeficijentima iz D oblika:

$$a = a_0 + a_1 1 + a_2 1^2 + a^3 1^3 + \ldots + a_n 1^n; \text{ no ovo je} =$$

$$a_0 + a_1 + a_2 + a_3 + \ldots + a_n. \text{ Ovo je član iz } D.$$

Dakle se svaki element iz $D(1)$ prikazuje formalno kao »*kvocijent*« uređene dvojke članova iz D (0 isključena kao djelitelj). Time se, dakle, iz *prstena D* dolazi do *tijela* $D(1)$ i to tijelo je upravo *tijelo racionalnih brojeva* (označujemo ga sa Q da se podsjetimo da su ovi elementi formalno dobiveni kao *kvocijenti* cijelih brojeva).

Tako smo izveli *definiciju* racionalnih brojeva, odnosno skup Q svih racionalnih brojeva.

3.5. Na vlas isto teče dokaz za svaku oblast O cijelih; $O(1)$ je tijelo. Pri tom, naravno, članovi u O ne moraju biti brojevi.

Ako istu stvar napravimo polazeći od Q, koje je ne samo kolo nego i tijelo, tada je $Q(1) = Q$; naprotiv »*priklapajući*« (*adjungirajući*) npr. $\sqrt{2}$ ka Q, dobije se $Q(\sqrt{2})$ kao *opsežnije tijelo od polaznog tijela Q*.

U tome novom tijelu $Q(\sqrt{2})$, naravno, možemo računati; napolje nećemo izaći pomoću prve četiri operacije, pa ni antikvadriranjem pojedinih **pozitivnih** brojeva; međutim, već jednadžba $x^2 = 3$ ili $x^2 + 1 = 0$ nema unutra rješenja. Ako »*adjungiramo*« i rješenje x posljednje jednadžbe (ono se obično označuje sa i) tada dobijemo tijelo:

$$Q(\sqrt{2})\ (i).$$

Niti u tome tijelu svaka kvadratna jednadžba s koeficijentima iz tog tijela nema rješenje!

3.6. Upravo se tako prelazi od tijela R realnih brojeva na tijelo $R(i)$ kompleksnih brojeva: *društvo ili korporaciju* (*tijelo*) R *proširimo novim članom* — onim što ga *formalno* zovemo *rješenjem* jednadžbe $x^2 + 1 = 0$ (s koeficijentima u matici R) i tako dođemo do množine $R(i)$ svih »*razlomljenih funkcija u i*« s koeficijentima iz R.

U ovom slučaju, naknadno se vidi da primajući u društvo R *jedno* rješenje iz $x^2 + 1 = 0$— označuje se sa i — *automatski se u* $R(i)$ pojavljuje i *drugo* rješenje, odnosno *svako* rješenje jednadžbe $x^2 + 1 = 0$ (naime, u općem slučaju stvar nije ovakva).

3.7. Opći postupak proširivanja. Nalazimo se u nekom društvu — tijelu k; nailazimo na „domaću“ jednadžbu:

$$(*) \qquad a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = 0$$

$$(\text{npr.}, \ x^{100} + 1 = 0),$$

tj. **s koeficijentima iz društva** k; ali se ustanovljuje da u društvu k nitko nije upravo onakav x za koji vrijedi veza (*). Zatim se odluči društvo k pro-

širiti nepoznatim, ali jednim jedinim „rođakom“ [1] x_0 iz (*) — nazovimo ga x_0 — primajući ga u ravnopravnu službu (s tim **određenim** x_0 vrše se, kao da je bio u k: zbrajanja, množenja, dijeljenja po uobičajenim pravilima). Tako se dolazi do *proširene korporacije* $k(x_0)$. I napokon se ipak ustanovi da se u $k(x_0)$ osim x_0 nalaze, u jednostavnijim slučajevima, i *svi drugi pripadnici zajednice* koja se sastoji od *svih* rješenja jednadžbe (*). Tako npr. $x^{100}+1=0$ nema u R ni jednog rješenja; a ako se dovede u R jedno jedino takvo podesno x i formira $R(x)$, tada se ustanovi da je svih 100 različitih x-ova koji zadovoljavaju $x^{100}+1=0$ u korporaciji $R(x)$.

U *zamršenijim* slučajevima stvari mogu biti i drukčije. Adjungiranjem jednog rješenja x_0 iz (*) ne moraju u $k(x_0)$ da se automatski nađu i *svi* x-ovi iz (*).

3.8. Zadaci o kolu polinoma.

1. Neka je $a=1+x$, $b=-2+x^2$, $c=1+x^3$. Provjeri direktno da je $(a\,b)\,c=a\,(b\,c)$ i to i u formalnom i u funkcionalnom pogledu. Promatraj specijalno slučaj prstena D, R, $I2$, $I3$.

2. Promatraj 1) $D[i]$, $D(i)$; 2) prikaži te skupove u brojevnoj ravnini.

3. Isto pitanje za $Q[\sqrt{2}]$, $Q(\sqrt{2})$.

4. Što je 1) $Q(\sqrt{2})$, 2) $Q(\sqrt{2})(\sqrt{3})$, 3) $Q(\sqrt{2}+\sqrt{3})$?

5. Kojoj normalnoj jednadžbi s cijelim koeficijentima i s najnižim stupnjem zadovoljava broj: 1) $\sqrt{2}$, 2) $\sqrt{3}$, 3) $\sqrt{2}+\sqrt{3}$, 4) $2^{3/4}$, 5) $4^{1/3}+2\cdot 2^{1/3}+3$?

6. Ako α znači broj iz zad. 5, promatraj $Q(\alpha)$ i $Q(\alpha')$, gdje α' označuje kojigod korijen jednadžbe koja je prema istom zadatku pridružena broju α. Da li je $Q(\alpha)=Q(\alpha')$?

7. Skupu Q racionalnih brojeva adjungiraj jedno rješenje α jednadžbe: 1) $x^2+2=0$, 2) $x^3=2$, 3) $x^2+x+1=0$; kako izgleda $Q(\alpha)$? Imenuj bar jedan broj koji ne leži u $Q(\alpha)$.

8. Neka je $a(x)\in D[x]$; dokaži ovo: $6\mid a(2)\wedge 6\mid a(3)\Rightarrow 6\mid a(5)$.

9. Ako su p, q dva različna prosta broja, tada ni za koje prirodne brojeve m, $n>1$ ne vrijedi $q^{1/n}\in Q(p^{1/m})$.

4. OSNOVNI TEOREM O DIOBI POLINOMA

4.0. Osnovni teorem o diobi brojeva poznajemo. Nešto analogno imamo i za polinome.

Razmatrajmo, npr., polinome s racionalnim koeficijentima; skup tih polinoma s obzirom na x kao „nepoznanicu“ ili neodređenicu označujemo sa $Q[x]$, da se istakne i nepoznanica x i skup Q racionalnih brojeva odakle su svi koeficijenti.

---

[1] Ta koeficijenti u (*) su iz k!

Ako za $a, b \in R[x]$ vrijedi da je $a\,b = c$, kaže se, kao i kod brojeva, da je c *dijeljivo sa* a [*sa* b] i da je *kvocijent* b (odnosno a).

Dolaze i drugi načini izražavanja: a dijeli c, itd. To označujemo kao i prije kod brojeva:

$$a \mid c, \text{ odnosno } b \mid c, \text{ odnosno } c \equiv 0 \pmod{a}, \text{ itd.}$$

Mnogo toga što je o kolu D cijelih rečeno ranije prenosi se na skup $Q[x]$ i sl.

⟶ **4.1. Osnovni teorem.** *Ako je k kakvo tijelo (korporacija) brojeva tada je time za svaku nepoznatu x određeno i tijelo $k(x)$ svih razlomaka kojima su brojnici i nazivnici polinomi u x s koeficijentima iz k; za svaki uređen par a, m članova iz $k[x]$, za koje je $m \neq 0$, postoji jedan jedini član $q \in k[x]$ i jedan jedini član $r \in k[x]$ sa svojstvom:*

$$a = m\,q + r, \text{ tj. } a(x) = m(x)\;q(x) + r(x),^{1)} \tag{1}$$

st $r <$ *st* m. Pišemo $E(a, m) = (q, r)$, $E_1(a, m) = q$, $E_2(a, m) = r$.

Određivanje kvocijenta q i ostatka r vrši se npr., ovako:

$$\begin{array}{r} x^5 : (x^2 - 1) = x^3 + x \\ \underline{-x^5 \mp x^3} \\ +x^3 \\ \pm x^3 - x \\ \hline + \\ \hline x \end{array}$$

tj. $x^5 = (x^2 - 1)(x^3 + x) + x$.

4.1.1. P r v i d o k a z. Najprije,

$$\text{ako je } \operatorname{st} a < \operatorname{st} m, \text{ onda je } q = 0,\ r = a. \tag{2}$$

Neka je zato $\operatorname{st} a \geq \operatorname{st} m$.

P r v i k o r a k: Najugledniji član $a_{st\,a}\, x^{st\,a}$ od a podijeli se najugledniji članom polinoma m; time se dobije potpuno određen član kvocijenta q; taj dobiveni član kvocijenta pomnoži se divizorom m i oduzme od dividenda a; dobivena se razlika zove *prvi ostatak* od a, simbolički $(a)_1$; svakako je $\operatorname{st} a > \operatorname{st} (a)_1$.

D r u g i k o r a k: Prethodni ostatak preuzima ulogu prethodnog dividenda.

T r e ć i k o r a k: Prethodni ostatak preuzima ulogu prethodnog dividenda, itd. do kraja.

Proces se mora završiti, i to onda kad se naiđe na jedan ostatak stupnja $< \operatorname{st} m$. Naime, stupanj od a veći je od stupnja njegova ostatka, a stupanj ovoga veći je od stupnja opet njegova ostatka, itd., tj. $\operatorname{st} a > \operatorname{st} (a)_1 > \operatorname{st} ((a)_1))_1 > \ldots$ i mora se doći na broj $< \operatorname{st} m$.

Time je dokazana i egzistencija članova q i r. Dolazi na red de se vidi da su q i r određeni *jednoznačno*. Dokaz je isti kao u poglavlju 6, § 9.3. za

---

[1]) Prema učinjenom dogovoru iz § 1.3: ako je $\operatorname{st} r < 0$, onda je $r = 0$.

kolo D; treba samo sada znak modula $|y|$, koji se tamo pojavljivao, čitati $\mathrm{st}\, y$; tamošnja relacija (3) sad bi glasila $\mathrm{st}\, m + \mathrm{st}\,(q-Q) = \mathrm{st}\,(r-R)$, itd.

4.1.2. Drugi dokaz (pomoću potpune indukcije). Indukciju sprovodimo s obzirom na $\mathrm{st}\, a$; prema (2) možemo pretpostaviti da je $\mathrm{st}\, a \geq \mathrm{st}\, m$; također je jasno da možemo pretpostaviti da je $\mathrm{st}\, m > 0$. Neka je n bilo koji broj $\geq \mathrm{st}\, m$ i sa svojstvom da je teorem istinit uz uslov $\mathrm{st}\, a \leq n$; dokažimo da je teorem istinit i pri $\mathrm{st}\, a = n+1$. Naime, podijelimo li $a_{n+1} x^{n+1}$ sa najuglednijim članom $a_\mu x^\mu$ polinoma m izlazi određeni kvocijent b i određen ostatak $q = a - a_\mu x^\mu b$, pri čemu je $q = 0$ ili $\mathrm{st}\, q < \mathrm{st}\, a$ pa ispravnost tvrdnje proizilazi iz identiteta

$$\frac{a(x)}{m} = b + \frac{q}{m} \quad \text{jer je } \mathrm{st}\, q \leq n.$$

4.2. Korolar. *Za svako* $a \in k[x]$ *i svaki normirani linearni dvočlan* $x - c \in k[x]$ *(dakle je* $c \in k$*) vrijedi:*

$$a = (x-c)\, q + a(c), \text{ tj. } r = a(c). \tag{3}$$

Naime, osnovna jednadžba (1) za $m = x - c$ postaje:

$$a(x) = (x-c)\, q(x) + r(x).$$

Stavi li se tu $x = c$, izlazi (3).

⟶ **4.3.** Korolar (Descartesov teorem). *Ako je* $a(c) = 0$, *tada je* $a(x)$ *djeljivo sa* $x - c$; *i obrnuto: ako je* $a(x)$ *djeljivo sa* $x - c$, *tada je* $a(c) = 0$. (v. § 10.1).

4.4. Primjedba. U osnovnom je teoremu važno ovo:

(1) Kvocijent $q(x)$ i ostatak $r(x)$ su *jednoznačno određeni.*

(2) Koeficijenti od q i r određuju se, *racionalnim* operacijama, pomoću koeficijenata od zadanih polinoma $a(x)$ i $m(x)$, tako da leže u *tijelu* što ga generiraju koeficijenti od $a(x)$ i $m(x)$.

4.5. Zadaci o dijeljenju polinoma.

1. Odredi $E(a, m)$ za ove polinome a, m:

   1) $x^3 + 1,\ x - 1$; 2) $x^3 + 1,\ x + 2$; 3) $x^4 + x^3 + x^2 + x + 1,\ x^2 + 1$;

   4) $5x^3 + 3x^2 + 2x + 2,\ 2x^2 + 1$; 5) $5x^3 + 3x^2 + 2x - 1,\ 2x^2 + 1$;

   6) $5x^3 + 3x^2 - 2x + 1,\ 2x^2 + 1$; 7) $5x^3 - 3x^2 + 2x + 1,\ 2x^2 + 1$;

   8) $-5x^3 + 3x^2 + 2x + 1,\ 2x^2 + 1$; 9) $5x^3 + 3x^2 - 2x - 1,\ 2x^2 + 1$, itd.

   Provjeri rješenje!

2. Isto pitanje za polinome:

   1) $(x+1)(x+3)(x+4),\ x^2 - 1$; 2) $10t^4 - 6t^5 + 1,\ t - 2t^2 + 1$;

   3) $(t^2+1)(3-t^3),\ (t-1)(\frac{2}{3} - 4t)$; 4) $0{,}02x^4 - x^3 + \frac{2}{3}x + 1$,

   $3x^2 - 0{,}5x + 5$.

3. Da li jednoznačnost preslikavanja $(a, m) \to E(a, m)$ vrijedi u prstenu polinoma nad prstenom 1) $I2$; 2) $I3$; 3) $I5$?

4. Da li je $x^5 - 5x^4 - x + 5$ djeljivo sa $x - c$, ako je c jednako: 1) 1; 2) -1; 3) 2; 4) 5? Odgovorite na pitanje a da se dijeljenje ne izvodi!

5. Odrediti brojeve a, b tako da izraz $x^5 - 5x^4 + ax + b$ bude djeljiv produktom korijenih faktora brojeva:

   1) -1, 1; 2) 2, 5; 3) i, $-i$; 4) $2i$, $3 + 5i$.

6. Neka je $f(x)$ algebarski polinom; neka su $x_1, x_2, \ldots, x_n$ različni brojevi; 1) nađi ostatak $E_2(f(x), (x - x_1)(x - x_2)\ldots(x - x_k))$ dijeljenja polinoma $f(x)$ sa $(x - x_1)(x - x_2)\ldots(x - x_k)$ za $k = 1, 2, 3, \ldots, m$;

   2) Nađi na dva načina $E_2(x^4 - 5x^3 + x^2 - 3x + 1, (x - 1)(x - 2))$;

   3) odredi $E_2(f(x), (x - x_1)^2)$;

   4) dokaži da $(x - 1)^2$ dijeli $(n - 1)(x^n + 1) - 2x(x^{n-2} + x^{n-3} + \ldots + x + 1)$ za $n = 2, 3, 4, \ldots$

7. Nađi ostatak dijeljenja od $\sin\alpha \cdot x^n - r^{n-1} \sin n\alpha \cdot x$ sa $x^2 - 2r\cos\alpha \cdot x + r^2$.

8. Odredi najveći prirodni broj m tako da $(x - 1)^m$ bude djelitelj izraza $x^{2n} - n^2 x^{n+1} + 2(n^2 - 1)x^n - n^2 x^{n-1} + 1$.

5. NAJVEĆI ZAJEDNIČKI DJELITELJ ZADANIH POLINOMA

5.1. Definicija (isp. poglavlje 6, § 10). *Najveći zajednički djelitelj (djelilac)* ili najveća zajednička mjera zadanih polinoma je *svaki polinom* koji je *djelitelj* tih polinoma, a *stupanj* mu je *maksimalan.*

Najveći zajednički djelilac polinoma a, b označuje se sa $\mathrm{M}(a, b)$ ili $a\,\mathrm{M}\,b$. Obično će se $a\,\mathrm{M}\,b$ uzeti tako da mu koeficijenti budu *najzgodniji, dogovorno ćemo zahtijevati da najstariji koeficijent bude normiran na 1.*

⟶ *Određivanje* $a\,\mathrm{M}\,b$ se provodi kao kod cijelih brojeva: pomoću Euklidova verižnog dijeljenja (isp. pogljavle 6, § 10.3). Poslednji divizor pri toj diobi je $a\,\mathrm{M}\,b$. To znači, specijalno, da je $a\,\mathrm{M}\,b$ takvo da se koeficijenti od $a\,\mathrm{M}\,b$ dobiju iz koeficijenata od a i koeficijenata od b pomoću niza *racionalnih operacija*, bez obzira na to iz kakve su veće ili manje množine uzeti polinomi a i b.

Važno je da koeficijenti od $a\,\mathrm{M}\,b$ leže u onom tijelu što ga rađaju koeficijenti od a i koeficijenti od b.

⟶ **5.3.** *Osnovni teorem o* $a\,\mathrm{M}\,b$ prenosi se s brojeva na polinome (poglavlje 6, § 10.6 i § 12.3).

Specijalno, jednadžba

$$a(x)\,A(x) + b(x)\,B(x) = a(x)\,\mathrm{M}\,b(x)$$

moguća je bar za jednu dvojku polinoma $A(x)$, $B(x)$ s koeficijentima koji se *racionalno* dobiju iz koeficijenata od zadanih polinoma $a(x)$, $b(x)$.

5.4. Bezoutova veza. [1] Ako je $a \,\mathrm{M}\, b = 1$, kaže se da su a i b *relativno prosti* ili međusobno prosti. Tako su npr. $x-3$, $x-5$, međusobno prosti.

Kao i za brojeve, dokazuje se i ovdje:

5.5. Teorem (Bezout). *Ako je* $a(x) \,M\, b(x) = 1$, *onda postoji veza* $a(x)\, A\, x) + b(x)\, B(x) = a(x) \,\mathrm{M}\, b(x)$; *pri tom su* $A(x)$, $B(x)$ *određeni polinomi sa koeficijentima koji se racionalno izražavaju pomoću koeficijenata od a i b; i obrnuto* (isp. poglavlje 6, § 10.8.).

5.5.1. Ako su a i b međusobno prosti u tijelu k, onda će oni biti relativno prosti i u svakom opsežnijem tijelu $k' \supset k$ (isp. 5.2).

5.6. Kao i kod brojeva, tako se i u kolu $k[x]$ polinoma dokazuje da je $a \,\mathrm{M}\, b$ djeljivo svakim djeliteljem od a, b.

5.7. Osnovni teorem. *Ako je ac djeljivo sa m te ako je* $a \,\mathrm{M}\, m = 1$, *tada je c djeljivo sa m* (isp. poglavlje 6, § 11.5).

Dokaz kao za brojeve.

5.8. Teorem. *Ako je a djeljivo sa b i c te ako je* $b \,\mathrm{M}\, c = 1$, *onda je a djeljivo sa produktom* $b\,c$ (isp. poglavlje 6, § 13.4).

Tim teoremom služimo se mnogo, i to radeći s brojevima, a još više radeći s polinomima.

Tako npr. promatrajmo izraz $x^5 - 5x^4 - x + 5$; on postaje 0 za $x = -1$, $+1$; zato je on djeljiv za $x+1$, $x-1$, dakle i njihovim produktom x^2-1.

6. NAJMANJI ZAJEDNIČKI KRATNIK DVAJU POLINOMA [2]

6.1. Najmanji zajednički kratnik polinomâ a, b je *svaki* polinom koji je djeljiv zadanim polinomima, a stupanj mu je *minimalan*. Oznaka kao kod brojeva $\mathrm{W}(a, b)$ ili $a \,\mathrm{W}\, b$.

6.2. Kao i kod brojeva, dokazuje se da je *svaki* kratnik dvaju polinoma kratnik njihova *najmanjeg* kratnika (poglavlje 6. § 11.3).

6.3. *Svi zajednički kratnici polinoma a i b čine kolo*

$$(a \,\mathrm{W}\, b)\, k[x], \tag{1}$$

koje je čak i ideal kola $k[x]$ jer produkt svakog člana iz tog kola (1) i svakog člana iz $k[x]$ opet je u (1).

6.4. Razredi ostataka. Kao i u kolu D, tako se i u kolu $k[x]$ definiraju posebni *razredi*; to su skupovi oblika:

$$m\, k[x] + r. \tag{2}$$

Oznaka (2) stoji za skup svih članova $m\, A(x) + r$, pri čemu $A(x)$ prolazi čitavim skupom $k[x]$. Naravno, m, r su članovi kola $k[x]$.

---

[1] E. Bezout [Bezu] (1730—1783), francuski matematičar.

[2] Isp. poglavlje 6, § 11.

Npr. svi izrazi oblika $f\cdot(x^2+1)+(3x-1)$, gdje je $f\in k[x]$ obrazuju razred $k[x]\cdot(x^2+1)+(3x-1)$; taj razred i razred $k[x]\cdot(x^2+1)+(3x+1)$ nemaju nijednoga zajedničkog člana.

6.5. Ako su dva elementa c, d takva da je $c-d$ djeljivo sa m, kaže se da su oni *kongruentni prema m kao modulu* i piše

$$c\equiv d \pmod m \text{ ili } m\,|\,(c-d). \tag{3}$$

Lako se dokazuje da (3) vrijedi onda i samo onda ako c, d leže u (2).

6.6. Kolo ili prsten svih razredâ modula *m*. *Svi razredi* (2), *kad r prolazi kroz* $k[x]$, *obrazuju kolo razredâ prema modulu m.*

Razmatranja su ista kao u specijalnom slučaju kola D cijelih brojeva (isp. poglavlje 6, § 2 i § 3).

6.7. Zadaci o najvećoj zajedničkoj mjeri i najmanjem zajedničkom kratniku polinoma. Razredi polinomâ.

1. Dokaži $(x-a)\,\mathrm{M}\,(x-b)\neq 1 \Leftrightarrow a=b$; a, b su proizvoljni realni ili kompleksni brojevi.

2. Neka je $f\,|\,g$ i $g\,|\,f$; odredi $\frac{f}{g}$ za slučaj da su f, g uzeti iz množine:
   1) N; 2) D; 3) $D+iD$ cijelih kompleksnih brojeva; 4) polinoma s realnim koeficijentima.

3. Nađi naveći zajednički djelitelj ovih mnogočlana:
   1) x^3-1, x^5-1; 2) $x^4-x^3+x^2+3x$, $2x^5-4x^4+7x^3-x^2+x+3$;
   3) $x^6+2x^5+3x^4+2x^3+1$, x^3-x^2-x; 4) $(x-1)(x+2)(x-3)$, x^6+x^4+1; 5) x^2-x-42, x^2-49, x^2-36; 6) $a=2x^5+3x^4-10x^3+12x^2+8x-3$, $b=-\frac{3}{2}x^6-\frac{9}{2}x^5+\frac{3}{2}x^4+\frac{1}{3}x^3-4x^2-15\frac{1}{3}x+5$.

4. Dokaži $(x^k-1)\,\mathrm{M}\,(x^n-1)=x^{k\,\mathrm{M}\,n}-1$.

5. U kolu $Q[x]$ riješi ove jednadžbe (nepoznate veličine su $X(t)$, $Y(t)$):
   1) $(t-1)X(t)+2(t+1)Y(t)=1$,
   2) $(t^4+1)X(t)+(at^3+3)Y(t)=2$.

6. Odredi prirodne brojeve n za koje je $(x+1)^n-x^n-1$ djeljivo sa x^2+x+1.

7. Dokaži: 1) $(x^k-1)\,|\,(x^{km}-1)$; 2) $(1+x+x^2)\,|\,(1+x^{3n+1}+x^{2(3n+1)})$;
   3) $(x-1)^2\,|\,(mx^{m+n}-(m+n)x^m+n)$, $(m, n\in N)$;
   4) $m\,|\,n \Leftrightarrow (1+x+x^2+\ldots+x^{m-1})\,|\,(1+x+x^2+\ldots+x^{n-1})$;
   5) $m\,|\,n \Leftrightarrow (x^m-y^n)\,|\,(x^n-y^n)$;
   6) n je neparno $\Leftrightarrow (1+x+x^2+\ldots+x^{n-1})\,|\,(1+x^2+x^4+\ldots x^{2n-2})$.

8. Da li je $x^{2n}-n^2 x^{n+1}+2(n^2-1)x^n-n^2 x^{n-1}+1$ djeljivo sa $(x-1)^4$?

9) Neka je R skup svih realnih brojeva; za dano $f\in R[x]$ odredi $E(f, x^2+1)$ i to posebno ostatak $E_2(f, x^2+1)$;

1) kad f prolazi kroz $R[x]$, što obrazuju svi ostaci $E_2(f, x^2+1)$?

2) što čine svi članovi f iz $R[x]$ za koje je ostatak $3x+1$?

3) odredi razred od $R[x]$ u kojem leži $3x-5$; 4) dokaži da su razredi $(x^2+1)R[x]+(2x+3)$, $(x^2+1)R[x]+(3x-1)$ bez zajedničkog člana;

5) dokaži ravnopravnost: $(a=a')\wedge(b=b')\Leftrightarrow(x^2+1)R[x]+(ax+b)=(x^2+1)R[x]+a'x+b')$.

10. Kako izgledaju razredi kola $R[x]$ za modul 1) $x+1$; 2) x; 3) x^3+2x; 4) $\sqrt{2}x^2+5x-1$? Navesti pojedinačne primjere.

7. PROSTI ILI IREDUCIBILNI POLINOMI. FAKTORIZACIJA

7.1. Definicija. Polinom $a(x)$ iz kola $k[x]$ je *prost* ili *nerastavljiv* u kolu $k[x]$[1] ili *nad tijelom k*, ako iz $a(x)=b(x)c(x)$ izlazi da je jedan od faktora b i c djeljiv sa a. Prosti brojevi ↔ prosti polinomi, odgovaraju jedni drugima[2].

Npr., polinom x^2+1 je prost u kolu $R[x]$, gde je R skup svih realnih brojeva. No, x^2+1 je rastavljiv u kolu $R(i)[x]$ svih polinoma s *kompleksnim* koeficijentima. Polinom x^2+5 nije rastavljiv u kolu $Q[x]$ ili, npr., $Q(\sqrt{2})[x]$, ali jest rastavljiv u kolu $Q[\sqrt{5}]$. Polinom x^3+x^2-2x-1 nije rastavljiv nad tijelom Q racionalnih brojeva; zato se, npr., ne može elementarno nacrtati pravilni sedmerokut (isp. poglavlje 5, § 8.6).

⟶ **7.2. Faktorizacija.** Teorem. *Svaki normirani član iz $k[x]$ ili je prost ili je produkt potpuno određene množine prostih članova iz $k[x]$ koji su $\neq 1$.*

To je osnovni teorem o faktorizaciji u $k[x]$. (isp. poglavlje 6 § 14).

7.3. Teorem. Ako *prost* polinom p nije prost prema polinomu a, onda je p *djelitelj* od a (kako glasi sličan teorem za brojeve?).

7.4. Gaussova lema o polinomima. *Ako je $f(x)$ normiran algebarski polinom s cijelim racionalnim koeficijentima, pa ako je $f(x)=g(x)h(x)$, gdje su g, h normirani polinomi s racionalnim koeficijentima, tada su koeficijenti polinomâ g, h cijeli racionalni brojevi.*

Dokaz. Neka je G najmanji zajednički kratnik nazivnikâ svih koeficijenata polinoma g; to znači da je G najmanji prirodni broj sa svojstvom da

---

[1] Znajmo da je $k[x]$ skup svih *polinoma* s obzirom na x i s koeficijentima iz tijela k.

[2] Stvar se prenosi i na opće prstene i na prstene $k[x]$ i to za druge korporacije ili tijela k, a ne samo kada k znači koje tijelo brojeva ili polinoma i sl.

je $G g_j \in D$; neka je isto tako H najmanji prirodni broj za koji je $H h_j \in D$. Pretpostavit ćemo da su koeficijenti od g, h u neskrativom obliku. Tada je:

$$\text{(1)} \qquad \mathop{\mathrm{M}}_{i} G g_i = 1,$$

$$\text{(2)} \qquad \mathop{\mathrm{M}}_{j} H h_j = 1,$$

pa su koeficijenti polinoma Gg i polinoma Hh cijeli brojevi. Imamo:

$$\text{(3)} \qquad \sum G g_i x^i \cdot \sum H h_j x^j = G H \sum f_k x^k.$$

Tvrdimo da je $G = H = 1$. U obratnom slučaju postojao bi *prost* broj $p \mid G H$; no kako su koeficijenti f_k cijeli, znači da bi, po (3), broj p morao dijeliti i lijevu stranu u (1). Međutim, zbog (1), odnosno (2), postoji bar jedan koeficijent $G g_t$ kao i jedan $H h_j$ koji nisu djeljivi sa p. Pa neka su $G g_r$, odnosno $H h_s$ *prvi* takvi koeficijenti. Onda znači da ni njihov produkt

$$\text{(4)} \qquad G g_r \cdot H h_s$$

ne bi bio djeljiv sa p. Međutim, to nije moguće jer uistinu ispoređivanjem u (3) koeficijenata od x^{r+s} lijevo i desno izlazi:

$$\text{(5)} \qquad \sum_{i,j} G g_i H h_j = G H f_{r+s}, \quad i + j = r + s.$$

U jednakosti (5) svaki član osim člana lijevo u (5) koji nastaje za $i = r$, $i = s$, *bio bi djeljiv sa* p; *a to je nemoguće.*

8. FAKTORIZACIJA NAD TIJELOM C KOMPLEKSNIH BROJEVA

8.1. Prema «*osnovnom teoremu algebre*« svaki polinom $\mathrm{st} > 1$ nad C rastavljiv je u tom tijelu; drugim riječima: ako polinom $a(x)$ ima koeficijente u tijelu kompleksnih brojeva, pa ako je $\mathrm{st}\, a > 1$, tada postoje dva polinoma nad C kojima je produkt $= a$ a nijedan od tih polinoma nije konstanta. Tako npr. $1 + x^2 = (1 + i x)(1 - i x)$. Nešto slično ne vrijedi za tijelo R realnih brojeva. Ali vrijedi ovo: svaki nerastavljivi polinom nad R i s koeficijentima iz R nužno je stupnja < 3 (isp. § 9.2). Tako npr. $1 + x^4$ je stupnja 4, ali nije nerastavljiv. Nad C ga je lako faktorizirati: $1 + x^4 = (1 + ix^2)(1 - ix^2)$. No, vidi se da je također $1 + x^4 = (1 - \sqrt{2}\, x + x^2)(1 + \sqrt{2}\, x + x^2)$; ovdje su koeficijenti realni (isp. § 9).

8.2. Spektar polinoma $a(x)$. Neka je $\mathrm{st}\, a = n$; dakle $a_n \neq 0$; ako je $a_{(0)}$ jedan kompleksan broj u kojem je a jednako 0, tj. $a(a_{(0)}) = 0$, onda znamo da je $a(x)$ djeljivo sa $x - a_{(0)}$; pa neka je $a(x) = (x - a_{(0)})\, q(x)$. Ako je $\mathrm{st}\, q(x) > 0$, možemo analogno zaključiti pa $q(x)$ faktorizirati:

$$q(x) = (x - a_{(1)})\, s(x); \text{ dakle je } a(x) = (x - a_{(0)})(x - a_{(1)})\, s(x), \text{ itd.},$$

dok se ne dođe do polinoma stupnja 0, i to je nužno koeficijent a_n. Na taj način imamo potpunu faktorizaciju polinoma a:

8.2.1. Teorem. *Za svaki prirodni broj n i svaki polinom $a(x) = a_0 + a_1 x + \ldots + a_n x^n$ stupnja n i s kompleksnim koeficijentima imamo*

$$a(x) = (x - a_{(1)})\,(x - a_{(2)}) \ldots (x - a_{(n)})\,a_n \tag{1}$$

pri čemu su $a_{(\nu)}$ ($\nu = 1, 2, \ldots, n$) kompleksni brojevi; među njima može biti i jednakih (razlikuj koeficijent a_ν od nulišta $a_{(\nu)}$).

Specijalno, ako je $a(x)$ *normirani polinom*, tj. $a_{stp} = 1 = a_n$, tada imamo:

$$a(x) = (x - a_{(1)})(x - a_{(2)}) \ldots (x - a_{(n)}). \tag{2}$$

8.2.2. Definicija. *Neuređen* niz

$$a_{(1)}, \ldots, a_{(n-1)}, a_{(n)} \tag{3}$$

zove se *spektar polinoma a*; označavat ćemo ga sa Sa ili $Sp(a)$. Tako npr. spektar trinoma $x^2 - 6x + 9$ je 3,3 jer je $(x^2 - 6x + 9) = (x - 3)(x - 3)$. Skup članova od Sa označivat ćemo σa.

8.3. Primjedba o oznaci koeficijenata i članova spektra. Koeficijenti zadanog polinoma $a(x) = a_0 x^0 + a_1 x^1 + a_2 x^2 + \ldots a_n x^n$ čine *potpuno određeni niz*

$$a_0, a_1, \ldots, a_{n-1}, a_n.$$

To je tako ako polinom poređamo uzlazno. Ako polinom sredimo silazno, onda koeficijenti polinoma a čine niz $a_n, a_{n-1}, \ldots, a_1, a_0$, pri čemu je prvi član sada $\neq 0$.

Nula-tačke polinoma $a(x)$ označujemo sa $a_{(n)}$, pri čemu $n = 1, 2, \ldots, n$. Oznaka je dosta slična oznaci koeficijenata: razlika je u tome što indeks stoji u zagradi i što ne postoji $a_{(0)}$ (kao ništište).

8.4. Sređivanje spektra. Spektar Sa polinoma a uredit ćemo po principu *prvih diferencija*. Naime, članovi spektra su kompleksni brojevi. A za dva kompleksna broja $a + bi$, $a' + b'i$ pisat ćemo $a + bi \leq a' + b'i$ onda i samo onda ako je ili $a < a'$ ili $a = a'$, $b \leq b'$, Time se čitava brojevna ravnina uređuje tako da je svaki član sa svake paralele s osi y ispred svakog člana sa svake paralele udesno; a na pojedinoj toj paraleli broj koji je niže smješten proglašen je manjim.

Na taj se način skup svih kompleksnih brojeva potpuno uredi, pa ćemo, specijalno, tako urediti i spektar svakog polinoma. Tako npr. spektar 3, 3, 2, 5, 2, 6 nije uređen; evo ga sređenog: 2, 2, 3, 3, 5, 6. Isto tako spektar $3 + 2i$, $4 - 5i$, $-2 + 4i$, $-2 + 4i$, 5, 0 glasi u sređenu obliku ovako:

$$-2 + 4i,\ -2 + 4i,\ 0,\ 3 + 2i,\ 5.$$

Na taj način, za svaki polinom $a(x)$ s kompleksnim koeficijentima potpuno je određen prvi, drugi, ..., n-ti član njegova sređenog spektra Sa i σa.

8.5. Teorem. *Neka su zadani: kompleksni broj z i algebarski polinom $a(x) = a_0 + a_1 x + \ldots a_n x^n$ stupnja $n \geq 1$ (dakle je $a_n \neq 0$).*

Tada zatvoreni krug $k\left(z, \leq \left|\left(\frac{a(z)}{a_n}\right)^{1/n}\right|\right)$ sadrži bar jedno ništište polinoma $a(x)$ (D. Simeunović).

D o k a z. Stavimo li u obrazac (1) vrednost $x=z$ izlazi

$$a(z)\equiv a_n(z-a_{(1)})\ldots(z-a_{(n)}); \tag{4}$$

neka je z_0 nulište od $a(z)$ koje je *najbliže do* z; dakle je $|z_0-z|\leqslant|z-a_{(\nu)}|$ za svako $\nu\in\{1, 2, \ldots, n\}$ pa jednakost (4) daje

$$|a(z)|\geqslant|a_n|\cdot|z-z_0|\ldots|z-z_0|=|a_n|\cdot|z-z_0|^n$$

odakle $|z-z_0|\leq||a_n|^{-1}|a(z)|^{1/n}|$; a to se teoremom 8.5 i tvrdi.

9. POLINOMI $p(x)$ S REALNIM KOEFICIJENTIMA. SPREGNUTE NULA-TAČKE

9.1. T e o r e m. *Ako je z nula-tačka algebarskog polinoma $p(x)$ s realnim koeficijentima, onda je spregnut (konjugovan) broj $\overline{z}$ također nula-tačka od $p(x)$.* Drugim riječima: ako su koeficijenti p_i polinoma $p(x)$ realni, tada iz $p(z)=0$ izlazi $p(\overline{z})=0$? pri tom za kompleksni broj $z=x+iy$ stavljamo $\overline{z}=x-iy$ (isti realni dio a protivno-jednak imaginarni dio).

Po pretpostavci je

$$p_0+p_1z+p_2z^2+\ldots=0.$$

Odatle, prelazeći na spregnutu ili konjugiranu vrijednost:

$$\overline{(p_0+p_1z+\ldots)}=0$$

i dalje zbog $\overline{a+b}=\overline{a}+\overline{b}$,

$$\overline{p_0}+\overline{p_1z}+\overline{p_2z^2}+\ldots=0.$$

Dalje, zbog $\overline{a\cdot b}=\overline{a}\cdot\overline{b}$:

$$\overline{p_0}+\overline{p_1}\,\overline{z}+\overline{p_2}\,\overline{z^2}+\ldots=0.$$

No $\overline{p_k}=p_k$ (jer je p_k realno) i $\overline{z^k}=\overline{z}^k$ pa imamo:

$$p_0+p_1\overline{z}+p_2\overline{z}^2+\ldots=0, \text{ tj.}$$

$$p(\overline{z})=0 \qquad \text{Q. E. D.}$$

9.2. T e o r e m. *Svaki nesvodljivi (ireducibilni) polinom $p(x)$ nad tijelom R realnih brojeva je stupnja <3.*

Naime, $p(x)$ je produkt linearnih izraza oblika $x-a-ib$, gdje su a, b realni brojevi. No, uz $a+ib=z$ kao nula-tačka javlja se i $\overline{z}=a-ib$ kao nula-tačka; zato dio faktorizacije $(x-z)(x+\overline{z})$ u kompleksnom području daje u realnom području $x^2-(z+\overline{z})x+z\cdot\overline{z}$; a ovo je sve realno jer je $z+\overline{z}=2a$, $z\overline{z}=a^2+b^2$.

9.3. Teorem. *Svaki polinom $p(x)$ nad R kojemu je stupanj neparan posjeduje bar jednu realnu nula-tačku.*

To je neposredna posljedica od 9.1.

10. O JEDNOJ RAZLICI IZMEĐU ALGEBARSKIH POLINOMA S JEDNOM VARIJABLOM I ALGEBARSKIH POLINOMA S DVIJE I VIŠE VARIJABLI

10.1. Teorem. Ako je $a(x)$ algebarski polinom, pa ako je $a(z)=0$, tada je $a(x)$ djeljivo sa $x-z$ pa se može pisati $a(x)=(x-z)\,q(x)$, gdje je $q(x)$ određen algebarski polinom stepena $\operatorname{st} a-1$ (Descartes, 1637) (v. § 4. 3).

Radeći slično sa $p(z)$ i ponavljajući taj postupak, zaključujemo da vrijedi ovaj:

Teorem. *Svakom algebarskom polinomu $a(x)$ pripada određen niz od $\alpha = st\ a$ brojeva*

$$a_{(0)},\ a_{(1)},\ a_{(2)},\ \ldots\ a_{(\alpha-1)}$$

za koje je

$$a(x)=a_{\alpha}.\ \prod_{k\in I\alpha}\ (x-a_{(k)}).$$

To znači da je $a(x)$ produkt koeficijenta a_{α} i α linearnih faktora $x-a_{(k)}$ za $k \in I\alpha=\{0, 1, 2, \ldots, \alpha-1\}$.

Tu je naglasak na činjenici da se $a(z)$ svodi (razlaže) na produkt *linearnih normiranih* polinoma.

10.2. *Analogno svojstvo za algebarske polinome s dvije i više varijabli ne vrijedi.* I to je razlika na koju smo mislili u nazivu ovog paragrafa.

10.3. Tako npr. već polinomi x^2+y^2+1, $1+xy$ stupnja 2 nisu produkt od linearnih funkcija. Dokažimo to za x^2+y^2+1.

Pretpostavimo, naime, da postoji rastav:

$$(1)\qquad (a\,x+b\,y+c)(a'\,x+b'\,y+c')=x^2+y^2+1.$$

Tu su a, b, c, a', b', c' brojevi.

Izmnožimo li na lijevoj strani i sredimo, izlazi:

$$(2)\qquad \begin{aligned} a\,a'\,x^2+(a\,b'+a'\,b)\,x\,y+b\,b'\,y^2+(a\,c'+a'\,c)\,x+\\ +(b\,c'+b'\,c)\,y+c\,c'=x^2+y^2+1. \end{aligned}$$

Ta identična jednakost ravnovažna je s ovih 6 jednakosti:

$$(3)\qquad \begin{aligned} a\,a'&=1 & a\,b'+a'\,b&=0\\ b\,b'&=1 & b\,c'+b'\,c&=0\\ c\,c'&=1 & a\,c'+a'\,c&=0. \end{aligned}$$

Iz lijevih triju jednadžbi izlazilo bi:

$$a' = a^{-1}, \quad b' = b^{-1}, \quad c' = c^{-1}, \tag{4}$$

jer su po pretpostavci a, b, c, a', b', c' brojevi, a sad vidimo da su oni $\neq 0$.

Na osnovu toga prva jednadžba desno u (3) postaje:

$$a\,b^{-1} + a^{-1}\,b = 0$$

$$\Updownarrow$$

$$a^2 + b^2 = 0 \tag{5}$$

$$\Updownarrow$$

$$b = \pm a\,i.$$

Analogno:

$$c = \pm a\,i \tag{6}$$

$$c = \pm b\,i. \tag{7}$$

Uvrstimo li izraz $b = \pm a\,i$ u (7), izlazi:

$$c = \pm a, \text{ što sa (6) daje:}$$

$$\pm a\,i = \pm a$$

A ta jednakost nije moguća jer je $a \neq 0$.

Dakle, rastav (1) nije moguć: kvadratni polinom $x^2 + y^2 + 1$ nije produkt od dvije linearne funkcije promjenljivicâ x, y.

10.4. Algebarske forme u dvije promjenljive. Promatrajmo sada slučaj da je polinom $a(x, y)$ homogen, tj. da mu je svaki član oblika:

$$a_{k,l}\,x^k\,y^l$$

uz uslov homogenosti:

$$k + l = \operatorname{st} a = \alpha.$$

To znači da je

$$a(x,y) = \sum a_{kl}\,x^k\,y^l = \sum_k a_{k,\,\alpha-k}\,x^k\,y^{\alpha-k} = \tag{1}$$

$$= y^\alpha \sum a_{k,\,\alpha-k}\,x^k\,y^{-k} = y^\alpha \sum a_{k,\,\alpha-k}\,(x\,y^{-1})^k.$$

Dakle je za homogene polinome $a(x, y)$ ispunjeno:

$$a(x,y) = y^\alpha \sum_k a_{k,\,\alpha-k}\,(x\,y^{-1})^k. \tag{2}$$

No, tu je faktor uz y^α određen polinom u odnosu na $x\,y^{-1}$, recimo $b(x\,y^{-1})$; njegov stupanj β je $\leqq \alpha$, jer neki koeficijenti $a_{k,\,\alpha-k}$ mogu biti 0. No, za polinom $b(x\,y^{-1})$ imamo rastav:

$$b(x\,y^{-1}) = b_\beta \prod_{l \in I\beta} (x\,y^{-1} - z_{(l)})$$

prema rezultatima u t. 1.

Zbog (3) postaje (2) oblika:

$$a(x,y)=y^{\alpha}\,b_{\beta}\prod_{l\in I\beta}(x\,y^{-1}-z_{(l)}). \tag{4}$$

Unesemo li u svaku od tih β zagrada po faktor y iz faktora y^{α}, daje (4) ovo:

$$a(x,y)=y^{\alpha-\beta}\,b_{\beta}\prod_{l\in I\beta}(x-z_{(l)}\,y). \tag{5}$$

Dakle imamo

10.5. Teorem. *Svaki* ***homogeni*** *algebarski polinom* $a(x,y)$ *produkt je nekog broja i* $\alpha=st\,a$ *linearnih homogenih funkcija varijabli* x, y.

10.6. Slučaj tri i više varijabli. Ako je $p(x,y,z)$ algebarski homogen polinoma u tri varijable stepena $n=\mathrm{st}\,p$, tada svaki njegov član sadrži bazu

$$x^k\,y^l\,z^m$$

uz uslov $k+l+m=\mathrm{st}\,p=n$; označimo li odgovarajući koeficijent sa p_{klm}, tada p glasi:

$$p(x,y,z)=\sum p_{k,l,m}\,x^k\,y^l\,z^m=\sum p_{k,l,n-(k+l)}\,x^k\,y^l\,z^{n-(k+l)}$$
$$=z^n\sum_{k,l}p_{k,l,n-(k+l)}\,(x\,z^{-1})^k\,(y\,z^{-1})^l;$$

pri tom k, l i $k+l$ leže u In. Tu koeficijet z u prethodnom izrazu može biti najopćenitiji polinom dviju veličina $x\,z^{-1}$, $y\,z^{-1}$ pa zato ne mora biti rastvoriv u produkt odgovarajućih faktora.

10.7. Na taj način vidimo da polinom $p(x,y,z)$ čak ako je i *homogen*, ne mora biti rastavljiv u produkt linearnih faktora, odnosno ne mora biti djeljiv nikakvom linearnom funkcijom

$$a\,x+b\,y+c\,z+d.$$

Tako se npr. može dokazati da homogeni trinom

$$x^2\,z+y^2\,z+z^3$$

nije djeljiv nikojom linearnom funkcijom varijabli x, y, z (vidi primjer u 10.3).

10.8. Zadaci o faktorizaciji polinomâ.

1. Rastavi na proste množitelje nad tijelom R realnih brojeva ove polinome: 1) x^3-1; 2) x^3+1; 3) x^3-y^3; 4) x^5-1; 5) $x^4-1000\,x\,y^3$; 6) $a^2-1-ab-b$; 7) $x^5-x^2-x^3+1$; 8) $9-x^2+9\,x^3-x^5$; 9) $x^3+x^2-2\,x-1$; 10) $x^3+y^3+z^3-3\,x\,y\,z$.
2. Isto pitanje za tijelo Q racionalnih brojeva.
3. Istò pitanje za 1) tijelo $I2$; 2) tijelo $I5$.
4. Isto pitanje za tijelo $R(i)$ kompleksnih brojeva.
5. Odredi spektar S i σ polinomâ iz zad. 1 1); 2); 4); 7); 8); 9).
6. Isto pitanje ako radimo u aritmetici mod. 2.

7. Kako glasi normiran polinom kojemu je spektar: 1) 4, 7, 8, 8; 2) 4, 7, 8, −8; 3) 4, 7, −8; −8; 4) 4, −7, −8, 8; 5′) 4, −7, −8, −8; 5″) −4, −7, −8, −8; 6) $2+3i$, $2-3i$, $6i$, $-6i$; 7) $2+3i$, $2-3i$, $6i$; 8) −1, −1, −1; 9) i, i, 1; 10) 1, 1, 1; 11) 2, 2, 2, 2; 12) 1, 1, 2, 2, 2.

8. 1) Dokaži: normiran polinom $a(x)$ djeljiv je normiranim polinomom $b(x)$, onda i samo onda ako je spektar od b podspektar spektra od a tj. svaki član od Sp (b) je član i od Sp (a); pritom i kratnost dolazi u obzir; 2) Ako je Sp $a=3, 3, 5, 6$, Sp $b=3, 3, 3, 5, 5, 6$, da li je $a \mid b$ ili $b \mid a$? 3) Ako je Sp $a=1, 1, 3, -3$, Sp $b=1, 2, -3$ nađi $a \,\mathrm{M}\, b$, $a \,\mathrm{W}\, b$, 4) Obrazuj slične zadatke!

9. Dokaži da je mnogočlan $x(x^{n-1}-n a^{n-1})+a^n(n-1)$ djeljiv sa $(x-a)^2$.

10. Dokaži da je $(1-x^n)(1+x)-2nx^n(1-x)-n^2x^n(1-x)^2$ djeljivo sa $(1-x)^3$; kojeg je stupnja količnik?

11. Ako je n neparan broj koji nije kratnik broja 3, tada je $(x+y)^n-x^n-y^n$ djeljivo sa $xy(x+y)(x^2+xy+y^2)$. Ako je $n=6k+1$, tada je $(x+y)^n-x^n-y^n$ djeljivo sa $xy(x+y)(x^2+xy+y^2)^2$.

12. Ako je n neparan prirodan broj, tad je $(x+y+z)^n-x^n-y^n-z^n$ djeljivo sa $(x+y+z)^3-x^3-y^3-z^3$.

13. $k=-3 \Leftrightarrow (x+y+z) \mid (x^3+y^3+z^3+kxyz)$. Dokaži!

14. Dokaži: 1) $(\cos\varphi+x\sin\varphi)^n-\cos n\varphi-x\sin n\varphi$ je djeljivo sa x^2+1. 2) $x^n\sin\varphi-\rho^{n-1}x\sin n\varphi+\rho^n\sin(n-1)\varphi$ djeljivo je sa $x^2-2\rho x\cos\varphi+\rho^2$,

15. Dokaži identitete: 1) $(x+y)^3-x^3-y^3=3xy(x+y)$;
2) $(x+y)^5-x^5-y^5=5xy(x+y)(x^2+xy+y^2)$;
3) $(x+y)^7-x^7-y^7=7xy(x^2+xy+y^2)^2$.

16. Dokaži da se ovaj izraz nad R odnosno $R(i)$ ne može prikazati kao produkt linearnih faktora: 1) $1+xy$; 2) $2+xy$; 3) $c+xy$ za $c\neq 0$; 4) $x^2z+y^2z+z^3$.

17. Faktoriziraj:
1) x^2+y^2; 2) x^2+3y^2; 3) $x^2-2xy+cy^2$; 4) $ax^2+bxy+cy$;
5) x^3+3y^3; 6) x^3-3y^3; 7) $x^3+x^2y+y^3$; 8) $x^3-xy^2-y^3$.

11. DERIVACIJA ALGEBARSKIH POLINOMA

11.1. Definicija. Svakom algebarskom polinomu p u jednoj varijabli (označimo je sa x) pridijelimo njegov derivat Dp ili $\frac{d}{dx}p$ ili p' po propisu:

$$Dx^n = nx^{n-1} \text{ za svaki prirodni broj } n$$

$$D \text{ konst} = 0$$

te da *D bude homogeno — linearno*, tj.

$$D(a\,p+b\,q)=a\,D\,p+b\,D\,q,$$

za proizvoljne konstante a, b i proizvoljne algebarske polinome p, q s obzirom na x.

Drugim riječima:

kako je:

(1) $$p=p_0+p_1\,x+p_2\,x^2+\ldots+p_n\,x^n,\ n=\mathrm{st}\,p\neq 0,$$

bit će

(2) $$D\,p=p'(x)=p_1+2\,p_2\,x+3\,p_3\,x^2+\ldots+n\,p_n\,x^{n-1}.$$

11.2. Drugi derivat $D^2\,p$ definira se *iterativno*, tj. kao *derivat derivata* od p, dakle $D^2\,p=D(D\,p)$. Analogno, $D^3=D\,D^2$, $D^4=D\,D^3$ itd.

Specijalno se vidi da je $D^n\,x^n=n!$

$$D^{n+1}\,x^n=0\ \text{ i }\ D^k\,x^n=0$$

za sve prirodne brojeve k, n za koje je $k>n$.

11.3. Induktivno se vidi da je $p(0)=p_0$, $p'(0)=p_1$, $p''(0)=2!\ p_2$, ... $p^{(k)}(0)=k!\,p_k$ za $k=0,\ 1,\ 2,\ldots,\ n$.

11.4. Derivat produkta. Lako se dokazuje da je

$$D(u\,v)=D\,u\cdot v+u\cdot D\,\mathrm{v}.$$

11.5. Primjedba. I za općenitije funkcije $p(x)$ (a ne samo za polinome) definira se $D\,p$, i to kao $\lim\limits_{h\to 0}\dfrac{p(x+h)-p(x)}{h}$.

Ako je p algebarski polinom od dvije ili više varijabli x, y, ..., onda se definira derivat od p s obzirom na x simbolički $\dfrac{\partial}{\partial x}p$ kao $D\,p$, smatrajući u p ostale varijable $\neq x$ kao da su konstante. Analogno se definiraju $\dfrac{\partial}{\partial y}p$. Piše se $\dfrac{\partial^2}{\partial x\,\partial y}$ da se naznači da se derivira najprije po x, a rezultat po y. Jasno je što će značiti, npr., operator $\dfrac{\partial^3}{\partial x\,\partial y\,\partial z}$. Tako npr.

$$\frac{\partial}{\partial y}\ 3\,y^4\,z^5=12\,y^3\,z^5.$$

$$\frac{\partial^2}{\partial y\,\partial z}\ 3\,y^4\,z^5=60\,y^3\,z^4$$

$$\frac{\partial^3}{\partial y\,\partial z\,\partial z}\ (3\,y^4\,z^5)=240\,y^3\,z^3.$$

12. TAYLOROV OBRAZAC ZA POLINOME

12.1. Za funkciju $f(x)=x^n$ imamo dvije vrste formula:

Prva vrsta:

$$(1)\qquad f(x)=(t+(x-t))^n=t^n+n\,t^{n-1}(x-t)+$$

$$+\frac{n(n-1)}{2!}t^{n-2}(x-t)^2+\ldots$$

Druga vrsta:

$$(2)\qquad \frac{d}{dx}f(x)=n\,x^{n-1},\ \text{tj.}\left(\frac{d}{dx}f\right)_{x=t}=n\,t^{n-1}$$

$$\frac{d^2}{dx^2}f=n(n-1)\,x^{n-2},\ \text{tj.}\left(\frac{d^2}{dx^2}f\right)_{x=t}=n(n-1)\,t^{n-2},\ldots$$

Ako ove izraze unesemo u (1), izlazi:

$$(3)\qquad f(x)=f(t)+Df(t)\cdot(x-t)+\frac{D^2f(t)}{2!}\cdot(x-t)^2+$$

$$+\frac{D^3f(t)}{3!}\cdot(x-t)^3+\ldots$$

Time smo dokazali da potencija x^n zadovoljava jednakost (3) za svako t.

12.2. *Jedan od osnovnih problema u matematici sastoji se u tome da se i druge funkcije* (*a ne samo* x^n) *preispitaju u pogledu jednakosti* (3), *koja se zove* **Taylorov razvoj funkcije** $f(x)$ **oko vrijednosti** $x=t$. Naime, smisao jednakosti (3) sastoji se u tome da, znajući tačku (broj) t, zatim znajući u t vrijednost funkcije $f(x)$ i njenih derivata, tada prema (3) automatski „znamo“ vrijednost funkcije $f(x)$ i za *druge vrijednosti varijable.*

12.3. Osnovna formula (3) odmah se prenosi s potencija x^n na svaki cijeli racionalni polinom $p(x)$. Naime, imamo ovako:

$$p(x)=\sum_n p_n x^n=\sum_n p_n\left(\sum_k\frac{1}{k!}(D^k x^n)\right)_{x=t}(x-t)^k=$$

$$=\sum_k\sum_n p_n\left(\frac{D^k x^n}{k!}\right)(x-t)^k=\sum_k\sum_n\frac{1}{k!}(D^k(p_n x^n))_{x=t}(x-t)^k=$$

$$=\sum_k\frac{1}{k!}\left(D^k\left(\sum p_n x^n\right)\right)_{x=t}(x-t)^k=\sum_k\frac{1}{k!}D^k p(t)(x-t)^k,$$

tj. polinom $p(x)$ zadovoljava (3). Čitalac neka pobliže obrazloži svaki od rečenih znakova = pri dokazu što ga izvedosmo.

—→ **12.4. Taylorov teorem.** *Za svaki cijeli racionalni polinom $p(x)$ vrijedi Taylorov razvoj*

$$(T) \qquad p(x)=\sum_{k=0}^{\infty}\frac{D^k p(t)}{k!}(x-t)^k \quad \textit{za svaki broj } t.$$

Specijalni slučaj $t=0$ daje Mac Laurinov razvoj:

$$p(x)=\sum_{k=0}^{\infty}\frac{D^k p(0)}{k!}x^k.$$

12.5. Činjenica je da je Newton došao i do binomskog razvoja (1) i do derivata funkcije uopće, a potencije posebno. U drugu ruku je činjenica da je do gornje osnovne formule (T) došao Taylor, i to istom god. 1715, dakle oko 50 godina poslije Newtonova otkrića izvodnih funkcija. Pravo je čudo da Newton (1642—1727) nije i sam otkrio gornji obrazac. *Taylorov obrazac pripada među najvažnije obrasce u matematici.*

12.6. Primjer. Za polinom $p(x)=x^3+2x+5$ razvoj oko $t=1$ daje

$$p(x)=8+5(x-1)+3(x-1)^2+(x-1)^3;$$

lako se vidi da je uistinu

$$8=(D^0 p)(1),\ 5=D^1 p(1),\ 3=(D^2 p)(1)/2,\ 1=(D^3 p)(1)/3!$$

Za cos x i razvoj oko 0 imamo:

$$\cos x=1-\frac{x^2}{2!}+\frac{x^4}{4!}-+\ldots$$

(ovdje se pojavljuje beskonačno mnogo članova; kod polinoma razvoj ima konačno mnogo članova jer su izvodi poretka $>\mathrm{st}\,p$ svi $=0$).

12.7. Drugi oblik Taylorova obrasca. U osnovnoj jednakosti (T) pojavljuje se promjena $x-t$ nezavisne varijable x i izvodi raznog poretka funkcije f. Produkt tih veličina ima svoje duboko značenje; beskonačno je dublja i dalekosežnija formula oblika

$$(T_d) \qquad f(x)=\sum_k \frac{d^k f}{k!}$$

jer se „diferencijali" $d^k f$ definiraju i nezavisno od derivata i jer obrazac (T_d) vrijedi u mnogo općenitijim slučajevima nego (T); specijalno, (T_d) vrijedi za slučaj da x predstavlja niz od 2 i više varijabli!

12.8. Zadaci o deriviranju ili izvođenju. Nekoliko vrsta polinomâ.

1. Nađi izvod po x ovih izraza:
   1) x^2; 2) x^2+3; 3) $(x^2+3)^3$; 4) $(x^2+3)^n$; 5) $(1+2ax+x^2)^n$.
2. Nađi onaj izvod najnižeg reda funkcije iz zad. 1 koji je
   1) konstanta; 2) identički 0.

3. Svaki od polinoma iz zad. 1 razvij u okolini broja
   1) 1; 2) -1; 3) 5.

4. Dokaži opet ovo: kratnost broja z s obzirom na polinom $a(x)$ je najveći redni broj r sa svojstvom da $a(x)$ bude djeljivo sa $(x-z)^r$ (isp. pogl. 5 § 4.2.7).

5. Ležandrovi polinomi [1] $X_n(x)$ definirani su ovako:

$$X_n(x)=\frac{1}{2^n n!} D^{(n)}(x^2-1)^n \text{ za } n=0, 1, 2, \ldots; \text{ specijalno } X_0(x)=1.$$

1) Dokaži da je

$$X_1(x)=x, \quad X_2(x)=\frac{3}{2}x^2-\frac{1}{2}, \quad X_3(x)=\frac{5}{2}x_3-\frac{3}{2}x,$$

$$X_4(x)=\frac{35}{8}x^4-\frac{15}{4}x^2+\frac{3}{8}, \ldots$$

$$X_n(x)=\sum_{k=0}^{n}(-1)^{n-k}\frac{1\cdot 3\cdot 5\cdot\ldots\cdot(2k-1)}{(n-k)!\,(2k-n)!\,2^{n-k}}-x^{2k-n},$$ (uz dogovor da se ispuste članovi u kojima je eksponent od x negativan).

2) Dokaži da je ispunjeno
$(x^2-1)D^2X_n(x)+2xDX_n(x)-n(n+1)X_n(x)=0.$

3) Uvjeri se o ispravnosti obrasca
$(n+1)X_{n+1}(x)-x(2n+1)X_n(x)+nX_{n-1}(x)=0.$

4) Zanimljivo je da $X_n(x)$ ima ovo karakterističnо svojstvo: $X_n(x)$ je upravo onaj normirani polinom stupnja n koji od ishodišta 0 ima najmanju razdaljinu.

6. *Čebiševljevi polinomi* [2] $T_n(x)$ definiraju se ovako:
$T_0(x)=1$, $T_n(x)=2^{-n+1}\cos(n \arccos x)$.

1) Uvjeri se da je $T_1(x)=x$, $T_2(x)=x^2-\frac{1}{2}$, $T_3(x)=x^3-\frac{3}{4}x$,

$$T_4(x)=x^4-x^2+\frac{1}{8}, \quad T_5(x)=x^5-\frac{5}{4}x^3+\frac{5}{16}x,$$

$$T_6(x)=x^6-\frac{3}{2}x^4+\frac{9}{16}x^2-\frac{1}{32}, \ldots$$

Dokaži da je $T_n(x)$ polinom stupnja n.

---

[1] A. M. Legendre (č. Ležandr) Recherches sur l'attraction des sphéroïdes homogènes — Istraživanja o privlačenju homogenih sferoida — (Mém. math. phys., Acad. Sci, 10 (1785), 411—434 — Recherches sur la figure des planètes — Istraživanja o obliku planetâ. (U istoj zbirci, 1784 str. 370—389).

[2] P. L. Čebišev (Tchebicheff): Sur les questions de minima qui se rattachent à la représentation des fonctions — O pitanjima najmanjih veličina koje se nadovezuju na prikazivanje funkcija (Mem. Akad. Petersburg — Lenjingrad, Ser. 6, sv. 7 (1859) 199—291: Сочинения II (1957) 151—236, posebno, § VI, 169—173. Oznaka T_n uvedena je prema početnom slovu neslavenskog načina pisanja prezimena Čebiševa.

2) Dokaži jednakost $(1-x^2)\,D^2\,T_n - x\,D\,T_n + n^2\,T_n = 0$.

3) Za $n>1$ vrijedi $T_{n+1}(x) = x\,T_n(x) - \frac{1}{4}\,T_{n-1}(x)$, $T_1 = x\,T_0$, $T_2 = x\,T_1 - \frac{1}{4}\,T_0 - \frac{1}{4}$,

4) Polinom $T_n(x)$ je onaj normirani polinom n-tog stupnja koji se najviše približuje konstanti 0 u intervalu $R[-1, 1]$.

5) $T_n(x) = 2^{-n}\left[\left(x+\sqrt{x^2-1}\right)^n + \left(x-\sqrt{x^2-1}\right)^n\right]$. Čebišev je u ovom obliku dao polinome $T_n(x)$.

7. Jakobijevi [1] polinomi $G_n(p, q, x) = \dfrac{x^{1-q}(1-x)^{q-p}}{q(q+1)\cdots(q+n-1)}\,D^n\left(x^{q+n-1}(1-x)^{p+n-q}\right)$. Tu se javljaju dva parametra p, q pa o njihovom izboru zavisi i polinom G_n.

1) Uvjeri se da je $G_0(p, q, x) = 1$, $G_1(p, q, x) = 1 - \binom{1}{1}\dfrac{p+1}{q}\,x$,

$$G_2(p, q, x) = 1 - \binom{2}{1}\frac{p+2}{q}\,x + \binom{2}{2}\frac{(p+2)(p+3)}{q(q+1)}\,x^2,$$

$$G_3(p, q, x) = 1 - \binom{3}{1}\frac{p+3}{q}\,x + \binom{3}{2}\frac{(p+3)(p+4)}{q(q+1)}\,x^2 - \binom{3}{3}\frac{(p+3)(p+4)(p+5)}{q(q+1)(q+2)}\,x^3.$$

2) Hipergeometrijski red glasi: $F(\alpha, \beta, \gamma, x) = 1 + \dfrac{\alpha}{1}\cdot\dfrac{\beta}{\gamma}\,x +$

$$+\frac{\alpha(\alpha+1)}{2!}\cdot\frac{\beta(\beta+1)}{\gamma(\gamma+1)}\,x^2 + \frac{\alpha(\alpha+1)(\alpha+2)}{3!}\cdot\frac{\beta(\beta+1)(\beta+2)}{\gamma(\gamma+1)(\gamma+2)}\,x^3 + \ldots$$

Uvjeri se da je $G_n(p, q, x) = F(p+n, -n, q, x)$.

3) Dokaži da je $X_n(x) = F\left(n+1, -n, 1, \dfrac{1-x}{2}\right)$.

4) Dokaži da je $T_n(x) = \dfrac{1}{2^{n-1}}\,F\left(n, -n, \dfrac{1}{2}, \dfrac{1-x}{2}\right)$.

8. *Hermitovi polinomi* H_n definiraju se ovako: $H_n(x) = (-1)^n\,e^{x^2}\,D^n\,e^{-x^2}$.

1) Njihov niz glasi:

$H_0(x) = 1$, $H_1(x) = 2x$, $H_2(x) = 4x^2 - 2$, $H_3(x) = 8x^3 - 12x$,
$H_4(x) = 16x^4 - 48x^2 + 12$, $H_5(x) = 32x^5 - 160x^3 + 120x$,
$H_6(x) = 64x^6 - 240x^4 + 360x^2 - 120$.

---

[1] C. G. Jacobi (č. Jakobi): Untersuchungen über die Differentialgleichung der hypergeometrischen Reihe — Istraživanja o diferencijalnoj jednadžbi hipergeometrijskog reda — Journal für die reine und angewandte Math. 56 (1859) 149—165; Werke 6, Berlin (1891) 184—202.

2) Vrijedi $D^2 H_n(x) - 2x D H_n(x) + 2n H_n(x) = 0$.

3) $H_{n+1}(x) = 2x H_n(x) - 2n H_{n-1}(x)$ za $n \geqslant 1$.

4) $H_n(x) = \sum_{k=0}^{E\frac{n}{2}} (-1)^k \frac{n!}{k!\,(n-2k)!} \cdot (2x)^{n-2k}$.

Hermite je došao do svojih polinoma 1865.

9. Lagerovi polinomi [1] $L_n(x) = e^x D^n (x^n e^{-x})$.

1) Uvjeri se da je $L_0(x) = 1$, $L_1(x) = -x + 1$, $L_2(x) = x^2 - 4x + 2$,

$L_3(x) = -x^3 + 9x^2 - 18x + 6$, $L_4(x) = x^4 - 16x^3 + 72x^2 - 96x + 24, \ldots$

2) $L_{n+1}(x) = (2n + 1 - x) L_n(x) + n^2 L_{n-1}(x)$ za $n = 1, 2, 3, \ldots$

3) $L_n(x) = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} \binom{n}{k} x^k$.

4) Vrijedi $x D^2 L_n + (1-x) D L_n + n L_n = 0$.

10. *Bernoullijevi brojevi* $B_1, B_2, \ldots$ (Jacob Bernoulli, Ars conjectandi Basel, 1713) definiraju se ovom simboličkom relacijom $(B\downarrow + 1)^n - B_n = 0$ za $n = 2, 3, 4, \ldots$; pri tom $B\downarrow^k \underline{\underline{\text{def}}} B_k$.

1) Dokaži da taj niz glasi: $-\frac{1}{2}, \frac{1}{6}, 0, -\frac{1}{30}, 0, \frac{1}{42}, 0, -\frac{1}{30}, 0, \frac{5}{66}, 0, -\frac{691}{2730}, 0, \frac{7}{6}, \ldots$

Zanimljive su ove formule:

2) $\operatorname{tg} x = \sum_{n=1}^{\infty} (-1)^n \frac{2^{2n}(2^{2n}-1) B_{2n}}{(2n)!} x^{2n-1}$,

3) $\frac{x}{\sin x} = \sum_{n=0}^{\infty} (-1)^{n-1} \frac{(2^{2n}-2) B_{2n}}{(2n)!} x^{2n}$,

4) $\sum_{n=1}^{\infty} \frac{1}{n^{2k}} = (-1)^{k-1} \frac{B_{2k} (2\pi)^{2k}}{2\,(2k)!}$; prema tome

5) $\operatorname{sg} n\, B_{2k} = (-1)^{k-1}$;

6) $\sum_{n=1}^{\infty} \frac{1}{(2n-1)^{2k}} = (-1)^k \frac{2^{2k}-1}{2\,(2k)!} B_{2k} \pi^{2k}$;

---

[1] E. Laguerre (č. Lager), fr. mat., došao je do svojih polinoma 1879. u članku Sur l' intégrale (O integralu) $\int_x^{\infty} \frac{e^{-x} dx}{x}$ (Bull. Soc. math. de France, 7 (1879) 72—81; Oeuvres 1 (1898) 428—437.

7) $(2B\downarrow + 1)^n = (2-2^n)B_n$;

8) $\dfrac{x}{e^x-1} = \sum_{n=0}^{\infty} \dfrac{B_n}{n!} x^n$;

9) Dokaži da su Bernoullijevi brojevi racionalni. Pogledati tablicu Bernoullijevih brojeva u knjizi: D. Mitrinović, *Zbornik matematičkih problema, I*, Beograd 1958_2 XXIV + 352, str. 348.

11. *Eulerovi brojevi* $E_0, E_1, E_2, \ldots$ definiraju se ovim simboličkim jednakostima: $(E\downarrow + 1)^n - (E\downarrow - 1)^n = 0$ za $n = 1, 2, 3, \ldots$ Dokaži da je $E_1 = E_3 = E_5 = \cdots = 0$ i da niz glasi $1, 0, -1, 0, 5, 0, -61, 0, 1385, 0, \ldots$

Vrijedi $1 - \dfrac{1}{3^{2k+1}} + \dfrac{1}{5^{2k+1}} - + \cdots = (-1)^k \dfrac{E_{2k}}{2^{2k+2}(2k)!} \pi^{2k+1}$;

$$(4B\downarrow + 1)^n = (2-2^n)B_n - n E_{n-1}$$

$$(4B\downarrow + 3)^n = (2-2^n)B_n + n E_{n-1}.$$

13. OSNOVNI STAVAK ALGEBRE

13.0. Izgradili smo tijelo R realnih kao i tijelo $R(i)$ kompleksnih brojeva pa nastaje pitanje šta je sa nulištima algebarskih polinoma s koeficijentima iz R, odnosno iz $R(i)$. Svakako, ima jednostavnih algebarskih polinoma nad R npr. $1 + x^2$ bez ikojeg ništišta u R. Šta je s polinomima iz $R(i)[x]$? Na to pitanje odgovor glasi:

13.1. Osnovni stavak algebre.

(i) Svaki algebarski polinom a (x) s koeficijentima iz tijela R realnih brojeva ima neko ništište koje je u tijelu R(i) kompleksnih brojeva.

(ii) Svaki algebarski polinom stepena $n \geq 1$ s koeficijentima iz tijela R ima upravo n ništišta iz R(i), pri čemu je svako ništište brojeno sa svojom kratnošću.

***(iii) Svaki algebarski polinom stepena $n \geq 1$ s koeficijentima iz tijela R(i) kompleksnih brojeva ima upravo n ništišta iz R(i) , pri čemu je svako ništište brojeno svojom kratnošću* (v. 29 § 6.5.).**

Dokaz gornjeg teorema je čisto egzistencijalan, težina je na izreci (*i*), jer izreke (*ii*) i (*iii*) neposredno izviru iz (*i*) (*v.* 7 § 8.2.1 za (*ii*) te 7 § 13.5.3 za (*iii*).

Prethodno ćemo dokazati 3 pomoćna stavka 13.2—13.4.

13.2. Kako se vlada polinom $a(x)$ stupnja ≥ 1 kad $x \to \infty$? Upravo onako kao i pri slučaju $\operatorname{st} a = 1$ ili $\operatorname{st} a = 2$:

Lema. *Ako je* $\operatorname{st} a \geq 1$, *tada*

$$|x| \to \infty \Rightarrow |a(x)| \to \infty.$$

Drugim riječima, za svaki realni broj $M>0$ *postoji realni broj* $r>0$ *(zavisan od* M*), tako da*

$$|x|>r \Rightarrow |a(x)|>M.$$

(Imajmo na umu da skup svih kompleksnih brojeva za koje je $|x|>r$ čine vanjštinu kruga sa središtem u 0 i s radijusom r.)

Dokaz leme. Neka je $\operatorname{st} a=n>0$, tada je

$$a(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n=a_nx^n[a_0a_n^{-1}x^{-n}+a_1a_n^{-1}x^{-n+1}+\cdots$$

$$+a_{n-1}a_n^{-1}x^{-1}+1].$$

Kad $|x|\to\infty$, tada $x^{-k}\to 0$ za svaki prirodni broj k; zato svaki član osim posljednjeg u [ ] teži ka 0, pa zato [ ]$\to 1$; prema tome, kako $|a_nx^n|\to\infty$, također će $|a(x)|\to\infty$ pri $|x|\to\infty$.

13.3. Lema o minimumu. *U svakom krugu* k *ima polinoma* $a|k$ *svoj minimum.*

Dokaz: Posmatrajmo broj

$$b=\inf_x|a(x)| \text{ pri } x\in k.$$

Naravno, b je određen broj, pa se sve svodi na to da dokažemo da funkcija a taj broj hvata pri nekom $x_0\in k$.

Razdijelimo skup k na 4 zatvorena dijela koji imaju istu širinu u smjeru x-osi i istu širinu u smjeru y-osi; neka je k_1 jedan od tih dijelova za koji je $b=\inf_k|a|=\inf_{k_1}|a|$, zatim ćemo iz k_1 na sličan način izvesti k_2 pa onda k_3, k_4,... itd. Zatvoreni skupovi k, k_1, k_2,... stežu se na određen jednočlan skup $\{x_0\}$; naravno $ax_0=b=\inf_{k_n}|a|$ za svako $n\geq 1$.

Nadalje je naravno $x_0\in k$ jer je x_0 član svakog skupa k_n. Tačka x_0 je ono što nam treba: $|a(x_0)|\leq|a(x)|$ za svako $x\in k$.

A sada dolazi odlučan rezultat prema kojemu funkcija $|a|$ svoj minimum ne postiže u središtu c kruga osim ako je slučajno $a(c)=0$.

13.4. D'Alembertova lema. *Ako je* $a(x)$ *polinom stupnja* $n\geq 1$ *pa ako za kompleksni broj* c *vredi* $a(c)\neq 0$, *tada funkcija* $|a|\,|K(c,r)$ *ne može imati minimum u* c. *Šta više, svaki krug* $k(c,\leq r)$ *sadrži neku tačku* c' *unutar toga kruga u kojoj je* $|a(c')|<|a(c)|$.

Poslužit ćemo se Taylorovom formulom (v. 7 § 12.4). Razvijamo polinom a oko tačke c:

$$(1)\qquad a(x)=a(c)+\frac{a'(c)}{1!}(x-c)+\frac{a''(c)}{2!}(x-c)^2+\cdots$$

Neka je

$$a^{(m)}(c)\neq 0,\ a^{(\mu)}(c)=0 \text{ za } \mu\in\{0,1,2,\ldots,m-1\}.$$

Time (1) postaje

$$(2)\qquad a(x)-a(c)=\frac{a'^{m)}(c)}{m!}(x-c)^m+\frac{a^{(m+1)}(c)}{(m+1)!}(x-c)^{m+1}+\cdots,\ \text{tj.}$$

$$(3)\qquad a(x)-a(c)=\frac{'a^{(m)}(c)}{m!}(x-c)^m(1+I),\quad I=\frac{a^{(m+1)}(c)}{(m+1)!}(x-c)+$$

$$+\frac{a^{(m+2)}(c)}{(m+2)}(x-c)^2+\cdots$$

No, broj $x-c$, se može uzeti tako malim po modulu, da modul izraza I bude manji od kojega god realnog broja >0, npr. da bude

$$(5)\qquad |I|<1 \text{ za } |x-c|<r_1 \text{ gdje je } 0<r_1<r.$$

A sad pređimo na procjenu faktora od $(1+I)$ u (3). Jasno je da se realni broj $\delta>0$ može odrediti iz zahtjeva

$$(6)\qquad |a(c)|\,\delta<\left|\frac{1}{m!}a^{(m)}(c)\,r_1^m\right|,$$

jer prema pretpostavci $a(c)\neq 0$.

Nadalje se može zahtijevati da bude

$$(6')\qquad 0<\delta<1$$

jer se broj r_1 u $(5)_2$ može uzeti kako god želimo malim.

Nadalje odredimo kompleksni broj h tako da bude

$$(7)\qquad \frac{h^m a^{(m)}(c)}{m!}=-a(c)\,\delta.$$

To je za h jedna binomska jednačina, pa se h iz (7) lako nađe. No, vidi se da iz (7) i (6) izlazi

$$(8)\qquad |h|<r_1.\ \text{Stavimo } c'=c-h \text{ za takvo } h.$$

Na osnovu obrazaca (8), (7) i (6) daje (3) ovo: $a(c')=a(c)(1-\delta)-$ $-\delta\,a(c)\,I.$

Odatle:

$$|a(c')|\leq|a(c)|(1-\delta)+\delta|a(c)|\cdot|I|<|a(c)|.$$

Odatle izlazi željeni D' Alembertov zaključak $|a(c')|<|a(c)|$.

13.5. Dokaz osnovnog teorema 13.5. (1) Za polinom a posmatrajmo broj $a(0)=a_0$. Ako je $a_0=0$, znači to da je 0 ništište za a pa je teorem ispravan. Preostaje još slučaj $a_0\neq 0$, tj. $a(0)\neq 0$. Tada možemo primijeniti lemu 13.2. za $M=|a(0)|$: postoji broj r sa svojstvom da

$$|x|>r\Rightarrow|a(x)|>|a(0)|.$$

Posmatrajmo zatvoreni krug $k=k(0,\leq r)$ i funkciju $|a|\|k$; prema lemi 13.3 dostiže ona u određenoj tački $x_0 \in k$ svoj minimum. *I upravo taj broj* x_0 *je traženo ništište*, tj. $a(x_0)=0$. Kad bi naime bilo $a(x_0)\neq 0$, bilo bi $|a(x_0)|>0$, pa bi prema D'Alembertovoj lemi postojao broj $x\in k$ za koji bi bilo $|a(x)|<|a(x_0)$ što je u suprotnosti s činjenicom da je $|a(x_0)|$ minimum svih brojeva $|a(x)|$ pri $x \in k$.

Time je osnovni stavak algebre 13.1. (i) potpuno dokazan.

13.5.2. Teorem 13.1. (ii) izlazi iz 13.5. (i) kao što smo to vidjeli u 8.2.

13.5.3. Dokažimo da 13.1. (iii) izlazi iz 13.1. (i).

Neka je $\bar{a}$ polinom koji se iz polinoma a dobije tako da se svako a_k nadomjesti sa $\bar{a}_k$; promatrajmo tada umnožak $q(x)=a(x)\bar{a}(x)$; i $q(x)$ je polinom u x; no njegovi su koeficijenti realni. Stvarno,

$$\bar{q}(x)=\overline{a(x)\bar{a}(x)}=\bar{q}(x)\bar{\bar{a}}(x)=\bar{a}(x)a(x)=a(x).\ \text{Tj.}\ \bar{q}(x)=q(x);$$

a to upravo znači da su koeficijenti od $q(x)$ realni brojevi. Zato prema teoremu 13.1. (i) postoji neki kompleksni broj z za koji je $q(z)=0$, tj. $a\cdot(z)\bar{a}(z)=0$. Odatle slijedi $a(z)=0$ ili $\bar{a}(z)=0$ ili oboje. U prvom i trećem slučaju z zadovoljava $a(z)=0$.

Ako je $\bar{a}(z)=0$, onda je $a(\bar{z})=0$; to izlazi neposredno iz relacije $\overline{\sum a_k z^k}=\sum \bar{a}_k \bar{z}^k$ koja je sa svoje strane poslijedica distributivnosti operatora $x\to\bar{x}$ u odnosu na zbrajanje i množenje.

Prema tome, u svakom slučaju polinom $a(x)$ ima neko kompleksno ništište. Time je na osnovu § 8 i teorem 13.1. (iii) dokazan (v. također 29 § 6.5).

Teorem 13.1. (iii) se izriče i ovako:

Tijelo kompleksnih brojeva je algebarski zatvoreno: pri tom se ima u vidu činjenica da obrazovanje jednadžbi s kompleksnim koeficijentima i rješavanje tih jednačina ne vodi nas van iz ukupnosti kompleksnih brojeva.

Izgleda dosta nevjerovatno da polazeći od tijela R realnih brojeva adjungiranje broja i kao rješenja jednadžbe $x^2+1=0$ dovodi do algebarski zatvorenog tijela $R(i)$. A ipak je to istina!

13.6. Historijat osnovnog teorema algebre. Osnovni teorem algebre kao slutnju izrekao je nizozemski matematičar A. Girard (1595—1632) u djelu *Invention nouvelle en algèbre* (Novi pronalasci u algebri), Amsterdam 1629. Girard je bio pristaša novih Viète-ovih pogleda u algebri. Sama izreka osnovnog teorema ujedno je važan prihvatljiv razlog da se prema kompleksnim brojevima stručnjak odnosi s više obzira. Inače je proteklo skoro dvije stotine godina od Girardove slutnje do njenog dokaza; mnogo je matematičara nastojalo tvrdnju i dokazati (J. d' Alembert 1746, L. Euler 1749, Daviet de Foncenex, Lagrange, 1772); pa i prvi Gaussov dokaz (nađen 1797, a objavljen 1799) ne smatra se potpunim; prvi potpun dokaz smatra se „drugi" Gaussov dokaz iz 1815, godine („treći" Gaussov dokaz potječe iz 1816, a „četvrti" iz 1849). Danas postoji ne samo mnogo dokaza osnovnog teorema nego i mnogo skupina dokaza toga teorema, specijalno postoje razni analitički, te razni funkcijsko-teorijski dokazi.

Inače, danas se „osnovni teorem algebre" ne smatra tako važnom teoremom.

Literatura: Sierpiński [2], Simonart [1], Weber [1].

POGLAVLJE 8.

UVOD U SISTEME LINEARNIH JEDNADŽBI. POJAM RJEŠENJA

1. O OZNACI NEPOZNANICE POMOĆU INDEKSA. POJAM RJEŠENJA

1.1. Razmatrajmo tri nepoznate veličine ili *nepoznanice*; možemo ih označiti, npr., sa x, y, z ili r, s, t, itd. Vrlo je poučno i korisno služiti se pri označavanju šiframa i indeksima. Mi ćemo tri nepoznate veličine označiti sa

$$x_0,\ x_1,\ x_2 \text{ ili sa } x_1,\ x_2,\ x_3, \tag{1}$$

jer će nam onda biti lakše promatrati kad radimo s još više nepoznanica, npr. 10, pa i 100 i više nepoznanica. Njih bismo tada označili sa

$$x_0,\ x_1,\ x_2,\ \ldots,\ x_{n-1}$$

počinjući s indeksom 0, ili sa

$$x_1,\ x_2,\ \ldots,\ x_n$$

počinjući s indeksom 1.

Tako npr. 10 nepoznanicâ bismo označili sa

$$x_0,\ x_1,\ x_2,\ x_3,\ x_4,\ \ldots,\ x_9;$$

tu nam kao indeksi služe brojke ili cifre. Zato se i služimo sa 0 kao indeksom, jer je 0 najosebujniji broj i najosebujnija cifra.

1.2. O oznaci koeficijenata pomoću indeksâ u sređenim jednadžbama. Recimo da imamo tri linearne jednadžbe ili veze za nepoznanice: x_1, x_2, x_3; svaku od tih jednadžbi možemo pretpostaviti u sređenom i odvojenom (separiranom)[1] obliku, pa sistem glasi:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 &= c_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 &= c_2 \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 &= c_3. \end{aligned} \tag{1}$$

[1] Jednadžba je u *separiranom* obliku ako se nepoznanice ne nalaze na objema njenim stranama.

Koeficijenti tih jednadžbi, tj. a-ovi i c-ovi, ne zavise od nepoznanica x_1, x_2, x_3. Pogledajmo kako su koeficijenti označeni pomoću indeksa. U *svakoj* jednadžbi *prvi* indeksi koeficijenata su jednaki, i to:

1 u *prvoj* jednadžbi

2 u *drugoj* jednadžbi

3 u *trećoj* jednadžbi.

Drugi indeks koeficijenta je isti kao *indeks kod nepoznanice* uz taj koeficijent.

Takva oznaka unosi mnogo reda i doprinosi velikoj preglednosti, pogotovu kad razmatramo obimne sisteme jednadžbi (npr. 1000 jednadžbi!).

1.3. O znakovima sumiranja. U sređenom obliku sistema jednadžbi svaki koeficijent ima svoje određeno mjesto. Tako npr. a_{12} je koeficijent u prvoj jednadžbi uz nepoznanicu x_2. Kad bi bila riječ o sistemu od 1000 jednadžbi za x-ove pa kad bi »*rodno*« (*generičko*) ime koeficijenta bilo k, tada bi, npr., $k_{5,17}$ bio koeficijent u jednadžbi oznake 5 a uz nepoznanicu oznake 17, tj. uz x_{17} (kad je riječ o x-ovima kao nepoznanicama). Sam bi sistem glasio:

$$k_{11}x_1 + k_{12}x_2 + \cdots + k_{1\,1000}x_{1000} = c_1$$

$$k_{21}x_1 + k_{22}x_2 + \cdots + k_{2\,1000}x_{1000} = c_2$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$k_{1000\,1}x_1 + k_{1000\,2}x_2 + \cdots + k_{1000\,1000}x_{1000} = c_{1000}.$$

To se piše kraće:

$$\sum_{n=1}^{1000} k_{1\,n}x_n = c_1$$

$$\sum_{n=1}^{1000} k_{2\,n}x_n = c_2$$

$$\cdots\cdots\cdots$$

$$\sum_{n=1}^{1000} k_{1000,\,n}x_n = c_{1000}$$

Ili još kraće:

$$\sum_n x_{s\,n}x_n = c_s, \quad (s, n = 1, 2, \ldots, 1000).$$

Ili, prema Einsteinu, još kraće:

$$x_{sn}x_n = c_s \quad (s, n = 1, 2, \ldots, 1000).$$

Pri tom se zna što sve tu s može biti pa zamišljamo da je tu na lijevoj strani *stavljen znak sumacije u odnosu na indeks koji se u monomu pojavljuje dvaput*.

1.4. Skup In (odnosno $1(n)$) cifara, odnosno prvih n rednih brojeva (koji su pozitivni).

1.4.1. Zapamtimo da za svaki redni broj n simbol In služi kao oznaka za „cifarsku“ množinu svih rednih brojeva koji su manji od n. Nnr.. $I2=\{0, 1\}$, $I10=\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$; za svaki prirodni broj n je

$$In=\{0, 1, 2, \ldots, n-1\}. \text{ Isto tako } 1(n) \overset{\text{Def}}{=} \underbrace{\{1, 2, 3, \ldots\}}_{n}.$$

Iz praktičnih razloga dopustit ćemo da In znači i identičko preslikavanje množine svih rednih brojeva koji su $<n$. Slovo I je početno slovo riječi interval.

1.4.2. $I\omega$ označujemo skup $\{0, 1, 2, 3, 4, \ldots\}$. Neka je $N=\{1, 2, 3, \ldots\}$ množina svih prirodnih brojeva. Po potrebi, $I\omega$ će označivati i identično preslikavanje množine prirodnih brojeva i 0.

1.4.3. Znajmo ovo: prvi ili početni redni broj „nulti“ označujemo cifrom (oznakom) 0; drugi redni broj označujemo cifrom (znakom) 1; treći redni označujemo cifrom (znakom) 2.

Zato je zgodno n i ω nepoznanica po redu označivati sa $x_0, x_1, x_2, \ldots$, tj. počinjući s indeksom 0.

1.5. Primjeri. — **1.5.1.** Kako bi glasio sređen separiran skup od 8 linearnih jednadžbi s 8 nepoznanica t, s koeficijentima nepoznanica m i desnim stranama d? Npr., treća jednadžba glasi ovako:

$$m_{31}\,t_1+m_{32}\,t_2+\cdots+m_{38}\,t_8=d_3 \text{ ili kraće:}$$

$$\sum_{s=1}^{8} m_{3s}\,t_s=d_3.$$

A čitav sistem se odatle dobije kad tu pustimo da znak 3 prođe skupom 1 (8), tj. da najprije 3 znači 1, pa 2, pa zbilja 3, pa 4, pa 5, pa 6, pa 7, i, najzad, 8.

Zbog kraćeg izražavanja, svaku jednadžbu smatramo i sistemom jednadžbi, tj. sistemom od jedne jednadžbe. Tog se dogovora držimo zato da se ono što govorimo o sistemu jednadžbi može primijeniti i na jednu jednadžbu.

1.5.2. U primjeru

$$0=2t_0+3t_1+2t_2+3t_3+2t_4+3t_5+\cdots$$

imamo posla s jednadžbom od „ω nepoznanica“ $t_0, t_1, t_2, \cdots$; tu je riječ o beskonačnom nizu nepoznanica.

1.5.3. U sistemu jednadžbi

$$x_n+(n+1)(n+2)\,x_{n+2}=0 \qquad (n\in I\omega)$$

riječ je o beskonačnom nizu nepoznanica

$$x_0,\ x_1,\ x_2,\ x_3, \ldots.$$

iako u svakoj jednadžbi rednog broja n ulaze samo dvije nepoznanice x_n i x_{n+2}.

1.6. Novo shvatanje nepoznanicâ. Skalarni produkt dvaju nizova.

1.6.1. U jednadžbi

$$2x_1 - 5x_2 + 5x_3 + 8x_4 = 9 \tag{1}$$

pojavljuju se četiri nepoznanice x_1, x_2, x_3, x_4. Umjesto da govorimo o četiri nepoznanice

$$x_1,\ x_2,\ x_3,\ x_4, \tag{2}$$

mnogo je jednostavnije govoriti o nizu ili slijedu (2) kao *jednoj jedinoj nepoznanici*. Označimo li taj niz (2) sa x, tada (1) predstavlja jednadžbu s **jednom** nepoznanicom, koja je po svom karakteru četvoročlan niz. Tako npr. ako je zadano

$$2x - 5y + z = 3$$
$$x + y - z = 2,$$

onda je tu nepoznanica tročlan niz x, y, z — označimo ga sa t — a rješenje je niz $\left[\frac{4}{5}m + \frac{5}{3}, m, \frac{1}{3}\right.$, tj. $t = \left(\frac{4}{3}m, m, \frac{7}{3}m - \frac{1}{3}\right)$, m je proizvoljno; npr. za $m = 0$, dobija se posebno rješenje $\left(\frac{5}{3}, 0, -\frac{1}{3}\right)$, tj. $x = 5/3$, $y = 0$, $z = -\frac{1}{3}$.

1.6.2. Promatrajmo lijevu stranu jednadžbe (1); riječ je o izrazu:

$$2x_1 - 5x_2 + 5x_3 + 8x_4. \tag{3}$$

Koeficijenti tog izraza čine niz:

$$2 \quad -5 \quad 5 \quad 8.$$

Iz toga niza — označimo ga sa a — kao jedne cjeline i iz niza nepoznanica x_1, x_2, x_3, x_4, formira se zadani izraz (3) na vrlo pregledan način: *svaki se član niza a množi odgovarajućim članom niza x i dobiveni produkti zbroje; kaže se da niz a množimo skalarno nizom x;* rezultat označujemo sa $a \circ x$ ili (a, x) ili $a x^T$ ili $x a^T$ [1].

⟶ **1.6.3.** Definicija. *Skalarni produkt* niza f od n članova i niza g s istim brojem članova dobije se tako da se svaki član f_i prvog niza pomnoži *odgovarajućim članom* g_i drugog niza i dobiveni produkti $f_i g_i$ zbroje; skalarni produkt niza f i niza g označuje se sa

$$f \circ g \text{ ili } (f, g) \text{ ili } f g^T \text{ ili } g f^T.$$

$$f \circ g = f_1 g_1 + f_2 g_2 + \cdots = \sum_i f_i g_i.$$

1.6.4. Okomitost. Ako je skalarni produkt dvaju nizova jednak 0, kaže se da su nizovi međusobno *okomiti* ili *ortogonalni*.

1.6.5. Tako npr. neka a označuje niz

$$a_1,\ a_2, \ldots, a_r$$

---

[1] Poslije ćemo vidjeti u kakvoj je vezi a^T sa a i x^T sa x (poglavlje 10, § 5.1).

od r članova a_i; neka sa svoje strane svako to a_i označuje opet neki niz

$$a_{i1}, a_{i2}, \cdots, a_{is},$$

recimo od s članova; neka, najzad, x bude također jedan niz od s članova x_i. Tada možemo promatrati ove skalarne produkte (njih r na broju):

$$\begin{aligned} a_1 \circ x &= a_{11} x_1 + a_{12} x_2 + \cdots + a_{1s} x_s \\ a_2 \circ x &= a_{21} x_1 + a_{22} x_2 + \cdots + a_{2s} x_s \\ &\vdots \\ a_r \circ x &= a_{r1} x_1 + a_{r2} x_2 + \cdots + a_{rs} x_s . \end{aligned}$$

Ako vrijednosti tih skalarnih produkata po redu daju niz c, tj. $c_1, c_2, \cdots c_r$ tada imamo ovaj sistem linearnih jednadžbi:

$$\begin{aligned} a_{11} x_1 + a_{12} x_2 + \cdots + a_{1s} x_s &= c_1 \\ a_{21} x_1 + a_{22} x_2 + \cdots + a_{2s} x_s &= c_2 \\ &\vdots \\ a_{r1} x_1 + a_{r2} x_2 + \cdots + a_{rs} x_s &= c_r . \end{aligned}$$

Čitav se taj sistem može simbolički pisati ovako:

$$a\, x^T = c^T .$$

Pri tom oznake a, x i c imaju prethodno značenje. Koliko je to pojednostavnjenje! No, c^T znači gornji niz zamišljen kao stupac

$$\begin{matrix} c_1 \\ c_2 \\ \vdots \\ c_r , \end{matrix}$$

jer se tako u jednadžbama taj niz pojavljuje.

Uopće, ako je niz y napisan kao *stupac* (redak), onda y^T znači taj isti niz ali zamišljen, odnosno napisan kao *redak* (stupac).

1.7. Skalarni produkt dviju funkcija. Neka su f, g dvije numeričke jednoznačne funkcije koje su definirane u istoj oblasti O; to znači da za svako $t \in O$ imamo brojeve $f(t)$, $g(t)$; time je određen i broj $f(t) \cdot g(t)$. U jednostavnijim slučajevima ima smisla govoriti i o sumi svih produkata $f(t)g(t)$ kada t prolazi kroz O. Ta se suma zove *skalarni produkt* od f i g i označuje se sa (f, g) ili $f \circ g$, pa i sa fg. Mi ćemo ga označivati sa $f \circ g$ jer nas taj znak o posjeća i na množenje i na početno slovo riječi „*skalar*".

Npr., skalarni produkt od dviju funkcija f, g koje su definirane u intervalu $[a, b]$ realnih brojeva označuje se i sa $\int_a^b f(t)\, g(t)\, dt$. Skalarni produkt funkcija je od osnovne važnosti. Mi ćemo se u ovoj knjizi baviti skalarnim produktima nizova[1]. Skalarno množenje pojavljuje se u matematici neprestano.

[1]) Skalarni produkt dvaju nizova je poseban slučaj skalarnog produkta dviju funkcija — slučaj kad je oblast O skup N prirodnih brojeva ili njegov dio, odnosno kad je O prebrojiv skup.

1.8. Zadaci o linearnim sistemima jednadžbi.

1. Označi pomoću Σ zbroj od 1) prvih; 2) drugih sto prirodnih brojeva; kolik je taj zbroj?

2. 1) Nađi $\sum_{n=1}^{k}(2n-1)!$; 2) $\sum_{n=1}^{k} n^2 = ?$

3. Nađi skalarni produkt $a \circ b$ ovih nizova a, b:
1) $(3, -2, 5)$, $(-2, 5, -4)$; 2) $(1, 2, 3, 4)$, (x^1, x^2, x^3, x^4);
3) (a, b, c), (a, b, c); 4) $(1, 2, 1, 2, 1, 2, \ldots)$, $(10^{-1}, 10^{-2}, 10^{-3}, 10^{-4}, \ldots)$;
5) $1, 2, 1, 2, \ldots)$, $(10^3, 10^2, 10^1, 10^0, 10^{-1}, 10^{-2}, \ldots)$.

4. Napiši 3 linearne jednadžbe s 5 nepoznanica; neka koeficijenti nose rodno ime a, desne strane c, a nepoznanice t; neka indeksi počinju s 1) 0, 2) 1, 3) 6.

5. Koliko ima uređenih parova (a, b) nizova $a = a_1, a_2, a_3$; $b = b_1, b_2, b_3$ cijelih brojeva ≥ 0 tako da bude $a \circ b = 10$.

6. Promatraj skup jednadžbi $f_{n+1} = f_{n-1} + f_n$ za $n = 2, 3, 4$; o koliko se jednadžbi tu radi? 1) Odredi Fibonačijev (Fibonacci) niz $f_1, f_2, f_3, \ldots$ tako da bude $f_1 = f_2 - 1$; 2) nađi f_{10}; 3) dokaži da je

$$f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right] \text{ (Binet).}$$

7. Napiši sistem jednadžbi u kojem je jednadžba $2x + 3y + 4z = 5$, a zatvoren je s obzirom na cikličku zamjenu nepoznanica.

8. Da li niz $2, -3, 5, -1$, zadovoljava bar jednu od ovih jednadžbi:

$$\begin{aligned} 2x - 3y + 4z - 5u &= 24 \\ x + y - z - u &= 0 \\ -3x - 5y - 4z - 2u &= 9 \\ x - 2y - 3z - 4u &= 1 \\ -5x - y - 4z - 3u &= 6. \end{aligned}$$

9. Da li je niz $a = 2, -3, 4, -1$ okomit na nizu $b = 5, -2, 4, 7$? Šta treba pisati umjesto 7 pa da bude $a \circ b = 0$?

10. Napiši i riješi još koji zadatak poput prethodnih!

2. POJAM RJEŠENJA I MNOŽINE SVIH RJEŠENJA. RJEŠAVANJE LINEARNIH SISTEMA JEDNADŽBI

2.1. Definicija. *Pod rješenjem zadanog sistema S jednadžbi sa n nepoznanica*

$$x_1, \ldots x_{n-1}, x_n$$

razumijevamo ***svaki*** *niz od n veličina koji, uvršten umjesto traženog niza x, zadovoljava* ***svaku*** *jednadžbu iz skupa S.* Specijalno, ako je nepoznanica jedna, tada se pod rješenjem razumijeva svaka veličina koja zadovoljava zadanu jednadžbu, odnosno zadane jednadžbe.

Tako npr. jednadžba $5x=4$ ima rješenje 4/5, tj. 0,8. Jednadžba $x^2=x$ ima brojeve 0 i 1 kao rješenje. Beskonačni skup jednadžbi

$$x_n+(n+1)(n+2)x_{n+2}=0 \qquad (n=0, 1, 2, \ldots)$$

ima kao rješenje sve nizove oblika:

$$(*) \quad x_0, x_1, -\frac{1}{2!}x_0, \frac{1}{3!}x_1, \frac{1}{4!}x_0, \frac{1}{5!}x_1, -\frac{1}{6!}x_0, -\frac{1}{7!}x_1, +, +, -, -, \ldots$$

Pri tom su x_0, x_1 *proizvoljni brojevi* ili *brojevni izrazi.* Naime, gornji sistem jednadžbi možemo pisati i u obliku:

$$x_{n+2}=-\frac{1}{(n+1)(n+2)}x_n, \qquad (n=0, 1, 2, \ldots$$

Stavimo li tu za n po redu 0, 1, 2, 3, . . . , izlaze osim x_0, x_1 svi članovi u nizu (*); x_0 i x_1 su neodređeni.

2.2. Skup *r S* svih rješenja sistema *S*. To je skup ili množina svih rješenja sistema S. Tako npr. $r(x^2=1)=\{-1, 1\}$.

2.3. Oprez! Pri pridruživanju $S \to rS$ treba imati na umu oblast i narav traženih rješenja. Jedino tada je rS određeno. Tako npr. ako S označuje jednadžbu $ff=1$, tada rS znači dvočlani skup $\{-1, 1\}$, jer pretpostavljamo da radimo s realnim ili kompleksnim brojevima. Međutim, radimo li samo s pozitivnim brojevima (kao što su, npr. radili stari Grci), onda bi rS bilo sastavljeno jedino od broja 1.

U današnjoj matematici, u kojoj je pojam strukture (skup i preslikavanje) osnovni pojam (i u kojoj obično s 1 označujemo identičko preslikavanje, a ff označuje: izvesti preslikavanje f pa na rezultatu opet izvesti preslikavanje f), ima jednakost $ff=1$ vrlo mnogo drugih rješenja. Tako npr. u skupu $\{a, b, c\}$! permutacijâ od a, b, c zadovoljavaju tu jednakost ove permutacije:

abc, acb, cba, bac.

2.4. Ekvivalentne ili ravnovažne jednadžbe. D e f i n i c i j a. Dva sistema jednadžbi S, S' međusobno su ekvivalentna ili *ravnopravna* ako imaju *ista rješenja,* tj. ako je

$$rS=rS'$$

te ako svako rješenje ima istu kratnost u S i u S' (isp. pogl. 5, § 11).

To znači da svako rješenje sistema S zadovoljava i sistem S', i obrnuto: svako rješenje sistema S' zadovoljava i sistem S i to s istom kratnosti.

2.5. Metoda protivno-jednakih koeficijenata pri rješavanju linearnih jednadžbi. Primjer:

$$\begin{array}{ll} (1) & 4x-5y=7 \mid \cdot -3 \\ (2) & \underline{6x+2y=4 \mid \cdot \ \ 2} \\ (3) & 0\cdot x+19y=-13 \\ & y=-13/19=-0{,}69. \end{array}$$

Riječ je o tome da se iz zadanog sistema *ukloni* (*eliminira*) koja nepoznanica. Po metodi *protivno-jednakih koeficijenata* to se radi tako da se dvije jednadžbe pomnože zgodnim izrazima $\neq 0$, tako da u novim dvjema jednadžbama jedna nepoznanica ima koeficijente koji su međusobno protivno-jednaki. Zatim se te dvije nove jednadžbe zbroje (saberu). Ta nova jednadžba može da zamijeni jednu od onih dviju jednadžbi iz kojih je nastala. Tako npr. u gornjem primjeru nova jednadžba (3) može da zamijeni jednadžbu (2), pa tako umjesto sistema zadanih jednadžbi (1), (2) imamo ekvivalentan sistem jednadžbi (1) i (3). No, ovaj novi sistem je lakše rijcšiti jer iz jednadžbe (3) izlazi $y=-13/19=-0{,}69$, što uvršteno u (1) daje $x=51/57=0{,}89$. Na taj način rješenje zadanih jednadžbi glasi:

$$x=51/57 \quad , \quad y=-13/19,$$

odnosno na 2 decimale:

$$x=\ 0{,}89 \quad , \quad y=-0{,}69.$$

Pokus:

$$\begin{array}{l} 4\cdot 51/57-5\cdot(-13/19)=7 \mid \cdot 57 \\ \underline{6\cdot 51/57+2\cdot(-13/19)=4 \mid \cdot 57} \\ 204+195=399 \qquad 399=399 \end{array}$$

, tj.

$$306-\ 78=228 \qquad 228=228.$$

Napravimo pokus za $x=0{,}89$ i $y=-0{,}69$:

$$\begin{array}{ll} 4\cdot 0{,}86-5\cdot(-0{,}69)=7 & 3{,}56+3{,}45=7 \\ \underline{6\cdot 0{,}89+2\cdot(-0{,}69)=3} & \underline{5{,}34-1{,}38=4} \\ & 7{,}01 \doteq 7 \\ & 3{,}96 \doteq 4 \end{array}$$

A to je tačno na 1 decimalu.

Pri rješavanju sistema jednadžbi s više nepoznanica pazimo na to da, uklanjajući jednu nepoznanicu, dobijemo za preostale nepoznanice pogodnije jednadžbe.

2.6. Topovski ili *T*-postupak eliminiranja. Objasnimo stvar na primjeru. —

2.6.0. Primjer. Riješi jednadžbe

$$(1)\qquad \left\{\begin{array}{rrrrr|l} 3x_1 + 5x_2 & \boxed{-\ x_3} & -2x_4 = & 11 & \Big] \cdot -1 \\ 2x_1 + 4x_2 & - x_3 & + x_4 = & 8 & \Big] \cdot 1 \\ 4x_1 - x_2 & + x_3 & = & -24 & \Big] \cdot -2 \\ 5x_1 + 3x_2 & -2x_3 & + x_4 = & -13. & \end{array}\right.$$

U prvoj jednadžbi sistema (1) izabrali smo nalijevo član $-x_3$ (top ili tvrđava) i pomoću toga „topa" poništili sve odgovarajuće članove „ispod" njega. Time izlazi sistem (2) pa ćemo u prvoj narednoj jednadžbi izabrati top itd. (topove uokružujemo ili uokvirujemo).

$$-1 \cdot \Big[\cdot 7 \Big[\begin{array}{rrrrr} \boxed{-x_1} & - x_2 & + 3x_4 = & -3 & \\ 7x_1 & +4x_2 & - 2x_4 = & -13 & \\ -x_1 & -7x_2 & - 5x_4 = & -35 & \end{array}$$

$$\begin{array}{rrrr|l} \boxed{-3x_2} & +19x_4 = & -34 & \cdot -2 & \\ -6x_2 & - 8x_4 = & -32 & \cdot 1 & + \\ \hline \boxed{-46x_4} & = & 46 & & \end{array}$$

I sada se ide natrag rješavajući unatrag *markirane* jednadžbe. Izlazi po redu: $x_4 = -1$, $x_2 = 5$, $x_1 = -5$, $x_3 = 1$.

Sad zadani sistem (1) ima isto rješenje (ekvivalentan je s jednadžbama u kojima su naznačeni „topovi"), i pripadni („topovski") sistem glasi:

$$\begin{array}{rrrrr} 3x_1 + 5x_2 & -x_3 & - 2x_4 = & 11 \\ -x_1 - & x_2 & + 2x_4 = & -3 \\ & -3x_2 & + 19x_4 = & -34 \\ & & -46x_4 = & 46. \end{array}$$

2.6.1. Primjedba. *T-postupak eliminiranja* pratit će nas neprestano, specijalno u računu s »*matricama*« ili *tablicama*. Imajmo na umu kako u šahovskoj igri djeluje top ili tvrđava: u horizontalnim i vertikalnim linijama. Poslije će i naš „top" tako djelovati.

2.6.2. Zlatno pravilo o linearnim jednadžbama. U toku izlaganja u ovoj knjizi uvjerit ćemo se da je rješavanje linearnih jednadžbi putem eliminiranja vanredno zgodna i sigurna metoda. Specijalno, T-postupak i Gaussov postupak, što ćemo ga opisati u narednom paragrafu, daju sve što je bitno za jedan sistem linearnih jednadžbi. Ostale metode (npr. pomoću determinanata) mogu dati bolji *formalni* uvid u gradnju rješenja i omogućiti da se traženo rješenje *formalno* izrazi na vrlo pregledan način. Posebno, naglašujemo ovo: kao što,

npr., linearna jednadžba $0x=2$ očigledno nema rješenja, tako se i pitanje da li zadan linearni sistem ima ili nema rješenja svodi putem eliminacije na slično pitanje: *ako nas eliminacije ne dovedu do apsurda* $0=top$, *znak je to da je rješenje linearnog sistema osigurano i da je to baš ono koje smo usput dobili ili ga već gotovo dobili.*

Dokaz gornjih tvrdnji iznijet ćemo u poglavlju 15. o rangu matrica.

2.7. Gaussov postupak pri rješavanju linearnih jednadžbi s *numeričkim koeficijentima*. Gaussov postupak je specijalan slučaj metode protivnojednakih koeficijenata.

Inače, možemo pretpostaviti da radimo sa sređenim sistemom linearnih jednadžbi.

2.7.1. *Kod Gaussova postupka je važno da u zadanom sistemu S jednadžbi odaberemo* ***jednu jedinu jednadžbu — vodeću jednadžbu*** i u njoj određenu **nepoznanicu**, odnosno ***vodeći član.*** Pred vodeću jednadžbu stavimo zvjezdicu da je lakše i bolje vidimo. Vodeći član u vodećoj jednadžbi markiramo također, npr. tako da ga uokružimo, podvučemo, uokvirimo i sl. Vodeću nepoznanicu ćemo eliminirati tako da primijenimo metodu protivno-jednakih koeficijenata, i to sparujući tu vodeću jednadžbu i **svaku** ostalu jednadžbu sistema.

Na tako dobiveni sistem jednadžbi primjenjuje se opet isti postupak, itd. do kraja.

2.7.2. *Rješenja sistema S' tako dobivenih »vodećih jednadžbi« podudaraju se s rješenjima polaznog sistema S.*

2.7.3. Izbor vodeće jednadžbe i vodeće nepoznanice. Izbor se vrši prema karakteru samog sistema jednadžbi. U praksi se obično radi ovako:

a) Uoči se ona nepoznanica x_k uz koju stoji koeficijent *najveće apsolutne* vrijednosti.

b) Zatim se ona, odnosno jedna jednadžba u kojoj dotični član dolazi, proglasi za vodeću; neka je to jednadžba *i*.

c) Ta se vodeća jednadžba *i* pomnoži recipročnom vrijednošću *»vodećeg koeficijenta«*; dakle se jednadžba *i* pomnoži sa a_{ik}^{-1}; time se dobije jednadžba *J*.

d) Zatim se ta nova jednadžba *J* pomnoži, za svaku jednadžbu $j \neq i$, koeficijentom — a_{jk} od x_k u jednadžbi *j* i napravi suma te nove jednadžbe i jednadžbe *J*.

Time se dobije novi sistem jednadžbi s nepoznanicama bez x_k u svima jednadžbama osim u jednoj. Na taj novi sistem primjenjuje se opet isti postupak: izabere se u njemu vodeća jednadžba i vodeća nepoznanica...

2.7.4. Zbirna kontrola. U praksi se uz svaku zadanu jednadžbu sistema nadopisuje u *poseban stupac* još i *suma svih njenih koeficijenata, pa se s tim sumama radi isto što i sa članovima dotične jednadžbe;* u svakoj novoj jednadžbi

koja se pri postupku dobije mora suma njenih koeficijenata biti jednaka broju koji se Gaussovim postupkom dobio na tom mjestu.

2.7.5. Važan slučaj iz prakse. Često se ima posla sa skupovima po n jednadžbi po n nepoznanica, no da *koeficijenti pri nepoznanicama ostaju isti: mijenjaju se samo desne strane. Time se podaci o rješavanju jednoga takvog sistema mogu upotrijebiti i za druge sisteme: ostaje sve isto osim onog dijela što se odnosi na desne strane.*

2.7.6. *Specijalno je važan slučaj kad su desne strane* »***jedinični nizovi***«, tj. nizovi sastavljeni od samih 0 osim jedne jedine 1. Ako je, npr., riječ o tri jednadžbe s tri nepoznanice, desne strane bi po redu bile:

$$\begin{matrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{matrix}$$ (ovo čitaj po stupcima!).

Pripadna su rješenja u vrlo pravilnoj vezi s rasporedom koeficijenata nepoznanicâ (isp. izračunavanje inverzne matrice a^{-1} zadane matrice a; poglavlje 12; § 5).

2.8. Zadaci o numeričkom rješavanju linearnih jednadžbi.

1. Primijeni topovski postupak i riješi ove jednadžbe; provedi zbirnu kontrolu i pokus.

1) $$\begin{aligned}-2x+3y+4z&=-8\\ 2x-3y+4z&=-16\\ 2x+3y-4z&=20.\end{aligned}$$

2) $$\begin{aligned}3x+5y+4z&=0\\ -6x-2y+5z&=1\\ 7x+y-9z&=-2.\end{aligned}$$

3) $$\begin{aligned}3x_1+2x_2+3x_3+x_4&=-29\\ -x_1+2x_2-3x_3+2x_4&=-2\\ 2x_1-4x_2+x_3-5x_4&=29\\ x_1+3x_2-x_3-x_4&=-2.\end{aligned}$$

4) $$\begin{aligned}3x-0{,}2y+0{,}03z&=4\\ 6x+3{,}5y+4{,}1z&=2{,}3\\ 8x-12y+0{,}4z&=6.\end{aligned}$$

5) $$\begin{aligned}x_1+x_2+x_3+x_4&=5\\ x_1-x_2-x_3+x_4&=3\\ 2x_1-3x_2-4x_3+5x_4&=-12\\ x_1+x_2-x_3+2x_4&=5\end{aligned}$$

6) $$\begin{aligned}5x-4y+3z+u&=-8\\ 2x-3y-z&=-1\\ 9x+7y-2u&=-9\\ -x+4y+z+3u&=0.\end{aligned}$$

7) $$\begin{aligned}2x_1+3x_2-x_3+5x_4&=2\\ 3x_1-x_2+2x_3-7x_4&=3\\ 4x_1+x_2-3x_3+6x_4&=4\\ x_1-2x_2+x_3-6x_4&=1.\end{aligned}$$

8) $$\begin{aligned}3a+4b-c-3d&=-1\\ a-b+2c-3d&=0\\ a+3b+c+d&=0\\ a+b+c+d&=0.\end{aligned}$$

9) $\begin{aligned} 3u_1+4u_2-\ u_3-3u_4&=-1\\ u_1-\ u_2+2u_3-3u_4&=\ 0\\ u_1+3u_2+\ u_3+\ u_4&=\ 0\\ u_1+\ u_2+\ u_3+\ u_4&=\ 0 \end{aligned}$

10) $\begin{aligned} x_1+x_2+\cdots+x_n&=1\\ x_1+x_3+x_4+\cdots+x_n&=2\\ x_1+x_2+x_4+\cdots+x_n&=3\\ &\cdots\cdots\cdots\\ x_1+x_2+\cdots x_{n-1}&=n. \end{aligned}$

2. Riješi ove skupove jednadžbi stavljajući na desnu stranu sve moguće odgovarajuće jedinične normirane vektore tj. jedinične nizove:

1) $\begin{aligned} 2x-3y&=1\ \big|\ 0\\ 5x-\ y&=0\ \big|\ 1 \end{aligned}$

2) $\begin{aligned} 3x+5y-\ 4z&=\\ 2x-3y+\ z&=\\ 6x+\ y-14z&= \end{aligned}$

3) $\begin{aligned} a-3b+4c-2d&=\\ -2a+\ b-2c+\ d&=\\ 3a-2b+5c-2d&=\\ -4a+\ b+2c+3d&= \end{aligned}$

Literatura: Faddejev-Faddejeva [1], Faddejev-Sominskij [1], Greub [1], Lichnerowicz [1], Mal'cev [1], Mitrinović-Mihailović [1], van der Waerden [1].

POGLAVLJE 9.

SISTEM LINEARNIH JEDNADŽBI S OPĆIM KOEFICIJENTIMA. POJAVA DETERMINANTE

1. DVIJE LINEARNE JEDNADŽBE. DETERMINANTE STUPNJA (2,2)

1.1. Neka za nepoznate vcličine x, y vrijedi:

$$\begin{array}{l} ax + by = c \\ a'x + b'y = c' \end{array} \quad \begin{array}{l|} \cdot b' \\ \cdot -b \end{array} + \begin{array}{l|} \cdot -a' \\ \cdot a \end{array} + \tag{1}$$

Pri tom su a, b, c, a', b', c' brojevi ili brojevni izrazi.

Pomnožimo prvu jednadžbu sa b', odnosno $-a'$, te drugu jednadžbu sa $-b$, odnosno a, i zbrojimo dobivene jednadžbe (taj smo posao naznačili u (1) simbolički s onim što smo pripisali desno od c-ova).

Dobijemo ove dvije jednadžbe:

$$\begin{aligned} (ab' - a'b)\,x &= b'c - bc' \\ (ab' - a'b)\,y &= ac' - a'c. \end{aligned} \tag{2}$$

1.2. Sistem (2) je *naročito jednostavno i pregledno građen;* naime;

1) *u svakoj jednadžbi sistema* (2) *dolazi jedna jedina od napisanih nepoznanica polaznog sistema* (1);

2) *koeficijent od svake nepoznanice u* (2) *je jedan te isti izraz naročito pravilno građen od koeficijenata svih nepoznanica u* (1);

(3) *i desna strana u novom sistemu* (2) *ima sličnu građu* (*strukturu*) kao i koeficijent nepoznanica u (2); ta se struktura sàstoji u tom da se radi *o razlici dvaju produkata po dva faktora.*

1.3. Definicija. Izraz $ab' - a'b$ zovemo *determinantom* ili *opredjeliteljem jednadžbi* (1) ili *pravokutne tablice*

$$\begin{matrix} a & b \\ a' & b' \end{matrix}$$

i ta se determinanta označuje sa

$$\det \begin{matrix} a & b \\ a' & b' \end{matrix} \quad \text{ili} \quad \det \begin{bmatrix} a & b \\ a' & b' \end{bmatrix} \quad \text{ili} \quad D \begin{matrix} a & b \\ a' & b' \end{matrix} \quad \text{ili} \quad \begin{vmatrix} a & b \\ a' & b' \end{vmatrix};$$

tj. oznaka determinante dobije se iz oznaka tablice tako da se pred tablicu stavi det ili D ili da se tablica stavi u *uspravne zagrade*. Prema tome

$$\begin{vmatrix} a & b \\ a' & b' \end{vmatrix} = ab' - a'b. \tag{3}$$

Smisao te definicione jednakosti sastoji se u tome da se *jedna strana jednakosti* (3) *može svuda zamijeniti drugom stranom te jednakosti* (3). Tako npr.

$$\begin{vmatrix} 2 & 7 \\ 3 & 10 \end{vmatrix} = 2 \cdot 10 - 7 \cdot 3 = -1$$

$$\begin{vmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{vmatrix} = \cos^2 x + \sin^2 x \,(=1)$$

$$2 \cdot 5 - 4 \cdot 6 = \begin{vmatrix} 2 & 4 \\ 6 & 5 \end{vmatrix} \text{ itd.}$$

1.4. Koeficijenti nepoznanica tvore »*tablicu koeficijenata*« pa se zovu *elementi* ili *članovi* ili *koordinate* ili *komponente te tablice*. Radi preglednosti, običaj je da se tablica stavi u *uglaste zagrade*. Ako tablicu koeficijenata proširimo i „stupcem“ ostalih koeficijenata jednadžbe, dobije se »*proširena tablica*« zadanog sistema jednadžbi (1); ona glasi:

$$\begin{matrix} a & b & c \\ a' & b' & c' \end{matrix} \text{ odnosno } \begin{bmatrix} a & b & c \\ a' & b' & c' \end{bmatrix}. \tag{4}$$

1.5. Réci ili redići, stupci i dijagonale pravokutnih tablica. Govori se o *prvom retku* ili *drugom* retku te tablice (4) ili kakve druge tablice. Specijalno u tablici

$$\begin{matrix} a & b \\ a' & b' \end{matrix}$$

koeficijenata nepoznanicâ jednadžbi (1) prvi redak ili prvi redić glasi $a\ b$; drugi redak glasi $a'\ b'$; prvi stubac je a; drugi stupac je b. Glavna dijagonala je $\begin{matrix} a \\ a' \end{matrix}$ $\begin{matrix} \\ b' \end{matrix}$, odnosno $a\ b'$; ona počinje lijevo gore. Sporedna dijagonala je $\begin{matrix} b \\ b' \end{matrix}$ $\begin{matrix} \\ a' \end{matrix}$, odnosno $b\ a'$, jer čitamo i pišemo najprije ono što je u gornjem retku pa onda ono što je u narednom retku. Sporedna dijagonala počinje desno gore.

1.6. *Retke numeriramo rednim brojevima* 0, 1, 2. . . . ili *prirodnim brojevima* 1, 2. . . . *odozgo prema dolje; stupce numeriramo slično, i to od lijeve strane prema desnoj strani.* Tako se govori o prvom retku, drugom retku itd. Isto vrijedi i za stupce: prvi stupac, odnosno po redu prvi stupac, drugi stupac itd.

Npr. u pravokutnoj tablici

3	4	5	redak prvi
−1	3	2	redak drugi
4	1	8	redak treći

redak drugi glasi −1 3 2.

Glavna „dijagonala“ je 3 3 8; a sporedna dijagonala je 5 3 4. „Sjecište“ ili „polje“ (1, 1) je zauzeto sa 3; ono drugo 3 leži u sjecištu (2, 2). Dijagonala koja završava dolje desno glasi 3 3 8; a ona koja završava dolje lijevo glasi 5 3 4.

1.7. Oblast (domen) ili **stupanj tablice.** Ako pravokutna tablica t ima r redaka i s stupaca, kaže se da je ona oblasti, ili poretka ili stupnja $r \times s$ ili potpunije $1(r) \times 1(s)$ i piše $\mathrm{Dom}\, t = r \times s$ ili potpunije $\mathrm{Dom}\, t = 1(r) \times 1(s)$; sjetimo se da $1(r) = \underbrace{\{1, 2, \ldots\}}_{r}$.

Umjesto $r \times s$ možemo pisati (r, s) odnosno $(1(r), 1(s))$.

1.8. Definicija determinante za tablicu stupnja 2×2. *Determinanta* ili *opredjelitelj pravokutne* — zapravo kvadratne — *tablice* stupnja 2×2 jest razlika produkta elemenata u tablici na glavnoj dijagonali i produkta onih elemenata koji su na sporednoj dijagonali.

Npr. $c = \begin{vmatrix} c & 1 \\ 0 & 1 \end{vmatrix}$ za svaki izraz c; $0 = \begin{vmatrix} 0 & 0 \\ 0 & 0 \end{vmatrix}$ čak je $0 = \begin{vmatrix} m & n \\ 0 & 0 \end{vmatrix}$

za bilo kakve brojevne izraze m, n.

1.9. Upotreba pojma i oznake za determinante. Smisao gornje definicije i oznake gornje determinante sastoji se u tome da se na pregledan način vidi veza između determinante i njenih elemenata prema ulozi koju ti elementi imaju. Ta će se ideja vidjeti osobito kasnije, kad nam pod ruku dođu determinante s mnogo više elemenata.

1.10. ***Cramerov teorem*** (*u specijalnom slučaju*) *glasi ovako*:

Iz

$$ax + by = c$$

$$a'x + b'y = c'$$

izlazi

$$\begin{vmatrix} a & b \\ a' & b' \end{vmatrix} x = \begin{vmatrix} c & b \\ c' & b' \end{vmatrix}$$

$$\begin{vmatrix} a & b \\ a' & b' \end{vmatrix} y = \begin{vmatrix} a & c \\ a' & c' \end{vmatrix}.$$

Riječima: *iz zadanog sistema jednadžbi* (1) *izlazi drugi sistem, koji je građen ovako*: *svaku nepoznanicu sistema* (1) *pomnožimo determinantom sistema* (1) *i napišemo da je taj produkt jednak determinanti koja iz determinante zadanog*

sistema (1) *izlazi tako da u njoj stupac koji odgovara dotičnoj nepoznanici zamjenimo onim što stoji na desnoj strani sistema* (1).

1.11. Cramerov teorem. *Vrlo je plodna naučna tekovina da taj izraz vrijedi ne samo za linearan sistem od 2 jednadžbe s 2 nepoznanice nego za svaki konačan linearan sistem koji ima toliko jednadžbi koliko ima nepoznanica. To je tzv. Cramerov teorem*[1] (za dokaz vidi pogl. 11 teor. 7.9.2. i 12, § 2.1.2).

1.11.1. Tako npr. iz

$$(1)\qquad \begin{aligned} 3x+5y&=-4\\ 2x-7y&=\ \ 3 \end{aligned}$$

izlazi odmah $$\begin{vmatrix} 3 & 5\\ 2 & -7 \end{vmatrix} x = \begin{vmatrix} -4 & 5\\ 3 & -7 \end{vmatrix},$$

tj. $$(-21-10)\,x = 28-15, \quad \text{tj.} \quad -31\,x = 13,$$

dakle $$x = -13/31 = -0{,}4\ldots$$

Slično $$-31\,y = \begin{vmatrix} 3 & -4\\ 2 & 3 \end{vmatrix}, \quad \text{tj.} \quad -31\,y = 17, \quad \text{tj.} \quad y = -17/31.$$

1.11.2. Iz jednadžbi

$$(1)\qquad \begin{cases} 2x+5y-4z=2\\ \ \ x-2y+\ \ z=5\\ 4x+5y-7z=0 \end{cases}$$

izlazi

$$(2)\qquad \begin{vmatrix} 2 & 5 & -4\\ 1 & -2 & 1\\ 4 & 5 & -7 \end{vmatrix} x = \begin{vmatrix} 2 & 5 & -4\\ 5 & -2 & 1\\ 0 & 5 & -7 \end{vmatrix}$$

$$(3)\qquad \begin{vmatrix} 2 & 5 & -4\\ 1 & -2 & 1\\ 4 & 5 & -7 \end{vmatrix} y = \begin{vmatrix} 2 & 2 & -4\\ 1 & 5 & 1\\ 4 & 0 & -7 \end{vmatrix}$$

$$(4)\qquad \begin{vmatrix} 2 & 5 & -4\\ 1 & -2 & 1\\ 4 & 5 & -7 \end{vmatrix} z = \begin{vmatrix} 2 & 5 & 2\\ 1 & -2 & 5\\ 4 & 5 & 0 \end{vmatrix}$$

---

[1] Gabriel Cramer [Kramer] (1704—1752): *Introduction à l' analyse des lignes courbes algébriques*, Genève 1790. (*Uvod u analizu algebarskih krivulja*). Tim djelom uvedene su determinante u naučnu literaturu.

1.11.3. Općenito (za dokaz vidi pogl. 11, 7.9.2.), ako imamo n nepoznatih veličina

$$x_1,\ x_2,\ \cdots,\ x_n$$

i n jednadžbi oblika[1)]

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= c_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= c_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots & \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &= c_n, \end{aligned} \tag{5}$$

tada je

$$\begin{vmatrix} a_{11}\,a_{12}\cdots a_{1n} \\ \cdots\cdots\cdots \\ a_{n1}\,a_{n2}\cdots a_{nn} \end{vmatrix} x_1 = \begin{vmatrix} c_1 & \text{Sve drugo} \\ \vdots & \text{ostaje} \\ c_n & \end{vmatrix}$$

$$\begin{vmatrix} a_{11}\cdots a_{1n} \\ \cdots\cdots\cdots \\ a_{n1}\cdots a_{nn} \end{vmatrix} x_2 = \begin{vmatrix} a_{11} & c_1 & a_{13}\cdots \\ \vdots & \vdots & \vdots \\ a_{n1} & c_n & a_{n3}\cdots \end{vmatrix}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\begin{vmatrix} a_{11}\cdots a_{1n} \\ \cdots\cdots\cdots \\ a_{n1}\cdots a_{nn} \end{vmatrix} x_n = \begin{vmatrix} a_{11}\cdots a_{1,n-1} & c_1 \\ \vdots\ \cdots\ \vdots & \vdots \\ a_{n1}\cdots a_{n,n-1} & c_n \end{vmatrix}.$$

Samo nastaje pitanje: što zapravo znači determinanta sistema linearnih jednadžbi (5) kad u njemu ima 3 ili više nepoznanica, tj. kad je $n \geq 3$?

Tako npr. šta bi značila determinanta trećeg stupnja:

$$?= \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = ?$$

1.12. Geometrijsko značenje determinante. Pogledajmo šta geometrijski zapravo znači determinanta

$$\begin{vmatrix} a & b \\ a & b' \end{vmatrix} = ab' - a'b.$$

Radimo u koordinatnoj ravnini. Svaki **stupac** koeficijenata sistema naših jednadžbi određuje jednu tačku; tako imamo tačke:

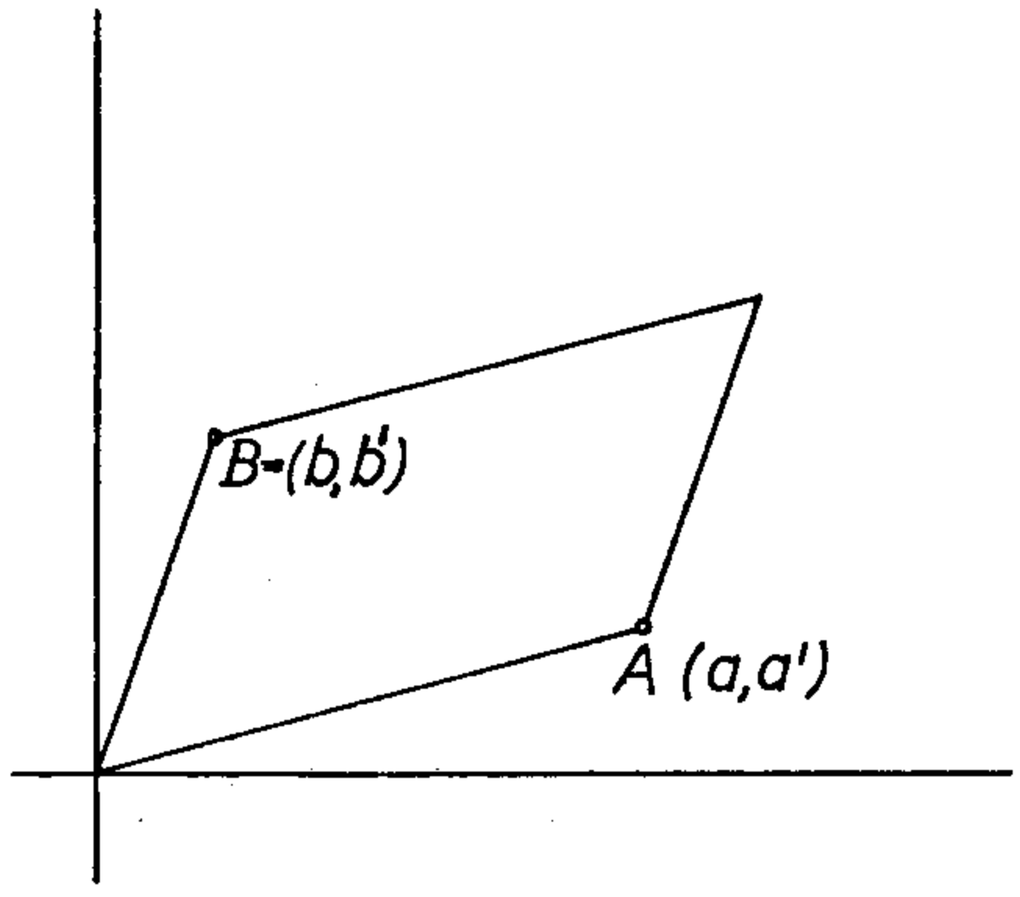
$$A = (a,\ a')$$

$$B = (b,\ b')$$

$$C = (c,\ c')$$

i pripadne radijus-vektore

$$\overrightarrow{OA},\ \overrightarrow{OB},\ \overrightarrow{OC}.$$



Sl. 9.1.12.

[1)] Jednadžbe (5) ne moraju biti linearne u odnosu na $x_1,\ x_2,\ \cdots,\ x_n$.

Nacrtajmo paralelogram sa stranicama $\overrightarrow{OA}$, $\overrightarrow{OB}$ i računajmo ploštinu p tog paralelograma; izlazi (B' odnosno A' je projekcija tačke B odnosno tačke A na x-os; tj. $B'=(b, 0)$, $A'=(a, 0)$):

$$p = 2\Delta OB'B + 2B'A'AB - 2OAA' =$$

$$= (a-b)b' + (a'+b')(a-b) - aa' = ab' - a'b,$$

$$p = \begin{vmatrix} a & b \\ a' & b' \end{vmatrix}.$$

To je osnovna ideja: *determinanta po svojem karakteru označuje* ***zapreminu*** *određenog paralelograma, odnosno paralelepipeda s vrhom u O, a osnovni su bridovi iz početka koordinata smješteni u tačkama kojima su koordinate upravo nizovi brojeva u stupcima determinante.*

Nastaje pitanje kako da tu zapreminu izračunamo u prostoru od 3 dimenzije, pa u „prostoru" od 4 dimenzije, 5 dimenzija itd., definirajući zapreminu paralelepipeda kao produkt zapremine njegove baze i visine (isp. pogl. 11, § 13).

1.11. Zadaci o determinantama stupnja 2×2.

1. Izračunaj

1) $\begin{vmatrix} 5 & 8 \\ 11 & 17 \end{vmatrix}$, 2) $\begin{vmatrix} 8 & 5 \\ 17 & 11 \end{vmatrix}$, 3) $\begin{vmatrix} 11 & 17 \\ 5 & 8 \end{vmatrix}$, 4) $\begin{vmatrix} 5 & 11 \\ 8 & 17 \end{vmatrix}$, 5) $\begin{vmatrix} 11 & 5 \\ 17 & 8 \end{vmatrix}$,

6) $\begin{vmatrix} 11 & 17 \\ 5 & 8 \end{vmatrix}$, 7) $\begin{vmatrix} 17 & 11 \\ 8 & 5 \end{vmatrix}$, 8) $\begin{vmatrix} a-b, & 1 \\ -1, & a+b \end{vmatrix}$, 9) $\begin{vmatrix} a & b \\ b & a \end{vmatrix}$,

10) $\begin{vmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & \cos\alpha \end{vmatrix}$, 11) $\begin{vmatrix} (m+n)^2 & 2mn \\ 2mn & (m-n)^2 \end{vmatrix}$, 12) $\begin{vmatrix} 0{,}345 & 5{,}4 \\ 9{,}4 & 1{,}272 \end{vmatrix}$,

13) $\begin{vmatrix} x-y, & x^{n+1} \\ y^{n+1}, & x^n + x^{n-1}y + \cdots + y^n \end{vmatrix}$, 14) $\begin{vmatrix} 2^{1/2} & 3^{1/3} \\ 4^{1/4} & 5^{1/5} \end{vmatrix}$, 15) $\begin{vmatrix} \frac{1+t^2}{1-t^2} & \frac{2t}{1-t^2} \\ \frac{2t}{1-t^2} & \frac{1+t^2}{1-t^2} \end{vmatrix}$,

16) $\begin{vmatrix} 1 & \log_b a \\ \log_a b & 1 \end{vmatrix}$, 17) $\begin{vmatrix} 1+x^2 & xy \\ yx & 1+y^2 \end{vmatrix}$.

2. Napiši u obliku determinante stupnja 2×2 ovaj izraz:
1) $4x-5y$; 2) $-7x^3+12y$; 3) m^2-n^2; 4) $\cos^2\alpha-\sin^2\alpha$; 5) a^2+b^2.

3. Napiši u obliku determinante stupnja 2×2 skalarni produkt ovih nizova: 1) 3, 4; 5,7; 2) a, c; x, y; 3) $-3, 8$; 3, 7.

4. Odrediti ploštinu paralelograma što ga određuju ova dva vektora položaja: 1) 3, 4; 5, 7; 2) a, c; x, y; 3) $-3, 8$; $3, 7$.

5. Na koliko se načina može izraz $a\,c - b\,d$ predočiti kao $\begin{vmatrix} x & y \\ u & v \end{vmatrix}$, pri čemu je $\{a, b, c, d\} = \{x, y, u, v\}$? Promatraj posebno slučaj kad među a, b, c, d 1) nema jednakih, 2) $a = b$.

6. Provjeri $\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \cdot \begin{vmatrix} a_1' & b_1' \\ a_2' & b_2' \end{vmatrix} = \begin{vmatrix} a_1 a_1' + a_2 a_2', & a_1 b_1' + a_2 b_2' \\ b_1 a_1' + b_2 a_2', & b_1 b_1' + b_2 b_2' \end{vmatrix}$.

Konkretiziraj!

7. Skup $\{a, b, c, d\}$ od 4 opća broja porazmjesti kao elemente determinante stupnja 2×2; koliko se različnih determinanata dobije?

8. Zadan je niz e_1, e_2, e_3, e_4 od 4 broja. Na koliko se načina članovi toga niza mogu porazmjestiti u $2 \cdot 2$ okna rešetke tipa 2×2 tako da u svako polje dođe jedan član niza. Neka je $D(e_1\, e_2\, e_3\, e_4)$ broj različnih determinanata koje se tako dobiju. Odredi sve moguće vrijednosti $D(e_1\, e_2\, e_3\, e_4)$ u zavisnosti od raznih izbora za e_1, e_2, e_3, e_4, npr. očigledno je $D(a, a, a, a) = 1$.

9. Riješiti $\begin{vmatrix} a-x, & b \\ b & c-x \end{vmatrix} = 0$; dokaži da je x realno, ako su realni a, b, c.

10. Ako je $\begin{vmatrix} a & b \\ b & c \end{vmatrix} = 0$, onda se izraz $a\,x^2 + 2\,b\,x + c$ može predstaviti kao kvadrat; i obratno.

11. Izraz $\dfrac{a\,x + b}{c\,x + d}$ za koji je $c\,d \neq 0$ ne zavisi od x onda i samo onda ako je $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = 0$.

12. Napravi i sam nekoliko zadataka poput prethodnih!

2. OPĆI SLUČAJ: *n* LINEARNIH JEDNADŽBI SA *n* NEPOZNANICA

1. Opet sistem od 2 jednadžbe, ali uz pomoć indeksa. Radi lakšeg prelaza na slučaj sistema sa 3 i više nepoznanica, obradimo opet linearan sistem s 2 nepoznanice, ali služeći se indeksima.

1.1. Nepoznanice označimo sa x_1, x_2. Tako se odmah vidi da bismo — u slučaju da se radi npr. o 100 nepoznanica — njih mogli označiti sa $x_1, x_2, \cdots, x_{100}$. *Generičko* (*rodno*) *ime* nepoznanica je isto, a nepoznanice razlikujemo po indeksima.

1.2. Svaku jednadžbu sredimo tako da najprije dolazi član sa x_1 (ako x_1 ne dolazi, pišemo ipak $0 \cdot x_1$ pa se tako x_1 ipak „pojavljuje"), zatim dolazi član s x_2; ostalo prebacimo na drugu stranu.

Tako *svaka* nepoznanica u *svakoj* jednadžbi ima svoje *polje* (*mjesto*) i *svoj koeficijent*.

1.3. Kao što je x generičko (rodno) ime za *nepoznanice*, tako neka a bude rodno ime za koeficijente, a c za članove na desnoj strani; desna će strana, dakle, biti c_1 u prvoj i c_2 u drugoj jednadžbi. Koeficijente imenujmo sa 2 indeksa, i to po redu a_{11} (čitaj a jedan jedan), a_{12}, a_{21}, a_{22}.

1.4. Tako imamo sređen ovaj sistem od 2 jednadžbe s 2 nepoznanice:

$$\begin{aligned} a_{11}\,x_1 + a_{12}\,x_2 &= c_1 \\ a_{21}\,x_1 + a_{22}\,x_2 &= c_2\,. \end{aligned} \tag{1}$$

1.5. Determinanta sistema (1) glasi:

$$\det \begin{matrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{matrix} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}\,a_{22} - a_{12}\,a_{21} \tag{2}$$

1.6. Imamo ovaj postupak:

$$\begin{array}{l} a_{11}\,x_1 + a_{12}\,x_2 = c_1 \mid \cdot \quad a_{22} \\ \underline{a_{21}\,x_2 + a_{22}\,x_2 = c_2 \mid \cdot -a_{12}} \end{array} +$$

$$(a_{11}\,a_{22} - a_{12}\,a_{21})\,x_1 = c_1\,a_{22} - c_2\,a_{12},$$

odnosno u novoj simbolici[1]:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} x_1 = \begin{vmatrix} c_1 & a_{12} \\ c_2 & a_{22} \end{vmatrix}. \tag{C}$$

1.7. *Sad ćemo taj postupak rješavanja gledati u svjetlu determinante i svaki korak nastojati dovesti u vezu s determinantom.* Tako smo npr. množili prvu jednadžbu sa a_{22}. A šta je a_{22}? To je ono što se dobije kad u determinanti izbrišemo sve ono što je u retku i stupcu u kojem se nalazi a_{11}. Označimo taj »*kofaktor*« od a_{11} sa $f(a_{11})$. Šta je nadalje — a_{12}, kojim smo množili drugu jednadžbu? To je „kofaktor" od a_{21}; na drugoj strani u (2) dobijemo to — a_{12} da *izbrišemo* sve elemente iz retka i stupca od a_{21}, a na lijevoj strani se isto to precrta i još pomnoži sa —1.

Dakle je $f\,a_{21} = -a_{12} = -\det a_{12}$.

1.8. Prema tome, prelaz od sistema (1) na (*C*) možemo opisati funkcionalno ovako:

$$\begin{array}{l} a_{11}\,x_1 + a_{12}\,x_2 = c_1 \mid \cdot f(a_{11}) \\ \underline{a_{21}\,x_1 + a_{22}\,x_2 = c_2 \mid \cdot f(a_{21})} \end{array} +$$

$$(a_1\ f(a_{11}) + a_{21} f(a_{21}))\,x_1 = c_1 f(a_{11}) + c_2 f(a_{21}),$$

[1] Preporučuje se pisati na „kineski" način: najprije stupce, a onda retke.

odnosno

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} x_1 = \begin{vmatrix} c_1 & a_{12} \\ c_2 & a_{22} \end{vmatrix},$$

gdje je

$$a_{11} f a_{11} + a_{21} f a_{21} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}.$$

2. TRI LINEARNE JEDNADŽBE S 3 NEPOZNANICE

2.1. Na osnovu gornjeg tumačenja u t. 1, taj sistem izlazi iz (1) nadopunjujući ga potrebnim dijelovima; glasi ovako:

$$\begin{aligned} a_{11} x_1 + a_{12} x_2 + a_{13} x_3 &= c_1 \\ a_{21} x_1 + a_{22} x_2 + a_{23} x_3 &= c_2 \qquad (1) \\ a_{31} x_1 + a_{32} x_2 + a_{33} x_3 &= c_3 . \end{aligned}$$

2.2. Simboličko rješenje. Ako radimo po kalupu po kojem smo rješavali dvije jednadžbe s 2 nepoznanice (v. § 1.6), onda bi iz (1) izlazilo (Cramerovo pravilo):

$$C(1) \qquad \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} x_1 = \begin{vmatrix} c_1 & a_{12} & a_{13} \\ c_2 & a_{22} & a_{23} \\ c_3 & a_{32} & a_{33} \end{vmatrix}.$$

Slično za ostale dvije nepoznanice; za x_2 bi c-ovi bili umjesto stupca koeficijenata od x_2 u determinanti

$$(2) \qquad \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

a za x_3 bi c-ovi bili umjesto trećeg stupca te „determinante". Samo se još radi o tome da odredimo šta taj simbol u (2) znači!

2.3. Primijenimo u novoj situaciji (1) postupak iz § 1.8: jednadžbe množimo po redu „kofaktorima" koeficijenata od x_1 i zbrojimo dobivene jednadžbe. No šta je u novoj situaciji $f a_{11}$? Dobije se kao i prije: treba precrtati sve ono što je u 1. retku i prvom stupcu; dakle je

$$(3) \qquad f a_{11} = \begin{vmatrix} \cancel{a_{11}} & \cancel{a_{12}} & \cancel{a_{13}} \\ \cancel{a_{21}} & a_{22} & a_{23} \\ \cancel{a_{31}} & a_{32} & a_{33} \end{vmatrix} = \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} = a_{22} a_{33} - a_{23} a_{32} .$$

Kako se dobije fa_{21}? Kao i prije: treba precrtati (izostaviti) sve ono što je u 2. retku i 1. stupcu u kojima je a_{21} i taj rezultat pomnožiti sa -1:

$$(4)\qquad fa_{21} = -\begin{vmatrix} \cancel{a_{11}} & a_{12} & a_{13} \\ \cancel{a_{21}} & \cancel{a_{22}} & \cancel{a_{23}} \\ \cancel{a_{31}} & a_{32} & a_{33} \end{vmatrix} = -\begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} = -(a_{12}a_{33} - a_{13}a_{32}).$$

Šta je najzad $f(a_{31})$? Opet ćemo *izostaviti redak i stupac u kojima je* a_{31}. Samo se još pitamo da li taj rezultat možda još treba pomnožiti sa -1 kao kad smo formirali fa_{21} ili da stavimo

$$(5)\qquad fa_{31} = \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} = a_{12}a_{23} - a_{13}a_{22}.$$

2.4. Radimo ovako:

$$(6)\qquad \begin{array}{l|l} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = c_1 & \cdot fa_{11} = \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 = c_2 & \cdot fa_{21} = -\begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} + \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 = c_3 & \cdot fa_{31} = \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} \end{array}$$

$$\Downarrow$$

$$(7)\qquad (a_{11}fa_{11} + a_{21}fa_{21} + a_{31}fa_{31})\,x_1 = c_1 fa_{11} + c_2 fa_{21} + c_3 fa_{31};$$

naime, koeficijenti od x_2 i x_3 u (7) su 0.

Došli smo do cilja: množeći jednadžbe „kofaktorima" koeficijenata od x_1, izlazi jednadžba bez ostalih nepoznanica.

Ako se u jednadžbi (7) provede račun imajući na umu značenja za kofaktore fa_{11}, fa_{21}, fa_{31} *prema* (3), (4) i (5), vidimo da iz zadanog sistema (6) izlazi:

$$(8)\qquad \begin{cases} (a_{11}a_{22}a_{33} - a_{11}a_{32}a_{23} - a_{21}a_{12}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} - a_{31}a_{22}a_{13})\,x_1 = \\ c_1a_{22}a_{33} - c_1a_{32}a_{23} - c_2a_{12}a_{33} + c_2a_{32}a_{13} + c_3a_{12}a_{23} - c_3a_{22}a_{13}. \end{cases}$$

Time je x_1 nađeno.

No, jednakost (8) čini se, bar na prvi pogled, *strahovito zamršena*! A odmah ćemo vidjeti kako je ona, ipak, *jednostavne matematičke strukture*!

2.5. Uspoređujući obrasce $C(1)$, (7) i (8), odmah se nameću postavke[1]:

$$(L) \qquad \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} fa_{11} + a_{21} fa_{21} + a_{31} fa_{31},$$

$$(D_3) \qquad \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} - a_{11}a_{32}a_{23} - a_{21}a_{12}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} - a_{31}a_{22}a_{13}.$$

I stvarno, svakom od tih jednakosti (L) i (D_3) možemo *definirati* determinantu poretka 3×3. Prva jednakost (L) lako se *prenosi* za slučaj „determinante" oblasti, stupnja 4×4, stupnja 5×5 itd. *Induktivno* bismo tako dobili *definiciju* determinante stupnja $n \times n$ za svaki prirodni broj n (naime za slučaj determinante oblasti, stupnja (1×1) stavljamo $\det b = b$ za svaki broj ili brojevni izraz b).

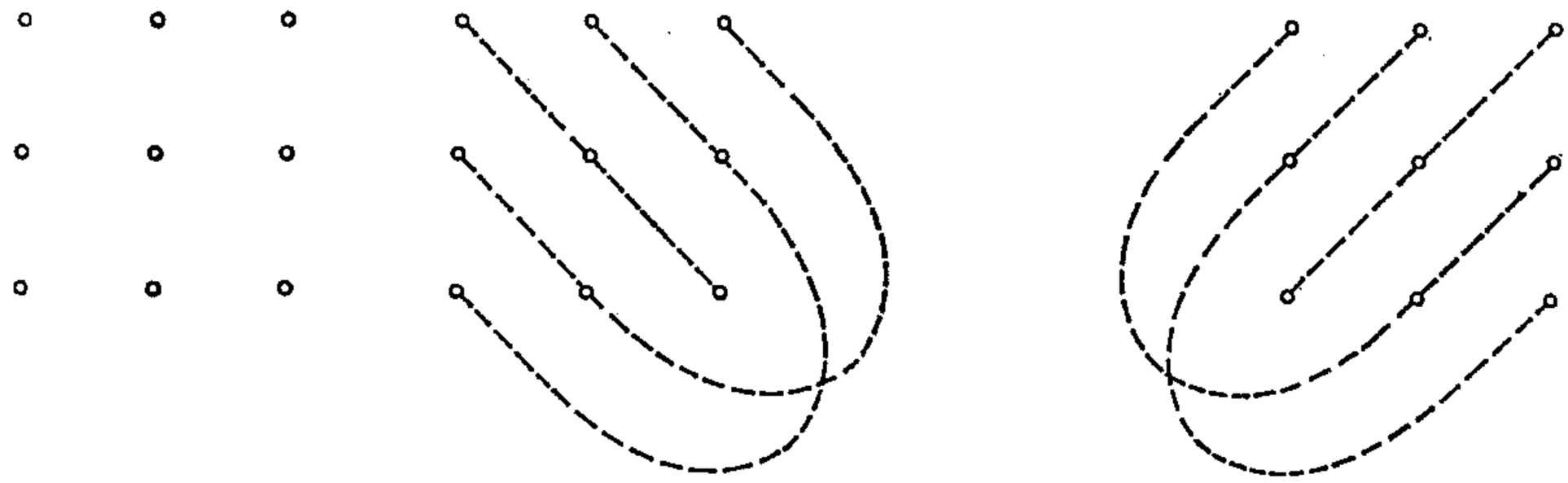
Ipak ćemo jednakost (D_3) a ne (L) *uzeti kao* ***definiciju*** *determinante* poretka 3×3; tu ćemo definiciju analizirati. A obrazac (L) i njegova generalizacija bit će osnovni *teorem* o determinantama (Laplaceov teorem o razvoju!).

2.6. Definicija determinante stupnja 3×3. *Determinanta ili opredjelitelj tablice* (a) *brojeva ili brojevnih izraza*:

$$(a) \qquad \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

definiramo jednakošću (D_3)*; desna strana jednakosti* (D_3) *je vrijednost determinante, a lijeva strana njena oznaka. Možemo je označiti i sa* $\det a$.

2.7. Mnemotehničko pravilo o formiranju determinante oblasti 3×3. — 2.7.1. Shematski, to je kvadratna tablica od 9 elemenata determinante. Tu imamo 3 retka, 3 stupca, zatim glavnu dijagonalu i sporednu dijagonalu; na



Sl. 9.2.7.1.

[1] Valja dodati da iz jednakosti $C(1)$ i (8) izlazi nužno da kvocijent koeficijenata od x_1 u $C(1)$ i (8) ne zavisi od x_1, no ne izlazi nužno da je on = 1.

svakoj od tih „linija“ leže tri komponente determinante. No „paralelno“ sa svakom dijagonalom imamo još po dvije linije po 2 elementa; ako svaku od tih kraćih linija nadopunimo s onim trećim elementom determinante koji leži u stranom retku i u stranom stupcu, dobit ćemo pomoćne tročlane linije, i to dvije paralelne s glavnom dijagonalom i dvije paralelne sa sporednom dijagonalom. Na prvoj, odnosno drugoj priloženoj slici 1, nacrtane su sve tri tročlane glavne kose linije, odnosno sve tri tročlane sporedne kose linije.

2.7.2. Praktično pravilo. *Determinanta stupnja* 3×3 *formira se tako da se članovi na svakoj tročlanoj kosoj liniji međusobno pomnože; znak* $+$ *dolazi pred produktom elemenata na svakoj glavnoj kosoj liniji, a znak* $-$ *dolazi pred produktom elemenata na svakoj sporednoj kosoj liniji; svi se ti izrazi zbroje.*

Imajući na umu orijentaciju tablice (prva os ide iz gornjeg lijevog ugla prema dolje, a druga nadesno!), vidimo da u razvijenom izrazu za determinantu stupnja 3×3 svaki član ima znak $+$ ili $-$, već prema tome da li dotična linija matrice ima pozitivan ili negativan gradijent prema prvoj osi.

2.7.3. Primjer.

$$\begin{vmatrix} 2 & 5 & 4 \\ 1 & -2 & 3 \\ 4 & 1 & 7 \end{vmatrix} = 2 \cdot -2 \cdot 7 + 5 \cdot 3 \cdot 4 + 4 \cdot 1 \cdot 1 - 4 \cdot -2 \cdot 4 - 3 \cdot 1 \cdot 2 - 7 \cdot 5 \cdot 1 =$$
$$= -28 + 60 + 4 + 32 - 6 - 35 = 27.$$

Taj rezultat možemo koristiti da riješimo ove 3 jednadžbe:

$$2x + 5y + 4z = 9$$
$$x - 2y + 3z = 5$$
$$4x + y + 7z = 0.$$

Naime,

$$(\det)\, x = \begin{vmatrix} 9 & 5 & 4 \\ 5 & -2 & 3 \\ 0 & 1 & 7 \end{vmatrix} = 9 \cdot -2 \cdot 7 + 4 \cdot 5 \cdot 1 - 3 \cdot 1 \cdot 9 - 7 \cdot 5 \cdot 5$$

$$27x = 9 \cdot -17 - 5 \cdot 31$$

$$x = -308/27$$

$$x = -11{,}407.. = -11{,}41 \quad \text{(na 2 decimale)}.$$

Dalje se može naći y i z.

2.8. Analiza definicione jednakosti (D_3). Algebarski izraz za determinantu poretka 3×3 ima 6 članova ili terma. Građa toga izraza čini se dosta zamršena! Kako indeksi u jednakosti (D_3) imaju nadasve odlučujuću ulogu, gledajmo kako se oni mijenjaju od člana do člana.

2.8.1. Vidimo da se u izrazu (D_3) za determinantu u svakom članu pojavljuju tri elementa iz kvadratne tablice, i to s drugim indeksima 1 2 3 svuda. To znači da *svaki član determinante sadrži bar jedan element iz svakog stupca tablice.*

2.8.2. No *nijedan član ne sadrži dva elementa iz istog stupca,* jer su prvi indeksi u svakom članu međusobno različiti. Naime, ti prvi indeksi u svih 6 članova determinante glase po redu od člana do člana determinante:

$$1\ 2\ 3 \qquad 1\ 3\ 2 \qquad 2\ 1\ 3 \qquad 2\ 3\ 1 \qquad 3\ 1\ 2 \qquad 3\ 2\ 1.$$

A to su upravo sve permutacije indeksâ 1 2 3.

Sada, dakle, znamo *pravilo o indeksima u izrazu* (D_3)*: Drugi indeksi daju svuda* 1 2 3, *a prvi indeksi daju sve permutacije tih drugih indeksâ.*

2.8.3. Još *ostaje da vidimo kako se u* (D_3) *pojavljuju članovi s koeficijentom* $+1$, *a kako s* -1. Ispišimo po redu, od člana do člana, u (D_3) faktor $+1$ ili -1 i pripadnu permutaciju drugih indeksa. Imamo ovu tablicu:

znak	$+$	$-$	$-$	$+$	$+$	$-$
permutacija	1 2 3	1 3 2	2 1 3	2 3 1	3 1 2	3 2 1.

Ako pogledamo koliko pojedina permutacija ima *inverzija,* tj. koliko se puta u njoj nalazi veći broj ispred manjega, onda taj broj inverzija iznosi po redu:

$$0, \qquad 1, \qquad 1, \qquad 2, \qquad 2, \qquad 3.$$

2.8.4. Za permutaciju p označimo sa ip broj njenih inverzija. Tada vidimo da predznak uz permutaciju p glasi $(-1)^{ip}$.

2.8.5. Na taj način za svaku permutaciju $p=p_1, p_2, p_3$ brojeva 1, 2, 3 imamo u izrazu za determinantu (D_3) potpuno određen odgovarajući član ili term

$$(9) \qquad (-1)^{ip}\, a_{p_1 1}\, a_{p_2 2}\, a_{p_3 3}.$$

Suma svih tih članova (9) daje traženi izraz za determinantu. Tako smo najzad došli do ove definicije.

2.9. Definicija determinante stupnja 3×3.

$$(10) \qquad \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \sum_p (-1)^{ip}\, a_{p_1 1}\, a_{p_2 2}\, a_{p_3 3};$$

p prolazi skupom [1, 3]! *svih jednoznačnih permutacija intervala* $[1, 3]=\{1, 2, 3\}$. Drugim riječima:

Determinantu (10) izračunavamo ovako:

Prvi korak: *u početnom stupcu treba izabrati jednu vrijednost tablice, recimo vrijednost* $a_{p_1 1}$, *te precrtati i čitav redak* p_1 *i čitav prvi stupac, zatim učiniti*

Drugi korak: *na preostatku tablice raditi kao maloprije: izabrati neku vrijednost — recimo imena* $a_{p_2 2}$, *precrtati čitav redak i čitav stupac u kojima je ta komponenta itd. do kraja. Zatim sve izabrane vrijednosti međusobno pomnožiti i time dobiti produkt* $a_{p_1 1}$, $a_{p_2 2}$, $a_{p_3 3}$.

I najzad, taj produkt pomnožiti sa $+1$ *ili* -1, *već prema tome da li je* $p_1\, p_2\, p_3$ *parna ili neparna permutacija, tj. da li se u permutaciji p pojavljuje paran ili neparan broj poremećenja poretka.*

Time se dobije opći član determinante.

2.9.3. Upamtimo dobro da pri tom procesu *svaka permutacija p ima posebnu ulogu.* Tako npr. permutacija 3 2 1 ukazuje da biramo najprije iz retka 3, pa iz retka 2 i, najzad, iz retka 1, tako da izabrane vrijednosti glase (gledaj samo *prve* indekse!):

$$a_{31},\ a_{22},\ a_{13}.$$

Odredimo još da li njihov produkt $a_{31}\, a_{22}\, a_{13}$ (pazi na *prve* indekse!) treba pomnožiti sa $+1$ ili sa -1. Permutacija 3 2 1 pokazuje 3 poremećaja poretka, i to: 3 ispred 2, 3 ispred 1 te 2 ispred 1; znači, da treba množiti sa $(-1)^3$, tj. sa -1; znači da permutaciji $p = 3\ 2\ 1$ odgovara ovaj član determinante:

$$-a_{31}\, a_{22}\, a_{13}$$

(gledaj kako je tu p smješteno kao prvi indeksi; drugi indeksi su uvijek 1 2 3).

2.9.2. Važno je da vidimo da **svakoj** permutaciji p odgovara posve *određen član* determinante i da time dobijemo *sve* članove determinante — ima ih koliko i permutacijâ.

2.9.3. Sad je jasno da se ***na posve sličan način obrazuje*** determinanta reda 4×4, reda $5 \times 5, \cdots$ uopće reda $n \times n$ za *svaki* prirodni broj $n > 1$.

Tako bi npr. determinanta *rodnog* imena *u* reda 6×6 imala simboličku oznaku

$$\begin{vmatrix} u_{11} & u_{12} & u_{13} & u_{14} & u_{15} & u_{16} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ u_{61} & u_{62} & u_{63} & u_{64} & u_{65} & u_{66} \end{vmatrix}.$$

Svakoj permutaciji p cifarskog skupa $[1, 6] = \{1, 2, 3, 4, 5, 6\}$ odgovara *posve određen član* te determinante. Npr. permutaciji $p = 5\ 6\ 4\ 1\ 2\ 3$ odgovara biranje iz redića 5 (tj. vrijednost u_{51}), pa iz redića 6 (vrijednost u_{62}), pa iz redića 4 (radi se o u_{43}), pa biranje u_{14}, pa u_{25} i još je ostalo u_{36}; odgovarajući član determinante glasi:

$$(11) \qquad (-1)^{\mathfrak{i}\, 564123}\, u_{51}\ u_{62}\ u_{43}\ u_{14}\ u_{25}\ u_{36}.$$

No $i\,564123 = ?$ Broji se po redu:

5 pokazuje 4 inverzije (naime sa 4, 1, 2, 3)

6 pokazuje 4 inverzije (naime sa 4, 1, 2, 3)

4 pokazuje 3 inverzije (naime sa 1, 2, 3).

Drugih inverzija nema. Svih inverzija ima 11.
Dakle je $i\,564123 = 11$, pa je time potpuno određeno da permutaciji $p = 5\,6\,4\,1\,2\,3$ odgovara izraz

$$-u_{51}\ u_{62}\ u_{43}\ u_{14}\ u_{25}\ u_{36}$$

kao član gornje u-determinante.

Taj član možemo simbolički označiti sa

$$-(5\,6\,4\,1\,2\,3)$$

jer znamo da kod svakog člana determinante dolazi 6 u-faktora, naime:

$$u_1 u_2 u_3 u_4 u_5 u_6,$$

pa se još to nadopunjuje *upisivanjem prvih indeksa* te faktora -1.

U toj simbolici determinanta poretka 6×6 bila bi, po definiciji, predočena ovom sumom:

$$\sum_{p \in 1(6)!} (-1)^{tp}(p),$$

u kojoj imamo 6! $(= 120)$ članova, jer toliko ima jednoznačnih permutacija intervala $[1, 6] = \{1, 2, 3, 4, 5, 6\}$.

Tako se definira i determinanta stupnja $n \times n$: treba u gornji simbolički izraz umjesto 6 pisati n. Ona ima $n! = 1 \cdot 2 \cdot 3 \cdot \cdots (n-1) \cdot n$ članova. A to je vrlo velik broj već i za manje n-ove!

Zato ako i važi Cramerovo pravilo za svako n, ono nam u *praktičnom* numeričkom rješavanju linearnih sistema za poveće n neće mnogo koristiti: računanja su predugačka.

S teoretske strane učinili smo velik napredak dobivši logički uvid u strukturu determinante i njenu ulogu kod linearnih jednadžbi. Međutim, uloga determinante mnogo je jača izvan linearnih jednadžbi u jednu ruku, a u drugu ruku ima posebnih postupaka kako se linearne jednadžbe rješavaju nezavisno od determinante. Jedan takav postupak je npr. topovski postupak eliminacije pomoću protivno-jednakih koeficijenata, odnosno specijalno Gaussov postupak (v. poglavlje 8, § 2.6. i 2.7).

2.10. Zadaci o determinantama stupnja 3×3.

1. Izračunaj ove determinante (ispisuj ih po stupcima!):

$$1)\begin{vmatrix} 2 & 5 & 3 \\ 4 & 6 & 7 \\ 1 & 0 & 8 \end{vmatrix},\quad 2)\begin{vmatrix} -3 & 5 & 3 \\ 10 & 6 & 7 \\ 12 & 9 & 8 \end{vmatrix},\quad 3)\begin{vmatrix} 2 & -3 & 3 \\ 4 & 10 & 7 \\ 1 & 12 & 8 \end{vmatrix},\quad 4)\begin{vmatrix} 2 & 5 & -3 \\ 4 & 6 & 10 \\ 1 & 9 & 12 \end{vmatrix},$$

5) $\begin{vmatrix} 34 & -53 & 16 \\ 39 & 42 & -20 \\ 10 & 20 & 30 \end{vmatrix}$, 6) $\begin{vmatrix} 2^3\cdot 5^2, & 3^2\cdot 7 & 7^3 \\ 2 & 5 & 7 \\ 2^4\cdot 5, & 2\cdot 5\cdot 7, & 2^2\cdot 5^2\cdot 7^3 \end{vmatrix}$, 7) $\begin{vmatrix} a & b & c \\ b & c & a \\ c & a & b \end{vmatrix}$,

8) $\begin{vmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{vmatrix}$, 9) $\begin{vmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{vmatrix}$, 10) $\begin{vmatrix} a & b & c \\ b & d & e \\ c & e & f \end{vmatrix}$,

11) $\begin{vmatrix} 1+a^2 & ab & ac \\ ba & 1+b^2 & bc \\ ca & cb & 1+c^2 \end{vmatrix}$, 12) $\begin{vmatrix} \cos x & \sin x & \cos y & \sin x & \sin y \\ -\sin x & \cos x & \cos y & \cos x & \sin y \\ 0 & -\sin y & \cos y & & \end{vmatrix}$.

2. Izračunaj 1) $\begin{vmatrix} a & x & y \\ 0 & b & z \\ 0 & 0 & c \end{vmatrix}$, 2) $\begin{vmatrix} a & 0 & 0 \\ x & b & 0 \\ y & z & c \end{vmatrix}$.

Da li rezultat zavisi o x, y, z? Izreci odgovarajuće pravilo!

3. Riješi $2x+5y+3z=-3$

$4x+6y+7z=10$

$x+9y+8z=12$; posluži se podacima (1—4) iz zadatka 1.

4. Gledaj zadatke iz pogl. 8 § 2. 8 pa ih riješi pomoću determinanata i Cramerova pravila.

5. 1) $\begin{vmatrix} a & b & a+b \\ b & a+b & a \\ a+b & a & b \end{vmatrix}$, 2) $\begin{vmatrix} \cos(a-b) & \cos(b-c) & \cos(c-a) \\ \cos(a+b) & \cos(b+c) & \cos(c+a) \\ \sin(a+b) & \sin(b+c) & \sin(c+a) \end{vmatrix}$.

6. 1) $\begin{vmatrix} x & -1 & 0 \\ 0 & x & -1 \\ a_0, & a_1, & a_2+x \end{vmatrix}$; 2) $\begin{vmatrix} a & x & x \\ x & b & x \\ x & x & c \end{vmatrix}$; 3) $\begin{vmatrix} x^2+1 & xy & xz \\ yx & y^2+1 & yz \\ zx & zy & z^2+1 \end{vmatrix}$.

7. Opiši riječima kako iz determinante

$D=\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$ nastaju ove determinante:

1) $\begin{vmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \\ a_{13} & a_{23} & a_{33} \end{vmatrix}$, (simetrija prema glavnoj dijagonali)

2) $\begin{vmatrix} a_{33} & a_{23} & a_{13} \\ a_{32} & a_{22} & a_{12} \\ a_{31} & a_{21} & a_{11} \end{vmatrix}$, (simetrija prema sporednoj dijagonali)

3) $\begin{vmatrix} a_{33} & a_{32} & a_{31} \\ a_{23} & a_{22} & a_{21} \\ a_{13} & a_{12} & a_{11} \end{vmatrix}$, (središnja simetrija)

4) (zakret D za $\pi/2$) 5) (zakret D za $-\pi/4$) 7) (zakret za $-3\,\pi/4$)

$$\begin{vmatrix} a_{13} & a_{23} & a_{33} \\ a_{12} & a_{22} & a_{32} \\ a_{11} & a_{21} & a_{31} \end{vmatrix}, \quad \begin{vmatrix} a_{21} & a_{11} & a_{12} \\ a_{31} & a_{22} & a_{13} \\ a_{32} & a_{33} & a_{23} \end{vmatrix}, \quad \begin{vmatrix} a_{32} & a_{31} & a_{21} \\ a_{33} & a_{22} & a_{11} \\ a_{23} & a_{13} & a_{12} \end{vmatrix}.$$

8. Izračunaj determinantu $a = \begin{vmatrix} 3 & 4 & 7 \\ 5 & 9 & 14 \\ 7 & 1 & 3 \end{vmatrix}$ kao i onu što iz a nastaje zaokretom za $\pi/2$ i prelaganjem oko glavne dijagonale.

9. Nađi $\det a = \begin{vmatrix} 2+3i & 4-i & 2+5i \\ i & -2 & 1+2i \\ -3 & -2-i & 4+2i \end{vmatrix}$ kao i $\det \bar{a}$, gdje je $\bar{a}_{ik} = \overline{a_{ik}}$ tj. elementi u $\det \bar{a}$ nastaju sprezanjem elemenata a_{ik}; dokaži da je $\det \bar{a} = \overline{\det a}$.

10. Nađi $\det a$ stupnja 3×3, ako je $a_{ik} =$ 1) $i+k$, 2) $i-k$, 3) $i \cdot k$, 4) $i : k$, 5) i^k, 6) $\log_{i+1} k$, 7) i^2+k^2, 8) $i^2+k^2-3ik+5$, 9) $i \,\mathrm{W}\, k$, 10) $i \,\mathrm{M}\, k$.

11. Nađi 1) $\begin{vmatrix} x & y & 1 \\ x_0 & y_0 & 1 \\ x_1 & y_1 & 1 \end{vmatrix}$, 2) $\begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix}$, 3) $\begin{vmatrix} x_1+c & y_1+c & 1 \\ x_2+c & y_2+c & 1 \\ x_3+c & y_3+c & 1 \end{vmatrix}$,

4) $\begin{vmatrix} x_1 \cos a + y_1 \sin a, & x_1 \sin a + y_1 \cos a, & 1 \\ x_2 \cos a + y_2 \sin a, & x_2(-\sin a) + y_2 \cos a, & 1 \\ x_3 \cos a + y_3 \sin a, & x_3(-\sin a) + y_3 \cos a, & 1 \end{vmatrix}$,

5) $\begin{vmatrix} x_1 \cos a + y_1 \sin a + c, & x_1(-\sin a) + y_1 \cos a + c, & 1 \\ x_2 \cos a + y_2 \sin a + c, & x_2(-\sin a) + y_2 \cos a + c, & 1 \\ x_3 \cos a + y_3 \sin a + c, & x_3(-\sin a) + y_3 \cos a + c, & 1 \end{vmatrix}$.

3. DEFINICIJA DETERMINANATA

Na osnovu razmatranja iz § 2. postavljamo ovu definiciju:

—→ **3.1. Definicija determinante.** Neka je n bilo koji prirodan broj; neka je zadana kvadratna tablica a od n nizova po n članova:

$$(1) \qquad \begin{matrix} a_{11} & a_{12} & a_{13} \cdots a_{1n} \\ a_{21} & a_{22} & a_{23} \cdots a_{2n} \\ \cdot & \cdot & \cdot \cdot \cdot \cdot \\ a_{n1} & a_{n2} & \cdot \cdot \cdot \quad a_{nn} \end{matrix}$$

ili kraće $a_{lk}(l,\ k\in\{n\}$, gdje je $\{n\}=\{1,\ 2,\cdots,\ n-1,\ n\}$. Neka je $\{n\}!$ skup svih permutacija intervala $\{n\}=[1,\ 2,\cdots,\ n]$; to znači da za svako $p\in\{n\}!$ imamo potpuno određen niz $p_1,\ p_2,\cdots,\ p_k,\cdots,\ p_n$ svih brojeva iz $\{n\}$; označimo sa ip koliko puta u tom nizu p dolazi veći član ispred manjega; tada za svako p iz $\{n\}!$ formirajmo monom

$$(-1)^{ip}\, a_{p_1 1}\ a_{p_2 2}\cdots a_{p_n n};$$

zbrojimo sve te monome; dobijemo izraz koji se zove determinanta ili opredjelitelj gornje tablice a; označuje sa $\det a$ ili Da, ili tako da se tablica stavi u uspravne zagrade:

$$(2)\qquad \det a=\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}=\sum_{p\in[1,\ n]!}(-1)^{i(p)}\, a_{p_1 1}\, a_{p_2 2}\cdots a_{p_n n}$$

ili kraće

$$\det a=\det (a_{lk})_{l,\ k\in[1,\ n]}=\sum_{p\in[1,\ n]!}(-1)^{i(p)}\, a_p,$$

stavljajući

$$a_p=a_{p_1 1}\ a_{p_2 2}\cdots a_{p_n n}.$$

Kaže se da je oblast ili domen tablice i njene determinante jednak $In\times In$ ili $n\times n$ i piše $\mathrm{Dom}\, a=In\times In$, odnosno $\mathrm{Do}\, a=n\times n$.

3.2. Za svaki broj ili izraz b stavljamo

$$\det b=b.$$

To su *determinante s oblasti* $I1\times I1$[1].

Npr. $\det(-5)=-5$. U ovom slučaju bilo bi nezgodno umjesto $\det(-5)$ pisati $|-5|$, jer je običaj da se za svaki broj b sa $|b|$ označi njegova apsolutna vrijednost.

Specijalno je $$\begin{vmatrix} u & v \\ x & y \end{vmatrix}=uy-vx.$$

3.3.1. Primjedba. Umjesto naziv *tablica* govorit ćemo također „*matrica*".

3.3.2. Primjer i teorem. Kao primjer kako da primijenimo gornje pravilo dokažimo da je

$$\begin{vmatrix} 2 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 8 \end{vmatrix}=2\cdot 5\cdot 2\cdot 8.$$

[1] Korisno je promatrati i determinantu s oblasti $I0\times I0$. Ona je bez elemenata.

Stvarno, identičnoj permutaciji od $\{r\}$ odgovara upravo napisani član $2\cdot 5\cdot 2\cdot 8$ determinante; neka je p bilo koja permutacija množine $\{4\}$ koja nije identična; to znači da je za neko $x\in\{4\}$ ispunjeno $p_x\neq x$; no to znači da je element $a_{p_x x}$ tablice $=0$, pa zato i pripadni član determinante iščezava jer kao produkt sadrži 0 kao faktor. Zaključak je općenit:

Teorem. *Ako su članovi kvadratne tablice koji su van glavne dijagonale jednaki* 0, *tada je pripadna determinanta jednaka produktu svih vrijednosti na glavnoj dijagonali.*

3.4. Važna primjedba o indeksima. Gornju tablicu napisali smo služeći se intervalom $\{n\}=\{1, 2, \cdots, n\}$ kao skupom indeksa. Međutim i brojevi $0, 1, 2, \cdots, n-1$ mogu se uzeti kao indeksi. Tada bi p trebalo da bude permutacija tog skupa $In=\{0, 1\ 2, \cdots, n-1\}$. Čak se za druge indekse mogu uzeti elementi $m_1, m_2, \cdots, m_n$ koje god množine M od n članova, a za prve indekse elementi $s_1, s_2, \cdots, s_n$ od bilo koje množine S od n *uzlaznih* brojeva. Tada bi opći član tablice glasio:

$$a_{s_k m_e}$$

(umjesto l, odnosno k stajalo bi m_e, odnosno s_k).

Tada bi definiciona jednakost (2) glasila:

$$\det a=\begin{vmatrix} a_{s_1 m_1} & a_{s_1 m_2} & \cdots & a_{s_1 m_n} \\ x_{s_2 m_1} & a_{s_2 m_2} & \cdots & a_{s_2 m_n} \\ \cdot & \cdot & \cdots & \cdot \\ a_{s_n m_1} & \cdot & \cdots & a_{s_n m_n} \end{vmatrix}=\sum_{p\in S!}(-1)^{ip}\, a_{p_1 m_1} a_{p_2 m_2}\cdots \tag{3}$$

Npr. za $M=\{15, 18\}$, $S=\{25, 30\}$ bilo bi $S!=\{25, 30;\ 30, 25\}$, tj. $S!$ se sastoji od dvije permutacije, i to 25, 30 te 30, 25; zato bi (3) dalo:

$$\begin{vmatrix} a_{25,15} & a_{25,18} \\ a_{30,15} & a_{30,18} \end{vmatrix}=(-1)^{i(25,30)}\, a_{25,15}\, a_{30,18}+(-1)^{i(30,25)}\, a_{30,15}\, a_{25,18}=$$
$$=a_{25,15}\, a_{30,18}-a_{30,15}\, a_{25,18}.$$

3.5. Zadaci o tvorbi determinanata.

1. Izračunaj: 0) $\begin{vmatrix} 2 & 5 \\ 7 & 6 \end{vmatrix}$ 1) $\begin{vmatrix} 2 & 5 & 0 \\ 7 & 6 & 0 \\ 0 & 0 & 1 \end{vmatrix}$ 2) $\begin{vmatrix} 2 & 5 & 0 & 0 \\ 7 & 6 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix}$, ...

2. Promatraj determinantu $\begin{vmatrix} 2 & 3 & 5 & 7 \\ 11 & 13 & 17 & 19 \\ 23 & 29 & 31 & 39 \\ 41 & 43 & 47 & 51 \end{vmatrix}$; odredi znak onog člana njenog razvoja koji sadrži 1) 2, 17, 29, 51; 2) 5, 11, 39, 43; 3) 41, 13, 31, 7.

3. U determinanti iz zad. 2 odredi onaj član njenog razvoja koji odgovara permutaciji 1) 2 3 4 1, 2) 4 3 1 2, 3) 2 3 4 1, 4) 4 3 2 1.

4. $\begin{vmatrix} x & -1 & 0 & 0 \\ 0 & x & -1 & 0 \\ 0 & 0 & x & -1 \\ a_0 & a_1 & a_2 & a_3 \end{vmatrix}$ 5. $\begin{vmatrix} x & -1 & 0 & 0 & 0 \\ 0 & x & -1 & 0 & 0 \\ 0 & 0 & x & -1 & 0 \\ 0 & 0 & 0 & x & -1 \\ a_0 & a_1 & a_2 & a_3 & a_4 \end{vmatrix}$.

6. Koliko članova ima opća determinanta stupnja 3×3, 4×4, 5×5, ... Nađi 1) četvrti član, 2) pretposljednji član prema alfabetskom uređenju permutacijâ.

7. Promatraj det a stupnja 5×5; 1) koliko ima vrijednosti a_{ik} (jednakih ili nejednakih)? 2) Odredi predznak članovima: $\pm a_{34}\, a_{55}\, a_{43}\, a_{12}\, a_{21}$, $\pm a_{15}\, a_{24}\, a_{33}\, a_{42}\, a_{51}$, $\pm a_{25}\, a_{13}\, a_{41}\, a_{34}\, a_{52}$; 3) Da li u razvoju determinante dolaze članovi: $\pm a_{11}\, a_{22}\, a_{33}\, a_{34}\, a_{55}$, $\pm a_{24}\, a_{13}\, a_{42}\, a_{51}\, a_{35}$, $\pm a_{11}\, a_{12}\, a_{13}\, a_{14}\, a_{15}$? 4) Odredi član što pripada permutaciji: 3 2 1 4 5, 5 4 1 2 3, 4 5 1 3 2, 7-oj, 49-oj, 120-oj permutaciji.

8. Izračunaj 1) $\begin{vmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & d \end{vmatrix}$ 2) $\begin{vmatrix} a & b & c & d \\ e & 0 & 0 & 0 \\ f & 0 & h & i \\ g & 0 & 0 & 0 \end{vmatrix}$ 3) $\begin{vmatrix} a & 0 & 0 & e \\ 0 & b & f & 0 \\ 0 & g & c & 0 \\ h & 0 & 0 & d \end{vmatrix}$

4) $\begin{vmatrix} 0 & a & b & 0 \\ i & c & d & k \\ j & e & f & l \\ 0 & g & h & 0 \end{vmatrix}$ 5) $\begin{vmatrix} a & 0 & 0 & j \\ b & 0 & 0 & i \\ c & 0 & 0 & h \\ d & e & f & g \end{vmatrix}$ 6) $\begin{vmatrix} d & 0 & 0 & g \\ c & e & f & h \\ b & 0 & 0 & i \\ a & 0 & 0 & j \end{vmatrix}$ 7) $\begin{vmatrix} a & b & c & d \\ 0 & 0 & e & 0 \\ 0 & f & 0 & 0 \\ g & h & i & j \end{vmatrix}$

8) $\begin{vmatrix} a & 0 & 0 & g \\ b & e & f & h \\ c & 0 & 0 & i \\ d & 0 & 0 & j \end{vmatrix}$ 9) $\begin{vmatrix} a & b & c & d \\ 0 & e & f & 0 \\ 0 & g & h & 0 \\ 0 & i & j & 0 \end{vmatrix}$ 10) $\begin{vmatrix} d & 0 & 0 & j \\ c & e & 0 & i \\ b & 0 & f & h \\ a & 0 & 0 & g \end{vmatrix}$.

Obrazuj kakve druge figure, slova itd. ispisivanjem po redu slova, brojeva itd. pa izračunaj nastalu determinantu.

9. 1) Svaku komponentu determinante iz zad. 2 pomnoži brojem k; kolika je nova determinanta? 2) Kako bi bilo da isto množenje vršimo na determinanti poretka $n \times n$?

10. Pomnoži brojem 5 elemente 3-eg stupca u determinanti iz zad. 2; kolika je nova determinanta? Poopći!

11. Prvom stupcu determinante iz zad. 2 dodaj sumu ostalih stupaca; kolika je nova determinanta?

12. Kako se mijenja vrijednost determinante kad joj se svi stupci pišu obratnim redom?

13. Nađi det a stupnja 4×4, 5×5, koja se formira kao u § 2.10.10.

14. $\begin{vmatrix} a & b & c & d \\ b & -a & d & -c \\ c & -d & -a & b \\ d & c & -b & -a \end{vmatrix} = ?$

15. Riješi: 1) $\begin{vmatrix} 1 & 1 \\ 1 & 1-x \end{vmatrix} = 0$;

2) $\begin{vmatrix} 1 & 1 & 1 \\ 1 & 1-x & 1 \\ 1 & 1 & 2-x \end{vmatrix} = 0$; 3) $\begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 1-x & 1 & 1 \\ 1 & 1 & 2-x & 1 \\ 1 & 1 & 1 & 3-x \end{vmatrix} = 0.$

16. 1) $\begin{vmatrix} a & b \\ b & a \end{vmatrix}$ 2) $\begin{vmatrix} a & b & c \\ b & c & a \\ c & a & b \end{vmatrix}$ 3) $\begin{vmatrix} a & b & c & d \\ b & c & d & a \\ c & d & a & b \\ d & a & b & c \end{vmatrix}$.

4. GLAVNA SVOJSTVA DETERMINANATA

Pri promatranju bilo koje matrice, odnosno determinante, imajmo na umu specijalno matrice poretka (2, 2) jer su one vrlo jednostavne; a u drugu ruku mnoga svojstva determinanata poretka (n, n) izriču se nezavisno od n.

4.1. Vidimo da je

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = -\begin{vmatrix} b & a \\ d & c \end{vmatrix}.$$

Permutiraju li se međusobno dva stupca tablice (kojoj je oblast $I2 \times I2$), *determinanta prelazi u protivno-jednaku.*[1)]

4.2. Vidimo da je

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = \begin{vmatrix} a & c \\ b & d \end{vmatrix}.$$

Permutira li se svaki redak s odgovarajućim stupcem, determinanta se ne mijenja.

[1)] Toj činjenici dobro je staviti nasuprot činjenicu da je sistem linearnih jednadžbi

$$\begin{matrix} ax + by = h \\ cx + dy = k \end{matrix} \quad \text{isto što i} \quad \begin{matrix} by + ax = h \\ dy + cx = k. \end{matrix}$$

I kod drugih iskaza o determinantama dobro je gledati kako se pojedina promjena na tablici očituje kod determinante, a kako kod „pripadnog" sistema linearnih jednadžbi.

4.3. $\begin{vmatrix} ka & kb \\ a & b \end{vmatrix} = 0$, odnosno $\begin{vmatrix} a & ka \\ c & kc \end{vmatrix} = 0$;

Ako je jedan redak (stupac) *proporcionalan s drugim retkom* (*stupcem*), *determinanta je jednaka* 0.

4.4. $\begin{vmatrix} a+kb & b \\ c+kd & d \end{vmatrix} = (a+kb)\,d - b\,(c+kd) = ad - bc = \begin{vmatrix} a & b \\ c & d \end{vmatrix}$:

Ako se neki stupac pomnoži sa k i doda nekom drugom stupcu, determinanta se ne mijenja.

Itd.

4.5. Dokaz tih i drugih zakonitosti o determinantama provest ćemo kasnije (v. poglavlje 11).

4.6. Tri važne primjedbe. Na ovom mjestu želimo istaknuti ovu principijelnu stvar.

4.6.1. Determinante su historijski nastale u vezi s proučavanjem sistema linearnih jednadžbi. Determinante su snažno pomoćno sredstvo u proučavanju linearnih sistema.

4.6.2. S linearnim jednadžbama izvodimo razne manipulacije i operacije, a da se rješenja ne mijenjaju. Tako je npr. očigledno da sistem jednadžbi $\begin{matrix} ax+by=0 \\ cx+dy=0 \end{matrix}$ i sistem jednadžbi $\begin{matrix} cx+dy=0 \\ ax+by=0 \end{matrix}$ znače jedno te isto. Naprotiv, pripadne determinante nisu iste!

4.6.3. Zato koliko god determinante bile korisne kod linearnih sistema, one nisu vjerno i potpuno ogledalo za linearne sisteme. Pravo ogledalo su tablice ili matrice. Zato je prirodno da se upoznamo s tim važnim matematičkim objektima!

4.7. Zadaci o determinantama reda (3,3).

1. Na determinantama stupnja 3×3, 4×4 provjeri ova pravila:

   1) Ako jedan stupac ima samo 0, determinanta je $= 0$.

   2) Ako u determinanti dva stupca zamijene svoja mjesta, determinanta prelazi u suprotno-jednaku vrijednost; slično za rediće. Npr.

$$\begin{vmatrix} 3 & 5 & 7 \\ 4 & 9 & -2 \\ 8 & 12 & 16 \end{vmatrix} = -\begin{vmatrix} 7 & 5 & 3 \\ -2 & 9 & 4 \\ 16 & 12 & 8 \end{vmatrix}$$ (prvi i treći stupac su međusobno smijenjeni).

   3) Ako se svaki redić smijeni odgovarajućim stupčićem, determinanta se ne mijenja Npr.

$$\begin{vmatrix} 5 & 6 & 9 \\ -3 & 4 & 8 \\ 1 & 2 & 3 \end{vmatrix} = \begin{vmatrix} 5 & -3 & 1 \\ 6 & 4 & 2 \\ 9 & 8 & 3 \end{vmatrix}.$$

4) Ako se elementi nekog stupca množe sa k, množi se i vrijednost determinante sa k; npr.

$$\begin{vmatrix} 5 & 4 & -3 & 2 & \cdot 6 \\ 1 & 3 & 8 & 2 & (-1) \\ 4 & 1 & 2 & 2 & \cdot 5 \\ 1 & 3 & 4 & 2 & \cdot 6 \end{vmatrix} = 2 \begin{vmatrix} 5 & 4 & -3 & 6 \\ 1 & 3 & 8 & -1 \\ 4 & 1 & 2 & 5 \\ 1 & 3 & 4 & 6 \end{vmatrix};$$

5) Ako se nekom stupcu determinante dodaju preostali stupci iste determinante umnoženi s kakvim izrazima, determinanta se ne mijenja.

Npr. $$\begin{vmatrix} 2 & 5 & 4 \\ 3 & 1 & 6 \\ 1 & 6 & 3 \end{vmatrix} = \begin{vmatrix} 2 & 5 & 4-2\cdot 2 \\ 3 & 1 & 6-2\cdot 3 \\ 1 & 6 & 3-2\cdot 1 \end{vmatrix} = \begin{vmatrix} 2 & 5 & 0 \\ 3 & 1 & 0 \\ 1 & 6 & 1 \end{vmatrix}$$

(trećem stupcu se dodao prvi stupac umnožen sa -2 i drugi stupac umnožen sa 0).

2. Slično kao zad. 1 radeći s redićima determinante.

3. Provjeri $$\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix} \cdot \begin{vmatrix} a_1' & b_1' & c_1' \\ a_2' & b_2' & c_2' \\ a_3' & b_3' & c_3' \end{vmatrix} =$$

$$= \begin{vmatrix} a_1 a_1' + a_2 a_2' + a_3 a_3', & a_1 b_1' + a_2 b_2' + a_3 b_3', & a_1 c_1' + a_2 c_2' + a_3 c_3' \\ b_1 a_1' + b_2 a_2' + b_3 a_3', & b_1 b_1' + b_2 b_2' + b_3 b_3', & b_1 c_1' + b_2 c_2' + b_3 c_3' \\ c_1 a_1' + c_2 a_2' + c_3 a_3', & c_1 b_1' + c_2 b_2' + c_3 b_3', & c_1 c_1' + c_2 c_2' + c_3 c_3' \end{vmatrix}.$$

4. Provjeri $\det a = a_{11} fa_{11} + a_{21} fa_{21} + a_{31} f_{31}$; pri tom fa_{ik} znači produkt broja $(-1)^{i+k}$ s determinantom što nastaje iz a brisanjem i-tog redića i k-og stupčića; npr.

$$\begin{vmatrix} 5 & 6 & 7 \\ 2 & 4 & 9 \\ 3 & 1 & 2 \end{vmatrix} = 5(-1)^{1+1} \begin{vmatrix} 4 & 9 \\ 1 & 2 \end{vmatrix} + 2\cdot(-1)^{2+1} \begin{vmatrix} 6 & 7 \\ 1 & 2 \end{vmatrix} + 3\cdot(-1)^{3+1} \begin{vmatrix} 6 & 7 \\ 4 & 9 \end{vmatrix}.$$

5. Uvjeri se da $\begin{vmatrix} x & y & 1 \\ x_0 & y_0 & 1 \\ x_1 & y_1 & 1 \end{vmatrix} = 0$ znači jednadžbu pravulje što prolazi tačkama (x_0, y_0), (x_1, y_1) u Euklidovoj ravnini s pravokutnim Kartezijevim koordinatama.

6. Ploština orijentiranog trokuta (x_0, y_0), (x_1, y_1), (x_2, y_2) glasi $\frac{1}{2}\begin{vmatrix} x_0 & y_0 & 1 \\ x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \end{vmatrix}$. Dokaži.

7. Neka su zadane 3 tačke (x_0, y_0), (x_1, y_1), (x_2, y_2) u ravnini; uvjeri se da jednadžba

$$\begin{vmatrix} x^2+y^2, & x, & y, & 1 \\ x_0^2+y_0^2, & x_0, & y_0, & 1 \\ x_1^2+y_1^2, & x_1, & y_1, & 1 \\ x_2^2+y_2^2, & x_2, & y_2, & 1 \end{vmatrix} = 0$$

predstavlja kružnicu koja prolazi tim trima tačkama.

8. Nađi ploštinu orijentiranog paralelograma što ga u koordinatnoj ravnini razapinju radius-vektori 1) (3, 5), (4, 2); 2) (−3, −5), (4, 2); 3) −3, −5), (−4, −2).

Analogni zaključci vrijede i za prostor!

9. Dokaži $\begin{vmatrix} \sin a & \cos a & 1 \\ \sin b & \cos b & 1 \\ \sin c & \cos c & 1 \end{vmatrix} = \sin(a-b) + \sin(b-c) + \sin(c-a).$

10. Za $\triangle ABC$ odredi $\begin{vmatrix} a^2 & b\sin\alpha & c\sin\alpha \\ b\sin\alpha & 1 & \cos\alpha \\ c\sin\alpha & \cos\alpha & 1 \end{vmatrix}$.

11. Ako je $1+x+x^2=0$ nađi

1) $\begin{vmatrix} 1 & x & x^2 \\ x & x^2 & 1 \\ x^2 & 1 & x \end{vmatrix}$ 2) $\begin{vmatrix} 1 & 1 & x \\ 1 & 1 & x^2 \\ x^2 & x & 1 \end{vmatrix}$ 3) $\begin{vmatrix} 1 & 1 & 1 \\ 1 & x & x^2 \\ 1 & x^2 & x \end{vmatrix}$

4) $\begin{vmatrix} x^2 & x & 1 \\ x & 1 & x^2 \\ 1 & x^2 & x \end{vmatrix}$ 5) $\begin{vmatrix} 1 & x^2 & x \\ x^2 & x & 1 \\ x & 1 & x^2 \end{vmatrix}$ 6) $\begin{vmatrix} 1 & x & x^2 \\ x^2 & 1 & x \\ x & x^2 & 1 \end{vmatrix}$.

12. Za determinante reda 2×2, 3×3 dokaži ovo:

ako je $a_{ik} = \overline{a_{ki}}$, tad je $\det a$ realan broj.

13.

$$\begin{vmatrix} \cos\varphi\cos\psi - \sin\varphi\sin\psi\cos\theta, & -\sin\varphi\cos\psi - \cos\varphi\sin\psi\cos\theta, & \sin\psi\sin\theta \\ \cos\varphi\sin\psi + \sin\varphi\cos\psi\cos\theta, & -\sin\varphi\sin\psi + \cos\varphi\cos\psi\cos\theta, & -\cos\psi\sin\theta \\ \sin\varphi\sin\theta, & \cos\varphi\sin\theta, & \cos\theta, \end{vmatrix} = ?$$

POGLAVLJE 10.

PRVI UVOD U RAČUN MATRICA

1. POJAM MATRICE ILI TABLICE

1.0. Vrlo često imamo posla s *tablicama* raznih podataka. Tako se npr. može govoriti o *tablici* iz koje će se za pojedine gradove (države, kontinente) vidjeti koliko je u njima prosječno bilo stanovnika u svakoj od godina 1900—1950. Ili npr. da je riječ o klasifikacionoj tablici učenika pojedinih razreda.

Oblik bi tablice bio:

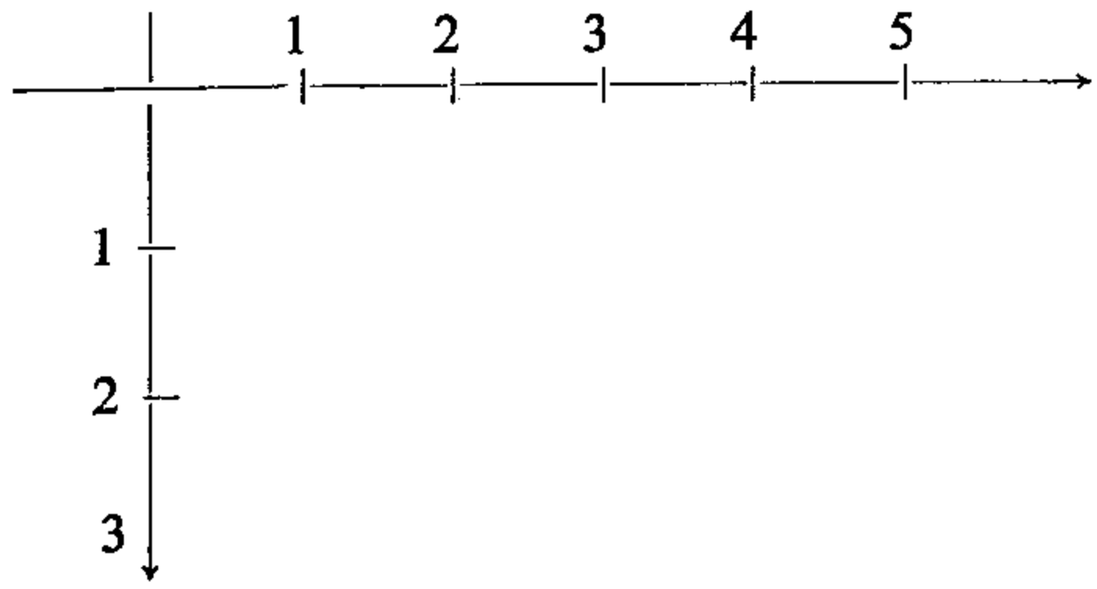
Godina / Grad	1900.	1901.	1902.	1903.
A				
B				
C				

Naznačeno polje odnosi se na grad imena *C* i godinu 1902, pa bi na tom polju trebalo pisati koliko je grad *C* imao stanovnika u godini 1902. Radi lakšeg snalaženja upisuju se takvi podaci na papiru s kvadratićima (karirani papir poput šahovske ploče); polja na papiru pravimo i sami crtajući niz vertikalnih i horizontalnih crta; sjeti se npr. klasifikacionih podataka za jedan razred u toku jedne godine, itd.

1.1. Označivanje poljâ ili parcelâ. Polja u tablici označujemo pomoću dva podatka: podatka nalijevo i podatka gore; npr. naznačeno polje u gornjoj tablici bilo bi „polje *C* 1902“ ili polje (*C*, 1902) i sl.

To polje leži u *trećem retku* i *trećem stupcu*; zato se ono može zvati polje (3, 3). Još je bolje da se služimo *rednim* pozitivnim brojevima 1, 2, 3, · · ·

U toj cifarskoj oznaci neispunjena tablica od $3 \cdot 5$ poljâ nosila bi okvirne oznake:



(Npr. lijevo 1 znači A iz prve tablice; gornje 1 zamjenjuje 1900 iz iste gornje tablice). U tablicu se upisuju odgovarajući podaci.

1.2. Primjer tablice u vezi s jednadžbama. Ako imamo jednadžbe

$$\begin{aligned} -5x + \quad y - 4t + \ 3u &= \ 4 \\ 5x + \ 6y + 7t + \ 8u &= \ 9 \\ 10x + 10y + 8t + 13u &= 14, \end{aligned}$$

tada sve te koeficijente možemo ispisati u odgovarajuću tablicu:

$$\begin{array}{rrrrr} -5 & 1 & -4 & 3 & 4 \\ 5 & 6 & 7 & 8 & 9 \\ 10 & 10 & 8 & 13 & 14. \end{array}$$

Svaki redak tablice se odnosi na odgovarajuću zadanu jednadžbu. Posljednji stupac odnosi se na desne strane jednadžbi; svaki preostali stupac odnosi se na određenu nepoznanicu u zadanim jednadžbama.

U tablici se pojavljuju dvije osmice; njihove se uloge međusobno razlikuju; prva je smještena u drugom retku i četvrtom stupcu napisane tablice t; zato tu osmicu možemo naznačiti sa t_{24}; slično bi druga osmica glasila $8 = t_{33}$. Naravno t_{13}, se ne čita »*te trinaest*«, nego »*te jedan tri*«.

1.3. Pojava Descartesova kvadra. Kad gledamo kakvu pravokutnu tablicu (kao npr. tablicu gornjih brojeva), tada treba u mislima zamisliti ili stvarno naznačiti okvirne podatke tablice t i npr. pisati ovako:

	1	2	3	4	5
1					
2					
3					

Okvir tablice

	1	2	3	4	5
1	11	12	13	14	15
→2	21	22	23	24	25
3	31	32	33	34	35

Ispisan raspored poljâ

→

−5	1	−4	3	4
5	6	7	8	9
10	10	8	13	14

Sama tablica

(Descartesov kvadar $[1, 3] \times [1, 5]$

Vidimo da se u ispisanom rasporedu poljâ pojavljuju uređeni parovi s ciframa 1, 2, 3 kao prvim članom i ciframa 1, 2, 3, 4, 5 kao drugim članom. Svi ti parovi čine Descartesov kvadar $[1, 3]\times[1, 5]$. Veza između toga Descartesova kvadra i napisane tablice t sastoji se u tome da svaki element (i, j) iz $[1, 3]\times[1, 5]$ ima svoje polje i, j na kojem u t stoji ispisan broj; označimo taj broj sa t_{ij}; tako npr. $-5=t_{11}$ (naime, -5 je u prvom retku i prvom stupcu). Šta je npr. t_{12}? To je ono što stoji u prvom retku i u drugom stupcu; dakle je $t_{12}=1$.

Na taj način gornja tabela t pruža (predstavlja) ovo preslikavanje Descartesova kvadra $[1, 3]\times[1, 5]$:

$$(11)\rightarrow -5, \quad 12\rightarrow 1, \quad 13\rightarrow -4, \quad 14\rightarrow 3, \quad 15\rightarrow 4$$

$$21\rightarrow 5, \quad \text{itd.}$$

ili kraće ovako:

$$t_{11}=-5, \quad t_{12}=1, \quad t_{13}=-4 \text{ itd.}$$

Na primjeru gornje tablice tipa $I3\times I5$ riječ je, dakle, o određenoj funkciji (radnji) na Descartesovu kvadru $1(3)\times 1(5)$ (od 15 polja).

1.4. Još dva primjera o Descartesovu kvadru. Budimo ***svjesni*** toga da npr. automatskim ispisivanjem niza prvih 15 rednih brojeva u obliku

$$\begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 & 9 \\ 10 & 11 & 12 & 13 & 14 \end{array}$$

vršimo potpuno određeno preslikavanje Descartesova kvadra $I3\times I5$; pri tom ispisivanju i, tj. kod te funkcije i, rada i, na kvadru $I3\times I5$ imamo:

$$i_{00}=0, \ i_{01}=1, \cdots, \text{ općenito: } i_{xy}=5x+y \text{ za svako } x\in I3$$

$$\text{i svako } y\in I5.$$

Isto tako pišući redne brojeve ovako:

$$\begin{array}{ccccc} 0, & 2, & 4, & 6, & 8, \cdots \\ 1, & 3, & 5, & 7, & 9, \cdots \end{array}$$

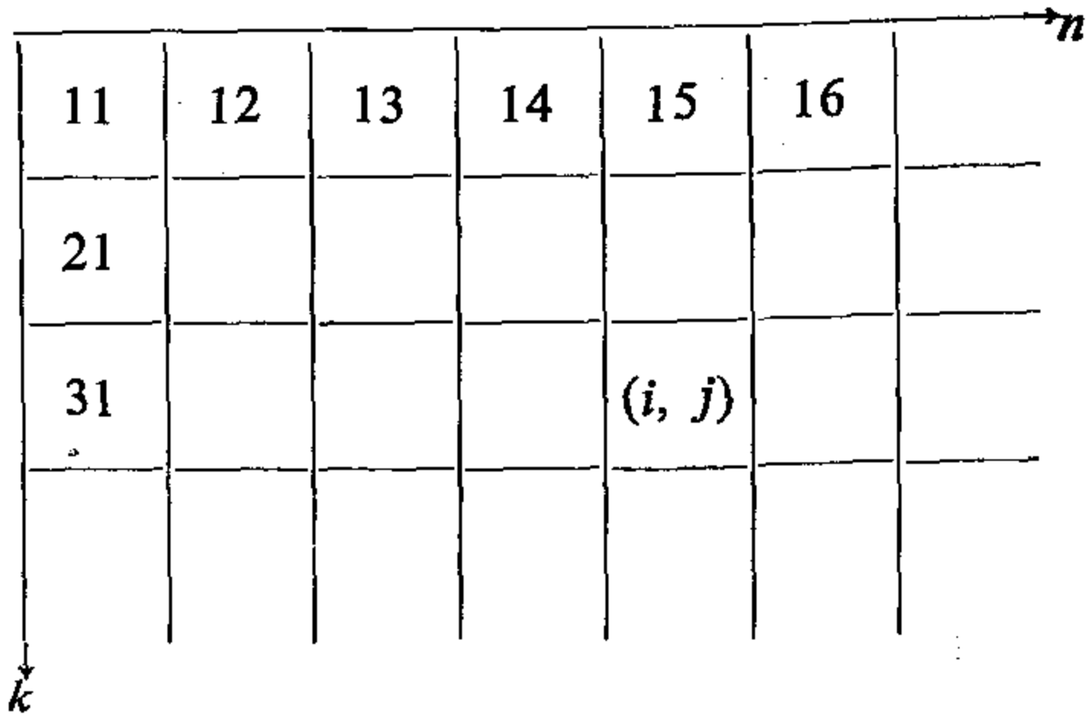
imamo potpuno određenu funkciju (tablicu) P na beskonačnu Descartesovu kvadru $I2\times I\omega$, gdje je $I\omega=\{0, 1, 2, \cdots\}$. Kod te funkcije P je

$$P(x, y)=x+2y.$$

Kad nam je to sada postalo posve jasno, prelazimo na definiciju matrica. Imajmo također u mislima Descartesov kvadar kao nešto što je ostvareno npr. kariranim papirom s odgovarajućim brojem poljâ.

1.5. Definicija matrica. — 1.5.0. Definicija matrice. Neka je (k, n) uređen par rednih brojeva >0 (jedan ili oba od tih brojeva može biti ω, za koji znamo da je $1(\omega)=\{1, 2, 3, \cdots\}$.

Promatrajmo pripadne intervale $\{k)=\{1, 2, \cdots\}$, $\{n)$ od prvih k, odnosno n rednih pozitivnih brojeva $1, 2, \cdots$ te njihov Descartesov produkt $\{k)\times\{n)=$ $=\{(i, j);\ i\in\{k),\ j\in\{n)\}$ položen ovako:



Ako svakom elementu (i, j) iz $\{k)\times\{n)$ (dakle $i\in\{k)$ te $j\in\{n)$ pridružimo neki predmet, skup, funkciju $\cdots a_{ij}$, tada se to preslikavanje (pridruživanje) $(i, j)\to a_{ij}$ zove *matrica a*, kojoj je *oblast ili domen jednak* $\{k)\times\{n)$; *govori se također da imamo posla s matricom a razreda ili poretka ili oblasti* $k\times n$ *odnosno* (k, n) (*ne brkaj poredak* (k, n) *s poretkom* (n, k). Piše se $\mathrm{Dom}\ a=\{k)\times\{n)$, tj. domen ili oblast matrice (funkcije) a je $\{k)\times\{n)$. Radi kratkoće pisat ćemo i $\mathrm{Dom}\ a=k\times n$ ili čak $\mathrm{D}\,a=k\times n$. Znak a_{ij} zove se *vrijednost* (također *element*, *komponenta*) matrice a u tački ili polju (i, j).

Specijalno će dolaziti pitanje da li a_{ij} jest ili nije 0. Ako a_{ij} nije 0, možemo a_{ij} (ili još bolje (i, j, a_{ij}) zvati *topom* matrice a.[1)]

1.5.1. U ovoj knjizi ćemo uglavnom pretpostavljati da je najmanje jedan od brojeva k, n konačan; ako su oba broja k, n beskonačna, onda ima iskazâ u ovoj knjizi koje bi trebalo mijenjati, prilagođivati i sl.

1.5.2. Oznaka matrica. Matrice se označuju (kao i druge funkcije): slovima, raznim znakovima itd. No postoji i posebna *matrična* ili *tablična oznaka*: oznaka u obliku tablice ili „matrice". *Vrijednost funkcije* (matrice) *slaže se u jednu pravokutnu tablicu, a onda se ta tablica još stavi obično u zagradu* (i to okruglu ili uglastu; zbog štampanja zgodnije se služiti *uglastim* zagradama). Tako npr. $\begin{bmatrix}1 & 2 & 3 & 4\\ 0 & 3 & -1 & 2\end{bmatrix}$ je tablica (matrica) poretka 2×4; označimo li je sa t, tada je $\mathrm{Do}\ t=\{2)\times\{4)$; tu je npr. $t_{11}=1$, $t_{23}=-1$.

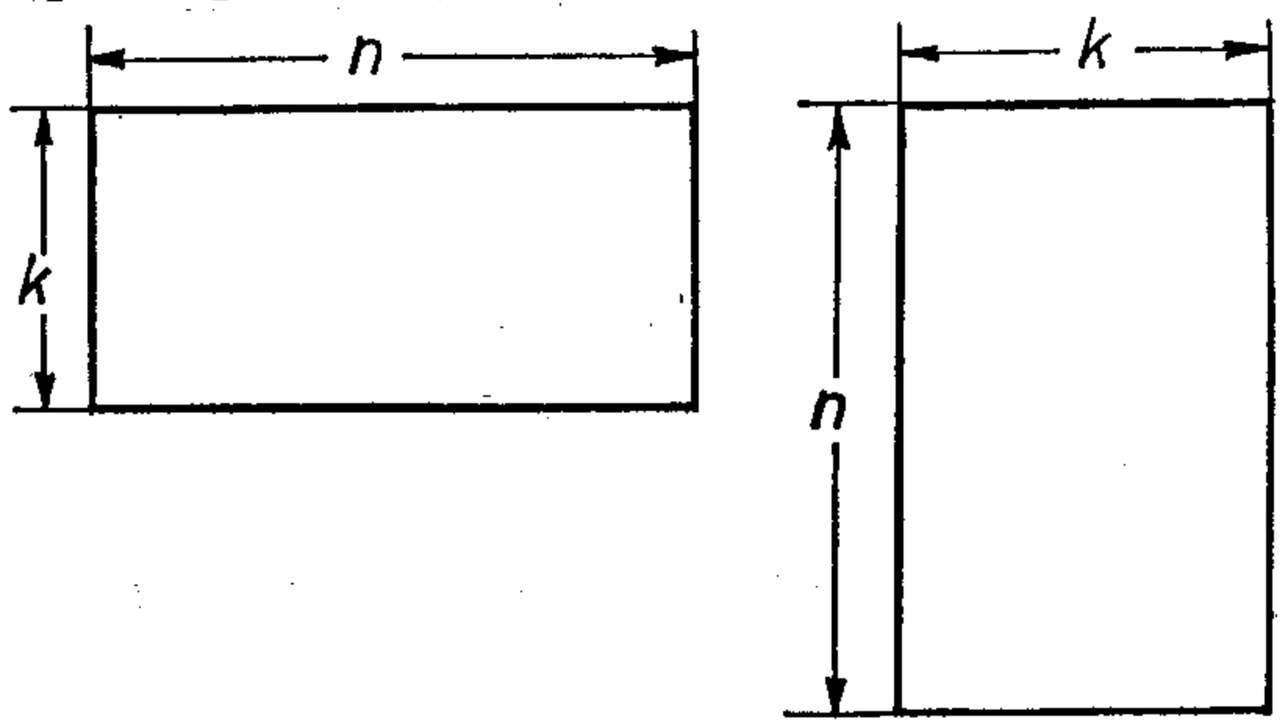
Shematski, može se matrica tipa $k\times n$ predstaviti kao pravokutnik (vidi sliku 10.1.5.2).

Ta matrica nije isto što i matrica razreda $n\times k$.

[1)] I svaki broj, vektor, $\cdots$ koji nije 0 može se zvati *topom* (isp. pogl. 8, § 2.6).

D e f i n i c i j a. *i*-ti redak (*i*-ti redić) matrice a jest ona podfunkcija $a_{i\cdot} = [a_{i1}\, a_{i2} \cdots a_{in}]$ matrice a za koju je $D_1 a_{i\cdot} = \{i\}$, $D_2 a_{i\cdot} = D_2 a$; *j-ti stupac matrice* a jest ona podfunkcija $a_{\cdot j} = \begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{kj} \end{bmatrix}$ kojoj je oblast $= D_1 a \times \{j\}$.

Pri tom je $D_1 a$ (odn. $D_2 a$) skup svih prvih (drugih) indeksâ, tj. $D_1 a = Pr_1 \operatorname{Dom} a$, $D_2 a = Pr_2 \operatorname{Dom} a$ (v. 3 § 5.7).



Sl. 10.1.5.2.

1.5.3. Reci, stupci i dijagonala matrice.

Dijagonala matrice a jest ona podfunkcija od a kojoj je oblast upravo dijagonala oblasti od a tj. skup $\{(1, 1), (2, 2), (3, 3) \cdots (e, e), \cdots\}$ gdje je $e = 1, 2, \cdots, \inf\{k, n\}$.

Prema tome, dijagonala matrice a nije podmatrica osim naravno ako je matrica a tipa (1, 1).

Ako je riječ o matrici a, tada ćemo njene retke označivati po redu sa $a_{1\cdot}$ ili $a_{(1)}$, $a_{2\cdot}$ ili $a_{(2)}$, $a_{3\cdot}$ ili $a_{(3)}, \cdots$; njene stupce ćemo označivati sa $a_{\cdot 1}$ ili $a^{(1)}$, $a_{\cdot 2}$ ili $a^{(2)}$, $a_{\cdot 3}$ ili $a^{(3)}$, itd. Prema tome $a_{1\cdot}$ znači *prvi redak* matrice a, tj. niz $a_{11}, a_{12}, \cdots, a_{1n}$.

Upotreba indeksa i u eksponentu ima velikih prednosti. Inače se ne treba bojati da se pobrka $a^{(2)}$ kao oznaka za drugi stupac matrice a i oznaka za »*kvadrat*« *matrice* a (v. pravilo M_4 u § 1.5.4); iz konteksta se uvijek vidi o čemu je riječ.

1.5.4. Organizacija matrica i veze s brojevima. Za matrice uvodimo ove uslove M_1—M_5 *o jednakosti i nejednakosti, računanju i vezama s brojevima i brojevnim izrazima:*

1) *Uslov* M_1 (*jednakost i nejednakost matrica*). *Matrica* a *jednaka je matrici* b, *simbolički*

(1) $a = b$, ako je

(2) $\operatorname{Dom} a = \operatorname{Dom} b$, te

(3) $a_{ij} = b_{ij}$

za svako $i \in 1\,(k)$, $j \in 1\,(n)$. *Ako nije* $a = b$, *kaže se da je* a *nejednako* b *i piše* $a \neq b$. Npr. $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 1 & \sin x \end{bmatrix} = \begin{bmatrix} \cos^2\alpha + \sin^2\alpha, & 2, & 5-2 \\ 2 \cdot 2 & 1, & 2\cos x/2 \sin x/2 \end{bmatrix}$.

⟶ Primjedba. Matrična jednakost (1) znači isto što $k \cdot n$ jednakosti (3) zajedno s jednakošću (2). To treba dobro držati na umu!

2. *Uslov* M_2 (*zbrajanje matrica*). *Suma matrica a, b definira se uz uslov da su one iste oblasti, a definira se kao matrica* $a+b$ *za koju je*

$$(a+b)_{ij} = a_{ij} + b_{ij}.$$

Drugim riječima: matrice se zbrajaju tako da im se zbroje odgovarajuće vrijednosti. Ako je oblast od a različita od oblasti matrice b, tada se suma $a+b$ ne definira. Npr.

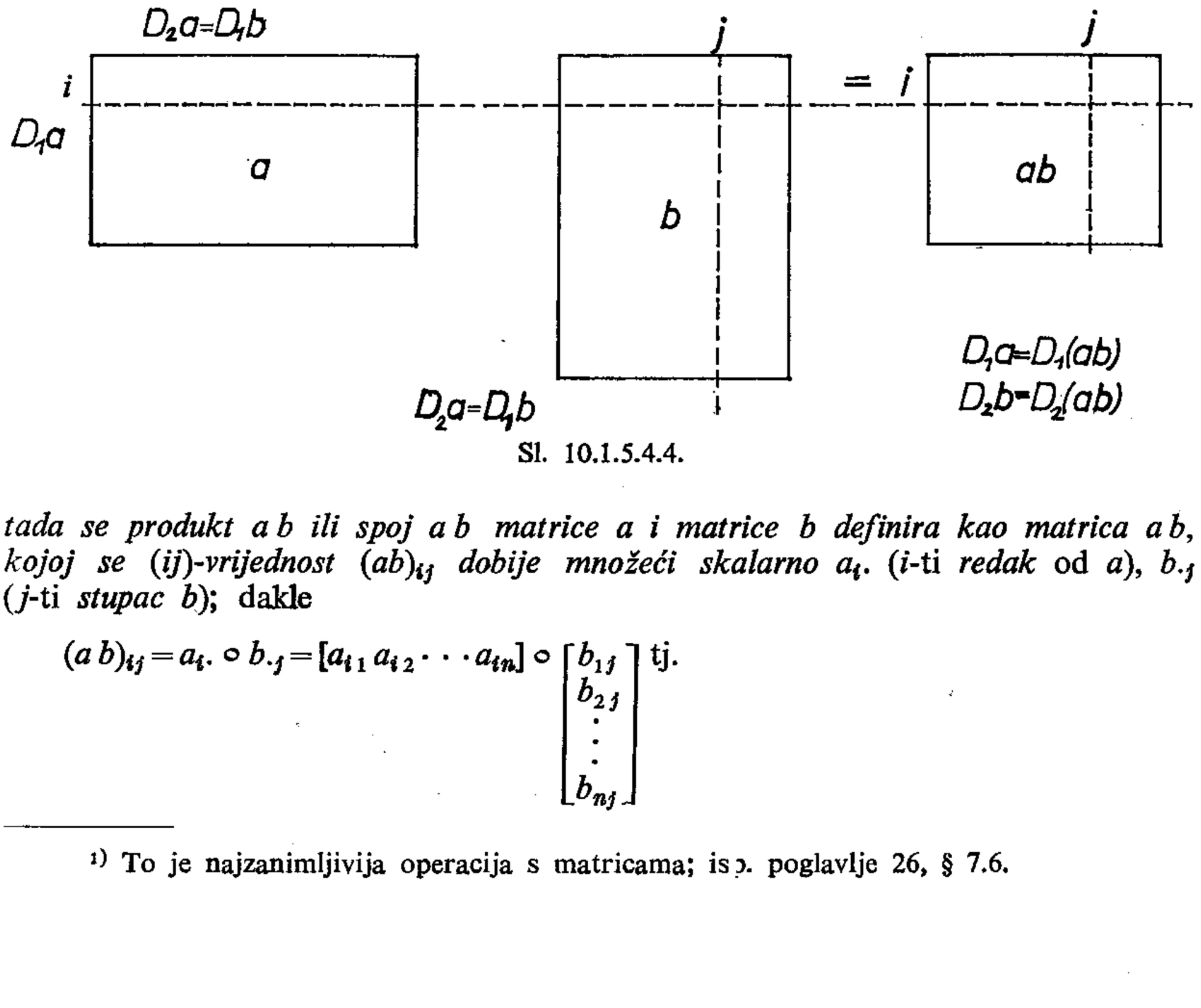
$$\begin{bmatrix} 2 & 3 & 4 \\ -3 & -2 & 5 \end{bmatrix} + \begin{bmatrix} 1 & 2 & 5 \\ 7 & 0 & 4 \end{bmatrix} = \begin{bmatrix} 2+1 & 3+2 & 4+5 \\ -3+7 & -2+0 & 5+4 \end{bmatrix} = \begin{bmatrix} 3 & 5 & 9 \\ 4 & -2 & 9 \end{bmatrix}$$

Npr. $[1 \quad 2] + [1 \quad 2 \quad 3]$ nije definirano.

3. **Uslov M_3 (množenje matrica i brojeva).** *Produkt matrice a i broja ili brojevnog izraza q dobije se tako da se svaka vrijednost matrice pomnoži sa q; produkt se označuje sa* $a\,q$. *Dakle je* $a\,q$ *matrica tipa* Dom a *te s vrijednostima* $(a\,q)_{ij} = a_{ij}\,q$. *Također je* $q\,a$ *matrica za koju je* $(q\,a)_{ij} = q\,a_{ij}$ tj. $q\,a = a\,q$.

Npr. $$3 \cdot \begin{bmatrix} 2 & 5 & 2 \\ 4 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 6 & 15 & 6 \\ 12 & 9 & 3 \end{bmatrix}.$$

4. **Uslov M_4 (množenje ili komponiranje matrica).**[1)] *Neka je* (a, b) *takav uređen par matrica da a ima toliko stupaca koliko b ima redaka* (v. skicu);



Sl. 10.1.5.4.4.

tada se produkt $a\,b$ *ili spoj* $a\,b$ *matrice a i matrice b definira kao matrica* $a\,b$, *kojoj se* (ij)*-vrijednost* $(ab)_{ij}$ *dobije množeći skalarno* $a_{i.}$ (i-ti *redak* od a), $b_{.j}$ (j-ti *stupac* b); dakle

$$(a\,b)_{ij} = a_{i.} \circ b_{.j} = [a_{i1}\, a_{i2} \cdots a_{in}] \circ \begin{bmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{nj} \end{bmatrix} \text{ tj.}$$

[1)] To je najzanimljivija operacija s matricama; isp. poglavlje 26, § 7.6.

$$(a\,b)_{ij} = a_{i1}\,b_{1j} + a_{i2}\,b_{2j} + \cdots + a_{in}\,b_{nj}. \qquad \text{Kraće}$$

$$(a\,b)_{ij} = \sum_{n'=1}^{n} a_{in'}\,b_{n'j}.$$

Tu se sumira po n' gdje je $n' \in \{n\} = \{1,\ 2, \cdots,\ n\}$. Prema tome je na slici $Do\,(a\,b) = \{k\} \times \{s\} = D_1\,a \times D_2\,b$. Npr.

$$\begin{bmatrix} 2 & 4 & 5 \\ 1 & 3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 1 & -2 & -5 \\ 5 & 4 & -3 \\ 3 & -3 & 4 \end{bmatrix} =$$

$$= \begin{bmatrix} 2\cdot 1 + 4\cdot 5 + 5\cdot 3 & 2\cdot -2 + 4\cdot 4 + 5\cdot -3 & 2\cdot -5 + 4\cdot -3 + 5\cdot 4 \\ 1\cdot 1 + 3\cdot 5 + 4\cdot 3 & 1\cdot -2 + 3\cdot 4 + 4\cdot -3 & 1\cdot -5 + 3\cdot -3 + 4\cdot 4 \end{bmatrix} =$$

$$= \begin{bmatrix} 37 & -3 & -2 \\ 28 & -2 & 2 \end{bmatrix}.$$

5. Uslov M_5 (most između matricâ i brojevâ odnosno izrazâ). *Svaku matricu razreda* (1, 1) *poistovećujemo s vrijednošću te matrice. Time se omogućuje da svaki broj i brojevni izraz postane matricom. Pri tom poistovećenju ne smijemo narušiti uslove M_3 i M_4.*

Npr. $[3] = 3$, $[\cos x] = \cos x$.

1.5.5. Primjedba na gornje definicije M_1—M_5. Pravila M_1—M_3 o matricama su pravila koja uvodimo i kod drugih funkcija (a ne samo kod matrica). *Tipično matrično pravilo je pravilo M_4 o množenju ili slaganju matricâ te matrično pravilo M_5, kojim se brojevi uključuju među matrice.* Kasnije ćemo vidjeti da se i tipično pravilo M_4 svodi na slaganje funkcija (isp. pogl. 23 te osobito 26, § § 7.5, 7.6).

1.5.6. Važna primjedba o oblasti matrice i o oblasti prve i druge varijable u matrici. Rekli smo da, radi kratkoće, govorimo da je neka matrica a razreda, oblasti, tipa, $\cdots$, $k \times n$, misleći pri tom stvarno da je ona određena funkcija s Kartezijevim produktom $\{k) \times \{n)$ kao svojom oblasti. Pri tom je za redne brojeve k, n simbol $\{k)$ (odnosno $\{n)$ prikrata za množinu svih prvih pozitivnih k (odnosno n) rednih brojeva. Trebalo bi umjesto »*matrica a razreda ili poretka* (k, n)« govoriti potpunije: »*matrica a kojoj je oblast* $\{k) \times \{n)$« ili naprosto »*matrica a sa* $Da = \{k) \times \{n)$« i sl.

No vrlo je važno imati na umu skupove $\{k)$, $\{n)$; to su projekcije oblasti Da matrice a; možemo ih kraće označiti sa

$$D_1\,a \text{ i } D_2\,a; \quad \text{dakle}$$

$D_1\,a$ je skup svih prvih indeksa 1, 2, $\cdots$ *u oznaci elemenata matrice a*; drugim riječima: $D_1\,a$ je domen *prve varijable* matrice (funkcije) a; isto tako $D_2\,a$ je domen $\{1, 2, \cdots\}$ *druge varijable* matrice (funkcije) a. Na taj način

$$Dom\,a = D_1\,a \times D_2\,a.$$

Ujedno, radi kratkoće, $D_1\,a$ (odn. $D_2\,a$) može značiti broj redaka (odn. stupaca) matrice a.

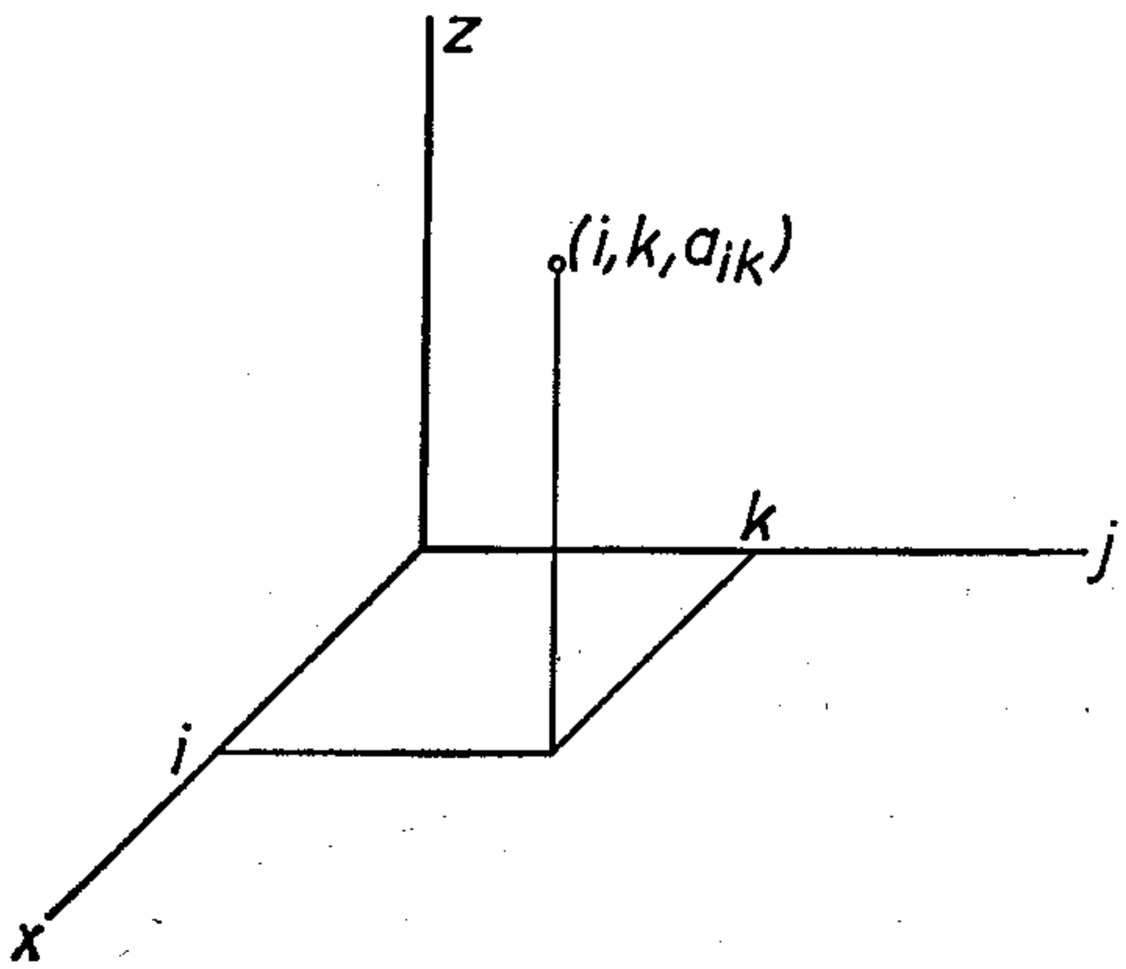
1.5.7. Važna primjedba o naravi matrica. Ne smetnimo nikad s uma *da su matrice određene funkcije s dvije varijable*; oblasti tih funkcija su Descartesovi produkti $\{k\}\times\{n\}$, gdje su k i n redni brojevi (konačni ili ne). No kod matrica se radi o jednom specijalnom, upravo matričnom, tabličnom *prikazivanju* funkcija. To se može koristiti i kod drugih općenitijih funkcija s dvije varijable. Inače znamo da se funkcija s dvije varijable, npr. $f(x, y)$ predstavlja u prostoru kao »*površina* $z=f(x, y)$«; stvarno je riječ o množini svih uređenih trojki $(x, y, f(x, y))$. To predstavljanje možemo, naravno, koristiti i kod matrica. Odgovarajući skup svih (x, y, a_{xy}), ako je riječ o matrici a, predstavljen je u prostoru s $k\cdot n$ tačaka. Te tačke (i, k, a_{ik}) možemo zvati *reprezentativnim tačkama matrice*.

Zato sada neće biti strano ako npr. gledajući matricu

$$\begin{bmatrix}2 & 0 & 0 & 2\\ 1 & 0 & 0 & 1\\ 2 & 1 & 2 & 1\end{bmatrix},$$

kažemo da se skup nula (topova) te matrice sastoji od 4 (odnosno 8) elemenata, mada sve te vrijednosti matrice (nula i topovi) čine skup, i to

tročlani skup $\{2, 0, 0, 2, 1, 0, 0, 1, 2, 1, 2, 1\}=\{0, 1, 2\}$.



Sl. 10.1.5.7.

1.6. P r i m j e d b a. Teoretski i operativno bilo bi mnogo opravdanije u gornjim definicijama umjesto $\{k\}$, $\{n\}$ upotrebljavati cifarske skupove Ik, In, da se mogu bolje iskoristiti dragocjena svojstva znaka i broja 0. Iz jezičnih i praktičnih razloga odustali smo od toga.

1.7. Zadaci o matricama. 1. Promatraj ove matrice

$$a=\begin{bmatrix}3 & -5\\ 4 & 2\end{bmatrix},\quad b=\begin{bmatrix}3 & 3\\ 4 & 2\\ 5 & 4\end{bmatrix},\quad c=[1,\ 5,\ 7,\ 8],\quad d=\begin{bmatrix}8 & x & y\\ 3 & 4 & 5\\ -2 & 3i & 54\end{bmatrix};$$

1) ispiši prvi stupac svake od tih matrica, 2) ispiši posljednji redić svake od tih matrica; 3) šta stoji na polju (1, 2)? 4) Odredi $a_{21}, b_{32}, c_{12}, d_{13}$; 5) riješi $a_{xy}=b_{xy}$; 6) odredi oblast svake od tih matrica a, b, c, d,

2. Zašto je $\begin{bmatrix}3+2 & 4-1 & 7\\ 3+i & 2 & 6\\ 4-1 & 5+7 & \log\ 100\end{bmatrix}=\begin{bmatrix}5 & 3 & 4+3\\ 3+i\frac{4}{2} & & 6\\ 3 & 12 & 2\end{bmatrix}$?

3. Nađi 1) $\begin{bmatrix}1 & 5\\3 & 7\end{bmatrix}+\begin{bmatrix}6 & -2\\4 & 3\end{bmatrix}$, 2) $\begin{bmatrix}1 & 5\\3 & 7\end{bmatrix}-\begin{bmatrix}6 & -2\\4 & 3\end{bmatrix}$.

4. Ako je $a=\begin{bmatrix}5 & -3\\7 & 2\end{bmatrix}$, $b=\begin{bmatrix}3 & 10\\-6 & 4\end{bmatrix}$, nađi:

1) $a_{\cdot 2}$; 2) $a_{2\cdot}$; 3) $b_{\cdot 2}$; 4) $a+b$; 5) $(a+b)_{\cdot 2}$; 6) $(a-b)_{1\cdot}$;
7) $(a+b)_{21}$; 8) $(ab)_{21}=a_{2\cdot}\circ b_{\cdot 1}$; 9) ab.

5. Kako glasi ispisana matrica x s oblasti 1) 2×2; 2) 3×4; 3) 6×12; 4) $(n-1)\times(n+1)$; 5) $(n-1)\times(n+2)$; 6) $r\times 5r$; 7) $5r\times r$?

6. U matrici $a=\begin{bmatrix}3 & -2 & 0 & 4\\7 & 2 & -1 & -2\\-1 & 3 & -5 & 4\end{bmatrix}$ riješi

1) $a_{xy}>0$; 2) $a_{xy}<0$; 3) $a_{xy}\leq 0$.

7. Za $a=\begin{bmatrix}5 & 10\\-3 & 6\end{bmatrix}$ nađi $a^2=a\cdot a$, $a^3=a^2\cdot a,\cdots$

8. Isto za matricu $X=\begin{bmatrix}\cos x & \sin x\\-\sin x & \cos x\end{bmatrix}$.

9. Nađi $\begin{bmatrix}3 & 4 & 5\\6 & 7 & 8\end{bmatrix}\cdot\begin{bmatrix}0 & 0\\0 & 0\\0 & 0\end{bmatrix}$.

10. Dokaži da zbroj i produkt matrica oblika

$$\begin{bmatrix}x & y\\-y & x\end{bmatrix}$$

ima opet takav oblik (x, y su realni brojevi).

11. Promatraj matrice $a, b, c,\cdots$ na oblasti 5×5 za koje je (i, k) — vrijednost: $a_{ik}=i+k$, $b_{ik}=i-k$, $c_{ik}=ik$, $d_{ik}=i:k$, $e_{ik}=i^k$, $f_{ik}=i^{1/k}$, $g_{ik}=\log_{i+1}k$, $h_{ik}=\cos i+\sin k$, $I_{ij}=ik+i^2k^2-10i$, $j_{ik}=i^3-4k^2-1$.
Nađi $a+b$, $c-d$, ae, $3a$, $3a-5f$, bd, $3bd,\cdots$
Kolike su pripadne determinante?

12. Kako glasi matrica koeficijenata ovog niza jednadžbi:

1) $3x-2y+4z=5$
$2x-y-2=0$
$x+5z=6$,

2) $5x_1+3x_2-4x_3+4x_4=5$
$2x_2-3x_1=6$
$x_4-2x_1=0$?

13. Kako glasi niz linearnih sređenih jednadžbi kojemu je matrica:

$$1)\ \begin{bmatrix} 2 & -3 & 4 \\ 3 & 2 & 1 \end{bmatrix}, \qquad \begin{bmatrix} 3 & 1 & 0 & 6 \\ 2 & 5 & 1 & 0 \\ 3 & 0 & 5 & 7 \end{bmatrix}?$$ Riješi te jednadžbe!

14. Zadane su jednadžbe $3x_1 - 2x_2 + 5x_3 = 4$

$$5x_1 + 3x_2 + 2x_3 = 5;$$

uvedi veličine y_1, y_2, y_4 pomoću veza:

$$x_1 = 2y_1 - y_2 + 3y_4,$$

$$x_2 = 5y_1 + 3y_2 - y_4,$$

$$x_3 = 6y_1 - y_2 + 5y_4.$$

Kako glasi matrica ishodnih jednadžbi a kako matrica dolaznih jednadžbi? Uvjeri se da je matrica novih nepoznanica u novom sistemu =

$$= \begin{bmatrix} 3 & -2 & 5 \\ 5 & 3 & 2 \end{bmatrix} \cdot \begin{bmatrix} 2 & -1 & 3 \\ 5 & 3 & -1 \\ 6 & -1 & 5 \end{bmatrix}.$$

15. Dokaži

$$1)\ \begin{bmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{bmatrix} \cdot \begin{bmatrix} \cos y & \sin y \\ -\sin y & \cos y \end{bmatrix} = \begin{bmatrix} \cos(x+y), & \sin(x+y) \\ -\sin(x+y), & \cos(x+y) \end{bmatrix},$$

$$2)\ \left(1 + \frac{a^2}{n^2}\right)^{1/2} \begin{bmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{bmatrix} = \begin{bmatrix} 1 & \frac{a}{n} \\ -\frac{a}{n} & 1 \end{bmatrix} \text{ za } a = n \operatorname{tg} x.$$

16. Koliko ima različitih dijadskih 1) matrica, 2) determinanata na oblasti 3×3? Nađi onu matricu kojoj je determinanta najveća odnosno najmanja. (Funkcija je dijadska ako su joj vrijednosti 0 ili 1.)

17. Isto pitanje ako su vrijednosti matrice u skupu 1) $\{-1, 1\}$, 2) $\{5, 8\}$.

18. U jediničnoj matrici

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

zamijeni jednu 0 brojem 1; a) koliko se dobije različitih 1) matrica, b) determinanata? c) Pomnoži svaku matricu sa svakom; da li se dobije koja nova matrica?

19. U matrici $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ permutiraj jednu 0 i jednu 1;

koliko se dobije različitih a) matrica, b) determinanata?

20. Promatraj šahovsku ploču kao matricu; nezauzeta polja neka budu ispunjena brojevima 0. Početni položaj je ovaj:

$$\begin{bmatrix} T & S & L & K & D & L & S & T \\ p & p & p & p & p & p & p & p \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ p & p & p & p & p & p & p & p \\ T & S & L & K & D & L & S & T \end{bmatrix}$$

Kolika je pripadna determinanta? Promatraj bilo koji položaj u šahovskoj igri ili problemu, promatraj pripadnu matricu i izračunaj pripadnu determinantu; učini to posebno, stavljajući:

$$p=1, \quad S=L=3, \quad T=4, \quad D=8, \quad K=10.$$

21. Na šahovska polja porazmjesti na sve moguće načine članove zadana niza od 64 člana među kojima može biti i jednakih; 1) koliko se dobije različitih tablica? 2) Promatraj poseban slučaj da su članovi 0 ili 1 i to 3) 30 nulâ i 30 jedinicâ, 4) 25 nulâ, 35 jedinica.

22. Dokazati.

1) $\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n & \binom{n}{2} \\ 0 & 1 & n \\ 0 & 0 & 1 \end{bmatrix}$, 2) za matricu $M = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$

vrijedi $M^n = M^{n-2} + M^2 - 1$ za $n = 3, 4, 5, \cdots$

2. MATRICA I NJENE PODMATRICE ILI MINORI

2.0. Priprava. Uz zadanu pravokutnu tablicu (matricu) možemo promatrati razne njene »*podmatrice*« (submatrice — dijelove koji su na stanovit način opet „pravokutne“ matrice (retke i stupce ubrajamo također među „pravokutne“ matrice). *Vrlo je važan odnos između matrice kao cjeline i njenih podmatrica kao stanovitih dijelova.* Odnos množine, odnosno funkcije, prema svojim podmnožinama, odnosno podfunkcijama, služi kao putokaz za promatranje podmatricâ zadane matrice.

2.1. Primjer. Promatrajmo sistem S jednadžbi:

$$S \qquad \begin{aligned} 2x+3y-4z &= 5 \\ 4x-5y+5z &= 3 \\ -x \qquad -8z &= -2. \end{aligned}$$

Jedan od njegovih podsistema (dijelova) je npr. ovaj:

$$T \qquad \begin{aligned} 2x+3y-4z &= 5 \\ -x \qquad -8z &= -2. \end{aligned}$$

Sastavljen je od prve jednadžbe j_1 i treće jednadžbe j_3 sistema S. Uz te sisteme S, T možemo promatrati tablice a, odnosno b, svih njihovih koeficijenata:

$$a=\begin{bmatrix} 2 & 3 & -4 & 5 \\ 4 & -5 & 5 & 3 \\ -1 & 0 & -8 & -2 \end{bmatrix},$$

odnosno

$$b=\begin{bmatrix} 2 & 3 & -4 & 5 \\ -1 & 0 & -8 & -2 \end{bmatrix}.$$

Kaže se da je matrica b podmatrica matrice a i da su joj reci ili redići po redu: prvi redak i treći redak od a, tj. $b=\begin{bmatrix} a_{1\cdot} \\ a_{3\cdot} \end{bmatrix}$; b nastaje iz a brisanjem (uklanjanjem) retka a_2.

2.2. Primjer. Ako u matrici a precrtamo redak a_2. te stupce $a_{\cdot 1}$, $a_{\cdot 3}$, preostaje od a ovo:

$$\left[\begin{array}{c|c|c|c} 2 & 3 & -4 & 5 \\ \hline -4 & -5 & 5 & 3 \\ \hline -1 & 0 & -8 & -2 \end{array}\right] = \begin{bmatrix} 3 & 5 \\ 0 & -2 \end{bmatrix}.$$

Ovaj je preostatak sadržan u recima $a_{1\cdot}$, $a_{3\cdot}$ te stupcima $a_{\cdot 2}$ $a_{\cdot 4}$; zato se taj preostatak matrice a može označiti

$$(*) \qquad a\,|\,\{1,3\}\times\{2,4\}, \quad \text{odnosno} \quad a^{(13)}_{(24)}$$

da se istaknu reci i stupci koji nisu precrtani.

Stvarno, funkcionalno se gornja submatrica ispisuje ovako u svojoj zavisnosti od a:

$$(*)=\begin{bmatrix} 3 & 5 \\ 0 & -2 \end{bmatrix}=\begin{bmatrix} a_{12} & a_{14} \\ a_{32} & a_{34} \end{bmatrix}.$$

Indeksi koji se tu pojavljuju upravo čine Kartezijev produkt

$$\{1,3\}\times\{2,4\}=\{1\,2,\ 1\,4,\ 3\,2,\ 3\,4\},$$

u kojem je naznačena potfunkcija funkcije a i definirana.

2.3. Podmatrica ima biti u prvom redu potfunkcija. Od bitne je važnosti da imamo na umu da je matrica određena funkcija s oblasti koja je *Kartezijev produkt* („pravokutnik").

To bitno svojstvo — i ništa više — tražit će se i od podmatrica kao potfunkcijâ.

2.4. Neke potfunkcije koje nisu podmatrice. U matrici

$$c=\begin{bmatrix} 8 & 8 & 8 \\ \boxed{8} & 8 & 8 \\ \boxed{8} & \boxed{8} & 8 \end{bmatrix}$$

naznačene tri osmice ne čine podmatricu funkcije c, mada je to određena potfunkcija g od matrice c kao funkcije; g nije podmatrica zato jer joj oblast nije Kartezijev produkt (nedostaje još ono 8 u sredini). Figura

8

8 8

za g ne može se dobiti iz figure za c *brisanjem potpunih redaka i potpunih stupaca.* Naznačene tri 8 leže na poljima (2, 1), (3, 1), (3, 2) domene $Da=[1, 3]\times[1, 3]$; projekcije od Dom g jesu $\{2, 3\}=D_1 g$, $\{1, 2\}=D_2 g$.

„Dijagonala" d

8

8

8

u matrici c potpuno je određena potfunkcija od c, ali *nije podmatrica* jer joj oblast nije Kartezijev produkt (nedostaju dva desna polja gore, dva krajnja u sredini i dva lijeva dolje). Gornja dijagonala ne može se dobiti brisanjem redaka i stupaca od c. Oblast ili domen dijagonale d je Dom $d=\{(1, 1), (2\ 2), (3\ 3)\}$; prvi brojevi tih parova daju prvu projekciju domena:

$$D_1 d=\{1, 2, 3\};$$

drugi brojevi daju drugu projekciju domena:

$$D_2 d=\{1, 2, 3\}.$$

Pripadni Kartezijev produkt $D_1 d\times D_2 d$ premašuje domenu dijagonale i ispunjava čak čitavu oblast polazne matrice c.

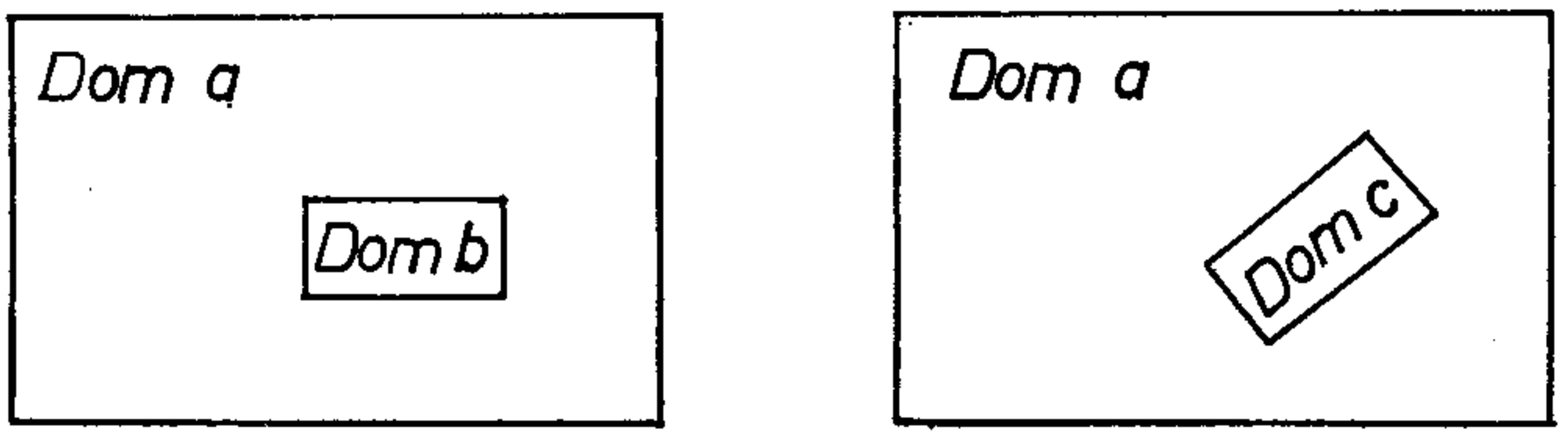
Na osnovu izloženog postavlja se ova osnovna definicija:

—→ **2.5. Definicija podmatrice ili minora.** *Ako je a zadana matrica tada se svaka potfunkcija b od a sa svojstvom da joj je domen Dom b Kartezijev produkt zove podmatrica ili minor matrice a*; to simbolički naznačujemo ovako: $b\subset a$.

Ako je $\mathrm{Dom}\, b = X \times Y$, može se pisati:

(1) $$b = a \mid X \times Y$$

da se vidi veza između b i a te da se vidi Kartezijev potkvadar $\mathrm{Dom}\, b = X \times Y$ kvadra $\mathrm{Dom}\, a$.



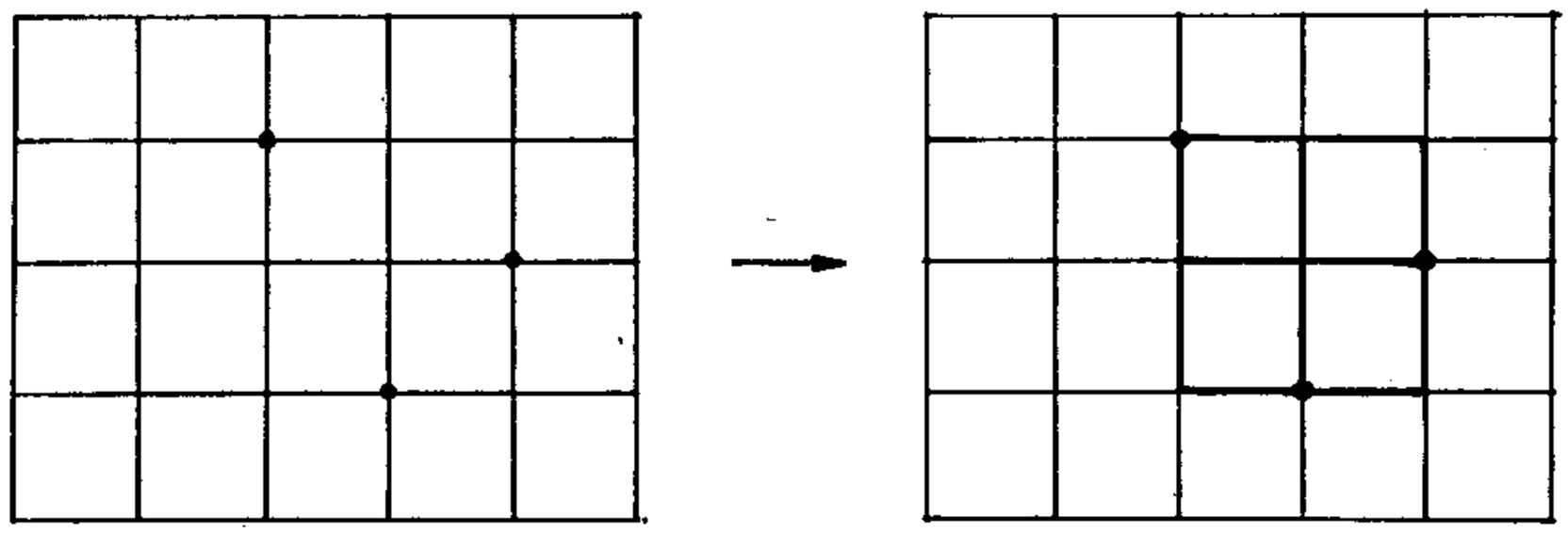
Sl. 10.2.5.

Drugim riječima, kod podmatrice b od a traže se dva i samo dva svojstva, i to: prvo, b je potfunkcija od a, tj. $Dom\, b \subset Dom\, a$; b i a *se podudaraju u* $Dom\, b$; drugo, *domen* od b *je Kartezijev kvadar*, tj.

$$Dom\, b = D_1 b \times D_2 b.$$

($D_1 b$ je prva projekcija od $Dom\, b$; to su redni brojevi *redića* u kojima je matrica b smještena.)

2.5.1. Primjer. Zadana je mreža — matrica



Sl. 10.2.5.1.

s označenim „topovima". Odredi najmanju podmrežu m u kojoj su ti topovi. Uvjeri se da je m sastavljeno od označena 3 čvorišta i onih čvorišta na koja djeluju po dva od tih topova. Tražena podmatrica čvorištâ je podebljana.

2.6. Uklanjanje redaka, stupaca. Oznaka submatricâ. Najjednostavniji slučaj da se dođe do podmatrice u a jest da se promatraju jedan ili više redaka (stupaca) te matrice i od njih formira odgovarajuća submatrica. Tako npr. u matrici

$$a = \left[\begin{array}{ccc|cc|c} 1 & 2 & 3 & 4 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 5 & 6 & 5 & 6 & 5 & 0 \\ 4 & 5 & 4 & 5 & 4 & 0 \\ \hline 7 & 2 & 7 & 2 & 7 & 0 \end{array}\right]$$

tvore reci $a_3.$, $a_4.$ podmatricu

$$\begin{bmatrix} a_3. \\ a_4. \end{bmatrix} = \begin{bmatrix} 5 & 6 & 5 & 6 & 5 \\ 4 & 5 & 4 & 5 & 4 \end{bmatrix};$$

možemo je označiti $a^{(3,4)}$; stupci $a_{(4)}$ i $a_{(5)}$ tvore matricu

$$[a_{.4}, a_{.5}] = \begin{bmatrix} 4 & 5 \\ 0 & 0 \\ 6 & 5 \\ 5 & 4 \\ 2 & 7 \end{bmatrix};$$

možemo je označiti sa $a_{(4,5)}$; presjek ili zajednički dio tih matrica daje opet određenu podmatricu, i to onu koja leži na *sjecištima* (presjecima) spomenutih redaka i stupaca (v. sliku), dakle

$$\begin{bmatrix} 6 & 5 \\ 5 & 4 \end{bmatrix}.$$

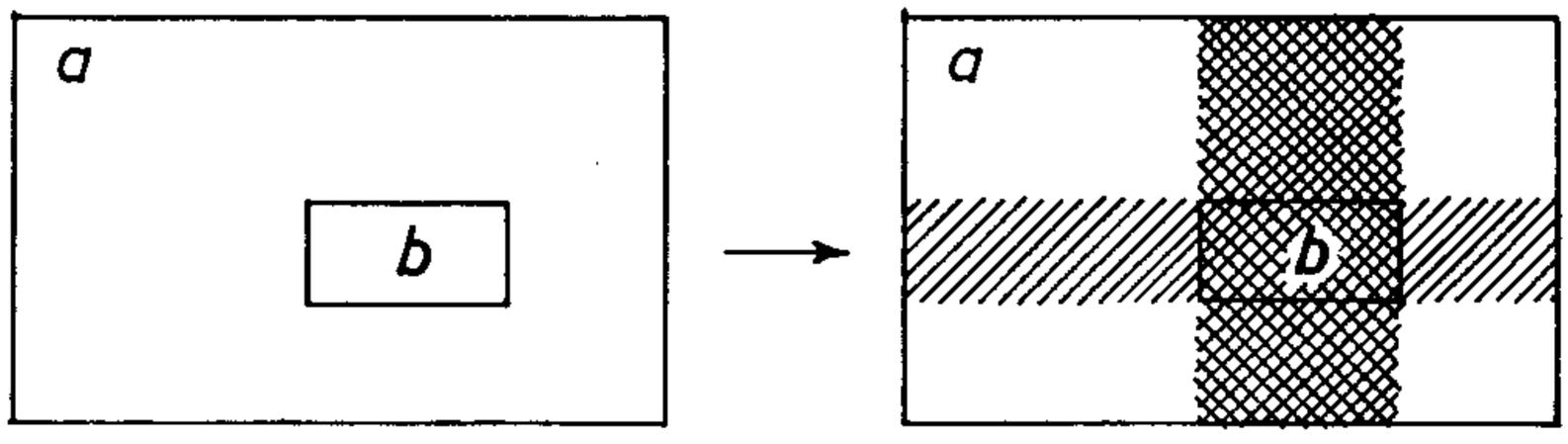
Možemo je označiti sa $a^{(3,4)} \cap a_{(4,5)}$ ili naprosto $a^{(3\,4)}_{(4\,5)}$, ili još kraće $a^{3\,4}_{4\,5}$. Prema tome, za svaku matricu x bilo bi

$$x^{(2\,4)}_{(3\,4)} = \begin{bmatrix} x_{23} & x_{24} \\ x_{43} & x_{44} \end{bmatrix}.$$

Zato je npr. $a_{ik} = a^{(i)} \cap a_{(k)} = a^i{}_k$.

2.7. Komplement zadane podmatrice *b* matrice *a* dobije se tako da se iz *a* izbrišu svi reci i stupci u kojima ima nešto od *b*.

Npr. komplement od uokvirene podmatrice je neisjenčan:



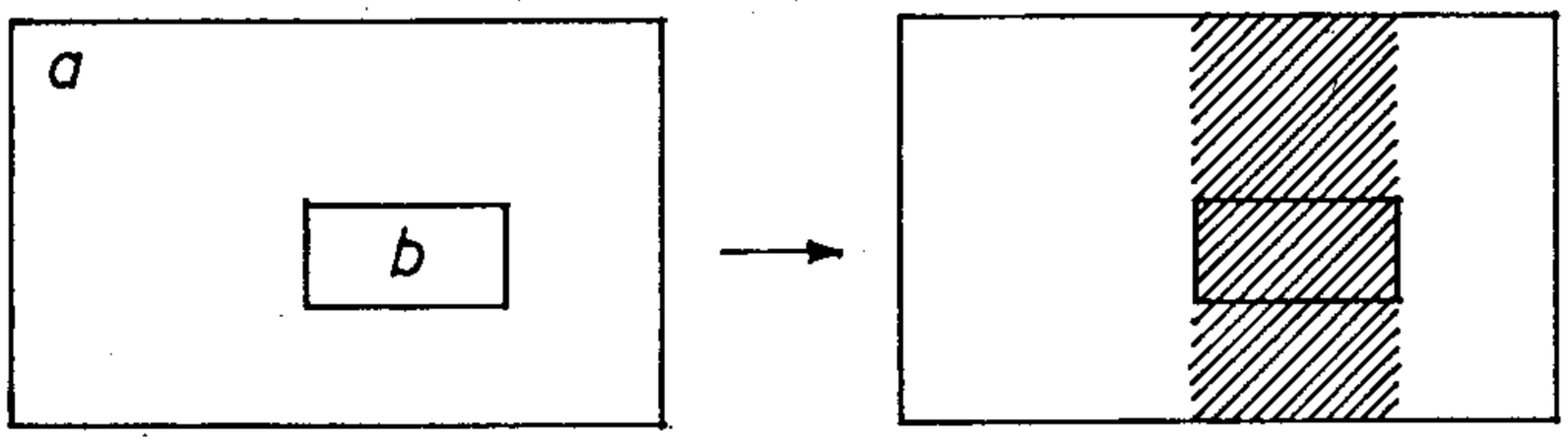
Sl. 10.2.7.

Npr. komplement od

$$\begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix} \quad \text{u} \quad \begin{bmatrix} 0 & 2 & 3 & 1 & 5 \\ 5 & 0 & 2 & 3 & \\ 6 & 4 & 5 & 0 & 0 \\ 7 & 8 & 9 & 0 & 0 \end{bmatrix} \quad \text{jest} \quad \begin{bmatrix} 5 & 2 & 3 \\ 7 & 0 & 0 \end{bmatrix}.$$

Komplement od *b* je načinjen od onih polja na koja ne bi mogli djelovati topovi iz poljâ podmatrice *b*.

2.8. Dvije nadmatrice zadane podmatrice. Komplement zadane podmatrice. Prva je omeđena iscrtkanim stupcima: sastavljena je od svih stupaca matrice a dobivenih produženjem *stupaca* podmatrice b; označit ćemo je sa $a_{(b)}$ ili $a_2(b)$ da se vidi da ona zavisi od a i b.



Sl. 10.2.8. Prelaz $b \to a_2(b)$

Dualno, radeći s recima, dolazimo do matrice $a^{(b)} = a_1(b)$: sastavljena je od svih redaka matrice a što se dobije produženjem redaka matrice b.

Prelazi $$b \to a^{(b)}$$

$$b \to a_{(b)}$$

vrlo su jednostavni i očigledni, a pokazat će se kao fundamentalni. Tako ćemo se npr. kasnije uvjeriti da prelaz $b \to a_{(b)}$ znači u zadanom skupu jednadžbi odabrati stanovit ekvivalentan podskup jednadžbi.

Posebno vidimo da je $a_{i.} = a^{(a_{ij})}$

$$a_{.j} = a_{(a_{ij})}.$$

2.9. Glavne podmatrice. Svaka podmatrica x zadane matrice a za koju je $D_1 x = D_2 x$ zove se *glavna podmatrica ili glavni minor*; drugim riječima: glavna podmatrica ima vrijednosti u svakom onom retku od a, ako ona u istoimenom stupcu od a nešto sadrži, i dualno. Oznaka glavnih minora je $a^{ijk\cdots}_{ijk\cdots}$ (dolje i gore dolaze *isti* indeksi). Među glavnim podmatricama od a ističu se *početne* (obuhvataju *početni komad* od $\operatorname{diag} a$) i *završne* (obuhvataju *završni komad* od $\operatorname{diag} a$); naravno, a je i početna i završna svoja glavna podmatrica. Npr. matrica

$$a = \begin{bmatrix} 2 & 5 & 7 \\ 3 & 4 & 9 \end{bmatrix}$$

ima jedino ove 3 glavne podmatrice:

$[2] = a^{(1)}_{(1)}$, $[4] = a^{(2)}_{(2)}$, $\begin{bmatrix} 2 & 5 \\ 3 & 4 \end{bmatrix} = a^{(12)}_{(12)}$; druga nije ni početna ni završna.

2.10. Zadaci o podmatricama.

1. Promatraj matricu $a = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{bmatrix}$ i njene potfunkcije:

1) $\begin{bmatrix} 1 & 2 & 3 \\ 9 & 10 & 11 \end{bmatrix}$, 2) $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \end{bmatrix}$, 3) $\begin{bmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \\ 9 & 10 & 11 \end{bmatrix}$,

4) $\begin{vmatrix} 1 & 4 \\ 9 & 12 \end{vmatrix}$, 5) $[9 \quad 10 \quad 11]$, 6) $\begin{bmatrix} 1 & 2 \\ 5 & 6 \\ 9 & 10 \end{bmatrix}$, 7) $\begin{bmatrix} 2 & 4 \\ 6 & 8 \\ 10 & 12 \end{bmatrix}$,

8) koje su od tih potfunkcija podmatrice? Kako bismo ih označili?

2. Za matricu b na oblasti 4×5 ispiši podmatrice 1) b^{13}_{13}, 2) b^{134}_{134}, 3) b^{134}_{24}, 4) b^{2}_{135}, 5) b^{23}_{1345} 6) b_{34}, 7) $b^{(34)}$.
8) Koje su tu glavne podmatrice?

3. Nađi komplementarne podmatrice gornjih matrica 1) — 7) u odnosu na matricu b; kakva im je oznaka?

4. 1) Nađi sve podmatrice oblasti 2×3 zadane matrice a oblasti 5×5; koliko ih ima? 2) Koliko podmatrica oblasti $r \times s$ ima u matrici a oblasti $k \times n$ za svako $r \leq k$, $s \leq n$?

5. Koliko matrica x oblasti $k \times n$ ima
1) potfunkcija, 2) podmatrica, 3) glavnih podmatrica?

3. NEKOLIKO VRSTA MATRICA

3.1. Kvadratne i nekvadratne matrice. Matrice s oblasti $n \times n$ zovu se *kvadratne matrice*; kaže se da su one *reda n*; matrice na oblasti $(k \times n)$, za koje je $k \neq n$, zovu se *nekvadratne matrice*.

3.2. Konačne i beskonačne matrice.[1] Matrice tipa $k \times n$, pri čemu su k, n prirodni brojevi, zovu se *konačne matrice* ili još bolje: *matrice s konačnom oblasti*; *beskonačne matrice*, tj. *matrice kojima je oblast beskonačna* su one kod kojih je bar jedan od brojeva k, n beskonačan.

Jednostrano-konačne matrice k, n jesu one kojima je bar jedan od brojeva k, n konačan.

3.3. Vektori. Matrice tipa $k \times 1$, odnosno $1 \times n$, zovu se *stupci*, odnosno *reci*, a zajednički se nazivaju *vektorima*. Ipak, obično ćemo nazivati vektorima matrice oblasti $k \times 1$, tj. *stupce*. Na isti način, svaka matrica oblasti $k \times n$ sastavljena je od n *stupaca-vektora*.

3.4. Nula-matrice. Konstantne matrice. Nula-matrice jesu one koje imaju 0 kao svoju jedinu vrijednost. Nula-matrica oblasti $n \times n$ može se ozna-

---

[1] Nekad se promatraju i *prazne matrice*; one su bez ikojeg člana (vrijednosti), a oblast im je: $Ik \times In$ ili čak prazni skup oblika $I0 \times In$ ili $Ik \times I0$.

čiti sa $0(n)$; a ako je nula-matrica poretka $k \times n$, može se ona označiti sa $0(k, n)$. Prema tome:

$$0(n)_{ij} = 0 \text{ za } i, j \in \{n\} = \{\underbrace{1,\ 2, \cdots n}_{n}\}.$$

Tako npr.

$$0(1) = [0], \quad 0(2) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad 0(3) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \cdots, \quad 0(\omega) = \begin{bmatrix} 0 & 0 & 0 \cdot \cdot \\ 0 & 0 & 0 \cdot \cdot \\ \vdots & \vdots & \vdots \end{bmatrix},$$

Sve su te matrice međusobno različite jer su im oblasti nejednake.

Nula-matrice su specijalni slučaj *konstantnih matrica*. Matrica je *konstantna ili konstanta* ako uzima svuda jednu te istu vrijednost. Ako je ta vrijednost c, pa ako je oblast matrice $k \times n$, može se ta konstantna matrica označiti sa

$$c(k, n) \text{ ili } \overset{c}{}_{(k, n)}.$$

3.5. Skalarne matrice. Matrica je *skalarna* ako joj je dijagonala konstantna te ako izvan dijagonale uzima svuda vrijednost 0. Ako je c vrijednost što je skalarna matrica uzima po dijagonali, može se matrica označiti sa $c_{(k, n)}$, pri čemu je $k \times n$ oblast matrice. U posebnom slučaju, kad je matrica kvadratna, možemo pisati

$$c_n \text{ umjesto } c_{(n, n)};$$

tako npr.

$$1_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

3.6. Jedinične matrice. Matrice oblika $1_n\ (n = 1, 2, \cdots)$ zovu se *jedinične matrice*. One su kvadratne i međusobno se razlikuju. Jedinične matrice označuju se sa 1 i I.

Posebno često dolazi *Kroneckerova* [*Kroneker*] *matrica*:

$$1_\omega \text{ a označuje se sa } \delta.$$

Njeni se elementi

$$(1_\omega)_{ij} \text{ označuju sa } \delta_{ij} \text{ ili sa } \delta^i_j; \text{ dakle je}$$

$$(1_\omega)_{ij} = \delta_{ij} = \delta^i_j = \begin{matrix} 1 \\ 0 \end{matrix} \text{ za} \begin{matrix} i=j \\ i \neq j \end{matrix}, \quad (i, j < \omega).$$

Očigledno je

$$c_{(k, n)} = c \cdot 1_{(k, n)} = 1_{(k, n)} \cdot c.$$

Primjer. Odredimo matricu a poretka 3×4 za koju je

$$a_{ij} = \delta_{1i}\, \delta_{2j}. \quad \text{Očigledno je} \quad a_{12} = \delta_{11}\, \delta_{22} = 1 \cdot 1 = 1;$$

za svako drugo $(ij) \in \{3\} \times \{4\}$ imamo $a_{ij} = 0$. Prema tome, tražena matrica a glasi

$$a = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix};$$

a nastaje iz konstante matrice $0(3, 4)$ tako da joj umjesto $(1, 2)$ — vrijednosti 0 pridijelimo vrijednost 1.

3.7. Konvencija ili dogovor. Kao što smo rekli, stavljamo $c_{(1,1)} = c$ za svako c. Ako u toku nekih istraživanja i računanja radimo neprestano s kvadratnim matricama s određenom oblasti $n \times n$, pisat ćemo radi kratkoće

umjesto $c_{(n,n)}$ naprosto $\operatorname{diag} c$ pa i c.

3.8. Dijagonalne matrice. Matrice kojima je vrijednost 0 izvan glavne dijagonale zovu se *dijagonalne matrice*. Takva je npr. matrica

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \end{bmatrix}.$$

Vrijednosti na dijagonali su 0, 1, 5.

Dijagonala $[x, y, z \cdots]$ ili $\operatorname{diag}[x, y, z, \cdots]$ označuje kvadratnu dijagonalnu matricu kojoj dijagonala glasi $x, y, z \cdots$ Npr.

$$\text{dijagonala } [2, -3] = \begin{bmatrix} 2 & 0 \\ 0 & -3 \end{bmatrix}.$$

Razlikuj pojam „dijagonalna matrica“ od pojma „dijagonala matrice“ (isp. § 1.5.3).

3.9. Normirane matrice. Njima je vrijednost 0 svuda osim možda na kojem početnom komadu glavne dijagonale gdje je vrijednost $= 1$; ako je r broj tih 1, onda će se normirana matrica s oblasti $k \times n$ označivati sa $1(k, n; r)$, tj.

$$1(k, n, r) = \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & r & \\ & & & & 1 \end{bmatrix} \begin{matrix} \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \overleftarrow{\qquad n \qquad} \\ \\ \\ \\ \\ \end{matrix} \Bigg\} k$$

Tako npr. $1(k, n; 0)$ je matrica poretka (k, n) a sa 0 kao jedinim vrijednostima; $1(n, n, n)$ je nova oznaka za jediničnu matricu poretka $n \times n$.

3.10. Zadaci o vrstama matrica.

1. Za svaku od slijedećih matrica navesti da li je kvadratna ili nekvadratna, vektor, konačna ili beskonačna, dijagonalna, skalarna, jedinična, ništična, normirana, konstantna:

$$1)\ a=\begin{bmatrix}0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix},\qquad 2)\ b=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\qquad 3)\ c=\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\end{bmatrix},$$

$$d=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0\end{bmatrix},\quad e=\begin{bmatrix}1\\ 2\\ 3\end{bmatrix},\quad f=[1\ \ 2\ \ 3],\quad g=\begin{bmatrix}1 & 0 & 0\\ 0 & 2 & 0\\ 0 & 0 & 3\end{bmatrix},$$

$$h=\begin{bmatrix}1 & 3 & 5 & 7 & 9\cdots\\ 2 & 4 & 6 & 8 & 10\cdots\end{bmatrix}\qquad i=\begin{bmatrix}1 & 0 & 0 & 0 & & \\ 0 & 2 & 0 & 0 & & \\ 0 & 0 & 3 & 0 & \cdot & \cdot\\ 0 & 0 & 0 & 4 & 0 & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot\end{bmatrix},$$

$$j=\begin{bmatrix}0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\end{bmatrix},\qquad k=\begin{bmatrix}0 & 0 & 1\\ 0 & 1 & 0\\ 1 & 0 & 0\end{bmatrix}.$$

2. Odredi sve konstantne podmatrice svake od prethodnih matrica.

3. Ispiši matrice $0(3,3)$, $2(3,3)$, 1_5, $\mathrm{diag}(5,\ 3,\ -2)$.

4. Dokaži da je $2(3,3)+5(3,3)=7(3,3)$. Kako glasi opće pravilo?

5. Da li je zbroj dviju dijagonalnih matrica iste oblasti opet dijagonalna matrica?

6. Odredi $\delta_{2,3}$ $\delta_{1,6}$, δ_{33}, $\delta_{10^6,\,10^3}$ $\delta_{1001,\,1001}$.

4. O RAČUNANJU S MATRICAMA

Izuzev zakona komutacije, koji pri množenju matrica općenito ne vrijedi, ostali zakoni o elementarnim operacijama prenose se sa brojeva na matrice.

4.1. Zbrajanje i oduzimanje matrica. — **4.1.1.** Zbrajanje matrica *definira* se kao i za druge funkcije: odgovarajuće komponente (vrijednosti) se zbrajaju; za funkcije f, g suma $f+g$ definira se tako da vrijedi

$$(f+g)\,x=fx+gx$$

za svako x iz oblasti funkcija f, g. Npr.

$$\begin{bmatrix}3 & 5 & 4\\ 2 & 1 & 3\end{bmatrix}+\begin{bmatrix}5 & -4 & -1\\ -1 & -1 & -1\end{bmatrix}=\begin{bmatrix}8 & 1 & 3\\ 1 & 0 & 2\end{bmatrix}.$$

4.1.1.1. Definicija oduzimanja. Za matrice a, b uz uslov $\mathrm{Dom}\, a = \mathrm{Dom}\, b$ razlika $b-a$ je *rješenje matričke jednakosti*

$$x + a = b.$$

Vidi se da je $(b-a)_{ij} = b_{ij} - a_{ij}$, tj. matrice na istoj oblasti oduzimaju se tako da se izvrši oduzimanje odgovarajućih komponenata.

4.1.2. Protivno označena matrica. Za svaku matricu a definira se i *suprotna matrica* ili *protivno-jednaka matrica* $-a$ kao produkt od broja -1 i matrice a, tj. $-a = -1 \cdot a$, dakle

$$(-a)_{ij} = -a_{ij}.$$

Pomoću matrice $-a$ može se, kao i kod brojeva, *oduzimanje svesti na dodavanje suprotnog*:

$$b-a = b + (-a).$$

Riječima: *oduzeti a znači dodati suprotno od a.*

4.1.3. Grupovni karakter množine svih realnih matrica zadane oblasti. Skup $S = R\{k, n\}$ matricâ zadane oblasti $k \times n$ kojima su vrijednosti u skupu R realnih brojeva čine *aditivnu grupu.* To drugim riječima znači da su ispravni ovi aksiomi 1—4 grupe:

1. Ako je $a, b \in S$, onda je $a + b \in S$, tj. ako su dvije matrice u S, onda je u S i njihova suma.

2. (*Zakon asocijacije za zbrajanje*):

Ako su $a, b, c \in S$, onda je

$$(a + b) + c = a + (b + c).$$

3. S sadrži *neutralni* element, i to konstantu $0(k, n)$ za koju je $a + 0(k, n) = a = 0(k, n) + a$ za svako $a \in S$.

4. Za svako $a \in S$ jednadžba

$$a + x = \text{neutralni element} = x + a$$

dopušta određeno rješenje, naime $x = -a$ koje leži u S.

Kako je k tome $a + b = b + a$, ta je grupa S *komutativna* ili *Abelova grupa.*
Dokažimo npr. svojstvo 2. No $(a+b)+c$ je suma matrice $(a+b)$ i matrice c pa po definiciji sume imamo:

$$[(a+b)+c]_{ij} = (a+b)_{ij} + c_{ij} = \text{(iz istog razloga)} = a_{ij} + b_{ij} + c_{ij} = \text{(na osnovu zakona asocijacije u } R) = a_{ij} + (b_{ij} + c_{ij}) = \text{(definicija sume } b + c) = a_{ij} + (b+c)_{ij} = \text{(po definiciji sume od } a \text{ i } (b+c)) = [a + (b+c)]_{ij}.$$

Dakle je $$[(a+b)+c]_{ij} = [a + (b+c)]_{ij}$$

za svako dopušteno (i, j) iz zajedničke oblasti matrica a, b, c. To po aksiomu M_1 o jednakosti matrica znači da je $(a+b)+c = a+(b+c)$, za čim i idemo.

4.2. Množenje matrica. — 4.2.1. Kao što znamo (isp. § 1.3.4.4), produkt ab matrica a, b definira se po obrascu

$$(ab)_{ij} = a_{i.} \circ b_{.j}, \text{ tj.}$$

(ij)-komponenta produkta jest skalarni produkt *i-retka* prvog faktora i *j-stupca* drugog faktora.

Npr. za

$$a = \begin{bmatrix} 2 & 3 & 4 \\ 3 & 5 & -2 \end{bmatrix}, \quad b = \begin{bmatrix} 3 & 1 & 4 \\ 5 & 2 & 2 \\ 4 & 5 & 6 \end{bmatrix}$$

imamo $(ab)_{23} = 3 \cdot 4 + 5 \cdot 2 + -2 \cdot 6 = 10$; inače izlazi

$$ab = \begin{bmatrix} 37 & 28 & 38 \\ 26 & 3 & 10 \end{bmatrix}.$$

Do te vrste množenja matrica dovodi nas ovaj

4.2.2. Osnovni vodeći primjer. Pođimo od skalarnog produkta dvaju nizova — označimo ih sa f, x; dakle je

$$f \circ x = f_1 x_1 + f_2 x_2 + \cdots = \sum_{i \in 1(n)} f_i x_i; \tag{1}$$

to znači da je n dužina nizova f i x.

Neka je sa svoje strane svako x_i skalarni produkt s nekim čvrstim nizom y dužine r; dakle y glasi $y_1, y_2, \cdots, y_r$; pa neka je

$$x_i = h_i \circ y = h_{i1} y_1 + h_{i2} y_2 + \cdots = \sum_{r'} h_{ir'} y_{r'} \quad (r' \in 1(r)). \tag{2}$$

Uvrstimo taj izraz za x_i u zadani skalarni produkt (1).

Izvedimo račun npr. za $n = 2$, $r = 4$.

Tu se pojavljuje tablica h koeficijenata h_{ik}:

$$h \cdots \begin{bmatrix} h_{11} & h_{12} & h_{13} & h_{14} \\ h_{21} & h_{22} & h_{23} & h_{24} \end{bmatrix}. \tag{3}$$

Imamo ovo:

$$f \circ x = f_1 x_1 + f_2 x_2 = f_1 (h_{11} y_1 + h_{12} y_2 + h_{13} y_3 + h_{14} y_4) +$$

$$+ f_2 (h_{21} y_1 + \cdots + h_{24} y_4) = (f_1 h_{11} + f_2 h_{21}) y_1 + \tag{4}$$

$$+ (f_1 h_{12} + f_2 h_{22}) y_2 + (f_1 h_{13} + f_2 h_{23}) y_3 + (f_1 h_{14} + f_2 h_{24}) y_4.$$

Šta je tu koeficijent od y_1? To je skalarni produkt zadanog niza f i prvog stupca $h_{.1}$ tablice h. Isto tako koeficijent od y_i jest skalarni produkt zadanog niza f i stupca $h_{.i}$ tablice h.

Drugim riječima:

$$f \circ x = (f \circ h_{.1}) \cdot y_1 + (f \circ h_{.2}) y_2 + (f \circ h_{.3}) y_3 + (f \circ h_{.4}) y_4. \tag{5}$$

Rezultat supstitucije (2) u unutrašnjem produktu (1) opet je unutrašnji produkt niza $f \circ h_{\cdot 1}, f \circ h_{\cdot 2}, \cdots$ i niza $y_1, y_2, \cdots$

Novi koeficijenti su skalarni produkti zadanog niza f i stupaca »*supstitucione* ***matrice***« h.

4.2.3. Sasvim bi analogni rezultat bio da smo pošli ne od jedne linearne forme veličinâ $x_1, x_2, \cdots$, nego od više njih:

Pođimo od k skalarnih produkata, odnosno linearnih formi:

$$a_{i\cdot} \circ x = a_{i1} x_1 + a_{i2} x_2 + \cdots = \sum_j a_{ij} x_j \tag{6}$$

s tablicom koeficijenata

$$a = \begin{bmatrix} a_{11}\, a_{12} \cdots \\ a_{21}\, a_{22} \cdots \\ \cdot \quad \cdot\cdot \quad \cdot \end{bmatrix}.$$

Pa neka je $x_j = \sum_e b_{je} y_e$; to znači da tablica b koeficijenata ima toliko redaka koliko tablica a ima stupaca; unošenjem tih izraza za x_j u linearne forme (6) x-ova imamo, za rezultat, linearne forme s obzirom na y-e. Nova tablica koeficijenata — označimo je sa p — nastaje skalarnim (unutrašnjim) množenjem *redaka* tablice a i *stupaca* tablice b.

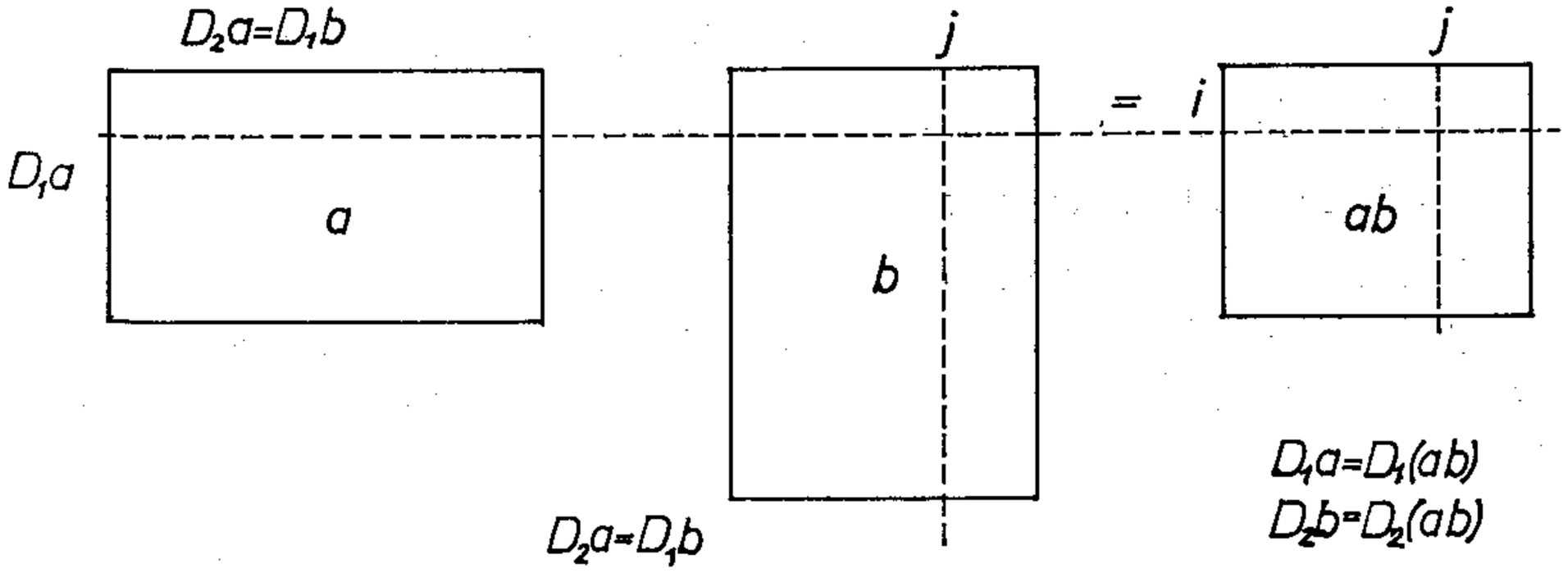
Drugim riječima: *pomnoži li se skalarno redak* $a_{i\cdot}$ *tablice* a *i stupac* $b_{\cdot j}$ *tablice* b, *nastaje element* p_{ij} *nove matrice* p:

$$p_{ij} = a_{i\cdot} \circ b_{\cdot j} = \sum_e a_{ie} b_{ej}.$$

Kaže se da *tablica* p *nastaje množenjem matrice* a *i matrice* b pa se piše $p = ab$. Matrica ab zove se *produkt matrice* a *i matrice* b. Tako se dolazi do definicije množenja matrica.

Treba imati na umu da je produkt matricâ a, b definiran jedino ako je ispunjen *uslov ukopčavanja*: $D_2 a = D_1 b$ (prvi faktor ima toliko stupaca koliko drugi faktor ima redaka).

Shematski to možemo prikazati ovako:



Sl. 10.4.2.3.

Primjer

$$\begin{bmatrix} 2 & 3 & 5 & -4 & 8 \\ -1 & 2 & -3 & 4 & 0 \end{bmatrix} \begin{bmatrix} 1 & 5 & -3 \\ 2 & -5 & 2 \\ -3 & 4 & 1 \\ 3 & 5 & 2 \\ 1 & -1 & 1 \end{bmatrix} = \begin{bmatrix} -11 & -13 & 5 \\ 24 & -7 & 12 \end{bmatrix};$$

tako je npr. ovo -7 na polju $(2,2)$ skalarni produkt drugog retka $-1, 2, -3, 4, 0$ i drugog stupca

$$\begin{matrix} 5 \\ -5 \\ 4 \\ 5 \\ -1 \end{matrix}$$

4.2.4. Teorem. *Za konačne matrice množenje je asocijativno*[1]:

$$(ab)\,c = a\,(bc). \tag{1}$$

Dokažimo jednakost (1), tj. dokažimo da je vrijednost od $(1)_1$ u polju (i,j) isto što i vrijednost od $(1)_2$ u (i,j). No produkt $(ab)\,c$ ima u (i,j) vrijednost:

$$[(ab)\,c]_{ij};$$

a ovo je po definiciji produkta matrice $a\,b$ i c jednako:

$$\sum_l (ab)_{il}\, c_{lj} = (\text{iz istog razloga}) = \sum_l (a_{i.} \circ b_{.l})\, c_{lj} = \sum_{l,f} a_{if}\, b_{fl}\, c_{lj} =$$

(po zakonu distribucije množenja brojeva prema zbrajanju brojeva)

$$= \sum_{l,f} a_{if}\, b_{lf}\, c_{lj} = \sum_f a_{if}\, (bc)_{fj} =$$

(po definiciji produkta $a\,(bc)$)

$$= (a\,(bc))_{ij}.$$

Dakle je zaista

$$[(ab)\,c]_{ij} = [a\,(bc)]_{ij}, \quad \text{za svako} \quad i,\ j$$

a to znači da je ispravna jednakost (1).

4.2.5. Komutativne matrice.

Množenje matrica općenito nije komutativno:

Ako za matrice a, b vrijedi $ab = ba$ [odnosno $ab = -ba$], kaže se da su one *komutativne* [odnosno *koso-komutativne*]. Čak ab može postojati, dok ba ne mora.

---

[1] Za beskonačne matrice množenje ne mora biti asocijativno; čak može biti $(a \cdot a) \cdot a \neq a \cdot (a \cdot a)$ (isp. 10, § 9.19).

Tako npr. redak · stupac = skalar, simbolički

$\longrightarrow \cdot \downarrow$ = skalar. Npr. $[a_0 \;\; a_1 \;\; a_2]\begin{bmatrix} b_0 \\ b_1 \\ b_2 \end{bmatrix} = a_0 b_0 + a_1 b_1 + a_2 b_2 .$

Naprotiv, množeći stupac retkom:

$\downarrow \cdot \longrightarrow$ = $\boxed{\text{kvadrat}}$ Npr. $\begin{bmatrix} b_0 \\ b_1 \\ b_2 \end{bmatrix}[a_0 \;\; a_1 \;\; a_2] = \begin{bmatrix} b_0 a_0 & b_0 a_1 & b_0 a_2 \\ b_1 a_0 & b_1 a_1 & b_1 a_2 \\ b_2 a_0 & b_2 a_1 & b_2 a_2 \end{bmatrix}.$

Zakon komutacije za množenje ne mora vrijediti ni za kvadratne matrice.

Npr. za $a = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, \quad b = \begin{bmatrix} 2 & 5 \\ 4 & 8 \end{bmatrix}$

imamo $(ab)_{11} = a_{1.} \cdot b_{.1} = 1 \cdot 2 + 2 \cdot 4 = 10$

$(ba)_{11} = b_{1.}\, a_{.1} = (2,5) \circ (1, 3) = 2 \cdot 1 + 5 \cdot 3 = 17.$

Dakle je $(ab)_{11} \neq (ba)_{11}$ pa zato i $a \cdot b \neq ba$.

$$ab = \begin{bmatrix} 10 & 21 \\ 22 & 47 \end{bmatrix}, \quad ba = \begin{bmatrix} 17 & 24 \\ 28 & 40 \end{bmatrix}.$$

4.2.6. Jedinična matrica i množenje. Ako je a kvadratna matrica, a I jedinična matrica iste oblasti, tada se vidi da je

$$a \cdot I = I \cdot a = a.$$

Tako npr.

$$\begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}.$$

Vidi se da je $a_{i.} = I_{i.}\, a, \quad a_{.j} = a \cdot I_{.j}.$

4.2.7. Pitanje o nula-divizorima. *Množenje (kvadratnih) matrica dopušta nula-divizore.* To znači da produkt dviju (kvadratnih) matrica može biti nula-matrica, a da nijedan faktor nije nula-matrica.

Npr. $$\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ z & u \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

za bilo koje brojeve x, y, z, u.

Kao što znamo, u skupu realnih, odnosno kompleksnih brojeva nema nula-divizora: produkt od dva broja je $= 0$ onda i samo onda ako je bar jedan od faktora $= 0$.

4.2.8. Potencije ili stepeni matrice. Stavlja se $aa = a^2$, $a^2 a = a^3, \cdots$, $a^n a = a^{n+1}$. Također se definira $a^0 = 1_n$, ako je $\mathrm{Dom}\, a = (n, n)$.

4.3. Zakoni distribucije množenja prema zbrajanju. Sva tri zakona distribucije množenja prema sabiranju matrica jesu na snazi:

Lijevi zakon distribucije:

$$(a+b)\,c = ac + bc \tag{1}$$

Desni zakon distribucije:

$$a\,(b+c) = ab + ac \tag{2}$$

Opći zakon distribucije:

$$(a+b)\,(c+d) = ac + bc + ad + bd. \tag{3}$$

Dokaz lijevog zakona distribucije:

$$[(a+b)\,c]_{ij} =$$

(po definiciji produkta)

$$= \sum_l (a+b)_{il}\, c_{lj} =$$

(po definiciji sume $a+b$)

$$= \sum_l (a_{il} + b_{il})\, c_{lj} =$$

(po zakonu distribucije za skalare)

$$= \sum_l (a_{il}\, c_{lj} + b_{il}\, c_{lj}) = \sum_l a_{il}\, c_{lj} + \sum_l b_{il}\, c_{lj} = (ac)_{ij} + (bc)_{ij} = (ac + bc)_{ij}.$$

Dakle je

$$[(a+b)\,c]_{ij} = [ac + bc]_{ij}$$

za svaku tačku (i, j) oblasti. A to znači da vrijedi (1).

Formula (2) dokazuje se slično kao formula (1).

Formula (3) je posljedica od (1) i (2) i asocijativnosti zbrajanja matrica. Naime:

$$(a+b)\,(c+d) = (\text{po } (2)) = (a+b)\,c + (a+b)\,d = (\text{po } (1)) =$$

$$= (ac + bc) + (ad + bd) = ac + bc + ad + bd.$$

4.4. Množenje skalara i matrice. To se radi kao i za druge funkcije: *produkt broja z i funkcije f je ona funkcija zf za koju ima vrijediti*

$$(zf)\,x = z\,(fx)$$

za *svaku* vrijednost x iz oblasti od f. Stavlja se $zf = f \cdot z$. Posebno, *matrica se množi brojem tako da se svaka vrijednost matrice pomnoži tim brojem.*

Pri tom vrijede uobičajena pravila, kao npr. $1\,a = a\,1 = a$ za svaku matricu a.

4.5. Množenje matrice i stupca. Npr.

$$\begin{bmatrix} 2 & 8 & 3 \\ 4 & -2 & 5 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ -2 \\ 4 \end{bmatrix} = \begin{bmatrix} 2\cdot 3 + 8\cdot -2 + 3\cdot 4 \\ 4\cdot 3 - 2\cdot -2 + 5\cdot 4 \end{bmatrix} = \begin{bmatrix} 2 \\ 36 \end{bmatrix},$$

tj. dobije se opet matrica tipa stupca. Zaključak je općenit: *produkt matrice i stupca je opet stupac* (naravno, dužina stupca ne mora biti ista kao dužina polaznog stupca). No množimo li *kvadratnu* matricu i stupac, dobit ćemo opet stupac *iste dužine*. To će nam pravilo često dolaziti.

4.6. Dijeljenje martica. 1. Dijeljenje matrica svodi se na množenje matrica. Naime, ako je $ab = c$, onda se kaže da je *a faktor matrice c*, i to *lijevi faktor*; pripadni *koeficijent* je *b*; isto tako, *b* je *desni faktor* matrice *c*, a pripadni koeficijent je *a*.

Od posebnog je interesa promatrati faktore jediničnih matrica

$$1 = 1_1 = I_1, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1_2 = I_2, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = 1_3 = I_3, \cdots$$

2. Pokušajmo riješiti matričnu jednadžbu

$$\begin{bmatrix} 1 & 5 \\ 4 & 3 \end{bmatrix} x = \begin{bmatrix} 3 & 5 \\ 4 & 1 \end{bmatrix}. \tag{1}$$

Matrica x mora biti oblasti 2×2; dakle je

$$x = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}$$

pa imamo

$$\begin{bmatrix} 1 & 5 \\ 4 & 3 \end{bmatrix} \cdot \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} = \begin{bmatrix} 3 & 5 \\ 4 & 1 \end{bmatrix},$$

tj.

$$\begin{bmatrix} x_{11} + 5\,x_{21} & x_{12} + 5\,x_{22} \\ 4\,x_{11} + 3\,x_{21} & 4\,x_{12} + 3\,x_{22} \end{bmatrix} = \begin{bmatrix} 3 & 5 \\ 4 & 1 \end{bmatrix}.$$

Ta *matrična jednakost* znači isto što i ove 4 *skalarne jednakosti*:

$$x_{11} + 5\,x_{21} = 3$$
$$4\,x_{11} + 3\,x_{21} = 4$$
$$x_{12} + 5\,x_{22} = 5$$
$$4\,x_{12} + 3\,x_{22} = 1.$$

Iz prve dvije jednadžbe nalazimo $x_{11} = 11/17$, $x_{21} = 8/17$,
a iz druge dvije jednadžbe nalazimo $x_{12} = -20/17$, $x_{22} = 19/17$.

Dakle je tražena matrica

$$x=\begin{bmatrix}11/17 & -20/17\\ 8/17 & 19/17\end{bmatrix}=17^{-1}\begin{bmatrix}11 & -20\\ 8 & 19\end{bmatrix}.$$

To je rješenje jednadžbe (1). Nađi, na sličan način, rješenje jednadžbe

$$y\begin{bmatrix}1 & 5\\ 4 & 3\end{bmatrix}=\begin{bmatrix}3 & 5\\ 4 & 1\end{bmatrix}.$$

Da li je $x=y$?

3. Drugi primjer:

$$a=\begin{bmatrix}0 & 0\\ 1 & 0\end{bmatrix},\quad c=\begin{bmatrix}0 & 0\\ 1 & 2\end{bmatrix}.$$

Nađi x iz $ax=c$. Radeći kao maloprije i stavljajući

$$x=\begin{bmatrix}x_{11} & x_{12}\\ x_{21} & x_{22}\end{bmatrix},$$

dobili bismo sistem linearnih jednadžbi:

$$0\cdot x_{11}+0\cdot x_{21}=0 \qquad 1\cdot x_{11}+0\cdot x_{21}=1$$

$$0\cdot x_{12}+0\cdot x_{22}=0 \qquad 1\cdot x_{12}+0\cdot x_{22}=2.$$

Odatle: $x_{11}=1$, $x_{12}=2$; ostale vrijednosti x_{21}, x_{22} su proizvoljne, tj.

$$x=\begin{bmatrix}1 & 2\\ \alpha & \beta\end{bmatrix},\ \alpha \text{ i } \beta \text{ su proizvoljni.} \tag{2}$$

U tom slučaju dijeljenje „sprijeda“ matrice

$$c=\begin{bmatrix}0 & 0\\ 1 & 2\end{bmatrix}\quad \text{sa}\quad a=\begin{bmatrix}0 & 0\\ 1 & 0\end{bmatrix}$$

ne daje jedan jedini rezultat, nego beskonačno mnogo rezultata oblika (2), jer je

$$\begin{bmatrix}0 & 0\\ 1 & 0\end{bmatrix}\cdot\begin{bmatrix}1 & 2\\ \alpha & \beta\end{bmatrix}=\begin{bmatrix}0 & 0\\ 1 & 2\end{bmatrix}.$$

Pokušajmo podijeliti straga

$$c=\begin{bmatrix}0 & 0\\ 1 & 2\end{bmatrix}\quad \text{sa}\quad a=\begin{bmatrix}0 & 0\\ 1 & 0\end{bmatrix},$$

tj. riješiti jednadžbu $xa=c$.

Rješenje ne postoji, jer bi posebno moralo biti $x_{2.}\circ a_{.2}=c_{22}$, tj. $x_{21}\cdot 0+x_{22}\cdot 0=2$; no to nije moguće!

Na taj način vidimo kako je dijeljenje matrica zamršeno već i u slučaju kvadratnih matrica.

4.6.4. Regularne matrice. Međutim, vidjet ćemo da je za *regularne matrice*, tj. za kvadratne matrice kojima je determinanta $\neq 0$, dijeljenje uvijek provedivo (v. pogl. 12, § 6) i da se svodi na množenje s „inverznom" matricom.

Primijetimo najzad i ovo: ako je $ax = c$, tada je također $aX = c$ za *svaku* matricu $X = x + z$ za koju je $az =$ nula-matrica s oblasti Dom c. To je također razlog da dijeljenje matrica ne mora biti jednoznačno.

4.7. Zadaci o računanju matricama.

1. Zadane su matrice: $a = \begin{bmatrix} 3 & 5 \\ 7 & 9 \end{bmatrix}$, $b = \begin{bmatrix} 4 & 1 \\ 2 & 1 \\ 5 & 1 \end{bmatrix}$, I_3, $0\,(3)$,

$$c = \begin{bmatrix} 3 & 2 & 1 & 5 \\ 1 & 2 & 1 & 4 \\ 2 & 1 & 2 & 1 \end{bmatrix}, \quad d = \begin{bmatrix} 7 & 9 \\ -3 & -2 \end{bmatrix}, \quad e = \begin{bmatrix} 1 & 3 & 5 & 7 \cdots \\ 2 & 4 & 6 & 8 \cdots \end{bmatrix},$$

$f = [3, \quad 6, \quad 9, \quad 12, \cdots]$.

Odredi sve uređene parove tih matrica koje se međusobno mogu: 1) zbrojiti, 2) pomnožiti.

2. Za matrice x iz zad. 1 odredi; oblast Dom x te brojeve D_1, D_2.

3. Ako je $a + b = c$, kakve veze postoje među brojevima $D_i x$ za $i = 1, 2$ $x \in \{a, b, c\}$?

4. Isto pitanje za jednakost $ab = c$.

5. Isto pitanje za $a^n = c$.

6. Neka je $a = \begin{bmatrix} 2 & 3 \\ 5 & -7 \end{bmatrix}$, $b = \begin{bmatrix} -1 & 3 \\ 4 & -2 \end{bmatrix}$; nađi $-a$, $a + b$, $a - b$, ab, ba, $ab - ba$, $a^2 = aa$, bb, $3a + 2b$, $\frac{1}{3}a^2 + \frac{1}{4}b^2$, $3\,(ab)$, $3a$, $a \cdot 3$, $(a + b)^2$, $(a + b)^3$.

7. Nađi x iz 1) $ax = 1\,(2, 2)$, 2) $xa = 1\,(2, 2)$, 3) $ax = \begin{bmatrix} 3 & 9 \\ 4 & 2 \end{bmatrix}$, 4) $ax = 5$; pri tom je $a = \begin{bmatrix} 2 & 5 \\ 4 & -2 \end{bmatrix}$.

8. Dokaži ovo: radeći s realnim matricama stupnja 2×2 i „poistovećujući" svaki realni broj x sa skalarnom matricom $\begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}$, tada matrica $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ igra ulogu imaginarne jedinice i; npr. $i^2 = -1$, tj. $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$; kompleksnom broju $z = x + iy$ odgovara matrica $\begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} + \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} y & 0 \\ 0 & y \end{bmatrix} = \begin{bmatrix} x & -y \\ y & x \end{bmatrix}$.

9. *Paulijeve matrice* (Pauli): $A=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$, $B=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$, $C=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$

su involutivne; $x^2=1$, vrijedi zakon kose komutacije (tj. $xy=-yx$) te $AB=iC$; izgradi tablicu množenja.

10. U teoriji kvaterniona dolaze matrice s oblasti 4×4:

$$I=\begin{bmatrix}0 & 1 & 0 & 0\\ -1 & 0 & 0 & 0\\ 0 & 0 & 0 & -1\\ 0 & 0 & 1 & 0\end{bmatrix},\quad J=\begin{bmatrix}0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ -1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0\end{bmatrix},\quad K=\begin{bmatrix}0 & 0 & 0 & 1\\ 0 & 0 & -1 & 0\\ 0 & 1 & 0 & 0\\ -1 & 0 & 0 & 0\end{bmatrix}.$$

Dokaži ove veze: $I^2=-1$, $IJ=K$, $IJK=-1$ i druge veze koje odatle izlaze cikličnom zamjenom slova I, J, K.

11. U kvantnoj mehanici pojavljuju se ove matrice:

$$\alpha_1=\begin{bmatrix}0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix},\quad \alpha_2=\begin{bmatrix}0 & -i & 0 & 0\\ i & 0 & 0 & 0\\ 0 & 0 & 0 & -i\\ 0 & 0 & i & 0\end{bmatrix},\quad \alpha_3=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0\\ 0 & 0 & -1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix},$$

$$\alpha_4=\begin{bmatrix}0 & 0 & 1 & 0\\ 0 & 0 & 0 & -1\\ 1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0\end{bmatrix},\quad \xi=\begin{bmatrix}0 & 0 & 1 & 0\\ 0 & 0 & 0 & -1\\ -1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\end{bmatrix},\quad \beta_1=\begin{bmatrix}0 & 0 & 0 & -1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ -1 & 0 & 0 & 0\end{bmatrix},$$

$$\beta_2=\begin{bmatrix}0 & 0 & 0 & i\\ 0 & 0 & i & 0\\ 0 & -i & 0 & 0\\ i & 0 & 0 & 0\end{bmatrix},\quad \beta_3=\begin{bmatrix}0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\end{bmatrix},\quad \beta_4=\begin{bmatrix}-1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}.$$

Provjeri relacije: $\alpha_k\alpha_n+\alpha_n\alpha_k=2\delta_{kn}\cdot 1_4$, $\xi\alpha_k=-\alpha_k\xi=-\xi$,
$\xi\beta_k=-\beta_k\xi=\alpha_k\xi^2=-1$, $\alpha_k\beta_k=\xi$ za $k=1,2,3,4$.

12. Nađi: 1) $\begin{bmatrix}a & b\\ -b & a\end{bmatrix}^n$, 2) $\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}^n$, 3) $\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}^n$, 4) $\begin{bmatrix}\cos x & \sin x\\ -\sin x & \cos x\end{bmatrix}^n$,

5) Dokaži $\begin{bmatrix}\operatorname{ch} x & \operatorname{sh} x\\ \operatorname{sh} x & \operatorname{ch} x\end{bmatrix}^n=\begin{bmatrix}\operatorname{ch} n x & \operatorname{sh} n x\\ \operatorname{sh} n x & \operatorname{ch} n x\end{bmatrix}$.

13. Ako za matrice a, b vrijedi $ab=ba$, onda je $(a+b)^2=a^2+2ab+b^2$, $(a+b)^3=a^3+3a^2b+3ab^2+b^3$, $(a+b)^n=a^n+na^{n-1}b+$

$$+\binom{n}{2}a^{n-2}b^2+\ldots+b^n, a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+a^{n-3}b^2+\ldots+b^{n-1}).$$

14. Neka je $a=\begin{bmatrix} 3 & -2 & 4 \\ 2 & 5 & 1 \\ -2 & 3 & 2 \end{bmatrix}$, $c=\begin{bmatrix} 3 & 4 & 5 \\ 4 & 2 & 1 \\ 1 & 3 & 2 \end{bmatrix}$; nađi x, ako je:

1) $ax=c_{\cdot 1}=\begin{bmatrix} 3 \\ 2 \\ -2 \end{bmatrix}$, 2) $ax=c_{\cdot 2}$, 3) $ax=c_{\cdot 3}$, 4) $ax=c$,

5) $xa=c$; 6) $ax=xa$.

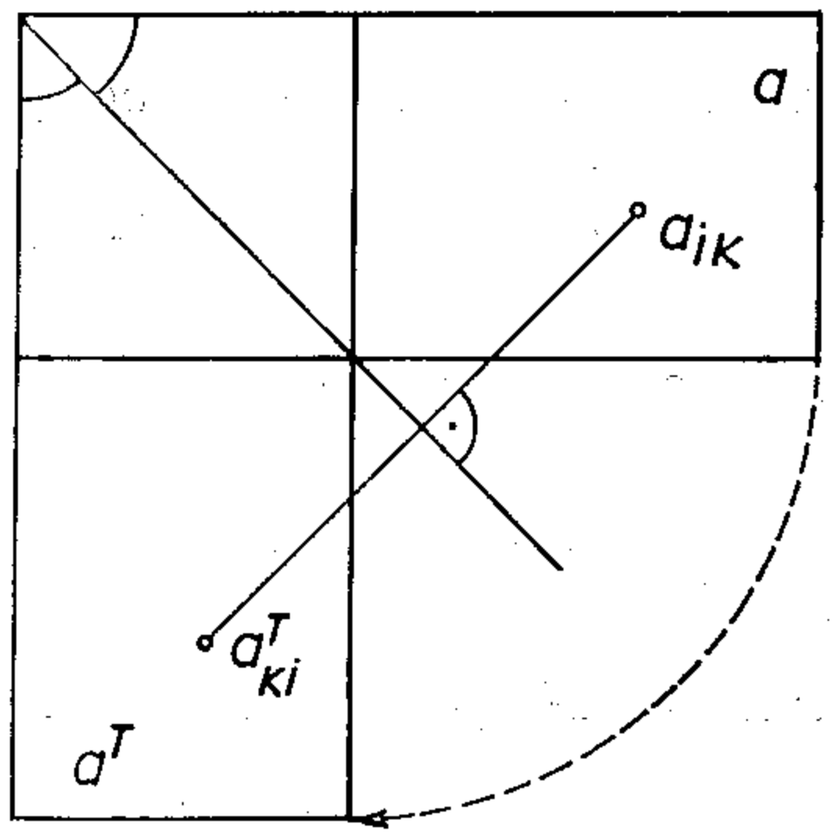
15. Neka je $fx=x^2+2x+1$; nađi fx za $x=0\,(3)$, I_3,

$$\begin{bmatrix} 2 & 1 & 3 \\ 4 & 5 & -2 \\ 3 & -3 & 4 \end{bmatrix}, \quad \begin{bmatrix} -2 & 4 & 3 \\ 1 & 5 & -3 \\ 3 & -2 & 4 \end{bmatrix};$$ uvjeri se da je $fx=(x+I)^2$.

16. Neka je $ax=c$, 1) Dom $a=4\times 5$, 2) Dom $c=4\times 6$; koliko skalarnih nepoznanica x_{ik} zamjenjuje matrična jednakost $ax=c$?

17. Neka je $c=c\,(k,k)=$konstantna matrica s oblasti $k\times k$; nađi a^n za svaki prirodni broj n.

5. Transponiranje matrica (transponirana, dualna ili dvojna matrica zadane matrice; operator apostrofiranja). — **5.1.** Definicija. *Transponirana* (*dualna ili dvojna*) *matrica* zadane matrice a nastaje iz a tako da retke matrice a pišemo po redu kao stupce, a stupce pišemo po redu kao retke. Označuje se sa a^T ili a'.



Sl. 5.1.

Formalno i funkcionalno:

$$(a^T)_{\cdot i}=a_{i\cdot} \text{ odnosno } (a^T)_{ij}=a_{ji} \text{ tj.}$$

$$a^T(i,j)=a(j,i).$$

Slikovito (posebno za kvadratne matrice) možemo reći da a^T nastaje iz a zrcaljenjem (ogledanjem) na *glavnoj dijagonali matrice* a. Ta jednostavna matrična veza $a\to a^T$ od izvanredne je važnosti, posebno u slučaju kad je riječ o stupcima i recima.

Npr. $\begin{bmatrix} 5 & 2 & 7 \\ 1 & 0 & 4 \end{bmatrix}^T=\begin{bmatrix} 5 & 1 \\ 2 & 0 \\ 7 & 4 \end{bmatrix}$.

5.2. Teorem. *Operator transponiranja matrica distributivan je prema zbrajanju, a obrnutim redom distributivan prema množenju matrica*:

$$(a+b)^T=a^T+b^T, \tag{1}$$

$$(ab)^T=b^T a^T. \tag{2}$$

D o k a z. $[(a+b)^T]_{ij} = [a+b]_{ji} =$ (definicija zbrajanja) $= a_{ji} + b_{ji} =$ (definicija) $= a_{ij}^T + b_{ij}^T = (a^T + b^T)_{ij}$. Dakle je $((a+b)^T)_{ij} = (a^T + b^T)_{ij}$ za svaku tačku (i,j) oblasti. A to znači, po definiciji, da vrijedi (1).

Dokažimo (2):

$$((ab)^T)_{ij} = (\text{definicija}) = (ab)_{ji} = (\text{definicija množenja}) =$$
$$= \sum_l a_{jl}\, b_{li} = \sum_l a_{lj}^T b_{il}^T = \sum_l b_{il}^T a_{lj}^T = (b^T a^T)_{ij}.$$

A to znači da vrijedi (2).

5.3 Induktivno se dokazuju pravila

$$\left(\sum_{i=1}^n a_i\right)^T = \sum_{i=1}^n a_i^T, \quad \left(\prod_{i=1}^n a_i\right)^T = a_n{}^T \cdot \cdots a_3{}^T\, a_2{}^T\, a_1{}^T$$

za svaki prirodan broj $n>1$.

Napose $$(a^n)^T = (a^T)^n.$$

5.4. Operator T za matrice jest *idempotentan*, tj.

$$(a^T)^T = a, \quad \text{tj.} \quad a^{TT} = a.$$

6. SIMETRIČNE I KOSOSIMETRIČNE MATRICE

6.1. D e f i n i c i j a. *Matrica a je simetrična ako je $a = a^T$*, tj. *ako je $a_{ij} = a_{ji}$.*

Matrica je *kososimetrična* ili *antisimetrična* ako je $a^T = -a$, tj. ako je $a_{ij} = -a_{ji}$.

6.2. Naravno, ako je a simetrična ili kososimetrična matrica, onda je a *kvadratna* matrica.

6.3. Specijalno, kod svake kososimetrične matrice dijagonala je $=0$. Naime, iz $a_{ji} = -a_{ij}$ za $i=j$ izlazi $a_{ii} = -a_{ii}$, odakle $a_{ii} = 0$.

6.4. *Za svaku kvadratnu matricu a matrica $a + a^T$ je simetrična; $a - a^T$ je kososimetrična.*

D o k a z: $(a \pm a^T)^T = a^T \pm a^{TT} = a^T \pm a = \pm a + a^T$, tj. $a + a^T$ je simetrično, odnosno $a - a^T$ je kososimetrično.

6.5. T e o r e m. *Jednakost* $$a = \frac{1}{2}(a + a^T) + \frac{1}{2}(a - a^T)$$ *pokazuje da je svaka kvadratna matrica suma od simetrične i kososimetrične matrice. Taj je rastav jednoznačan.*

Drugim riječima: svaka kvadratna matrica može se prikazati na jedan i samo jedan način kao suma simetrične i kososimetrične matrice.

Naime, ako je

$$a = x + y, \quad x^T = x, \quad y^T = -y,$$

tada je

$$a^T = x - y,$$

Iz te dvije jednadžbe, dakle, izlazi $a + a^T = 2x$, $a - a^T = 2y$, itd.

6.6. Gauss-Gram-ov produkt zadane matrice. Gaussov ili Gramov produkt pridružen matrici a jest matrica $a^T a$. Taj produkt postoji za svaku konačnu matricu i predstavlja *simetričnu* matricu.

Naime, $(a^T a)^T = a^T \cdot a^{TT} = a^T a$ (isp. pogl. 26, § 10.2. o kongruentnim matricama).

Od posebnog su značenja matrice a za koje je $a^T a = a a^T$; zovu se *normalne realne matrice*; takve su matrice npr. sve simetrične, sve kososimetrične matrice te stupci i réci. Normalne matrice odlikuju se nekim vrlo važnim svojstvima u vezi s tzv. *svojstvenim* vektorima (isp. 27 § 9.4).

7. HERMITSKI KONJUGIRANE MATRICE. HERMITSKO MNOŽENJE

7.1. Definicija. Za matricu a kojoj su vrijednosti *kompleksni izrazi, spregnuta ili konjugirana matrica* $\bar{a}$ definira se tako da se umjesto svakog elementa a_{ij} u a stavi spregnut (*konjugirani*) *element* $\bar{a}_{ij}$:

$$(\bar{a})_{ij} = \bar{a}_{ij}$$

Pri tom za kompleksni broj $x + iy$ definiramo $\overline{x + iy} = x - iy$ (simetrija prema apscisnoj osi).

Ako je matrica a realna, tj. ako su svi a_{ij} realni brojevi, onda je naravno $\bar{a} = a$.

$\bar{\bar{a}} = a$, tj. operator je idempotentan.

7.2. Definicija. *Hermitski pridružena matrica od a jest* $\overline{a^T}$; *označuje se obično sa* $a^\star$, tj.

$$(a^\star)_{ij} = \overline{a_{ji}}.$$

7.3. Teorem. *Za hermitsko pridruživanje* $a \to a^\star$ *vrijede uglavnom pravila analogna pridruživanju* $a \to a^T$:

$$(a + b)^\star = a^\star + b^\star, \quad (ab)^\star = b^\star a^\star, \quad (a^n)^\star = (a^\star)^n.$$

Razlika je u tome što je

$$(xa)^\star = \bar{x} a^\star, \quad (xa)^T = x a^T \quad \textit{za svaki broj } x, \text{ odnosno}$$

$$(xa + yb)^\star = \bar{x} a^\star + \bar{y} b^\star$$

$$(xa + yb)^T = x a^T + y b^T$$

za proizvoljne *brojeve* x, y.

To znači da zvijezdovanje, tj. *-operacija *nije linearna*, dok je *T-operator* linearan.

7.4. Hermitsko množenje matrica (vektora).

7.4.1. Definicija. *Pod hermitskim produktom niza* (vektora) $a = a_1, a_2, \ldots$ i jednakobrojna niza (vektora) $b = b_1, b_2, \cdots$ razumijevamo skalarni produkt prvog i konjugiranog drugog; označuje se sa $\mathrm{H}(a, b)$ ili $a\,\mathrm{H}\,b$ ili naprosto (a, b); dakle

$$\mathrm{H}(a, b) = a\,\mathrm{H}\,b = (a, b) = a \circ \overline{b} = a_1\overline{b_1} + a_2\overline{b_2} + \cdots$$

pri tom $\overline{b_k}$ označuje broj koji je konjugiran ili spregnut sa b_k.

Shvatimo li a, b kao *stupce* tj. kao matrice u oblasti $n \times 1$, tada se hermitski produkt $a\,\mathrm{H}\,b$ prikazuje ovako kao matrični produkt:

$$a\,\mathrm{H}b = (a, b) = a^T\overline{b}.$$

Kad bi a, b bile matrice poretka $1 \times n$ (dakle redići) bilo bi

$$a\,\mathrm{H}\,b = (a, b) = ab^*.$$

Hermitsko množenje matrica od izvanredne je važnosti. Posebno se vidi da se u slučaju nizova (vektorâ) s *realnim* vrijednostima hermitsko množenje svodi na *obično* (*unutrašnje*) *množenje nizova* (*vektora*). Razlog zašto se promatra i hermitsko množenje vektora jest u tome da se osigura da produkt vektora $\neq\vec{0}$ sa samim sobom bude $\neq 0$; tako npr. unutrašnji kvadrat vektora $\begin{bmatrix} 1 \\ i \end{bmatrix}$ glasi $[1, i].\begin{bmatrix} 1 \\ i \end{bmatrix} = 1 + i2 = 0$, tj. dobije se 0, mada je polazni vektor $\neq\vec{0}$. Hermitski kvadrat toga vektora glasi $1 \cdot 1 + (-i)\,i = 1 - i^2 = 2$.

7.4.2. Teorem. *Za hermitsko množenje vektora analogon zakona komutacije glasi:*

$$H(x, y) = \overline{H(y, x)},$$

tj. promijeni li se redoslijed faktora u hermitskom množenju dvaju vektora, prelazi produkt u konjugiranu vrijednost.

Dokaz:

$$H(y, x) = y \circ \overline{x} = y^T\overline{x} = \sum y_j\overline{x_j} = \sum\overline{y_j}\,x_j = \overline{\sum y_j\,x_j} = \overline{x^T\,y} = \overline{H(x, y)}.$$

7.5. *Hermitska simetrija, hermitska kosa simetrija, hermitska normalnost matrice a i hermitska ortogonalnost matrice a na matricu b definiraju se, po redu, jednakostima:*

$a = a^*$ (*hermitska simetrija*)

$a = -a^*$ (*hermitska kosa simetrija*)

$a^*\,a = aa^*$ (*hermitska normalnost*)

$a^*\,b = 0$ (*hermitska ortogonalnost*).

Ti pojmovi poopćuju uobičajenu simetriju, kosu simetriju, normalnost i ortogonalnost, koje se dobiju u slučaju $\overline{a} = a$, tj. kad je matrica a realna.

Posebno, kaže se da je vektor x *ortogonalan*, odnosno *hermitski ortogonalan* na vektoru y ako je $x^T y = 0$, odnosno $x^\star \cdot y = 0$.

Vidi se da iz ortogonalnosti (hermitske ortogonalnosti) od x na y izlazi i ortogonalnost (hermitska ortogonalnost) od y na x.

8. VEKTORI. KOVARIJANTNI I KONTRAVARIJANTNI VEKTORI

8.1. Definicija. *Matrice koje se sastoje od jednog jedinog stupca ili jednog jedinog retka zovu se vektori. Ako se radi o matrici — stupcu,* govori se o stupčanom ili *kontravarijantnom vektoru* ili o *vektoru-stupcu.* Ako se radi o retku, govori se o *vektoru-retku* ili *kovarijantnom vektoru.*

U toku daljih razmatranja vidjet ćemo kako su te dvije vrste vektora međusobno povezane.

Ubuduće, *ako izričito ne kažemo drukčije, riječ »vektor« odnosit će se na vektor kao stupac* (tj. na koordinatnu liniju koja je paralelna s „apscisnom" osi u Descartes-ovu pravokutniku i matričnoj shemi).

Tako npr. ako sa v označimo vektor

$$\begin{bmatrix} 3 \\ 4 \\ 8 \end{bmatrix},$$

tada ćemo govoriti i o pripadnom vektoru v^T kao retku:

$$v^T = [3, \quad 4, \quad 8],$$

jer je tako *zgodnije pisati.*

Zadan je vektor v, recimo $v^T = [3, 4, 8]$. To znači da je zadani vektor v upravo stupac

$$\begin{bmatrix} 3 \\ 4 \\ 8 \end{bmatrix}^{1)}.$$

8.2. Skalarno množenje nizova kao matrično množenje.
Neka su f, g dva niza po n članova:

$$f_0 \cdots f_{\dot{n}} \, (\dot{n} \in In)$$

$$g_0 \cdots g_{\dot{n}} \, (\dot{n} \in In).$$

---

[1]) Treba biti načistu s ovim *činjenicama: mi pišemo i čitamo u recima slijeva nadesno, i reci se nižu odozgo naniže. Crtamo i slikamo slijeva nadesno* i idući *naviše. Koordinatni sistem u ravnini uređen je tako da* odgovara *crtanju a ne pisanju;* zato apscisna os obično i ide horizontalno slijeva nadesno, a ordinatna os ide *odozdo prema gore.* Kod *matrica* ima *hibridna* stvar: *orijentacija koordinatnih osi je kao i inače*: ordinatna os nastaje iz apscisne osi rotacijom u pozitivnom smislu za kut $< \pi$ (obično za kut $\pi/2$); u drugu ruku, kod matrica je sačuvan *princip međunarodnog pisanja slijeva nadesno.* Zato su „*stupci*" matrice, u stvari, *koordinatne linije*

$$y = konst,$$

tj. kod njih je *druga koordinata konstanta.* A te koordinatne linije *u matematici* i *pri crtanju* obično su *horizontalne.*

Shvatimo li f i g kao *vektore*, tj. kao *stupce*, tada je *skalarni* produkt

$$f \circ g = \sum_n f_n g_n$$

isto što i *matrični* produkt $f^T.g$ odnosno $g^T f$.

Naime, f kao *vektor* glasi

$$f = \begin{bmatrix} f_0 \\ f_1 \\ \vdots \end{bmatrix}, \quad g = \begin{bmatrix} g_0 \\ g_1 \\ \vdots \end{bmatrix}, \text{ pa je } f^T = [f_0, f_1, \cdots]$$

$$g^T = [g_0, g_1 \cdots], \text{ dakle } f^T \cdot g = [f_0 f_1 \cdots] \begin{bmatrix} g_0 \\ g_1 \\ \vdots \end{bmatrix} = f_0 g_0 + f_1 g_1 + \cdots = g^T f.$$

8.3. Vektori vezani uz zadanu matricu. Riječ je *o stupcima* zadane matrice a kao *vektorima*. Njihov niz određuje potpunu matricu a. Zato se matrica a i može označiti sa $[a_{\cdot 1}, a_{\cdot 2}, \cdots]$. Upotreba vektorskog rječnika vrlo je sugestivna, kao što ćemo se na svakom koraku uvjeriti.

U čitavom narednom poglavlju o determinantama treba gledati kako *determinanta matrice a* zavisi od njenih *vektora*. Naime, *determinanta det a* je *funkcija od n vektora* $a_{\cdot 1}, a_{\cdot 2}, \cdots$

8.4. Geometrijsko gledanje na vektore i matrično gledanje na vektore. Radimo npr. u trodimenzionalnom koordinatnom prostoru R^3; njega možemo shvatiti i kao skup svih uređenih trojki (x_1, x_2, x_3) realnih brojeva. Ta trojka je tačka prostora. Istaknuta tačka je (0, 0, 0). No trojku (x_1, x_2, x_3) možemo shvatiti i kao vektor

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix};$$

na taj način tački $(x_1, x_2, x_3,)$ prostora odgovara radijus-vektor $[x_1, x_2, x_3]^T$. Uređenom paru tačaka (x_1, x_2, x_3), (y_1, y_2, y_3) odgovara vektor $[y_1 - x_1, y_2 - x_2, y_3 - x_3]^T$. Itd.

Znamo kako se s vektorima *računa* (zbrajanje, oduzimanje, množenje brojem, unutrašnje množenje). Posebno, vidimo da vrijedi formula

$$x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + x_2 \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + x_3 \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

To znači da je u prostoru od 3 dimenzije *svaki vektor x linearni spoj posebnih triju vektora*

$$e_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad e_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

Naprotiv, *ova tri vektora linearno su nezavisna* jer nijedan od njih nije linearan spoj od preostala dva. Tako npr. svaki linearni spoj od e_1 i e_2 ima treću vrijednost 0, a ne 1, kao što je u vektoru e_3.

Analogna razmatranja vrijede za prostor R^{I4} od 4 dimenzije nad tijelom R realnih brojeva: treba samo svuda umjesto broja 3 u gornjim razmatranjima uzeti broj 4. Slično za prostor R^{I5} i uopće za prostor R^{In} kao skup svih nizova po n članova iz tijela R realnih brojeva.

8.5. *Linearni spoj zadanih vektora* je svaki vektor koji se iz zadanih vektora dobije služeći se konačnim brojem ovih dviju operacijâ: 1) Množenje vektorâ i skalarâ, 2) Vektorsko zbrajanje. Tako npr. svi linearni spojevi gornjih triju vektora e_1, e_2, e_3 čine čitav prostor od 3 dimenzije.

9. Zadaci o matricama.

1. *Transponirane matrice.* Za svaku matricu x iz § 1.5 i § 4.7 nađi pripadnu transponiranu ili dvojnu matricu x^T. Koja je od tih matrica simetrična, kososimetrična, hermitska, kosohermitska?

2. Neka je

$$a=\begin{bmatrix}2 & 1\\ 3 & 5\end{bmatrix},\quad =b\begin{bmatrix}3+2i & 4 & \\ 7 & 5 & -i\end{bmatrix},\quad f(x)=3x^2-x+1;$$

za $x=a, b$ nađi $f(x)$, $f(x)^T, x^T$, $f(x^T)$ i dokaži da je $(f(x))^T=f(x^T)$.

3. Isto pitanje za matrice $\overline{x}$, $\overline{f(x)}$, $f(\overline{x})$.

4. Prikaži ove matrice kao zbroj simetrične i kososimetrične matrice:

$$a=\begin{bmatrix}3 & -5 & 4\\ 2 & 1 & 5\\ 1 & 3 & 4\end{bmatrix},\quad b=\begin{bmatrix}2-i & -3 & 4i\\ 5i & 2 & 4\\ 1 & -3 & 5\end{bmatrix},\quad c=\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 0\\ 0 & 1 & i\end{bmatrix}.$$

5. Promatraj matrice I, J, K iz teorije kvaterniona (zad. 4.7.9) i matrice, $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \beta_1, \beta_2, \beta_3, \beta_4, \xi$ iz kvantne teorije (zad. 4.7. 10). Svaku od tih matrica prikaži kao sumu simetrične i kososimetrične matrice, odnosno kao sumu hermitske i kosohermitske matrice.

6. Koje od slijedećih matrica zadovoljavaju jednakost normalnosti $x^* x=x x^*$:

$$a=\begin{bmatrix}3 & 2\\ 2 & 3\end{bmatrix},\quad b=\begin{bmatrix}-3 & 1 & 5\\ -1 & -3 & 4\\ -5 & -4 & -3\end{bmatrix},\quad c=\begin{bmatrix}0 & 1 & 5\\ -1 & 0 & 4\\ -5 & -4 & 0\end{bmatrix},$$

$$d=\begin{bmatrix}2-i & 5+4i\\ 5-4i & -7\end{bmatrix},\quad e=\begin{bmatrix}0 & 4+i & 3-2i\\ -4+i & 0 & 6\\ -3-2i & -5 & 3\end{bmatrix},$$

$$f=\begin{bmatrix}\cos a & \sin a\\ -\sin a & \cos a\end{bmatrix},\quad g=\begin{bmatrix}\operatorname{ch} a & \operatorname{sh} a\\ \operatorname{sh} a & \operatorname{ch} a\end{bmatrix}?$$

7. Nađi $\det(x^* x)$, $\det(x x^*)$ za matrice x iz prethodnog zadatka.

8. Ispiši sve kovarijantne i sve kontravarijantne vektore matrice x iz zadatka 5.

9. Ovaj skalarni produkt prikaži kao matrični produkt:
1) $ax+by$, 2) $3x-2y+z$. 3) $\cos^2 x-\sin^2 x$, 4) $a(xy-yz)+$ $+b(yz-zx)+c(zx-xy)$, 5) $a_0+a_1x+a_2x^2+\cdots+a_nx^n$;
6) $a_0e^{ic_0}+a_1e^{ic_1}+\cdots+a_ne^{ic_n}$.

10. Za matricu $a=\begin{bmatrix}3 & 2 & 4\\ 5 & 1 & 6\end{bmatrix}$ nađi skalarni produkt vektora:

1) $a_{\cdot 1}, a_{\cdot 3}$ 2) $a_{\cdot 2}$, $a_{\cdot 3}$, 3) $a_{1\cdot}$, $a_{3\cdot}$, 4) $a_{2\cdot}$, $a_{3\cdot}$, 5) $3a_{\cdot 2}$, $4a_{\cdot 3}$,
6) $-\frac{1}{3}a_{\cdot 3}, \frac{2}{5}a_{\cdot 2}$.

11. Za prethodnu matricu a ispiši matricu:

1) $[a_{\cdot 1}\, a_{\cdot 3}]$, $[a_{\cdot 1}, a_{\cdot 3}, a_{\cdot 2}, a_{\cdot 1}]$ i dualno: $\begin{bmatrix}a_{1\cdot}\\ a_{3\cdot}\end{bmatrix}$, $\begin{bmatrix}a_{1\cdot}\\ a_{3\cdot}\\ a_{2\cdot}\\ a_{1\cdot}\end{bmatrix}$;

2) $[3a_{\cdot 1}, a_{\cdot 2}+a_{\cdot 3}, a_{\cdot 1}-a_{\cdot 3}]$, 3) $[a_{\cdot 1}-2a_{\cdot 2}, a_{\cdot 1}-3a_{\cdot 3}, a_{\cdot 1}-a_{\cdot 2}]$.

12. Zadan je vektor $v=\begin{bmatrix}2\\ 4\\ 7\end{bmatrix}$; ispiši matricu:

1) $[v,\ 3v]$, 2) $[v^0,\ v,\ v^2]$, 3) $\begin{bmatrix}v^T\\ 3v^T\\ 5v^T\end{bmatrix}$.

13 Neka je $a=\begin{bmatrix}3 & -5 & 4\\ 2 & 4i & 7\\ 2 & 5 & 3i\end{bmatrix}$; obrazuj matricu b za koju je

1) $b_{\cdot 1}=a_{\cdot 1}$, $b_{\cdot 2}=2a_{\cdot 2}$, $b_{\cdot 3}=-3a_{\cdot 3}$; 2) $b_{\cdot 1}=-a_{\cdot 1}+a_{\cdot 2}$, $b_{\cdot 2}=a_{\cdot 2}$, $b_{\cdot 3}=a_{1\cdot}+a_{2\cdot}+a_{3\cdot}$, $b_{\cdot 4}=\vec{0}$.

14. Neka je m bilo kakva konačna kvadratna matrica, a $f(x)$, $g(x)$ algebarski mnogočlani; obrazuj matrice fa, $ga\pm ga$, $f(a)\,g(a)$ i dokaži da je $f(a)\cdot g(a)=g(a)\cdot f(a)$.

15. (*kljetne matrice*). Promatraj jediničnu matricu I_2; zamijeni joj vrijednost na polju (i, k) matricom: (I) $a_{ik} = \begin{bmatrix} 2i & 3i+1 & 4k \\ 3i & 6ik & -2i+k \\ 1 & 2 & ik \end{bmatrix}$,

(II) $b_{ik} = [i-k]$; 1) kako glase dobivene matrice A, B i njihove oblasti? 2) Nađi $A \pm B$, i dokaži da se do rezultata može doći na ova dva načina: naći $A_{ik} + B_{ik}$ odnosno naći $a_{ik} + b_{ik}$ i rezultat upisati u polje (i, k) tj. $(A+B)_{ik} = a_{ik} + b_{ik}$; 3) nađi umnožak AB i dokaži da je $(AB)_{ik} = a_{i1}\, b_{1k} + a_{i2}\, b_{2k}$.

16. Dokaži da pravila kao u zad. 15. vrijede općenito za matrice s kljetkama **(blokovne matrice):** operacije se vrše kao da se ne radi o kljetkama ili blokovima nego o običnim komponentama.

17. Promatraj matricu

$$a = \left[\begin{array}{ccc:ccc} 2 & 3 & 4 & 5 & 6 & 0 \\ 3 & 2 & 4 & 1 & 3 & 5 \\ 4 & 2 & 1 & 2 & 0 & 3 \\ \hdashline 1 & 2 & 4 & 0 & 0 & 5 \\ 3 & 3 & 3 & 1 & 1 & 1 \\ 2 & 4 & 0 & 3 & 2 & 1 \end{array}\right]$$

i njeno naznačeno razbijanje u kljetke $\begin{bmatrix} B & C \\ D & E \end{bmatrix}$;

nađi $\det a$, $\det (BE-CD)$; da li je $\det a = \det (BE-CD)$?

18. Dokaži: 1) ako je kvadratna matrica a *idempotentna* ($a^2 = a$), tada je matrica $2a-1$ *involutivna* tj. zadovoljava $x^2 = 1$; 2) ako je kvadratna matrica a involutivna, tada je matrica $\frac{1}{2}(a+1)$ idempotentna.

19. *Povreda zakona asocijacije za množenje*. Promatraj onu matricu a beskonačnog poretka (ω, ω), kojoj je prvi redak konstanta 1, a i-ti redak konstanta $(-1)^i\, i^{-\alpha}$; neka je b ona matrica poretka (ω, ω) za koju je $b_{ii} = 0$, a inače $b_{ik} = (-1)\, k^{\alpha} (i^2 - k^2)^{-1}$; pri tom je $0 < \alpha < 0{,}5$. Ispiši matrice $a, b, p = a + b$; nađi pp, $(pp)\,p$, $p\,(pp)$ i dokaži da je $(pp)\,p \neq p\,(pp)$.

Literatura: Anđelić [3], Blanuša [1], Denis-Papin, Kaufmann [1], Gantmaher [1]' Križanič [1], Kurepa Svetozar [1], Lichnerowicz [1], Mac Duffee [1], Mal'cev [1], Zurmühl [1].

POGLAVLJE 11.

DETERMINANTA ZADANE MATRICE. GLAVNA SVOJSTVA DETERMINANATA

1. UVODNA RAZMATRANJA

Uz matricu su vezani razni pojmovi i razna svojstva. Jedan od vrlo važnih pojmova vezanih za matricu jesu *vektori* (stupci) matrice te *determinanta* matrice (za kvadratne matrice a kao „volumen“ kvadra što ga određuju *stupci* matrice). Na taj način dolazimo do pridruživanja $a \to \det a$.

Važna primjedba. Imajmo na umu da pri pridruživanju $a \to \det a$ imamo određenu funkciju pa $\det a$ zavisi u isto vrijeme: i od matrice a i od svih vektorâ-stupaca $a_{\cdot 1}, a_{\cdot 2}, \ldots$ i od svih vektora-redaka $a_{1\cdot}, a_{2\cdot}, \ldots$ i od svih vrijednosti (komponenata $a_{11}, a_{12}, \ldots, a_{nn}$). Specijalno je korisno shvatiti $\det a$ kao funkciju stupaca ili vektorâ $a_{\cdot 1}, a_{\cdot 2}, \ldots$ pa $\det [a_{\cdot 1}, a_{\cdot 2} \ldots]$ pokazuje kako volumen kvadra zavisi od osnovnih bridova $a_{\cdot 1}, a_{\cdot 2}, \ldots$ Prema tome $\det [a_{\cdot 1}, a_{\cdot 2}, \ldots]$ je funkcija od n argumenata (varijabli) $a_{\cdot 1}, a_{\cdot 2}, \ldots$ i te su varijable vektori $a_{\cdot 1}, a_{\cdot 2}, \ldots$

Uvjerit ćemo se da je za matricu a bitno da li je $\det a = 0$ ili $\det a \neq 0$.

1.0. Definicija. **Regularne i singularne matrice.** *Konačna kvadranta matrica* (odnosno *determinanta* $\det a$) je *neregularna* (singularna) ili *regularna*, već prema tome da li je $\det a = 0$ ili $\det a \neq 0$.

Determinantu $\det a$ za slučaj kvadratnih matrica oblasti (n, n) za

$$n = 1, 2, 3, \ldots$$

definirali smo u pogl. 9, § 3. ovako:

$$\det a = \sum_p (-1)^{ip} \; a_{p_1 1} \cdot a_{p_2 2} \cdot \cdots \cdot a_{p_n n},$$

pri čemu p prolazi skupom svih permutacija množine $1\,(n) = \{1, 2, \ldots, n\}$.

Sad ćemo dokazati neka važna svojstva determinanata. Pri tom je vrlo korisno imati na umu specijalno matrice, odnosno determinante reda 2, jer su one vrlo jednostavne, a u drugu ruku mnoga svojstva determinanata se izriču nezavisno od njihova reda. Nadalje je vrlo korisno imati na umu i *geometrijsko*

značenje determinante kao *mjere* za sadržinu orijentiranog kvadra kojemu se *vektori osnovnih bridova* što izlaze iz jednog vrha podudaraju sa *stupcima matrice* (isp. poglavlje 9, § 1.10).

Imajmo na umu činjenicu da $\det a$ zavisi od n vektorâ $a_{.1}, a_{.2}, \ldots a_{.n}$; ispitat ćemo kakva je to funkcija!

1.1. *Determinanta dijagonalnih kvadratnih matrica i trokutastih matrica.* Neka je *a dijagonalna kvadratna matrica* poretka (n, n); to znači da je $a_{ij}=0$ za $i \neq j$. Posmatrajmo opći član u $\det a$; on glasi:

$$(-1)^{ip}\, a_{p_1 1}\; a_{p_2 2}\; a_{p_3 3} \ldots,$$

gdje p prolazi permutacijama množine $1\,(n)$. No ako je p različito od identičke permutacije, onda je za bar jedno $e \leq n$, $p_e \neq e$, a time $a_{p_e e}=0$, pa odgovarajući član u $\det a$ iščezava. To znači da je $\det a = a_{11}\; a_{22} \ldots$; tako smo dokazali

1.2. Teorem. *Determinanta dijagonalne matrice jednaka je produktu vrijednosti na dijagonali te matrice.*

1.2.1. Korolar. *Determinanta svake jedinične matrice je* 1.

Npr. $\begin{vmatrix} 3 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 6 \end{vmatrix} = 3 \cdot 5 \cdot 4 \cdot 6 = 360.$

Isto tako se dokazuje

1.3. Teorem. *Determinanta svake konačne kvadratne trokutaste matrice jednaka je produktu članova na dijagonali.*

Uistinu, neka je a kvadratna matrica poretka (n, n), gdje ie n prirodni broj; prema pretpostavci a je trokutasta matrica, tj.

(*) $$a_{ej}=0 \text{ za } e>j.$$

Pa neka je

(1) $$(-1)^{ip}\; a_{p_1 1}\; a_{p_2 2} \ldots$$

neki član od $\det a$ koji je $\neq 0$. Zbog pretpostavke (*) mora biti

$$p_1 \leq 1, \qquad p_2 \leq 2, \ldots;$$

odatle po redu izlazi $p_1=1$, $p_2=2$ (jer $p_1 \neq p_2$), $p_3=3$ (jer je $p_3 \neq p_2$) itd.

Dakle se permutacija p svodi na identičku permutaciju množine $1\,(n)$, a to upravo znači da je član (1) produkt vrijednosti na dijagonali.

2. Determinanta je alternirajuća funkcija svojih vektora (stupaca).

$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = -\begin{vmatrix} b & a \\ d & c \end{vmatrix}$, općenito:

2.1. Teorem. *Determinanta kvadratne matrice je alternirajuća funkcija stupaca* (*vektora*) *te matrice.*

Drugim riječima: *Ako u kvadratnoj matrici dva njena stupca zamijene svoja mjesta, determinanata prelazi u suprotno-jednaku.* Npr. (zamjena $2 \rightleftarrows 1$)

$$\det [a_{.1},\ a_{.2},\ a_{.3} \ldots] = -\det [a_{.2},\ a_{.1},\ a_{.3}, \ldots].$$

Govoreći geometrijski: permutiraju li se dva osnovna brida u kvadru, sadržina se kvadra ne mijenja, ali mu orijentacija prelazi u suprotnu.

Recimo da se radi o matrici a sa stupcima $a_{.1}, a_{.2}, \ldots$

Recimo da stupci $a_{.1}, a_{.2}$ zamijene svoja mjesta. Neka je b ta nova matrica; za nju je dakle

(1) $$b_{.1} = a_{.2},\ b_{.2} = a_{.1},\ \text{te}\ a_{.j} = b_{.j}\ \text{za}\ j > 2.$$

Permutaciji $p = p_1 p_2 \ldots$ množine $1(n)$ odgovara ovaj član $b(p)$ u $\det b$:

$$b(p) = (-1)^{ip}\, b_{p_1 1}\ b_{p_2 2} \ldots\ b_{p_n n}.$$

Zbog (1) to je dalje jednako

(2) $$b(p) = (-1)^{ip}\, a_{p_1 2}\ a_{p_2 1}\ a_{p_3 3} \cdots = (-1)^{ip}\ a_{p_2 1}\ a_{p_1 2}\ a_{p_3 3} \cdots$$

U indeksima se tu pojavljuje permutacija $p' = p_2 p_1 p_3 \cdots p_n$ koja iz p nastaje transpozicijom prvih članova p_1, p_2. No, transpozicijom članova u permutaciji mijenja se broj inverzija za neparan broj (isp. pogl. 3, § 8.6.2): to znači da je $ip' = ip \pm$ neparno, dakle

$$(-1)^{ip'} = -(-1)^{ip}.$$

Unesemo li odatle $(-1)^{ip}$ u (2), dobijemo

$$b(p) = -(-1)^{ip'}\ a_{2p1}\ a_{p_1 2}\ a_{p_3 3} \ldots, \quad \text{tj.}\ b(p) = -a(p'),$$

gdje je $a(p')$ član determinante a što odgovara permutaciji p'. No, kad p prolazi kroz skup $1(n)!$ svih permutacija od $1(n)$, prolazi također p' kroz $1(n)!$ pa je zato

$$\det b = \sum_{p} b(p) = -\sum_{p' \varepsilon\, 1(n)!} a(p') = -\det a.$$

Sasvim se slično dokazuje stvar ako koja god dva susjedna stupca zami jene svoja mjesta. A odatle izlazi teorem za transpoziciju bilo kojih dvaju stupaca — bili oni susjedni ili ne bili.

2.2. K o r o l a r: *Ako kvadratna matrica ima dva jednaka stupca, onda je ona singularna,* tj. $\det a = 0$.

Stvarno transpozicijom tih dvaju jednakih stupaca *matrica se ne mijenja;* dakle se ne mijenja ni determinanta $\det a$; no prema teoremu 2.1. prelazi $\det a$ u $-\det a$; dakle je $\det a = -\det a$; odatle izlazi da je $\det a = 0$.

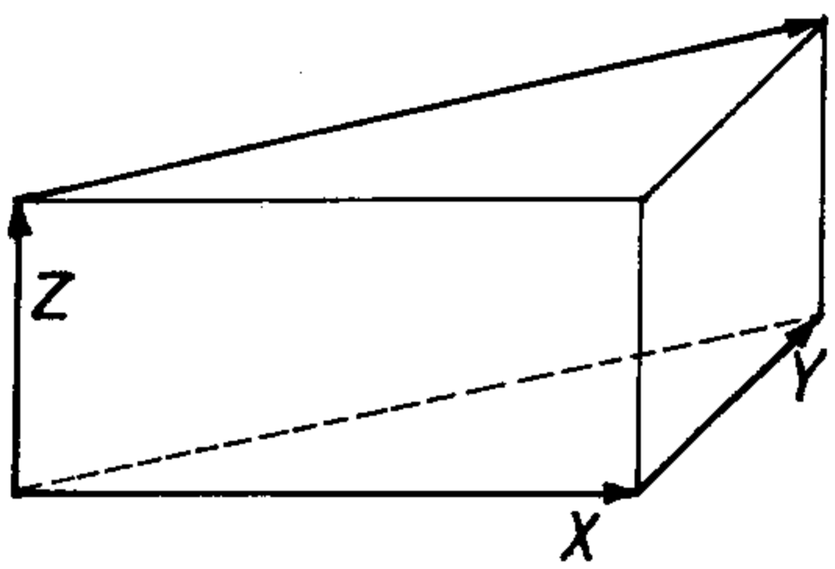
3. DETERMINANTA JE LINEARNO-HOMOGENA FUNKCIJA SVAKOG SVOJEG VEKTORA (STUPCA)

3.1. Lema. *Pomnoži li se neki stupac determinante nekim izrazom, množi se tim izrazom i sama determinanta.*

Geometrijski: Ako u nekom kvadru jedan osnovni brid pomnožimo sa c, pomnoži se sa c i mjera kvadra.

Dokaz. Neka je npr. $b_{.1}=c\cdot a_{.1}$, $b_{.j}=a_{.j}$ za $j>1$; tada svaki član u $\det b$ sadrži kao faktor: c kao i jedan član od $\det a$; dakle je $\det b=c\cdot\det a$.

3.2. Lema. $\begin{vmatrix} x+x' & y \\ u+u' & v \end{vmatrix} = \begin{vmatrix} x & y \\ u & v \end{vmatrix} + \begin{vmatrix} x' & y \\ u' & v \end{vmatrix}$, tj.



Sl. 11.2.

ako je jedan stupac determinante suma od dva niza, tada je determinanta jednaka sumi od odgovarajuće dvije determinante koje se iz zadane dobiju tako da se odgovarajući stupac zamijeni prvim, odnosno drugim nizom. Drugim riječima: *Determinanta je aditivna funkcija svakog svojeg vektora.* Geometrijski:

$$\mathrm{Pl}(\vec{x},\vec{z})+\mathrm{Pl}(\vec{y},\vec{z})=$$
$$=\mathrm{Pl}(\vec{x}+\vec{y},\vec{z});$$

tu $\mathrm{Pl}(x, z)$ znači orijentiranu ploštinu kvadra što ga razapinju radijusvektori $\vec{x}$, $\vec{z}$.

Dokaz. Pa neka je matrica b takva da je npr.

$$b_{.1}=\vec{f}+\vec{g},\ b_{.j}=a_{.j}\ \text{za}\ j=2,\ 3,\ldots;$$

pri tom su $\vec{f}$, $\vec{g}$ dva stupca po n članova. Permutaciji $p\in 1(n)!$ odgovara u $\det b$ član

$$b(p)=(-1)^{ip}\ b_{p_1 1}\ b_{p_2 2}\ldots,\ \text{tj.}$$
$$\sum_p b(p)=\sum_p(-1)^{ip}(f_{p_1}+g_{p_1})\,b_{p_2 2}\ldots=\sum_p(-1)^{ip}\,f_{p_1}a_{p_2 2}\ldots+$$
$$+\sum(-1)^{ip}\cdot g_{p_1}a_{p_2 2}\ldots=\det[\vec{f},a_{.2},a_{.3}\ldots]+\det[\vec{g},a_{.2},a_{.3}\ldots].$$

Kombinirajući prethodna dva rezultata, imamo ovaj teorem:

3.3. Teorem. *Determinanta je homogeno-linearna funkcija svakog svojeg vektora.*

Tako npr.

$$\begin{vmatrix} 2\cdot5-3\cdot2, & 2, & 3 \\ 2\cdot7-3\cdot1, & 4, & 5 \\ 2\cdot4-3\cdot5, & 8, & -4 \end{vmatrix} = 2\begin{vmatrix} 5 & 2 & 3 \\ 7 & 4 & 5 \\ 4 & 8 & -4 \end{vmatrix} - 3\begin{vmatrix} 2 & 2 & 3 \\ 1 & 4 & 5 \\ 5 & 8 & -4 \end{vmatrix}.$$

3.3.1. Primjer. Nađite determinantu produkta kvadratnih matrica tipa (2. 2). Neka su zadane matrice

$$a=\begin{bmatrix} p & q \\ s & t \end{bmatrix},\ b=\begin{bmatrix} u & v \\ x & y \end{bmatrix}.$$

Tada je

$$ab=\begin{bmatrix} pu+qx & pv+qy \\ su+tx & sv+ty \end{bmatrix};$$

dakle je

$$\det(ab)=\begin{vmatrix} pu+qx & pv+qy \\ su+tx & sv+ty \end{vmatrix}=\text{(shvaćajući prvi stupac kao sumu)}$$

$$=\begin{vmatrix} pu & pv+qy \\ su & sv+ty \end{vmatrix}+\begin{vmatrix} qx & pv+qy \\ tx & sv+ty \end{vmatrix}=\text{(shvaćajući druge stupce kao sume)}$$

$$=\begin{vmatrix} pu & pv \\ su & sv \end{vmatrix}+\begin{vmatrix} pu & qy \\ su & ty \end{vmatrix}+\begin{vmatrix} qx & qv \\ tx & sv \end{vmatrix}+\begin{vmatrix} qx & qy \\ tx & ty \end{vmatrix}=\begin{cases}\text{(izlučujući faktore iz poje-}\\ \text{dinih stupaca)}\end{cases}$$

$$=u\begin{vmatrix} p & p \\ s & s \end{vmatrix}v+u\begin{vmatrix} p & q \\ s & t \end{vmatrix}y+x\begin{vmatrix} q & p \\ t & s \end{vmatrix}v+x\begin{vmatrix} q & q \\ t & t \end{vmatrix}y=0+u\det a\cdot y-x\det a\cdot v+0$$

$$=\det a\cdot(uy-vx)=\det a\cdot\det b,\quad \text{tj.}\quad \det(a\cdot b)=\det a\ \det b.$$

Analogan zaključak vrijedi za konačne kvadratne matrice uopće (teorem 9.2).

4. TRI KARAKTERISTIČNA SVOJSTVA DETERMINANATA

Rezultate iz prethodna tri paragrafa možemo skupiti zajedno pa tako spoznajemo da za kvadratne konačne matrice $x=[x_{.1},\ x_{.2},\ldots]$ pridruživanje

(1) $$x\to\det x \text{ odnosno } [x_{.1},\ x_{.2},\ldots]\to\det[x_{.1},\ x_{.2},\ldots]$$

ima ova tri svojstva:

1. *Determinanta matrice je alternirajuća funkcija stupaca* (vektorâ) (vidi teorem 2.1),

2. *Determinanta matrice je homogeno-linearna funkcija od svakog svojeg vektorskog argumenta* (teorem 3.3).

3. *Determinanta jedinične matrice je* 1 (korolar 1.2).

Zanimljivo je da su ta tri svojstva *i dovoljna da okarakteriziraju funkciju* (1) *u skupu kvadratnih konačnih matrica.* (K. Weierstrass).

Stvarno, neka je a proizvoljna matrica poretka (n, n), $n\in N$; tada je

$$a=[a_{.1},\ a_{.2},\ a_3\cdots];$$

no za svaki vektor $a_{\cdot j}$ matrice a vrijedi

$$a_{\cdot j} = a_{1j}\, e_1 + a_{2j}\, e_2 + \cdots + a_{ij}\, e_i + \cdots,$$

gdje je

$$e_i = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \end{bmatrix} \Big\} i.$$

Na taj način imamo ovaj prikaz matrice

$$a = [a_{11}\, e_1 + a_{21}\, e_2 + \cdots + a_{i1}\, e_i + \cdots,\ a_{12}\, e_1 + a_{22}\, e_2 \cdots,\ \cdots]. \tag{2}$$

Tu se pojavljuju sve vrijednosti a_{ij} matrice a. Uzmimo sada u prikazu (2) iz prvog stupca $a_{\cdot 1}$ jedan član, recimo član $a_{p_1 1}\, e_{p_1}$; neka je isto tako $a_{p_2 2}\ e_{p_2}$ jedan član u $a_{\cdot 2}$ itd. Za svaki n-član niz $p = p_1, p_2, p_3, \ldots$ brojeva iz $1\,(n)$ možemo promatrati determinantu

$$\left| a_{p_1 1}\, e_{p_1},\ a_{p_2 2}\, e_{p_2}, \ldots \right|. \tag{3}$$

Ona je prema lemi 3.1. jednaka

$$\left| a_{p_1 1}\, a_{p_2 2} \cdots \right| e_{p_1}, e_{p_2}, \cdots \left|. \right. \tag{4}$$

No, kod nizova p možemo se ograničiti na one bez jednakih članova, jer ako u nizu $p_1, p_2, \cdots$ ima *jednakih* članova, tada je determinanta u (4) ednaka 0 (v. korolar 2.2). Ostaje, dakle, slučaj da među n brojeva $p_1, p_2, \cdots$ iz $1\,(n)$ nema jednakih; to znači da je $p \in 1\,(n)$!. Tada je očigledno

$$\left| e_{p_1}, e_{p_2}, \cdots \right| = (-1)^{ip} \left| e_1,\ e_2,\ e_3, \cdots \right|.$$

No prema korolaru 1.2. imamo

$$\left| e_1,\ e_2 \cdots \right| = 1.$$

Na taj način determinanta, (4), odnosno (3), postaje

$$(-1)^{ip}\ a_{p_1 1}\ a_{p_2 2} \cdots \tag{5}$$

No, prema teoremu 3.3. suma svih determinanata (3) je $= \det a$. Dakle je prema (4) i (5) zaista

$$\det a = \sum_{p \in 1\,(n)!} (-1)^{ip}\, a_{p_1 1}\, a_{p_2 2} \cdots \tag{6}$$

A (6) je u pogl. 6, § 3. bila upravo definiciona formula za det a.

5. TRANSPONIRANJEM KVADRATNE MATRICE NE MIJENJA SE DETERMINANTA

Dosad smo ispitivali svojstva determinante u zavisnosti od njenih *stupaca*. Sad ćemo dokazati da analogna svojstva postoje i u pogledu *redaka*. Naime, transpozicijom $a \to a^T$ postaju reci ili redići stupcima, a stupci rečima. Pri tom, općenito, *matrica se mijenja*; naprotiv, *determinanta se ne mijenja*. Dokazat ćemo, naime, da vrijedi

—→ **5.1.** Teorem

$$\begin{vmatrix} x & y \\ u & v \end{vmatrix} = \begin{vmatrix} x & u \\ y & v \end{vmatrix},$$

tj. $\det a = \det a^T$ za matricu poretka (2, 2). Općenitije, *za svaku konačnu kvadratnu matricu a vrijedi*

$$\det a = \det a^T.$$

Permutira li se svaki redak s odgovarajućim stupcem determinanta se ne mijenja.

Dokaz. Neka je $b = a^T$; permutaciji p množine $1(n) = \{1, 2, \ldots, n\}$ odgovara član

$$b(p) = (-1)^{ip} b_{p_1 1} b_{p_2 2} \cdots \tag{1}$$

u $\det b$; no $b_{ij} = a_{ji}$ pa zato izraz $b(p)$ postaje

$$b(p) = (-1)^{ip} a_{1p_1} a_{2p_2} \cdots \tag{2}$$

Tu se pojavljuje produkt $a_{1p_1} a_{2p_2} \cdots$; napišimo taj produkt tako da *drugi* indeksi budu po redu 1, 2, $\cdots$; neka time *prvi* indeksi daju permutaciju q; dakle je

$$a_{1p_1} a_{2p_2} \cdots = a_{q_1 1} a_{q_2 2} \cdots \tag{3}$$

No, to *mijenjanje redoslijeda* faktora ima za posljedicu stanovit broj k transpozicijâ u permutaciji p, čime ona prelazi u identičku permutaciju kao i isto tolik broj k transpozicijâ u permutaciji $1(n)$, čime ona prelazi u permutaciju q; zato je $(-1)^{ip} = (-1)^k$, $(-1)^{iq} = (-1)^k$, tj.

$$(-1)^{ip} = (-1)^{iq} \tag{4}$$

Na osnovu (3) i (4) daje (2) ovo:

$$b(p) = (-1)^{iq}\ a_{q_1 1} a_{q_2 2} \cdots$$

A to znači da je $b(p)$ član $a(q)$ u $\det a$ koji odgovara permutaciji q; no kad p prolazi kroz $1(n)!$, prolazi i q kroz $1(n)!$, pa je dakle

$$\sum_p b(p) = \sum_q a(q). \tag{5}$$

No, po definiciji je $(5)_1 = \det b$, $(5)_2 = \det a$, pa zbog $b = a^T$ jednakost (5) daje traženu jednakost $\det a^T = \det a$.

5.2. P r i m j e d b a. Mada je tek za *neke* matrice a ispunjeno $a^T = a$, ipak je $\det a^T = \det a$ za *svaku* kvadratnu *konačnu* matricu.

Već i za slučaj $n = 2$ dobiva se time pravilnost koja s obzirom na *geometrijsko* značenje determinante nije nipošto očigledna.

Kombinirajući teorem 2.1 i 5.1, dolazimo do ovog teorema:

5.3. T e o r e m. *Determinanta kvadratne matrice je alternirajuća funkcija svojih stupaca* (*redaka*).

5.4. P r i m j e r. U kakvoj su vezi determinante matrica

$$a = [a_{.1},\ a_{.2},\ a_{.3}, \cdots], \quad [a_{.3},\ a_{.1},\ a_{.2},\ a_{.4}, \cdots]?$$

Transpozicijom stupaca $a_{.2}$, $a_{.3}$ prelazi matrica a u $[a_{.1}, a_{.3}, a_{.2}, a_{.4} \cdots]$; ako ovdje transponiramo stupce $a_{.1}$, $a_{.3}$, dolazimo do matrice b; kako determinanta svaki put prelazi u suprotnu, znači da je:

$$\det [a_{.3}\, a_{.1}\, a_{.2} \cdots] = -\det [a_{.1}\, a_{.3}\, a_{.2} \cdots] = -(-\det a).$$

Na isti se način dokazuju ova dva teorema:

5.5. T e o r e m. *Ako u matrici a stupac* (*redak*) *x premjestimo kao početni stupac* (*redak*), *dobiva se matrica kojoj je determinanta* $= (-1)^x \det a$.

5.6. T e o r e m. *U matrici a promatrajmo redak* $a_{i.}$ *i stupac* $a_{.j}$; *premjestimo taj redak da postane prvi redak, a u rezultatu premjestimo stupac j tako da dođe na prvo mjesto; za dobivenu matricu b vrijedi ovo:*

$$\det b = (-1)^{i+j} \det a,$$

$$b_{11} = a_{ij}.$$

6. O POJEDNOSTAVLJENJU DETERMINANATA

6.1. T e o r e m. *Ako u determinanti koji stupac* (redak) *dodamo kojem drugom stupcu* (retku) *determinante, determinanta ne mijenja svoje vrijednosti. Isto vrijedi ako smo prethodno stupac* (redak) *koji smo dodavali pomnožili kakvim izrazom.*

Dokaz mu je kratak. Tako npr. ako u matrici a dvostruk stupac $a_{.3}$ dodamo stupcu $a_{.1}$, dobivamo matricu

$$[a_{.1} + 2\,a_{.3},\ a_{.2},\ a_{.3}, \ldots]$$

pa za pripadnu determinantu imamo

$$\det [a_{.1} + 2\,a_{.3},\ a_{.2}, \ldots] = \det [a_{.1}\ \ a_{.2} \ldots] + \det [2\,a_{.3}\ \ a_{.2}\ \ a_{.3}\ \ a_{.4} \ldots] =$$

$$= \det a + 2 \det [a_{.3}\ \ a_{.2}\ \ a_{.3}\ \ a_{.4} \ldots].$$

No, posljednja determinanta $= 0$, jer ima dva jednaka stupca: prvi i treći. Teoremom 6.1. mnogo se služimo.

6.1.1. Primjer.

$$\det a = \begin{vmatrix} 1 & 5 & 4 \\ 2 & 3 & 6 \\ 4 & 7 & -3 \end{vmatrix} = \det [a_{1.}\ a_{2.}\ a_{3.}]^T = \det [a_{1.},\ a_{2.}\ -2\,a_{1.},\ a_{3.}\ -4\,a_{1.}]^T =$$

$$= \left.\begin{vmatrix} 1 & 5 & 4 \\ 0 & -7 & -2 \\ 0 & -13 & -19 \end{vmatrix}\right\}. \quad -13/17 = \begin{vmatrix} 1 & 5 & 4 \\ 0 & -7 & -2 \\ 0 & 0 & 26/7-19 \end{vmatrix} =$$

$$= (\text{po teoremu } 1.3) = 1.\ -7 \cdot (26/7 - 19) = -26 + 133 = 107.$$

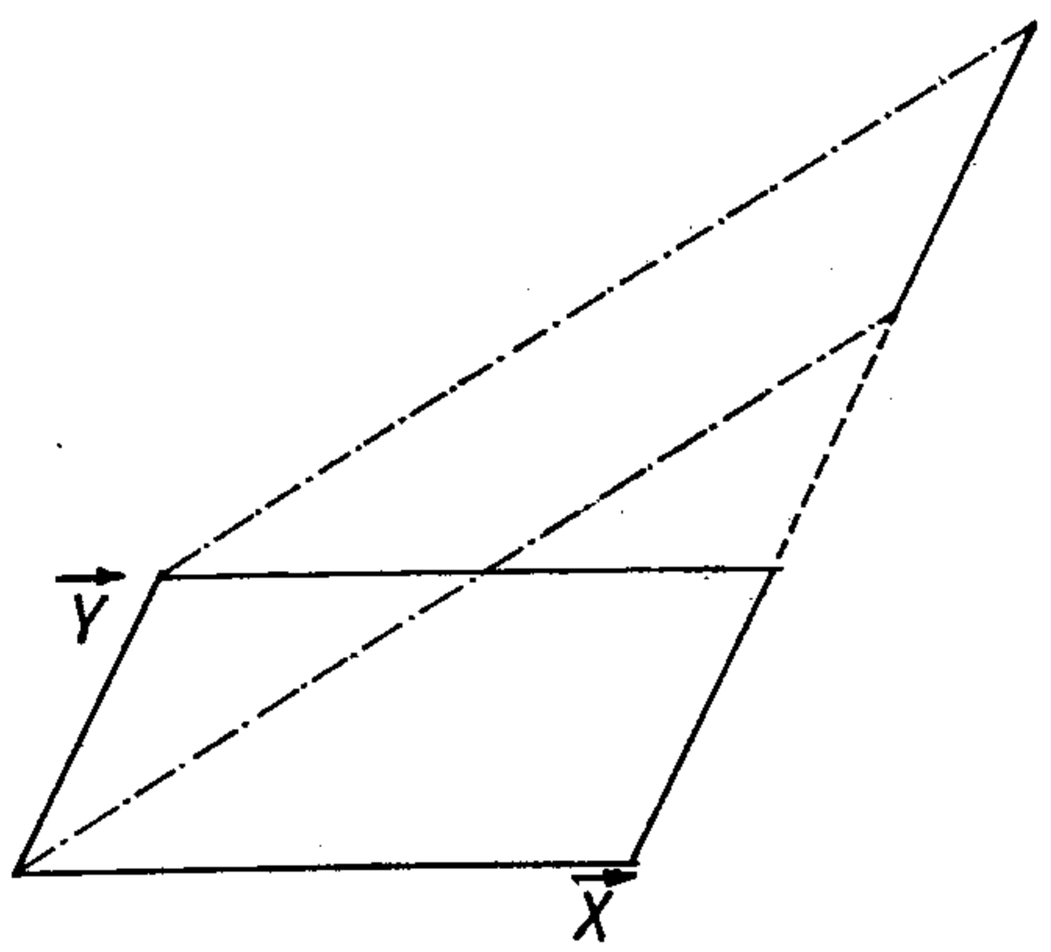
Dakle je $$\begin{vmatrix} 1 & 5 & 4 \\ 2 & 3 & 6 \\ 4 & 7 & -3 \end{vmatrix} = 107.$$

Primjenjujući uzastopno teorem 6.1, možemo dokazati da vrijedi ovo:

—→ **6.2.** Teorem. *Ako kojem određenom, inače proizvoljnom stupcu (retku) determinante pribrojimo linearan spoj ostalih njenih stupaca (redaka), determinanta se ne mijenja.*

To znači ovo:

Ako uočimo proizvoljan stupac (redak) l pa svaki drugi stupac (redak) x pomnožimo nekim izrazom g(x), koji može biti i 0, pa sve te produkte xg(x) pribrojimo liniji l, novonastala matrica, koliko god se razlikovala od polazne matrice a, ipak ima istu determinantu kao i a.



Sl. 11.11.6.

Geometrijski je taj teorem generalizacija činjenice o *jednakosti ploština svih paralelograma s istom bazom i istom visinom* (v. sl. 11·11.6.) ,gdje je

$$[\vec{x},\ \vec{y}] = [\vec{x} + 2\vec{y},\ \vec{y}].$$

6.3. Napomena. Treba imati na umu da se ***istodobnim*** dodavanjem jednih redaka drugima determinanta *može promijeniti*. Tako npr. kad bismo u matrici poretka (n, n) od početnog retka oduzeli redak 2, od retka 2 redak 3,..., a od posljednjeg retka oduzeli početni, dobili bismo jednu *singularnu* matricu.

Npr. $$\begin{vmatrix} c & d \\ c' & d' \end{vmatrix} = \begin{vmatrix} c-c' & d-d' \\ c' & d' \end{vmatrix}$$

$$\begin{vmatrix} c & d \\ c' & d' \end{vmatrix} = \begin{vmatrix} c & d \\ c'-c & d'-d \end{vmatrix}$$

Ali je $\begin{vmatrix} c & d \\ c' & d' \end{vmatrix} = \begin{vmatrix} c-c' & d-d' \\ c'-c & d'-d \end{vmatrix}$.

U ovom slučaju smo **istodobno** oduzimali redak 2 od retka 1 kao i redak 1 od retka 2. *A ova se operacija ne može svesti na* ***uzastopno*** *nizanje operacija opisanih u teoremu* 6.2.

6.4. Teorem. *Ako je koji stupac* (*redak*) *determinante linearan spoj ostalih stupaca* (*redaka*) *determinante, tada je determinanta jednaka* 0.[1)]

Dokaz. Recimo da je redak $a_{1.}$ linearna kombinacija ostalih redaka; to znači da se niz $a_{1.} = a_{11}, a_{12}, \ldots$ može prikazati u obliku

$$a_{1.} = \lambda_2 a_{2.} + \lambda_3 a_{3.} + \cdots,$$

gdje su $\lambda_2, \lambda_3, \cdots$ brojevi (neki ili svi mogu biti 0). No, ako u matrici a pomnožimo redak $a_{2.}$ sa $-\lambda_2$, redak a_3 sa $-\lambda_3 \cdots$ i te produkte pribrojimo retku $a_{1.}$, tada iz a nastaje matrica b, kojoj je prvi redak $b_{1.}$ ispunjen samim nulama; dakle je $\det b = 0$; u drugu ruku prema teoremu 6.2. vrijedi $\det a = \det b$. Dakle je $\det a = 0$.

6.4.1. Primjedba. Poslije ćemo u § 10.4. dokazati da vrijedi i obrat teorema 6.4. (v. teorem 10.5). Taj je obrat vrlo koristan teorem.

7. LAPLACEOV TEOREM. RAZVIJANJE DETERMINANTE PO ELEMENTIMA NEKOG STUPCA ILI RETKA

7.1. Uočimo neku kvadratnu (n, n)-matricu tj. matricu a poretka (n, n), i njenu determinantu

$$\det a = \sum_p (-1)^{ip} \; a_{p_1 1} \; a_{p_2 2} \cdots; \tag{1}$$

ip je broj inverzija u permutaciji p.

Tu p prolazi skupom $1\,(n)!$ svih permutacija množine $1\,(n)$. Promatrajmo sve one permutacije p koje počinju sa 1; one su oblika $1\,q$, gdje je q proizvoljna permutacije množine $\{2, \cdots, n\}$; no za svaku takvu permutaciju q očigledno je $iq = i\,(1, q)$. Nadalje je očigledno

$$\sum_{q \in \{2, 3, \ldots\}!} (-1)^{ip} \, a_{q_2 2} \; a_{q_3 3} \cdots = \begin{vmatrix} a_{22} & a_{23} \cdots a_{2n} \\ a_{32} & a_{33} \cdots a_{3n} \\ \cdot & \cdot \; \cdot \; \cdot \; \cdot \; \cdot \\ a_{n2} & a_{n3} \cdots a_{n,n} \end{vmatrix}.$$

[1)] Geometrijski je stvar evidentna; npr., ako iz zadana dva radijus-vektora $\vec{u}, \vec{v}$ formiramo njihov linearni spoj $\vec{w} = \lambda \vec{u} + \mu \vec{v}$, tada je „volumen" kvadra nad bridovima $\vec{u}, \vec{v}, \vec{w}$ jednak 0, jer je broj dimenzija toga kvadra < 3.

Ova determinanta je determinanta matrice, koja se iz matrice a dobije tako da joj se precrta prvi redak i prvi stupac: ta se determinanta zove *kofaktor vrijednosti* a_{11} *u odnosu na matricu* a i označuje se sa $f a_{11}$ ili $f(a_{11})$, ili preciznije $f_a a_{11}$, ili također a^{11}.

Na taj način vidimo da se u izrazu $(1)_2$ za $\det a$ pojavljuje i dio $a_{11} f a_{11}$.

7.2. Nađimo sada onaj dio u $(1)_2$ u kojem se pojavljuje faktor a_{21}. Taj se slučaj svodi na prethodni. Naime, transpozicijom redaka $a_{1.}$ i $a_{2.}$ u matrici a dolazi se do matrice b, kojoj je determinanta $= -\det a$ (v. teorem 2.1); no komponenta a_{21} je sada $= b_{11}$. Prema prethodnom slučaju, u izrazu za $\det b$, odnosno za $-\det a$ pojavljuje se dio $b_{11} f_b b_{11}$, dakle $a_{21} f_b b_{11}$. To znači, da se u izrazu za $\det a$ pojavljuje dio $-b_{11} f_b b_{11}$, tj. $a_{21} . (-f_b b_{11})$. No, $f_b b_{11}$ dobije se iz b ispuštanjem 1. retka i 1. stupca; a to znači da $f_b b_{11}$ nastaje iz a ispuštanjem 2 retka i 1. stupca. Drugim riječima, onaj izraz $f a_{21}$ kojim se a_{21} množi u izrazu za $\det a$ dobije se tako da se determinanta što se iz a dobije ispuštanjem 2. retka i 1. stupca pomnoži sa -1. Upravo se zato taj izraz

$$-\begin{vmatrix} a_{12} & a_{13} & \cdots & a_{1,n} \\ a_{32} & a_{33} & \cdots & a_{3,n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n2} & \cdots & \cdots & a_{nn} \end{vmatrix} = (-1)^{2+1} \det (a \setminus a_{21})$$

i naziva kofaktorom $f a_{21}$ od a_{21} u odnosu na matricu a. Općenito, neka važi ova definicija.

7.3. Definicija kofaktora. *Kofaktor ili algebarski komplement od vrijednosti komponente* a_{ij} *u matrici* a, *simbolički*

$$f a_{ij} \text{ ili } f_a a_{ij} \text{ ili } a^{ij},$$

jest produkt broja $(-1)^{i+j}$ *i determinante matrice* $a \setminus a_{ij}$, *koja iz* a *nastaje brisanjem retka* i *te stupca* j;

dakle je

$$f_a a_{ij} = (-1)^{i+j} \det (a \setminus a_{ij}) = (-1)^{i+j} \begin{vmatrix} & & & \text{j} & \\ a_{11} & a_{12} & & & \\ a_{21} & \cdot & & & \\ \text{i} & \cdots & \cdots & \cdots & \cdots \\ & & & & \end{vmatrix}$$

Tako npr.

$$f a_{42} = (-1)^{4+2} \begin{vmatrix} & & 2 & \\ & & & \\ \cdots & \cdots & \cdots & \cdots \\ & & & \end{vmatrix} 4.$$

Ako se u matrici a permutiraju reci 4 i 3 pa u rezultatu réci 3 i 2 i, najzad, 2 i 1, dolazi se do matrice koja iz a nastaje tako da joj se redak 4 premjesti kao početni redak; ako se u rezultatu još permutiraju stupci 1 i 2, dobit će se matrica x, kojoj je $x_{11} = a_{42}$ te $f x_{11} = f_a a_{42}$.

7.4. Riješimo sad problem općenito: *zadana je kvadratna matrica* a i njena (i, k)-komponenta a_{ik}; treba naći onaj faktor $f a_{ik}$ kojom treba množiti a_{ik} pa da se dobije najviše članova u izrazu za $\det a$. No, postepenim permutiranjem retka i s prethodnim $i-1$ pa u rezultatu permutiranjem retka $i-1$ i retka $i-2$ itd. dolazi se nakon i koračaja do matrice koja iz a nastaje tako da joj se redak i napiše kao početni redak; determinanta te nove matrice je $(-1)^i \det a$, jer pri svakom koraku determinanta mijenja znak. Ako u novoj matrici, sličnim postupkom sa stupcima, dopremimo stupac k da bude početni stupac (to se postiže pomoću k uzastopnih transpozicija stupca k, $k-1$ pa $k-1$, $k-2$ itd.), dolazi se najzad do određene matrice; označimo je sa $(i, k)a$, da se vidi da ona zavisi od matrice a i njene (ik) — komponente. Naravno,

$$\det ((ik)a) = (-1)^{i+k} \det a, \text{ tj.}$$

$$\det a = (-1)^{i+k} \det ((ik)a).$$

Nadalje je (1, 1) — komponenta u $(ik)a$ upravo a_{ik}; te dvije komponente imaju iste komplemente: precrtavanjem retka i i stupca k u matrici a dobije se ista matrica $c\, a_{ik}$ kao kad se u $(ik)a$ precrta prvi redak i prvi stupac. No, u $\det (ik)a$, tj. u $(-1)^{i+k} \det a$ množi se a_{ik} determinantom tog komplementa; dakle se u $\det a$ množi a_{ik} sa $(-1)^{i+k} \det c\, a_{ik}$; ovaj se produkt zove *algebarski komplement* ili *kofaktor* komplementa a_{ik}.

Time smo dokazali ovaj rezultat.

7.5. Lema. Izraz $\det a$ obuhvata izraz $a_{ik} f a_{ik}$ za zvaku komponentu a_{ik}.

7.6. Promatrajmo sad dvije komponente iz istog stupca, npr. komponente a_{11} i a_{21}; izraz $\det a$ obuhvata i $a_{11} f a_{11}$ i $a_{21} f a_{21}$; no, u ovim izrazima nema jednakih članova; uopće, *svaki* od n polinoma

$$a_{11} f a_{11}$$

$$a_{21} f a_{21}$$

$$\cdots\cdots$$

$$\cdots\cdots$$

$$a_{n1} f a_{n1}$$

ima po $(n-1)!$ članova determinante; zajedno, dakle, daju oni $n \cdot (n-1)!$ članova determinante, tj. sve članove determinante; drugim riječima:

$$\det a = a_{11} f a_{11} + a_{21} f a_{21} + a_{31} f a_{31} + \cdots$$

To je *Laplaceov razvoj determinante po prvom stupcu.*

Iz tog se razvoja vidi ne samo da je determinanta *linearna forma svojeg prvog stupca* nego i kako je *ta linearna funkcija građena* (isp. pogl. 11, § 3.3). Analogan razvoj vrijedi po *bilo kojem stupcu*, jer svaki stupac možemo dopremiti da bude početni.

Prelazom od matrice a na transponiranu matricu a^T i služeći se pravilom da je $\det a = \det a^T$ (teorem 5.1), vrijedi pravilo da se determinanta može razviti i po svakom svojem retku.

Dokazali smo ovaj osnovni teorem o determinantama:

—→ **7.7 (Laplaceov teorem).** *Skalarni produkt svakog stupca* (retka) *determinante s pripadnim algebarskim komplementima daje vrijednost te determinante:*

$$\sum_i a_{ij} \, f \, a_{ij} = \det a \quad (\textit{razvoj determinante po stupcu } j)$$

$$\sum_j a_{ij} \, f \, a_{ij} = \det a \quad (\textit{razvoj determinante po retku } i).$$

7.8. Što se dobije množeći skalarno stupac komplementima nekog drugog stupca?

Promatrajmo razvoj determinante matrice a npr. po prvom stupcu:

$$a_{11} \, f \, a_{11} + a_{21} \, f \, a_{21} + \cdots = \det [a_{.1}, \; a_{.2}, \ldots].$$

To vrijedi za determinantu; ako u toj jednakosti umjesto koeficijenata a_{11}, a_{21}, odnosno stupca $a_{.1}$ stavimo izraze a_{12}, $a_{22}, \ldots$, odnosno stupac $a_{.2}$ matrice a, onda dobijemo ovo:

$$a_{12} \, f \, a_{11} + a_{22} \, f \, a_{12} + \cdots = \det [a_{.2} \; a_{.2}, \; a_{.3}, \ldots].$$

No ta je determinanta $= 0$ jer su joj prva dva stupca jednaka (v. korolar 2.2).

Na isti se način zaključuje da je skalarni produkt bilo kojeg stupca (retka) determinante s algebarskim komplementima kojeg drugog stupca (retka) determinante jednak 0. Ako tu činjenicu spojimo s gornjim teoremom 7.7, dolazimo do ovog osnovnog Laplaceova teorema o determinantama.

P. S. Laplace [Laplás] (1749—1827) veliki francuski matematičar

—→ **7.9. Teorem (Laplaceov teorem o razvijanju determinante).** [1] ***Neka je a kvadratna matrica oblasti*** (n, n) ***gdje je n prirodni broj*** > 1. ***Skalarni produkt svakog stupca matrice i algebarskih komplemenata toga (odnosno bilo kojega drugog) stupca te matrice daje za rezultat*** $\det a$ ***(odnosno 0); simbolički: za svako*** i, $k \in [1, n]$ ***vrijedi***

$$(L) \qquad a_{.i} \circ f \, a_{.k} = \delta_{ik} \cdot \det a \quad \textbf{tj.} \quad \sum_{\nu=1}^{n} a_{\nu i} \, f \, a_{\nu k} = \delta_{ik} \cdot \det a;$$

[1] P. S. Laplace [Laplás] (1749—1827), veliki francuski matematičar i Napoleonov suradnik.

odnosno za retke:

$$(\mathrm{L}^T) \qquad a_{i.} \circ f\, a_{k.} = \delta_{ik} \det a \quad \text{tj.} \quad \sum_{\nu=1}^{n} a_{i\nu}\, f\, a_{k\nu} = \delta_{ik} \cdot \det a;$$

pri tom je

$$\delta_{ik} = \begin{cases} 0 & i \neq k \\ 1 & i = k. \end{cases} \quad \text{za}$$

Taj Laplaceov teorem spada među najvažnije matematičke činjenice.

Za vježbu je vrlo korisno formule (L), (L^T) *konkretizirati*, npr. napisati ih za $n=5$, $i=3$, $k=3,\ 4,\ 5$.

7.9.1. Primjedba. Vrlo je zgodno taj Laplaceov teorem uzeti za *definiciju* determinante, pri čemu se, *po definiciji*, uzima da je $\det[b]=b$ za svaki brojevni izraz b.

Tako npr. razvijajući po prvom stupcu, imamo:

$$\begin{vmatrix} u & v \\ x & y \end{vmatrix} = u f u + x f x = u \cdot \det y + x \cdot -[v] = u y - x v.$$

Analogno:

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = a_1 f a_1 + a_2 f a_2 + a_3 f a_3 = a_1 \begin{vmatrix} b_2 & c_3 \\ b_3 & c_3 \end{vmatrix} +$$

$$+ a_2 \cdot (-1)^{2+1} \begin{vmatrix} b_1 & c_1 \\ b_3 & c_3 \end{vmatrix} + a_3 (-1)^{3+1} \begin{vmatrix} b_1 & c_1 \\ c_2 & c_2 \end{vmatrix} = \cdots.$$

7.9.2. *Dokaz Cramerova teorema kao jedna primjena Laplaceova teorema* (isp. pogl. 9, § 1.9).

Neka za n veličina $x_1.\ x_2, \ldots,\ x_n$ vrijedi ovih n jednadžbi

$$(1) \qquad \begin{array}{l|l} a_{11} x_1 + a_{12} x_2 + \cdots + a_{1n} x_n = c_1 & \cdot f\, a_{11} + \\ a_{21} x_1 + a_{22} x_2 + \cdots + a_{2n} x_n = c_2 & \cdot f\, a_{21} + \\ \cdots\cdots\cdots\cdots\cdots\cdots & \cdots\cdots \\ \sum_{\nu=1}^{n} a_{n\nu} x_\nu = c_n & \cdot f\, a_{n1} \end{array}$$

$$(2) \quad (a_{11} f a_{11} + a_{21} f a_{21} + \cdots) x_1 + (a_{12} f a_{11} + a_{22} f a_{21} + \cdots + a_{n2} f a_{n1}) x_2 + \cdots =$$

$$= c_1 f a_{11} + c_2 f a_{21} + \cdots + c_n f a_{n1}.$$

Prema Laplaceovu pravilu tu je koeficijent od x_1 upravo $\det a$; koeficijenti od $x_2,\ x_3 \cdots$ su 0; na desnoj strani u (2) je determinanta $a(1)$ kojoj matrica nastaje tako da se stupac $a_{.1}$ zamijeni sa

$$\vec{c} = \begin{bmatrix} c_1 \\ \cdot \\ \cdot \\ \cdot \\ c_n \end{bmatrix}.$$

Dakle je $\det a \cdot x_1 = a(1) = \det [\vec{c},\ a_{.2},\ a_{.3}, \ldots]$.

Analogno je $\det a \cdot x_2 = a(2) = \det [a_{.1},\ c,\ a_{.3}, \ldots]$

$$\det a \cdot x_3 = a(3) = \det [a_{.1},\ a_{.2},\ \vec{c},\ a_{.4}, \ldots], \text{ itd.}$$

A to je upravo Cramerovo pravilo (v. pogl. 9, teorem 1.8. i 1.9.3).

8. POOPĆENJE LAPLACEOVOG TEOREMA

8.1. Pođimo od kvadratne matrice oblika

$a = \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}$; tu su x, y zadane *matrice*, pa sa $\begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}$

označujemo matricu kojoj je x submatrica u gornjem lijevom uglu, y je submatrica u donjem desnom uglu, a *sve su ostale komponente* $=0$. Nađimo determinantu od a. Naravno,

$$\det a = \sum_p (-1)^{ip}\, a_{p_1 1}\, a_{p_1 2} \cdots$$

Pri tom je p proizvoljna permutacija množine $[1\ n]_N$, gdje je $n \times n$ oblast matrice a. Neka je $\operatorname{Dom} x = (\alpha,\ \alpha)$, $\operatorname{Dom} y = (\beta,\ \beta)$, dakle $n = \alpha + \beta$. Tada je $a_{1k} = 0$ za $k > \alpha$; zato se u permutaciji p može uzeti da je $p_1 \in 1\,(\alpha)$; iz istog razloga može se uzeti da je $p_b \in 1\,(\alpha)$ za $l \leq \alpha$ te

$$\alpha < p_1 \leq n \quad \text{za} \quad l \in (\alpha,\ n].$$

No svaka takva permutacija p izlazi tako da se na proizvoljnu permutaciju q množine $[1,\ \alpha]$ pripiše proizvoljna permutacija i množine $(\alpha,\ n]$; k tome za broj inverzija ip, iq, it u permutacijama p, q, t vrijedi

$$ip = iq + it,$$

jer je svaki član od q manji od svakog člana u t; dakle je

$$\sum_{p\,\varepsilon\,1\,(n)!} (--1)^{ip}\, a_{p_1 1}\, a_{p_2 2} \cdots =$$

$$\sum_{\substack{q\,\varepsilon\,(1,\,\alpha]! \\ t\,\varepsilon\,(\alpha,\,n]!}} (-1)^{iq}\, x_{q_1 1}\, x_{q_2 2} \cdots x_{q_\alpha \alpha}\, (-1)^{it}\, y_{t_{\alpha+1}\alpha+1}\, y_{t_{\alpha+2}\,\alpha+2} \cdots y_{t_n n}$$

$$= \sum_{q\,\varepsilon\,1\,(\alpha)!} (--1^{iq}\, x_{q_1 1} \cdots x_{q_\alpha \alpha} \sum_{t\,\varepsilon\,(\alpha,\,n)!} (-1)^{it}\, y_{t_{\alpha+1}\alpha+1} \cdots y_{t_n n} = \det x\ \det y.$$

8.2. Lema. Dakle vrijedi

$$\det \begin{vmatrix} x & 0 \\ 0 & y \end{vmatrix} = \det x \ \det y.$$

8.3. Uzmimo sada slučaj da je matrica a takva da su zadane matrice x, y njene komplementarne matrice i da su sve druge komponente jednake 0.

Taj se slučaj svodi na prethodni, s tim da postupnim transpozicijama redaka i stupaca unutar matrice a dolazimo do matrice $g\,a$ oblika

$$\begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}$$

No, $\det g\,a = \pm \det a$; vidi se ovo: ako reci matrice x dolaze u recima $m_1, m_2 \cdots$ matrice a dok stupci matrice x dolaze u stupcima $u_1, u_2 \cdots$ matrice a, tada je

$$\det g\,a = (-1)^{m_1+m_2+\cdots+u_1+u_2+\cdots} \det a$$

Drugim riječima:

$$\det a = \det x \cdot (-1)^{m_1+m_2+\cdots+u_1+u_2+\ldots} \det y.$$

Ovaj faktor od $\det x$ zove se *kofaktor od* x u a pa se može označiti sa $f\,x$ ili $f_a\,x$.

8.4. Definicija kofaktora. Za zadanu matricu a i njenu podmatricu x *kofaktor od* x je produkt od

$$(-1)^{m_1+m_2+\cdots+u_1+u_2+\cdots}$$

i determinante matrice što se iz a dobije brišući u njoj one retke $m_1, m_2, \cdots$ i stupce $u_1, u_2, \ldots$ koji sadrže bar jednu komponentu od x; kofaktor od x označujemo sa $f\,x$ (ili preciznije $f_a\,x$).

Vrijedi ovaj iskaz:

8.5. Lema. Ako su x i y komplementarne podmatrice u matrici a[1], pa ako su vrijednosti od a koje su izvan x i y sve $=0$, tada je $\det a = \det x \det y$.

Specijalno ako je x bilo koja submatrica od a, tada je $\det x\,f\,x$ determinanta matrice koja se iz a dobije tako da se sve one komponente od a koje su u recima od x i stupcima od komplementa od a zamijene sa 0.

—→ **8.6. Opći Laplaceov teorem.** *U kvadratnoj* (n, n)*-matrici* a *promatrajmo njenih* r *redaka; dakle* $r \in [1, n)$, *tj.* r *može biti* $1, 2, \ldots, n-1$; *determinanta matrice* a *»razvija« se po tim recima tako da se najpre formiraju sve* (r, r)*-subdeterminante od tih* r *redaka, svaka od njih pomnoži svojim kofaktorom u odnosu na* a *i dobiveni produkti zbroje.*

Analogno, teorem vrijedi za razvoj po određenom broju stupaca determinante a.

Dokaz se nalazi niže u § 8.6.2.

---

[1] To znači da je $D_1\,x = D_1\,a \setminus D_1\,y$, $D_2\,x = D_2\,a \setminus D_2\,y$.

8.6.1. Primjer. Razvijmo determinantu matrice

$$a=\begin{bmatrix} 3 & 4 & 3 & 2 \\ 1 & 4 & 5 & 3 \\ 2 & 3 & 5 & 1 \\ 2 & -3 & 4 & -5 \end{bmatrix}$$

po prvom i trećem stupcu. Matrica tih uočenih stupaca glasi:

$$[a_{.1}\ a_{.3}]=\begin{bmatrix} 3 & 3 \\ 1 & 5 \\ 2 & 5 \\ 2 & 4 \end{bmatrix};$$

pripadne subdeterminante glase po redu:

$$\begin{vmatrix} 3 & 3 \\ 1 & 5 \end{vmatrix}, \begin{vmatrix} 3 & 3 \\ 2 & 5 \end{vmatrix}, \begin{vmatrix} 3 & 3 \\ 2 & 4 \end{vmatrix}, \begin{vmatrix} 1 & 5 \\ 2 & 5 \end{vmatrix}, \begin{vmatrix} 1 & 5 \\ 2 & 4 \end{vmatrix}, \begin{vmatrix} 2 & 5 \\ 2 & 4 \end{vmatrix}.$$

Pripadni kofaktori u odnosu na a glase po redu:

$$(-1)^{1+2+1+3}\begin{vmatrix} 3 & 1 \\ -3 & -5 \end{vmatrix}, \begin{vmatrix} 4 & 3 \\ -3 & -5 \end{vmatrix}, -\begin{vmatrix} 4 & 3 \\ 3 & 1 \end{vmatrix}, -\begin{vmatrix} 4 & 2 \\ -3 & -5 \end{vmatrix}, \begin{vmatrix} 4 & 2 \\ 3 & 1 \end{vmatrix}, -\begin{vmatrix} 4 & 2 \\ 4 & 3 \end{vmatrix}.$$

Skalarni produkt tih dvaju nizova proizvodi broj $\det a$:

$$\det a = 12 \cdot 12 + 9 \cdot -11 + 6 \cdot 5 + -5 \cdot 14 + -6 \cdot -2 + -2 \cdot 4- =$$

$$= 144-99+30-70+12+8 = 194-169 = 25.$$

8.6.2. Dokaz teorema 8.6. Neka je x bilo koja subdeterminanta poretka (r, r) iz matrice promatranih r redaka; neka je fx njen kofaktor u odnosu na matricu a; tada produkt xfx daje svakako jedan dio izraza za $\det a$; u xfx dolazi $r!\,(n-r)!$ članova za $\det a$; no x se može izabrati na $\binom{n}{r}$ načina: treba, naime, uočiti bilo kojih r stupaca u matrici od r izabranih redaka; prema tome, suma $\sum_x xfx$ daje svega

$$\binom{n}{r}\cdot r!\,(n-r)! \tag{1}$$

članova od $\det a$; no (1) je dalje $= \dfrac{n(n-1)\cdot\cdot\cdot(n-r+1)}{r!}\cdot r!\,(n-r)! = n!$

Dakle se na gornji način dobije svih $n!$ članova determinante.

8.7. Jedan nuždan uslov za relaciju $\det a \neq 0$. Očigledno je da iz $\det a \neq 0$ proizlazi da svaki redak i svaki stupac ima bar jednu vrijednost $\neq 0$; međutim,

iz općeg Laplaceova teorema proizlazi da *svakih s* stupaca (redaka) mora sadržavati jednu *regularnu podmatricu* poretka (s, s), jer je $\det a$ linearan spoj determinanata svih tih podmatrica. Pri tom je s proizvoljan prirodan broj $<n$.

—→ **8.8. Teorem o razvijanju determinante po retku i stupcu u isto vreme:**

$$\det a = a_{11} f a_{11} - \sum_{i,k=2}^{u} a_{i1}\, a_{1k} (-1)^{i+k} \det (a \setminus a_{i1} \setminus a_{1k}). \tag{1}$$

(razvoj po 1. retku i 1. stupcu).

D o k a z. Razvijmo $\det a$ po 1. retku:

$$\det a = a_{11} f a_{11} + \sum_{k=2}^{n} a_{1k} (-1)^{1+k} \det (a \setminus a_{1k}).$$

Dalje je

$$\det (a \setminus a_{1k}) = (\text{razvoj po 1. stupcu}) = \sum_{i=2}^{n} a_{i1} (-1)^{i-1+1} \det (a \setminus a_{ik} \setminus a_{i1}).$$

Unese li se to u gornji razvoj za $\det a$, izlazi upravo napisani obrazac (1).

8.9. Zadaci o razvoju determinanata.

1. Promatraj jediničnu matricu

$$e = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix};$$

1) nađi $\det [e_{.3}\, e_{.1}\, e_{.2}]$; 2) neka je $p = p_1, p_2, p_3$ bilo koja permutacija brojeva 1, 2, 3; odredi matricu $[e_{.p_1}, e_{.p_2}, e_{.p_3}]$ i pripadnu determinantu.

2. Isto pitanje za jedinične matrice oblasti (4, 4), (5, 5), ...

3. Promatraj matrice

$$a = \begin{bmatrix} 3 & 4 & 5 & 7 \\ -2 & 5 & -3 & 4 \\ 6 & 3 & 2 & 1 \\ 0 & 1 & 3 & 4 \end{bmatrix}, \qquad b = [a_{.4}\, a_{.3}\, a_{.2}\, a_{.1}], \qquad c = [a_{.3}\, a_{.1}\, a_{.2}\, a_{.4}];$$

1) odredi $\det a$ i pomoću toga odredi $\det b$; $\det c$. 2) Odredi $\det a$ dodavanjem kratnika stupca $a_{.2}$ preostalim stupcima tako da dobijemo matricu kojoj je (4, 2) — vrijednost jedini top u 4. retku. 3) Odredi $\det a$ tako da u 4. stupcu dođu vrijednosti 0 osim u polju (3, 4); 4) isto samo da „stožerno polje" bude (3, 3). 5) Ako je matrica x poretka (n, n), dokaži da za svaku permutaciju $p = p_1, p_2, \ldots, p_n$ množine $\{1, 2, \ldots, n\}$ vrijedi

$$\det [a_{.p_1}, a_{.p_2}, \ldots, a_{.p_n}] = (-1)^{ip} \det [a_{.1}, a_{.2} \cdot \cdot \cdot a_{.n}].$$

4. Za gornju matricu a nađi 1) a^T, $\det a^T$; 2) $a + a^T$ i $\det (a + a)^T$; 3) $a\, a^T$, $\det (a\, a^T)$; 4) $a^T a$, $\det a^T a$.

5. Gornju determinantu od a razvij po Laplasovu pravilu po 1) 1. stupcu, 2) 3. stupcu, 3) 4. retku, 4) po prva dva stupca, 5) po krajnjim stupcima.

6. Za istu matricu a nađi 1) a^2-1 i $\det(a^2-1)$ razvijajući po 3. stupcu, 2) $(a+3)(2a+5)$, $\det(a+3)(2a+5)$ razvijajući po 2. rediću.

7. Obrazuj matricu a^Γ, za koju je $a^\Gamma_{ik}=f a_{ki}$ ($f a_{ki}$ je algebarski komplement od a_{ki} u odnosu na matricu a). Nađi $\det a^\Gamma$.

8. Promatraj matricu b oblasti (4, 4) za koju je 1) $b_{.i}=a_{.1}+a_{.2}+\cdots+a_{.i}=\sum_{k=1}^{i} a_{.k}$; 2) $b_{.i}=a_{.1}\cdot a_{.2}\cdots a_{.i}=\prod_{k=1}^{i} a_{.k}$ $(i=1,\ 2,\ 3,\ 4)$;

9. Promatraj kvadratnu matricu c za koju je $c_{.1}=3a_{.1}+2a_{.3}$, $c_{.2}=-a_{.1}+5a_{.3}$, $c_{.3}=5a_{.1}+a_{.3}$, $c_{.4}=-a_{.1}+7a_{.3}$; nađi $\det c$.

10. Dokaži: 1)
$$\begin{vmatrix} a_0, & -1 & & & \\ a_1 & x, & -1 & & \\ a_2 & & x, & & \\ \cdot & & \cdot & & \\ \cdot & & & \cdot & \\ \cdot & & & & \\ a_{n-1} & & & x, & -1 \\ a_n & & & & x \end{vmatrix} = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n.$$

Posebno promotri slučajeve $n=2,\ 3$.

Opiši kako je građena matrica na lijevoj strani.

2)
$$\begin{vmatrix} 1 & x_1 & x_1\cdots x_1 \\ 1 & x & x_2\cdots x_2 \\ 1 & x_3 & x\cdots\cdot \\ \cdot & \cdot & x_4\cdots x_4 \\ \cdot & \cdot & \cdot\cdots\cdot \\ 1 & x_n & x_n\cdots x \end{vmatrix} = (x-x_1)(x-x_2)\cdots(x-x_{n-1});$$

3)
$$\begin{vmatrix} 1 & 2 & 3 & \cdots n \\ -1 & 0 & 3 & \cdots n \\ -1 & -2 & 0 & \cdots\cdot \\ \cdots & \cdots & \cdots & \cdots \\ -1 & -2 & -3 & n \\ -1 & -2 & -3 & 0 \end{vmatrix} = n!$$

4)
$$\begin{vmatrix} 1 & 2 & 3\cdots n-1 & n \\ 1 & 3 & & \\ & & 5 & \\ & & & 7 \\ \cdot & \cdot & \cdot\cdots & \cdot \\ 1 & & & 2n-1 \end{vmatrix} = (n-1)!;$$

(izvan dijagonale svaki stupac je konstanta);

5) $\begin{vmatrix} 1 & 2 & 2 & 2 \cdots 2 \\ 2 & 2 & & \\ & & 3 & \\ & & & 4 \\ & 2 & & n \end{vmatrix} = -2(n-2)!$; (komplement dijagonale je konstanta 2; poopći tako da ta konstanta bude k);

6) $\begin{vmatrix} x & a & \cdot\cdot a \\ a & x & \\ & \cdot & \\ & & \cdot \\ & & \cdot \\ a & & x \end{vmatrix} = [x+(n-1)a](x-a)^{n-1}$ (izvan dijagonale vrijednosti su a);

7) $\begin{vmatrix} x & \cdots\cdots\cdots \\ \cdot & x \cdots a \cdots \\ -a & \cdots\cdots\cdots \\ & \cdots\cdots\cdots x \end{vmatrix} = \frac{1}{2}[(x-a)^n + (x+a)^n]$;

8) $\begin{vmatrix} -a_1 & a_1 & & 0 \\ & -a_2 & a_2 & \\ & & \cdots\cdots & \\ & & \cdots\cdots & \\ & & 0 \cdots & -a_n, \ a_n \\ 1 & & 1 \cdots & 1 \quad 1 \end{vmatrix} = (-1)^n (n+1) a_1 a_2 \cdots a_n$;

9) $\begin{vmatrix} a_1, & -a_2 & & & & \\ & a_2, & -a_3 & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & & a_{n-1}, & -a_n \\ 1 & \cdot & \cdot & \cdot & 1 \quad 1 & 1+a_n \end{vmatrix} = a_1 \cdots a_n (1 + a_1^{-1} + a_2^{-1} \cdots + a_n^{-1})$;

10) $\begin{vmatrix} h & -1 & 0 & 0 & \cdots 0 \\ hx & h & -1 & 0 & \cdots 0 \\ hx^2 & hx & h & -1 & \cdots 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ hx & hx^{n-1} & hx^{n-2} & hx^{n-3} \cdots & h \end{vmatrix} = h(x+h)^n$;

11) $\begin{vmatrix} 0 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & x & \cdots & x & x \\ 1 & x & 0 & \cdots & x & x \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & x & x & \cdots & 0 & x \\ 1 & x & x & \cdots & x & 0 \end{vmatrix} = (-1)^{n-1}(n-1)x^{n-2}$;

12) $\begin{vmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & 0 & a_1+a_2 & \cdots & a_1+a_n \\ 1 & a_2+a_1 & 0 & \cdot & a_2+a_n \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & a_n+a_1 & a_n+a_2 & \cdots & 0 \end{vmatrix} = (-1)^n 2^{n-1} a_1 \cdots a_n (a_1^{-1} + a_2^{-1} + \cdots + a_n^{-1})$;

13) $$\begin{vmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & 1 & 1 & \cdots & 1 & 1-n \\ 1 & 1 & 1 & \cdots & 1-n & 1 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 1 & 1-n & 1 & \cdots & 1 & 1 \end{vmatrix} =$$

$$= (-1)^{\frac{n(n-1)}{2}} \frac{1}{2} \cdot n^{n-1}(n+1);$$

14) $$\begin{vmatrix} 2 & 1-\frac{1}{n} & 1-\frac{1}{n} & \cdots & 1-\frac{1}{n} \\ 1-\frac{1}{n} & 2 & 1-\frac{1}{n} & \cdots & 1-\frac{1}{n} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 1-\frac{1}{n} & 1-\frac{1}{n} & 1-\frac{1}{n} & \cdots & 2 \end{vmatrix} = (n+1)^{n+1} \cdot n^{-n};$$

15) $$\begin{vmatrix} 1 & a & a^2 & a^3 & \cdots & a^n \\ x_{11} & 1 & a & a^2 & \cdots & a^{n-1} \\ x_{21} & x_{22} & 1 & a & \cdots & a^{n-2} \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot \\ x_{n1} & x_{n2} & x_{n3} & x_{n4} & \cdots & 1 \end{vmatrix} =$$

$$= \prod_{k=1}^{n} (1 - a\, x_{k,\,k});$$

16) $$\begin{vmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 2 & 3 & \cdots & n-1 \\ 3 & 2 & 1 & 2 & \cdots & n-2 \\ 4 & 3 & 2 & 1 & \cdots & n-3 \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot \\ n & n-1 & n-2 & n-3 & \cdots & 1 \end{vmatrix} =$$

$$= (-1)^{n-1} 2^{n-2} (n+1);$$

17) $$\begin{vmatrix} a_0 & b_1 & 0 & 0 & \cdots & 0 & 0 \\ a_1 & -b_0 & b_2 & 0 & \cdots & 0 & 0 \\ b_2 & 0 & -b_1 & b_3 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ a_{n-1} & 0 & 0 & 0 & \cdots & -b_{n-2} & b_n \\ a_n & 0 & 0 & 0 & \cdots & 0 & -b_{n-1} \end{vmatrix} =$$

$$= (-1)^n \, (a_0 b_0 + a_1 b_1 + \cdots + a_n b_n)\, b_1 b_2 \cdots b_{n-1};$$

18)
$$\begin{vmatrix} x & y & 0 & \cdots & 0 & 0 \\ 0 & x & y & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & x & y \\ y & 0 & 0 & \cdots & 0 & x \end{vmatrix} = x^n + (-1)^{n-1} y^n;$$

19)
$$\begin{vmatrix} 1+x_1y_1 & 1+x_1y_2 & \cdots & 1+x_1y_n \\ 1+x_2y_1 & 1+x_2y_2 & \cdots & 1+x_2y_n \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ 1+x_ny_1 & 1+x_ny_2 & \cdots & 1+x_ny_n \end{vmatrix} = 0 \text{ za } n > 2;$$

20)
$$\begin{vmatrix} a_1-b_1 & a_1-b_2 & \cdots & a_1-b_n \\ a_2-b_1 & a_2-b_2 & \cdots & a_2-b_n \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ a_n-b_1 & a_n-b_2 & \cdots & a_n-b_n \end{vmatrix} = 0 \text{ za } n > 2;$$

21)
$$\begin{vmatrix} 1 & 2 & 3 & 4 & \cdots & n-1 & n \\ -1 & x & 0 & 0 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \cdots & x & 0 \\ 0 & 0 & 0 & 0 & \cdots & -1 & x \end{vmatrix} = \frac{n+1}{1-x} + \frac{x^{n+1}-1}{(1-x)^2};$$

22)
$$\begin{vmatrix} 1 & 0 & 0 & \cdots & 0 & 1 \\ 1 & C_1^1 & 0 & \cdots & 0 & x \\ 1 & C_2^1 & C_2^2 & \cdots & 0 & x^2 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 1 & C_n^1 & C_n^2 & \cdots & C_n^{n-1} & x^n \end{vmatrix} = (x-1)^n, \; C_n^r = \binom{n}{r};$$

23)
$$\begin{vmatrix} a & a & a & \cdots & a & 0 \\ a & a & a & \cdots & 0 & b \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ a & 0 & b & \cdots & b & b \\ 0 & b & b & \cdots & b & b \end{vmatrix} = (-1)^{\frac{n(n+1)}{2}} \frac{ab}{a-b} (b^{n-1} - a^{n-1});$$

24)
$$\begin{vmatrix} a_1 & x & x & \cdots & x \\ y & a_2 & x & \cdots & x \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ y & y & y & \cdots & a_n \end{vmatrix} = \frac{xf(y) - yf(x)}{x-y} \text{ gdje je } f(x) = \prod_{k=1}^{n} (a_k - x);$$

25)
$$\begin{vmatrix} x & a_1 & a_2 & \cdots & a_n \\ a_1 & x & a_2 & \cdots & a_n \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ a_1 & a_2 & a_3 & \cdots & x \end{vmatrix} = (x + \sum_{k=1}^{n} a_k) \prod_{k=1}^{n} (x - a_k).$$

26) $$\begin{vmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} & a_n \\ -y_1 & x_1 & & & & \\ & & x_2 & & & \\ & -y_2 & & \ddots & & \\ & & & & x_{n-1} & \\ & & & & -y_{n-1} & \\ & & & & & x_n \\ & & & & & -y_n \end{vmatrix} =$$

$$= a_0 x_1 x_2 \cdots x_n + a_1 y_1 x_2 x_3 \cdots x_n + a_2 y_1 y_2 x_3 \cdots x_n + \cdots + a_n y_1 y_2 \cdots y_n;$$

27) $$\begin{vmatrix} a^n & -a^{n-1} b & a^{n-2} b^2 & \cdots & (-1)^{n-1} ab^{n-1} & (-1)^n b^n \\ n & 1 & & & & \\ & & 2 & & & \\ & n-1 & & \ddots & & \\ & & & & 2 & n-1 \\ & & & & 1 & n \end{vmatrix} = n!(a+b)^n$$

11. Neka je $x_1, x_2, \ldots x_n$ proizvoljan n-član niz brojeva, a $f_1, f_2 \ldots, f_n$ n-član niz cijelih racionalnih polinoma za koje je st $f_\nu < \nu - 1$ ($\nu = 1, 2, \ldots, n$); ispiši matricu a poretka (n, n) za koju je $a_{ik} = f_i(x_k)$; dokaži da je $\det a = 0$.

12. *Kontinuante.* Kontinuanta je determinanta kojoj je linija iznad glavne dijagonale $a_1, a_2, \ldots, a_n$ konstanta 1, a linija ispod glavne dijagonale je konstanta -1; sve ostalo je konstanta 0; označuje se sa K_n i $(a_1, a_2, \ldots, a_n)$; dakle $K_n = (a_1 a_2 \cdots a_n) =$

$$\begin{vmatrix} a_1 & 1 & 0 & 0 & 0 & \cdots & 0 \\ -1 & a_2 & 1 & 0 & & & \vdots \\ 0 & -1 & a_3 & 1 & & & \vdots \\ 0 & 0 & -1 & a_4 & & & \vdots \\ \vdots & 0 & 0 & -1 & \ddots & & \vdots \\ \vdots & & & & & & \vdots \\ \vdots & & & & & & 1 \\ 0 & \cdots & \cdots & \cdots & \cdots & -1 & a_n \end{vmatrix}.$$

Specijalno stavljamo $K_1 = (a_1) = a_1$; nadalje je $K_2 = (a_1, a_2) = a_1 a_2 + 1$. Neka k_n označuje koliko K_n ima članova. Dokaži:

1) $K_n = a_n K_{n-1} + K_{n-2}$; 2) $k_n = k_{n-1} + k_{n-2}$ tj. niz k_n je Fibonačijev niz;

3) $\dfrac{(a_1,\ a_2,\ldots\ a_n)}{(a_2,\ a_3,\ldots\ a_n)} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots\ + \cfrac{1}{a_n}}}$; 4) $k_{n-1}{}^2 + k_n{}^2 = k_{2n}$

(Razvij K_n po prvih r redaka; izlazi $(a_1 \cdot \cdots a_n) = (a_1 \cdot \cdots a_r)\,(a_{r+1} \cdot \cdots a_n) + (a_1 \cdot \cdots a_{r-1}) \cdot (a_{r+2} \cdot \cdots a_n)$; 5) $k_n = \binom{n}{0} + \binom{n-1}{1} + \binom{n-1}{2} + \cdots$; pri tom dogovorno vrijedi da je $\binom{n}{k} = 0$ za cijele brojeve n, k za koje je $k > n$ te za $k < 0$.

13. Zadanu determinantu razviti istovremeno po zadanom retku i zadanom stupcu te determinante (v. 11, § 8.8).

9. MNOŽENJE DETERMINANATA. DETERMINANTA KVADRATNE MATRICE KOJA JE PRODUKT MATRICA. BINET-CAUCHYJEV TEOREM

9.0. Problem je ovaj: *zadana je kvadratna matrica*

$$c = a\,b$$

kao produkt matrica a i b; treba naći det c.

9.1. Ako je $\mathrm{Dom}\, a = \mathrm{Dom}\, b = n \times n$ i k tome $n = 1$ ili 2, tada se odmah vidi da je $\det(a\,b) = \det a\ \det b$ (isp. § 3.3.1). Sad ćemo dokazati da analogan zaključak vrijedi i za $n = 3,\ 4,\ 5, \ldots$

—→ **9.2.** Teorem. *Za kvadratne matrice a, b konačne oblasti vrijedi*

$$\det(a\,b) = \det a\ \det b,$$

tj. *operator det je distributivan prema množenju kvadratnih matrica.*

Dokaz. Neka je $c = a\,b$. Prema pravilu o množenju matrica, komponenta c_{lk} je skalarni produkt od retka l od a i stupca k od b, tj.

$$c_{lk} = a_{l.} \circ b_{.k} = \sum_j a_{lj}\, b_{jk}.$$

Na taj način vidimo da je stupac $c_{.k}$ matrice c suma od n nizova. Služeći se aditivnim svojstvom determinanata, vidi se da je $\det c$ suma determinanata kojima je k-stupac jedan od n nizova (vektorâ) kojih je suma jednaka k-stupcu matrice c, i to za svako $k \in N\,[1, n]$. Ako iz sume za vektor $c_{.k} = ab_{.k}$ $(k = 1, 2, \ldots)$ odaberemo njegov određen sumand, npr. p_k-ti sumand (za $k = 1, 2, 3, \ldots, n$), dobivamo time: određen niz p brojeva $p_1, p_2, \ldots, p_n$ i niz vektora $a_{.p_k}\ b_{p_k k}$ $(k = 1, 2, \ldots)$ koji čine određenu matricu $[a_{.p_1}\ b_{p_1 1}, a_{.p_2} b_{p_2 2}, \ldots]$; označimo sa $d(p)$ determinantu te matrice:

$$d(p) = \det[a_{.p_1}\, b_{p_1 1}, a_{.p_2}\, b_{p_2 2}, \ldots]. \tag{1}$$

Prema aditivnom svojstvu determinanata, suma svih tih $d(p)$ daje $\det c$; na taj način imamo formulu

$$\det c = \sum_p d(p), \tag{2}$$

pri čemu p prolazi svim n-članim nizovima kojima su članovi u skupu $N[1, n]$.

No, izlučujući iz svakog stupca determinante u (1) zajednički faktor, vidimo da jednakost (1) postaje

$$d(p) = \det [a_{.p_1}\, a_{.p_2} \cdot \cdot \cdot] b_{p_1 1}\, b_{p_2 2} \cdot \cdot \cdot \tag{3}$$

Ako u nizu p ima *jednakih* članova npr. $p_2 = p_5$, tada je $d(p) = 0$, jer napisana matrica u (3) ima jednakih stupaca (u našem primjeru stupac 2 i stupac 5). Zato u obrascu (2) možemo *pretpostaviti* da niz p *nema jednakih* članova, tj. da p prolazi skupom $[1, n]!$ *permutacija* množine $[1, n]$; time obrazac (2), na osnovu (3), daje

$$\det c = \sum_{p \in 1(n)!} \det [a_{1 p_1}\, a_{2 p_2} \cdot \cdot \cdot]\ b_{p_1 1}\, b_{p_2 2}, \cdot \cdot \cdot, \tag{4}$$

No, transpozicijom stupaca može se napisana determinanta u $(4)_2$ prevesti u oblik $\pm \det a$, s tim da će znak $+$ vrijediti ako je p parna permutacija, a znak $-$ ako je p neparna permutacija. Drugim riječima, napisana determinanta u $(4)_2$ je $= (-1)^{ip} \det a$, gdje je $i\,p$ broj inverzije permutacije p; zato jednakost (4) postaje

$$\det c = \sum_{p \in [1,n]!} (-1)^{ip}\ \det a \cdot b_{p_1 1}\, b_{p_2 2} \cdot \cdot \cdot,$$

tj.

$$\det c = \det a \cdot \sum_{p \in [1,n]!} (-1)^{ip}\, b_{p_1 1}\, b_{p_2 2} \cdot \cdot \cdot = \det a \cdot \det b \qquad \text{Q. E. D.} \tag{5}$$

9.3. Četiri mogućnosti množenja determinanata. Za kvadratne matrice a, b vrijedi obrazac

$$\det a\ \det b = \det (a\, b) \rightarrow \cdot \downarrow \quad \text{(množenje redaka sa stupcima).} \tag{6}$$

No, znamo da transpozicija $a \rightarrow a^T$, $b \rightarrow b^T$ ne mijenja vrijednost determinante (v. 11 § 5.1); zato iz obrasca (6) proizilaze i ovi obrasci;

$$\det a\ \det b = \det (a^T\, b) \qquad \downarrow \cdot \downarrow \tag{7}$$

$$\det a\ \det b = \det (a\, b^T) \qquad \rightarrow \cdot \rightarrow \tag{8}$$

$$\det a\ \det b = \det (a^T\, b^T), \qquad \downarrow \cdot \rightarrow \tag{9}$$

Obrazac (6) iskazuje se također ovako:

9.3.1. Dvije determinante istog stupnja množe se tako da se *reci prve* determinante *množe* skalarno *stupcima druge* determinante. To je shematski prikazano strelicama nadesno u (6).

Analogno se obrazac (7), odnosno (8), iskazuje da se dvije determinante množe tako da se *stupci* (reci) *prve množe* skalarno *stupcima* (recima) druge determinante. Prema (9), dvije determinante mogu se množiti i tako da se *stupci prve množe* skalarno *recima druge* determinante. Ukratko, dvije determinante istog stupnja mogu se množiti na četiri načina, i to po shemama:

$$\rightarrow\cdot\downarrow,\quad \rightarrow\cdot\rightarrow,\quad \downarrow\cdot\rightarrow,\quad \downarrow\cdot\downarrow.$$

Kao rezultat izlazi uvijek ista determinanta.

To je jedan neobičan rezultat!

9.3.2. P r i m j e d b a. Matrice se množe po shemi

$$\rightarrow\cdot\downarrow;$$

zato je zgodno da tako množimo i determinante.

9.4. Primjedba o jednakosti determinanata i množenju determinanata nejednakog poretka. Treba imati na umu da je determinanta određen *skalar*; zato može biti vrlo *raznovrsnih matrica*, a da im je determinanta *ista*. Tako npr. skalar

$$1=\begin{vmatrix}1&0\\0&1\end{vmatrix}=\begin{vmatrix}1&0&0\\0&1&1\\0&0&1\end{vmatrix},$$

mada su pripadne matrice

$$\begin{bmatrix}1&0\\0&1\end{bmatrix},\quad \begin{bmatrix}1&0&0\\0&1&1\\0&0&1\end{bmatrix}$$

nejednake. Nadopisujući u zadanoj kvadratnoj matrici a novi ugao oblika

$$\begin{matrix}&&&0\\&&&0\\&&&\cdot\\&&&\cdot\\&&&\cdot\\0&\cdots&0&0&1,\end{matrix}$$

pripadna determinanta se ne mijenja:

$$\det a=\det\begin{bmatrix}a&0\\0&1\end{bmatrix},$$

pri tom naravno pišemo

$$\begin{bmatrix}a&0\\0&1\end{bmatrix}=\begin{bmatrix}a_{11}&\cdots&a_{1n}&0\\\cdots&\cdots&\cdots&\cdots\\a_{n1}&\cdots&a_{nn}&0\\0&\cdots&0&1\end{bmatrix},\quad \text{tj.}\quad \begin{bmatrix}a&0\\0&1\end{bmatrix}$$

nastaje iz matrice a tako da glavnu dijagonalu produžimo dolje s 1, a redak i stupac te jedinice nadopunimo potrebnim brojem 0. Na taj način vidimo da svaka determinanta $\det a$ može biti napisana i kao determinanta od nadmatrice za a, kojoj je stupanj proizvoljno velik: dovoljno je glavnu dijagonalu od a produžiti *traženim brojem* jedinica pa na ostala mjesta staviti 0.

Zato se dvije *determinante* mogu množiti po shemi $\rightarrow\downarrow$ i onda kad se *pripadne matrice ne mogu množiti*: dovoljno je jednu od njih produžiti na gornji način pa da nastanu matrice istog poretka.

Tako npr.

$$\begin{vmatrix} 2 & 3 \\ 4 & 5 \end{vmatrix} \cdot \begin{vmatrix} 5 & 1 & -1 \\ 4 & 2 & 2 \\ 3 & 0 & 1 \end{vmatrix} = \begin{vmatrix} 2 & 3 & 0 \\ 4 & 5 & 0 \\ 0 & 0 & 1 \end{vmatrix} \cdot \begin{vmatrix} 5 & 1 & -1 \\ 4 & 2 & 2 \\ 3 & 0 & 1 \end{vmatrix} = (\rightarrow \cdot \downarrow) =$$

$$= \begin{vmatrix} 22 & 8 & 4 \\ 40 & 14 & 6 \\ 3 & 0 & 1 \end{vmatrix}, \quad \text{tj.} \quad \begin{vmatrix} 2 & 3 \\ 4 & 5 \end{vmatrix} \cdot \begin{vmatrix} 5 & 1 & -1 \\ 4 & 2 & 2 \\ 3 & 0 & 1 \end{vmatrix} = \begin{vmatrix} 22 & 8 & 4 \\ 40 & 14 & 6 \\ 3 & 0 & 1 \end{vmatrix}.$$

Uvjerimo se da je ta jednakost ispravna, npr. tako da obje determinante oblasti (3, 3) razvijemo po trećem retku:

$$-2\left(3 \cdot \begin{vmatrix} 1 & -1 \\ 2 & 2 \end{vmatrix} + 1 \cdot \begin{vmatrix} 5 & 1 \\ 4 & 2 \end{vmatrix}\right) = 3 \begin{vmatrix} 8 & 4 \\ 14 & 6 \end{vmatrix} + \begin{vmatrix} 22 & 8 \\ 40 & 14 \end{vmatrix}$$

$$-2(12+6) = 3 \cdot -8 - 12.$$

9.5. O krakovijanima. U *astronomskim preračunavanjima* razvila se *jedna vrsta matričnog računanja*: ono je slično računanju s matricama, s jedinom razlikom u definiciji *množenja*. Dok se produkt $a\,b$ od a i b dobije kod matrica po shemi $\rightarrow\cdot\downarrow$, tj.

$$(a\,b)_{ik} = a_{i.} \circ b_{.k},$$

dotle je kod »*krakovijana*« produkt $a\,K\,b$ definiran po shemi $\downarrow\cdot\downarrow$, tj.

$$(a\,K\,b)_{ik} = a_{.k} \circ b_{.i}.$$

Oprez! *Prvi indeks* u produktu hvata *drugi*, a *ne prvi* faktor! Pri tom krakovskom množenju *ne vrijedi* zakon asocijacije! (v. § 10.8.2).

Naziv »*krakovijan*« dolazi od poljskog grada Krakov, jer su poljski astronomi (specijalno Banachiewicz [Banahjevič]) koji su radili u Krakovu uveli taj način računanja.

9.6. Stupac × redak matrice. To su matrice koje su produkt *stupca* i *retka*:

$$\downarrow\cdot\rightarrow$$

Npr. $$\begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \end{bmatrix} [y_1\, y_2 \cdots] = \begin{bmatrix} x_1 y_1 & x_1 y_2 & x_1 y_3 \cdots \\ x_2 y_1 & x_2 y_2 & x_2 y_3 \cdots \\ \cdot & \cdot & \cdot \cdots \end{bmatrix}.$$

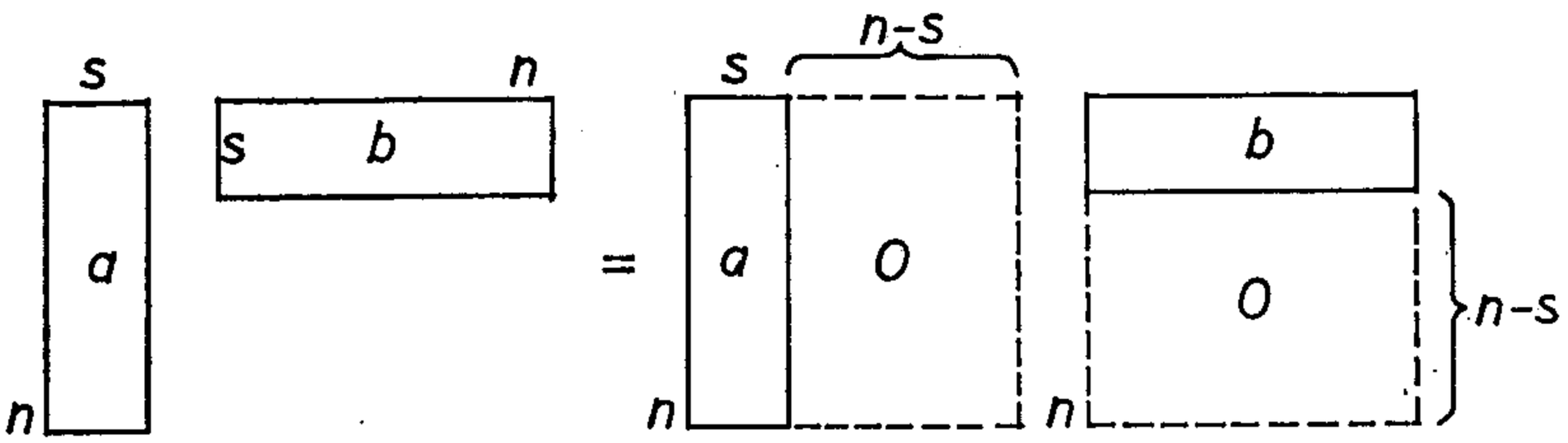
Ako kvadratna matrica stupac × redak ima više od jedne komponente, njena je determinanta $=0$.

Da se to vidi, dovoljno je u pripadnoj determinanti izlučiti faktor x_1 iz prvog, a x_2 iz drugog retka.

9.7. Općenito, odmah ćemo vidjeti da vrijedi ovo:

(1) $$\det\begin{bmatrix} \square & \square \end{bmatrix}=0.$$

Stvarno, vidi se da vrijedi: Ako je $D_1 a > D_2 a$, tada je



No, tu su nadesno *kvadratne* matrice; u prvoj je bar jedan stupac, a u drugoj bar jedan redak sastavljen od 0; zato su pripadne njihove determinante jednake 0; dakle je i produkt tih determinanata jednak 0; a to znači da vrijedi simbolička jednakost (1).

9.8. Treći slučaj kvadratnih matrica *a b*. Ako matrica ab ima da bude poretka (n, n), onda je svakako (poredak od a) por $a=(n, s)$, por $b=(s, n)$, gdje su $D_1 a = D_2 b = n$, $D_2 a = D_1 b = s$ određeni brojevi. Dosad smo razmatrali slučajeve: $n=s$ (§ 9.2) i $n>s$ (§ 9.7).

Ostaje treći slučaj $D_1 a = n < D_2 a = s$. Takav je slučaj npr. kad množimo redak stupcem $\rightarrow \cdot \downarrow$, čime se dobije skalarni produkt toga retka i stupca; npr.

$$[3,\ -2,\ 4]\cdot\begin{bmatrix} 5 \\ 1 \\ -3 \end{bmatrix}=[3\cdot 5+-2\cdot 1+4\cdot -3]=$$

$$=3\cdot 5+-2\cdot 1+4\cdot -3=1.$$

Što bi bilo npr.

$$\det\begin{bmatrix} \cdot\!-\!\cdot\!-\!\cdot\!-\!\cdot & \vdots & \vdots \\ \cdot\!-\!\cdot\!-\!\cdot\!-\!\cdot & \vdots & \vdots \\ & & \end{bmatrix}?$$

Provjerite da je npr.

$$\det\left(\begin{bmatrix} x & y & z \\ x' & y' & z' \end{bmatrix}\cdot\begin{bmatrix} X & X' \\ Y & Y' \\ Z & Z' \end{bmatrix}\right)=\begin{vmatrix} x & y \\ x' & y' \end{vmatrix}\cdot\begin{vmatrix} X & X' \\ Y & Y' \end{vmatrix}+$$

$$+\begin{vmatrix} x & z \\ x' & z' \end{vmatrix}\cdot\begin{vmatrix} X & Z \\ X' & Z' \end{vmatrix}+\begin{vmatrix} y & z \\ y' & z' \end{vmatrix}\cdot\begin{vmatrix} Y & Z \\ Y' & Z' \end{vmatrix}.$$

Ta se formula dokazuje na isti način kao teorem 9.2; uopće vrijedi

9.8.1. Teorem. *Pomnoži li se* (n, s)*-matrica* a (s, n)*-matricom* b*, za koje je* $s > n$*, tada se determinanta matrice-produkta* $a\,b = c$ *dobije kao suma svih produkata proizvoljne* (n, n)*-subdeterminante prve matrice i odgovarajuće* (n, n)*-subdeterminante druge matrice.*

Drugim riječima:

$$\det(a\,b)=\sum_{x\in\binom{1\,(s)}{n}}\det[a_{.x_1}\,a_{.x_2}\cdots a_{.x_n}]\det\begin{bmatrix} b_{x_1.} \\ b_{x_2.} \\ \cdots \\ b_{x_n.} \end{bmatrix}.$$

Sjetimo se da $\binom{1\,(s)}{n}$ označuje množinu svih dijelova po n članova izvađenih iz $\{1, 2, \ldots, s\} = 1\,(s)$.

Dokaz se provodi slično kao dokaz teorema 9.2.

Provedimo dokaz (imajmo na umu npr. slučaj $n=3$, $s=5$). Znamo da je $(ab)_{ik} = a_{i.} \circ b_{.k} = \sum_{p=1}^{s} a_{ip}\,b_{pk} =$ (umjesto varijabilnog indeksa p pišimo slova p_i zbog preglednijeg izlučivanja faktora pri narednom koraku)

$$= \sum_{p_i=1}^{s} a_{ip_i}\,b_{p_ik}.$$ Dakle

$$\det(a\,b)=\begin{vmatrix} \sum_{p_1=1}^{s} a_{1p_1}\,b_{p_11} & \cdots & \sum_{p_1=1}^{s} a_{1p_1}\,b_{p_1n} \\ \cdots & \cdots & \cdots \\ \sum_{p_n=1}^{s} a_{np_n}\,b_{p_n1} & \cdots & \sum_{p_n=1}^{s} a_{np_n}\,b_{p_nn} \end{vmatrix}.$$

Primijenimo na tu determinantu i njen prvi redak aditivno svojstvo; izlazi:

$$(1)\quad \det(ab)=\sum_{p_1} a_{1p_1}\begin{vmatrix} b_{p_1 1} & \cdots & b_{p_1 n} \\ \cdots & \cdots & \cdots \\ \sum_{p_n=1}^{s} a_{np_n} b_{p_n 1} & \cdots & \sum_{p_n=1}^{s} a_{np_n} b_{p_n n} \end{vmatrix} = (\text{iz istog razloga}) = \cdots =$$

$$= \sum_{p_1=1}^{s} a_{1p_1} \cdots \sum_{p_n=1}^{s} a_{1p_n} \begin{vmatrix} b_{p_1 1} & \cdots & b_{p_n n} \\ \cdots & \cdots & \cdots \\ b_{n_1 1} & \cdots & b_{p_n n} \end{vmatrix} = \sum_{p_1, p_2 \cdots p_n} a_{1p_1} a_{2p_2} \cdots a_{np_n} \begin{vmatrix} b_{p_1 1} & \cdots & b_{p_1 n} \\ \cdots & \cdots & \cdots \\ b_{p_n 1} & \cdots & b_{p_n n} \end{vmatrix}.$$

Pri tom $p_1, p_2, \ldots p_n$ prolaze, nezavisno jedan od drugoga, skupom $1(s)=S$. Ako se desi da je tu npr. $p_1=p_2$, onda je posljednja napisana determinanta $=0$; zato možemo suponirati da u nizu $p_1, p_2, \ldots, p_n$ nema jednakih članova. A to znači da taj niz p daje određen dio x upravo od n brojeva množine $1(s)$. Skupimo sve p-ove koji nastaju permutiranjem istog skupa x od n brojeva iz $1(s)$; to znači da je x jedna kombinacija n-tog razreda; svi pripadni p-ovi prolaze skupom $x!$ svih permutacija množine x. Na taj način obrazac (1) prelazi u ovaj:

$$(2)\quad \det(ab)=\sum_{x\in\binom{1(s)}{n}} \sum_{p\varepsilon x!} a_{1p_1}\cdots a_{np_n} \begin{vmatrix} b_{p_1 1} & \cdots & b_{p_1 n} \\ \cdots & \cdots & \cdots \\ b_{p_n 1} & \cdots & a_{p_n n} \end{vmatrix} = \sum_x t(x),$$

gdje smo stavili

$$(3)\quad t(x)=\sum_{p\varepsilon x!} a_{1p_1}\cdots a_{np_n} \begin{vmatrix} b_{p_1 1} & \cdots & b_{p_1 n} \\ \cdots & \cdots & \cdots \\ b_{p_n 1} & \cdots & b_{p_n n} \end{vmatrix}.$$

Neka su $x_1, x_2, \ldots, x_n$ elementi množine x u prirodnom poretku, tj. $x_1<x_2<\cdots<x_n$. Tada se determinanta pod znakom $\sum$ u (3) može transpozicijom redaka prevesti u determinantu

$$\pm \begin{vmatrix} b_{x_1 1} & \cdots & b_{x_1 n} \\ \cdots & \cdots & \cdots \\ b_{x_n 1} & \cdots & b_{x_n n} \end{vmatrix}.$$

Kako kod svake transpozicije determinanta mijenja znak, bit će determinanta pod $\sum$ u (2) jednaka $(-1)^{i(x_1 \ldots x_n)}$. Drugim riječima, obrazac (3) glasi:

$$(4)\quad t(x)=\left(\sum_{p\varepsilon x!} (-1)^{ip} a_{1p_1}\cdots a_{np_n}\right) \begin{vmatrix} b_{x_1 1} & \cdots & b_{x_1 n} \\ \cdots & \cdots & \cdots \\ b_{x_n n} & \cdots & b_{x_n n} \end{vmatrix}.$$

No, izraz (·) u $(4)_2$ je upravo

$$\begin{vmatrix} a_{1x_1} \cdot \cdot \cdot a_{1x_n} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{nx_1} \cdot \cdot \cdot a_{nx_n} \end{vmatrix}. \tag{5}$$

Time je $t(x)$ produkt determinante (5) i determinante što se pojavljuje u $(4)_2$; gornji obrazac (2) daje, dakle, traženu formulu u teoremu 9.8.1. Q. E. D.

9.8.2. Primjer. Nađite determinantu matrice što nastaje kao produkt matrica

$$a = \begin{bmatrix} 2 & 3 & -1 & 4 \\ 5 & 2 & 1 & 3 \end{bmatrix}, \qquad b = \begin{vmatrix} 0 & 1 \\ -3 & 5 \\ 2 & 4 \\ 3 & 2 \end{vmatrix}.$$

Produkt tih matrica je

$$a\,b = \begin{bmatrix} 1 & 21 \\ 5 & 25 \end{bmatrix}; \quad \text{zato je } \det(a\,b) = -80.$$

S druge strane radimo po gornjem obrascu.

Tu je $n=2$, $s=4$; ako npr. iz množine $1(4)$ uzmemo ambu $\{1, 4\}$, onda je pripadna subdeterminanta $t\{1, 4\}$ matrice a jednaka

$$\begin{vmatrix} 2 & 4 \\ 5 & 3 \end{vmatrix}, \quad \text{a od matrice } b \text{ je } \begin{vmatrix} 0 & 1 \\ 3 & 2 \end{vmatrix}.$$

Tražena determinanta je jednaka:

$$\begin{vmatrix} 2 & 3 \\ 5 & 2 \end{vmatrix} \cdot \begin{vmatrix} 0 & 1 \\ -3 & 5 \end{vmatrix} + \begin{vmatrix} 2 & -1 \\ 5 & 1 \end{vmatrix} \cdot \begin{vmatrix} 0 & 1 \\ 2 & 4 \end{vmatrix} + \begin{vmatrix} 2 & 4 \\ 5 & 3 \end{vmatrix} \cdot \begin{vmatrix} 0 & 1 \\ 3 & 2 \end{vmatrix} +$$

$$+ \begin{vmatrix} 3 & -1 \\ 2 & 1 \end{vmatrix} \cdot \begin{vmatrix} -3 & 5 \\ 2 & 4 \end{vmatrix} + \begin{vmatrix} 3 & 4 \\ 2 & 3 \end{vmatrix} \cdot \begin{vmatrix} -3 & 5 \\ 3 & 2 \end{vmatrix} + \begin{vmatrix} -1 & 4 \\ 1 & 3 \end{vmatrix} \cdot \begin{vmatrix} 2 & 4 \\ 3 & 2 \end{vmatrix} =$$

$$= -11 \cdot 3 + 7 \cdot -2 - 14 \cdot -3 + 5 \cdot -22 + 1 \cdot -21 - 7 \cdot -8 =$$

$$= -33 - 14 + 42 - 110 - 21 + 56 = -80.$$

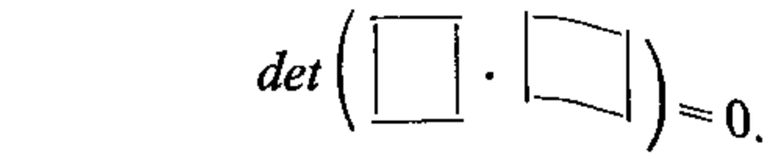
Rezultat je na oba načina isti.

9.9. Binet-Cauchyjev [Biné, Koši] teorem. Gornje rezultante možemo skupiti pa imamo ovaj opći teorem.

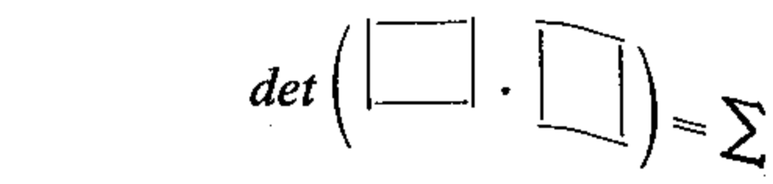
—→ **9.9.1.** Teorem. *Neka su a, b konačne matrice za koje produkt ab postoji, i to kao kvadratna matrica oblasti* $n \times n$.

Ako su i a i b kvadratne matrice, tada je $\det(ab) = \det a \det b$.

Ako a ima više redaka nego stupaca, tada je $\det(a\,b)=0$, *tj. matrica* $a\,b$ *je singularna; simbolički:*



Ako a ima manje redaka nego stupaca, tada je $\det(a\,b)$ *suma svih produkata što se dobiju množeći svaku subdeterminantu oblasti* $n\times n$ *prvog faktora a odgovarajućom subdeterminantom oblasti* $n\times n$ *drugog faktora b (Binet-Cauchyjev teorem); simbolički:*



Primjene toga teorema vrlo su brojne.

U vezi s Binet-Cauchyjevim teoremom zanimljivo je napomenuti da je on u neku ruku karakterističan za funkciju $a\to\det a$ unutar kvadratnih matrica. Može se, naime, dokazati da vrijedi ovaj

9.9.2. Teorem. *Ako je u skupu svih kvadratnih matrica oblasti* (n, n) *definirana numerička funkcija* $F: a\to F(a)$, *pa ako je* $F(a\,b)=F(a)\,F(b)$, *tada je* $F=f(\det a)$, *gdje je f određena funkcija s kompleksnim argumentom za koju je* $f(x\,y)=f(x)\,f(y)$. *Ako je F neprekidna funkcija i* $\not\equiv 0$, *tada je* $f(x)\in\{x, \operatorname{sgn} x^{\alpha}\}$, *tj.* $F(a)=(\det a)^{\alpha}$; *pri tom je* α *neki konstantan broj (nezavisan od a)* (M. *Kucharzewski*; v. str. 110 u *S. Kurepa, Functionl Equations for invariants of a matrix* Glasnik mat-fiz-astr. Zagreb 14 (1959) 97—113 kao i *On a characterisation of a determinant*, isti časopis 19 (1964) 189—198.)

9.10. Završna primjedba o množenju determinanata. Činjenica da npr. za kvadratne konačne matrice a, b vrijedi $\det(a\,b)=\det a\det b$ izvor je brojnih algebarskih identiteta, jer je u toj jednakosti lijeva strana određen izraz, a desna strana je produkt od dva izraza koja su analogno građena. Već najjednostavniji slučaj

$$\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}\cdot\begin{vmatrix} c & d \\ c' & d' \end{vmatrix}=\begin{vmatrix} a\,c+b\,c' & a\,d+b\,d' \\ a'\,c+b'\,c' & a'\,c'+b'd' \end{vmatrix}$$

daje zanimljiv identitet:

$$(a\,b'-a'\,b)(c\,d'-c'\,d)=(a\,c+b\,c')(a'\,d+b'\,d')-(a\,d+b\,d')(a'\,c+b'\,c').$$

10. ŠTO ZA KVADRATNU MATRICU ZNAČI DA JOJ JE DETERMINANTA JEDNAKA 0?

10.1. Uz kvadratnu n-matricu a vezano je n vektora — stupaca $a_{\cdot 1}, \ldots, a_{\cdot n}$, koje možemo smatrati kao radijus-vektore, odnosno bridove određenog

kvadra. Zapremina tog kvadra jest upravo $=\det a$ (uz zgodan izbor jedinice) (isp. § 13). Prema tome, *jednakost* $\det a = 0$ *značit će da se n-dimenzionalni kvadar izrodio* (*da je degenerirao*) *i ima manje od n dimenzija*: *bar jedan od n stupaca-vektora može se linearno izraziti pomoću ostalih stupaca-vektora zadane matrice.*

Na taj način naslućujemo da će vrijediti

10.2. Teorem. *Ako je kvadratna matrica singularna, tada joj je bar jedan stupac linearna kombinacija ostalih njenih stupaca* (isp. teorem 4.3 u pogl. 9).

Dokažimo to i formalno. Prema pretpostavci je $\det a = 0$. Neka je $r(a)$ r_a (ili kraće r) *maksimalni* stupanj *regularne podmatrice u a*; to znači da *postoji* u a podmatrica, c, poretka $(r \times r)$ i sa svojstvom $\det c \neq 0$, dok za *svaku* kvadratnu *nadmatricu* x od c vrijedi $\det x = 0$ (sjetite se da $a \subset x$, za matrice, znači da je a podmatrica od x).

Dokažimo da je *svaki stupac* $a_{\cdot r'}$ *linearna kombinacija od onih r stupaca u kojima leže stupci matrice c.*

Prvi slučaj: matrica c je smještena *u lijevom gornjem uglu* matrice a,

tj. $$c_{i\cdot} \subset a_{i\cdot}, \quad c_{\cdot i} \subset a_{\cdot i}, \quad \text{za svako} \quad i = 1, 2, \ldots, r.$$

Evo *odlučnog koraka u dokazu*:

Obrubimo matricu c *proizvoljnim* retkom $a_{l\cdot}$ i *proizvoljnim* stupcem $a_{\cdot m}$ matrice a za koji je $r < m \leq n$ (a je tipa $n \times n$), tj. formirajmo matricu

$$c(l,m) = \begin{bmatrix} & & \cdot \\ & c & \cdot \\ & & \cdot \\ \cdot & & \cdot \\ \cdot & \cdot & a_{lm} \end{bmatrix} = \begin{bmatrix} c_{11} & \cdots & c_{1r}, & a_{1m} \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ c_{r1} & \cdots & c_{rr} & a_{rm} \\ a_{l1} & \cdots & a_{lr} & a_{lm} \end{bmatrix}.$$

Odmah ćemo vidjeti da je $a_{\cdot m}$ izrazivo pomoću stupaca $a_{\cdot r'}$. Kao i obično: $r' = 1, 2, \ldots, r$. U prvom redu, $\det c(l,m) = 0$. Uistinu, ako je $l \leq r$, tada matrica $c(l,k)$ ima dva jednaka retka: l i r, pa je, dakle, singularna. A ako je $l > r$, tada je $c(l,m)$ podmatrica u a tipa $(r+1, r+1)$, pa je, po definiciji broja r, matrica $c(l,m)$ singularna.

Razvijmo determinantu $c(l,m)$ po posljednjem retku. Neka je B_i algebarski komplement u $c(l,m)$ od a_{li}. Tada je prema Laplaceu:

$$\sum_{i=1}^{r \neq m} a_{li} B_i + a_{lm} \det c = \det c(l,m) = 0,$$

tj.

$$a_{lm} = -\sum_{r'} \frac{B_{r'}}{\det c} a_{lr'} \quad \text{za svako} \quad l, \quad \text{tj.}$$

$$a_{\cdot m} = -\sum_{r'} \frac{B_{r'}}{\det c} a_{\cdot r'}$$

jer pri $l=r+1,\ r+2,\ldots,\ n$ pri fiksnom $m\in\{r+1,\ldots,\ n\}$ veličine $B_{r'}$ $(r'=1,2,\ldots,\ r)$ ne zavise od l nego samo od $a_{1m},\ldots,\ a_{rm}$.
Dakle je uistinu stupac $a_{.m}$ linearna kombinacija stupaca $a_{.1}\cdots a_{.r}$.

Drugi slučaj: *c nije u lijevom gornjem uglu* matrice *a*. Ovaj se slučaj svodi na prethodni. Tako npr. ako nije $c_{1.}\subset a_{1.}$, nego je $c_{1.}\subset a_{l_1}$. uz $l_1>1$, tada se uzastopnim transpozicijama redaka $l_1,\ l_1-1,\ldots$ prevede a u takvu matricu u kojoj je prvi redak $=a_{l_1.}$ i sadrži $c_{1.}$; analogno možemo postići pomoću transpozicija da drugi redak $c_{2.}$ od c dođe u drugi redak, itd. Slično je sa stupcima. Tako formirana matrica A zadovoljava relaciju $r_a=r_A$, gdje je $(r_A,\ r_A)$ maksimalni stupanj regularnih kvadratnih podmatrica $\subseteq A$. Stvarno prelazom $a\to A$, prelazi svaka *regularna* (*singularna*) kvadratna podmatrica x od a u određenu *regularnu* (*singularnu*) kvadratnu podmatricu x od A. No, u matrici A ostvaren je *prvi slučaj*, pa je zato $A_{.m}$ za svako $k>r$ linearna kombinacija od stupaca $A_{.i}$; no $A_{.m}$ je određen stupac u a izvan podmatrice c.

Time je gornji teorem dokazan.

Na sličan način dokazuje se i ovaj važni teorem (čitan bez [ ]):

—→ **10.3. Osnovni teorem.** ***Neka za kvadratnu ili nekvadratnu |konačnu ili beskonačnu matricu a broj r kazuje da je (r, r) maksimalni stupanj kvadratne regularne podmatrice od a; ako je $r<\infty$ te ako je c kakva regularna podmatrica od a stupnja (r, r) tada se svaki stupac [redak] matrice a izražava linearno pomoću upravo onih r stupaca [redaka] matrice a iz kojih je izvađena podmatrica c.***

Analogno je stvar iskazana za *retke* matrice *a* (čitaj sa [ ]).

Naime, iz matrice *a* proizvodimo i transponiranu matricu a^T; znamo da je $\det a^T=\det a$; zato je uz $\det a=0$ također $\det a^T=0$; prema teoremu 10.2. znači da je bar jedan stupac u a^T linearna kombinacija ostalih stupaca u a^T. No, stupci u a^T su redići u *a*. To znači da je zaista ispravan i tekst sa [ ] u teoremu 10.3. Posebno je na snazi:

10.4. Teorem. *Iz jednakosti* $\det a=0$ *proizlazi da je bar jedan redak od a linearno izraziv pomoću ostalih redaka* (isp. 10.2).

Obrat toga iskaza već je dokazan u 6.4.

Na taj način imamo ovaj važan teorem:

—→ **10.5.** Teorem. **Prvi kriterij o singularnosti kvadratne matrice.** *Da kvadratna konačna matrica bude singularna, nužno je i dovoljno da joj bar jedan stupac bude linearna kombinacija ostalih njenih stupaca*; i dualno za retke.

10.6. Drugi kriterij o singularnosti kvadratne matrice. Upravo dokazasmo da je $\det a=0$, ako je *svaki* stupac od *a* linearna kombinacija od stanovitog broja $m<n$ vektorâ *v*, koji su stupci te iste matrice *a*. Međutim, mi ćemo pokazati da pri tom nije bitno da *v* budu vektori baš matrice *a*:

Teorem. *Za kvadratnu matricu a jednakost* $\det a=0$ *vrijedi onda i samo onda ako je svaki stupac* (*redak*) *matrice linearna kombinacija od stanovitog broja m vektora* $v_1,\ldots,\ v_m$, *pri čemu je* $m<n$ *te* $\mathrm{Dom}\,a=n\times n$.

Nužnost je iskazana prvim dijelom teorema 10.5; dokažimo da je uslov teorema i dovoljan, bez obzira na to da li su vektori $v_1, \ldots, v_m$ linije matrice a.

Prema pretpostavci je $a_{\cdot n'}$ linearna kombinacija nizova $v_{\cdot m'}$:

$$a_{\cdot n'} = \sum_{m'} x_{n'\,m'}\, v_{\cdot m'}\,.$$

No, $\det a$ je linearno-homogena funkcija svakog svojeg stupca $a_{\cdot n'}$; zato se postepenim razlaganjem po svakom stupcu vidi da je $\det a$ homogeno-linearna funkcija determinanata d, u kojima su stupci uzeti među zadanim vektorima $v_{m'}$. Kako je $\mathrm{Dom}\, d = \mathrm{Dom}\, a = n \times n$, $n > m$, znači to da se u d pojavljuju dva jednaka stupca; dakle je $d = 0$, a time i $\det a = 0$.

⟶ **10.7. Teorem. Treći kriterij o singularnosti kvadratne matrice.**

Za svaku konačnu matricu a jednakost

(1) $$\boldsymbol{\det a = 0}$$

ima za posljedicu da postoji bar jedan vektor $\vec{x}$ ***za koji je***

(2) $$\boldsymbol{\overrightarrow{a\,x} = \vec{0}, \quad \vec{x} \neq \vec{0}.}$$

I obrnuto: iz **(2)** ***izlazi*** **(1).**

Dokažimo, najprije, da iz (2) izlazi (1). To odmah izlazi iz Cramerova teorema (v. teor. 7.9.2), prema kojemu iz (2) neposredno izlazi da je

(3) $$\det a \cdot x_\nu = 0 \text{ za svako } \nu = 1,\ 2, \ldots,\ n.$$

Kako je prema (2) $\vec{x} \neq \vec{0}$, znači to da je $x_\nu \neq 0$ za neko $\nu \leq n$, pa je zbog (3) nužno ispunjeno (1).

Dokažimo sada da iz (1) izlazi (2). Neka je r najveća širina nesingularne kvadratne podmatrice b u a. Posmatrajmo u nizu jednadžbi

$$\sum_{n'} a_{n'} \cdot \vec{x}_{n'} = 0$$

onaj najuži podsistem kojemu matrica koeficijenata obuhvata matricu b. Konkretno možemo uzeti da je matrica b smještena u gornjem lijevom uglu matrice a. Taj sistem razriješimo po odgovarajućim nepoznanicama $x_1, \ldots, x_r$ služeći se npr. Cramerovim pravilom. Time su nepoznanice $x_{r'}$ izražene pomoću preostalih nepoznanica $x_{r+1}, x_{r+2}, \ldots$, koje mogu biti proizvoljne, pa dakle i posebno $x_{r+1} \neq 0$. To znači da pripadni niz x nije $= \vec{0}$.

No, *svako rješenje* ***prvih r*** *jednadžbi rješenje je i* ***svih*** *jednadžbi s matricom a:*

$$a_{r'} \cdot \vec{x} = 0 \Rightarrow x_{n'}\ \vec{x} = 0.$$

Stvarno, prema teoremu 10.3, redak $a_{l\cdot}$ matrice a za $l \geq r$ je linearna kombinacija redaka $a_{r'\cdot}$, a to upravo znači da je svako rješenje x sistema $a_{r'}\, x = 0$ ujedno i rješenje sistema $a_{n'}\, x = 0$. Time je teorem 10.7 potpuno dokazan.

10.8. Zadaci o množenju determinanata.

1. Zadane su matrice $a=\begin{bmatrix} 3 & 5 & 1 \\ 2 & 4 & -2 \\ 3 & 2 & 1 \end{bmatrix}$, $b=\begin{bmatrix} -1 & 2 & -3 \\ 2 & 7 & -5 \\ -2 & 4 & 1 \end{bmatrix}$.

1) Pomnoži na sva četiri načina determinante tih matrica i uvjeri se u međusobnu jednakost dobivenih rezultata; 2) nađi $-a$ i $\det(-a)$; 3) odredi $\det(a+b)$.

2. Zadane su matrice $a=\begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix}$, $b=\begin{bmatrix} 2 & 5 \\ 8 & -4 \end{bmatrix}$, $c=\begin{bmatrix} -8 & -3 \\ 1 & 5 \end{bmatrix}$;

1) Nađite: $a\,K\,b$, $(a\,K\,b)\,K\,c$, $b\,K\,c$, $a\,K\,(b\,K\,c)$ i pripadne determinante.
2) Da li je u kojem tom slučaju operator det distributivan prema K?
3) Da li je $(a\,K\,b)\,K\,c=a\,K\,(b\,K\,c)$? (v. § 9.5).

3. 1) Dokažite da za krakovsko množenje $a\,K\,b$ matrica vrijedi $a\,K\,b=b^T a$. 2) Izraziti $(a\,K\,b)\,K\,c$, $a\,K\,(b\,K\,c)$ kao produkt matrica.
3) Je li $\det(a\,K\,b)=\det a\ \det b$?

4. Za slijedeće parove matrica a, b nađi $a\,b$, ba (ukoliko je to moguće) te pripadnu determinantu produkta:

1) $a=\begin{bmatrix} 3 & 4 & 5 \\ 2 & 1 & 5 \end{bmatrix}$, $b=\begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix}$; 2) a^T, b^T iz slučaja 1);

3) $a+b^T$, $a-b^T$; 4) $b+a^T$, a^T.

5. Odredi

1) $\begin{vmatrix} a & b & c & d \\ -b & a & d & -c \\ -c & -d & a & b \\ -d & c & -c & a \end{vmatrix}$, 2) $\begin{vmatrix} a & b & c & d & e & f & g & h \\ -b & a & d & -c & f & -e & -h & g \\ -c & -d & a & b & g & h & -e & -f \\ -d & c & -b & a & h & -g & f & -e \\ -e & -f & -g & -h & a & b & c & d \\ -f & e & -h & g & -b & a & -d & c \\ -g & h & e & -f & -c & d & a & -b \\ -h & -g & f & e & -d & -c & b & a \end{vmatrix}$

i to prethodnim kvadriranjem tih determinanata.

6. Odredi vrijednost ovih determinanata a poretka (n, n) prikazujući ih kao produkt dviju determinanata gdje a_{ik} znači:
1) $1+x_i y_k$; 2) $\cos(\alpha_i-\alpha_k)$; 3) $\sin(\alpha_i+\alpha_k)$.

7. Zadan je vektor— stupac $\vec{v}$ sa $\vec{v}=[x_1, x_2, \ldots, x_n]^T$;

1) napiši matricu $V_n=[\vec{1}=\vec{v}^0, \vec{v}, v^2, \ldots, v^{n-1}]$; nađi $V_n{}^T V_n$. Matricu $V_n=[\vec{1}=\vec{v}^0, v^2, \ldots, v^{n-1}]$ obrubi odozdo s retkom $1, x, x^2, \ldots, x^n$,

a zdesna sa $x_1^n,\ x_2^n, \ldots,\ x_n^n,\ x^n$ odnosno s nulama osim na polju $(n+1,\ n+1)$ kamo dolazi broj 1; neka su $a,\ b$ dobivene matrice. Nađi umnožak $a^T b$.

8. Neka je a zadana kvadratna matrica reda n; neka je 1_n jedinična matrica reda n; 1) neka b označuje matricu dobivenu iz 1_n međusobnom zamjenom i-og i k-og retka; nađi $\det(a \cdot b)$, $\det(b\,a)$; zaključak? 2) Neka b označuje matricu reda n kojoj je dijagonala konstanta 1, a na preostalim poljima i-og redića i k-tog stupčića vrijednosti su $=c$; nađi $\det(a\,b)$, $\det(b\,a)$ i primijeni teorem o množenju. Zaključak?

9. Na osnovu formule $\begin{vmatrix} x & y & z \\ y & z & x \\ z & x & y \end{vmatrix} = 3\,xyz - x^3 - y^3 - z^3$ dokazati da je produkt od dvije funkcije oblika $3\,xyz - x^3 - y^3 - z^3$ opet takvog oblika: $(3\,abc - a^3 - b^3 - c^3)(3\,xyz - x^3 - y^3 - z^3) = 3\,XYZ - X^3 - Y^3 - Z^3$; odredi $X,\ Y,\ Z$. Poopći!

10. Provjeri da je $\begin{vmatrix} -a & b & c & d \\ b & -a & d & c \\ c & d & -a & b \\ d & c & b & -a \end{vmatrix} = -(a+b+c-d)(b+c+d-a)(c+d+a-b)(d+a+b-c)$

(Uputa: lijevu determinantu pomnoži sa

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 \end{vmatrix}$$

11. *Eulerov identitet*. Množeći dvije determinante oblika

$$\begin{vmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & -x_1 & -x_4 & x_3 \\ x_3 & x_4 & -x_1 & -x_2 \\ x_4 & -x_3 & x_2 & -x_1 \end{vmatrix}$$

dokaži Eulerov identitet $(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) =$

$$= (x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4)^2 + (x_1 y_2 - x_2 y_1 - x_3 y_4 + x_4 y_3)^2 +$$

$$+ (x_1 y_3 + x_2 y_4 - x_3 y_1 - x_4 y_2)^2 + (x_1 y_4 - x_2 y_4 - x_3 y_2 - x_4 y_1)^2.$$

12. Ako je $x+y+z=0$, tada je $\begin{vmatrix} 1, & \cos z & \cos y \\ \cos z, & 1, & \cos x \\ \cos y & \cos x, & 1 \end{vmatrix} = 0.$

13. Neka su (x_1, y_1), (x_2, y_2), (x_3, y_3) analitičke oznake triju tačaka u ravnini s ortogonalnim Dekartovim koordinatama; dokaži da pri promjeni koordinatne baze tj. supstitucijom

$$x_i = x'_i \cos\alpha - y' \sin\alpha + x_0$$
$$y_i = x'_i \sin\alpha + y' \cos\alpha + y_0 \text{ determinanta}$$

1) $\begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}$, 2) $\begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix}$

prelazi u analognu determinantu u kojoj dolaze slova s crticom; odatle zaključiti na značenje dviju zadanih determinanata.

14. Neka su $\vec{a}_1 = \begin{bmatrix} a_{11} \\ a_{21} \\ a_{31} \end{bmatrix}$, $\vec{a}_2 = \begin{bmatrix} a_{12} \\ a_{22} \\ a_{32} \end{bmatrix}$, $\vec{a}_3 = \begin{bmatrix} a_{13} \\ a_{23} \\ a_{33} \end{bmatrix}$ tri ortonormirana vektora u Dekartovom ortogonalnom sistemu; 1) promatraj matricu $[a_1\, a_2\, a_3]$ tih vektora i dokaži da joj je determinanta $= \pm 1$. 2) Poopći.

15. Neka su $\vec{a} = [a_1\ a_2\ a_3]^T$, $\vec{b} = [b_1\ b_2\ b_3]^T$ dva vektora veličine 1 u pravokutnom Dekartovu sistemu; dokaži da je $\sin^2 \sphericalangle(\vec{a}_1, \vec{a}_2) =$
$= \det [\vec{a}, \vec{b}]^T\ [\vec{a}, \vec{b}] = (a_1 b_2 - a_2 b_1)^2 + (a_2 b_3 - a_3 b_2)^2 + (a_3 b_1 - a_1 b_3)^2$.

16. Neka su a, b, c tri jedinična vektora u Dekartovom sistemu; dokaži da je $\det [\vec{a}, \vec{b}, \vec{c}]^2 = 1 - \cos^2 \sphericalangle(\vec{a}; \vec{b}) - \cos^2 \sphericalangle(b, c) -$
$-\cos^2 \sphericalangle(\vec{c}, \vec{a}) + 2\cos \sphericalangle(\vec{a}, \vec{b}) \cos \sphericalangle(\vec{b}, \vec{c}) \cos \sphericalangle(\vec{c}, \vec{a})$.

17. Ako je red kvadratne matrice a paran broj, dokaži da postoji kososimetrična matrica b za koju je $\det b = \det(a^2)$.

11. TEHNIKA IZRAČUNAVANJA DETERMINANATA

Sad znamo što je determinanta i kako dolazi pri rješavanju linearnih sistema. Važno je da se umije izračunati determinanta na što brži način.

11.1 Teorem. *Determinanta trokutne tablice jednaka je produktu vrijednosti što stoje na dijagonali tablice*:

$$\begin{vmatrix} a_{11} & & \wedge \\ & a_{22} & \\ & & \ddots \\ & & & \ddots \\ 0 & & & a_{nn} \end{vmatrix} = a_{11} \cdots a_{n-1,\,n-1}\, a_{n\,n};$$

pri tom iznad dijagonale može stajati što god (v. teorem 1.3).

11.1.1. K o r o l a r. *Determinanta dijagonalne kvadratne matrice jednaka je produktu vrijednosti što su na glavnoj dijagonali matrice* (v. teorem 11.1).

11.2.1. K o r o l a r. *Determinanta skalarne matrice stupnja n ima vrijednost* c^n, *gdje je c konstantna vrijednost po dijagonali.*

11.2. Korištenje Laplaceova teorema od znatne je teoretske i praktične pomoći.

11.3. *Dobavljanje što više* 0 *u pojedini redak* (*stupac*) *čest je pripremni korak pri izračunavanju determinanata.* P r i m j e r. Neka je

$$a=\begin{bmatrix} 2 & 5 & 4 & 3 \\ 7 & -2 & -3 & -4 \\ -3 & \boxed{2} & 2 & 3 \\ 3 & -4 & 2 & 4 \end{bmatrix}.$$

Uočimo tu jedan top npr. $a_{32}=2$; uvedimo na preostala mjesta tog 3. retka same 0 (isp. primjer 6.1.1). Oduzmemo li od $a_{.3}$ stupac $a_{.2}$, nastaje matrica

$$b=\begin{bmatrix} 2 & 5 & -1 & 3 \\ 7 & -2 & -1 & -4 \\ -3 & 2 & 0 & 3 \\ 3 & -4 & 6 & 4 \end{bmatrix},$$

u kojoj je $b_{33}=0$; ta se operacija nameće.

Isto tako, nađemo li matricu

$c=\left[a_{.1}+\frac{3}{2}a_{.2},\ a_{.2},\ a_{.3}\ -a_{.2}\ a_{.4}+a_{.2}\left(-\frac{3}{2}\right)\right]$, tada se vidi da je

$c_{3.}=0\quad 2\quad 0\quad 0$ i da je $\det a=\det c$.

Stvarno je

$$c=\begin{bmatrix} 19/2 & 5 & -1 & -9/2 \\ 4 & -2 & -1 & -1 \\ 0 & 2 & 0 & 0 \\ 9 & -4 & 6 & 10 \end{bmatrix};$$

po teoremu 3.1. vrijedi $\det a=\det c$. No, $\det c$ se lako izračuna razvijanjem po c_3. (Laplaceovo pravilo); imamo

$$\det c=1\cdot f\ 2=2\cdot(-1)^{3+2}\begin{vmatrix} 19/2 & -1 & -9/2 \\ 4 & -1 & -1 \\ 9 & 6 & 10 \end{vmatrix}\ \text{itd.}$$

Pri tom se koristimo ovom činjenicom:

11.3.1. T e o r e m. *Ako je za kvadratnu matricu a vrijednost* $a_{lk}\neq 0$, *tada se matrica a može* (*elementarno*) *prevesti u matricu b tako da bude* $a_{lk}=b_{lk}$,

$\det a = \det b$, *dok su inače sve vrijednosti u retku* $b_{l.}$ (*stupcu* $b_{.k}$) *jednake* 0 (isp. primjer 6.1.1).

Takve su npr. ove dvije matrice:

$$\left[a_{.1} - \frac{a_{l1}}{a_{lk}} a_{.k},\ a_{.2} - \frac{a_{l2}}{a_{lk}} a_{.k},\ \ldots,\ a_{.k-1} - \frac{a_{lk-1}}{a_{lk}} a_{.k},\ a_{.k},\ a_{k+1} - \frac{a_{lk+1}}{a_{lk}} a_{.k}, \ldots \right]$$

odnosno

$$\left[a_{1.} - \frac{a_{1k}}{a_{lk}} a_{l.},\ a_{2.} - \frac{a_{2k}}{a_{lk}} a_{l.},\ \ldots,\ a_{l-1.} - \frac{a_{l-1k}}{a_{lk}} a_{l.},\ a_{l.},\ a_{l+1.} - \frac{a_{l+1k}}{a_{lk}} a_{l.} \cdots \right]^T$$

Opiši riječima kako se prave te dvije matrice.

11.4. Kondenzacija oko jednog mjesta (Gauss-Chiòov [Gaus, Kió] postupak). Neka je $a_{lk} \neq 0$; tada se radi o *kondenzaciji oko položaja* a_{lk}; kaže se također da je a_{lk} pivotni ili stožerni položaj.

Objasnimo stvar na slučaju da je $\mathrm{Dom}\, a = 3 \times 3$ i da je $a_{11} \neq 0$. Provedimo npr. kondenzaciju stupaca (dualno se radi s redovima). Svaki preostali stupac množimo sa a_{11}; simbolički:

$$a \to [a_{.1},\ a_{11}\ a_{.2},\ a_{11}\ a_{.3}] = b$$
$$[a_{.1},\ a_{11}\ a_{.2} - a_{12}\ a_{.1},\ a_{11}\ a_{.3} - a_{13}\ a_{.1}] = c.$$

Drugi je korak $b \Rightarrow c$ očigledan: radilo se tako da se stupac $b_{.1} = a_{.2}$ množi sa a_{1k} za svako $k > 1$ i to oduzme od novog k-stupca $b_{.k}$. Tako nastaje matrica c za koju je $c_{.k} = a_{11}\ a_{.k} - a_{1k}\ a_{.1}$ tj. $c_{ik} = a_{11}\ a_{ik} - a_{1k}\ a_{i1}$ ili u drugoj oznaci (pišimo odmah kao da je $\mathrm{Dom}\, a = n \times n$)

$$(1) \qquad c_{ik} = a^{1i}_{1k} = a_{11}\ a_{ik} - a_{1k}\ a_{i1} \quad (i,\ k = 2,\ 3, \ldots).$$

Za determinante u gornjem postupku imamo (izlučujući faktor a_{11} iz svakog $b_{.2},\ b_{.3}, \ldots$):

$$\det a = a_{11}^{(n-1)} \det b, \qquad \det b = \det c.$$

No $c_{11} = a_{11}$, inače je $c_{ik} = 0$; razvijajući $\det c$ po retku $c_{1.}$, i eliminirajući b i c iz gornjih jednakosti, izlazi:

$$(2) \qquad \det a = a_{11}^{n+2} \begin{vmatrix} \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}, \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{23} \end{vmatrix} \cdots \\ \\ \begin{vmatrix} a_{11} & a_{12} \\ a_{31} & a_{32} \end{vmatrix}, \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix} \cdots \\ \cdots \qquad \cdots \end{vmatrix} = a_{11}^{n+2} \begin{vmatrix} & & & \\ a^{12}_{12} & a^{12}_{13} & \cdots & a^{12}_{1n} \\ \cdot & \cdot & \cdot & \cdot \\ a^{1n}_{12} & a^{1n}_{13} & \cdots & a^{1n}_{1n} \\ & & & \end{vmatrix}$$

Struktura determinante (2) je očigledna.

Za $n=3$ izlazi da je

$$\det a = a_{11}^{-1} \begin{vmatrix} a_{11}\ a_{22} - a_{12}\ a_{21} & a_{11}\ a_{23} - a_{12}\ a_{21} \\ a_{11}\ a_{32} - a_{12}\ a_{31} & a_{11}\ a_{33} - a_{13}\ a_{31} \end{vmatrix}.$$

11.5. Vandermondeova [Vandermond] determinanta. Radi se o ovom: zadan je *niz* $x = x_0,\ x_1,\ x_2, \ldots,\ x_{n-1}$; time su određene i potencije x^k toga niza; naime, $x^k = x_0^k,\ x_1^k, \ldots,\ x_{n-1}^k$; tako se npr. stavlja $x^0 = 1,\ 1, \ldots,\ 1$. *Vandermondeova matrica ima za stupce nizove* x^n; ona glasi

$$V_n(x) = [x^0,\ x,\ x^2, \ldots,\ x^{n-1}],\ \text{tj.}$$

$$V_n(x) = \begin{bmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ 1 & x_{n-1} & x_{n-1}^2 & & x_{n-1}^{n-1} \end{bmatrix} \text{ ili kraće } V_n[x_0\ x_1 \cdots x_{n'} \cdots]^T$$

Nađimo $\det V_n(x)$.

No, važi ovo:

$$\det V_n(x) = \det [x^0,\ x - x_0\ x^0,\ x^2 - x_0\ x, \ldots,\ x^{n-1} - x_0\ x^{n-2}] =$$

$$= \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & x_1 - x_0 & x_1^2 - x_0 x_1 & \cdots & \\ 1 & \cdot & & & \\ \cdot & \cdot & & & \\ \cdot & \cdot & & & \\ 1 & x_{n-1} - x_0 & x_{n-1}^2 - x_0 & x_{n-1} & x_{n-1}^{n-1} - x_0 x_{n-1}^{n-2} \end{bmatrix}.$$

Razvijajući ovu determinantu po prvom retku izlučujući faktore

$$x_1 - x_0,\ x_2 - x_0, \ldots,\ x_{n-1} - x_0$$

po redu u preostalim recima, izlazi da je ona jednaka

$$\det V_n(x) = (x_1 - x_0)(x_2 - x_0) \cdots (x_{n-1} - x_0)\ \det V_{n-1} \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_{n-1} \end{bmatrix}.$$

Time se dobiva *rekurziona formula.*

Radeći dalje na sličan način *do kraja*, izlazi ovo:

$$\det V_n(x) = (x_1 - x_0)(x_2 - x_0)\cdots(x_{n-1} - x_0)$$
$$(x_2 - x_1)\cdots(x_{n-1} - x_1)$$
$$\cdots\cdots\cdots$$
$$(x_{n-1} - x_{n-2}),$$

tj.
$$\det V_n [x_0\, x_1 \cdots x_{n-1}]^T = \prod_{i<k<n} (x_k - x_i).$$

Na taj način izlazi da je na snazi

11.5.1. Teorem.

$$\det V_n \begin{bmatrix} x_0 \\ x_1 \\ \cdot \\ \cdot \\ x_{n-1} \end{bmatrix} = \det \begin{bmatrix} 1 = x_0^0 & x_0 & x_0^2 & x_0^3 & \cdots & x_0^{n-1} \\ 1 = x_1^0 & x_1 & x_1^2 & x_1^3 & & x_1^{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 = x_{n-1}^0 & x_{n-1} & x_{n-1}^2 & x_{n-1}^3 & \cdots & x_{n-1}^{n-1} \end{bmatrix} = \prod_{i<k<n} (x_k - x_i).$$

Ako u nizu x ima jednakih članova, tada je $\det V(x) = 0$; *i obrnuto ako je* $\det V_n(x) = 0$, *tada u nizu* $x = (x_{n'})_{n'<n}$ *ima jednakih članova.*

Tako npr. za $n = 3$ imamo

$$\det V_3 \begin{bmatrix} x_0 \\ x_1 \\ x_2 \end{bmatrix} = \begin{vmatrix} x_0^0 & x_0^1 & x_0^2 \\ x_1^0 & x_1^1 & x_1^2 \\ x_2^0 & x_2^1 & x_2^2 \end{vmatrix} = (x_1 - x_0)(x_2 - x_0)(x_2 - x_1) =$$
$$= x_1 x_2^2 - x_0 x_2^2 + x_0^2 x_2 - x_1^2 x_2 + x_0 x_1^2 - x_0^2 x_1.$$

11.5.2. Zanimljivo je u ovom izrazu upotpuniti svaki član tako da dolaze sve tri veličine $x_3 = x_0, x_1, x_2$ eventualno s eksponentom 0; gornji izraz postaje:

$$x_0^0 x_1^1 x_2^2 - x_0^1 x_1^0 x_2^2 + x_0^2 x_1^0 x_2^1 - x_0^0 x_1^2 x_2^1 + x_0^1 x_1^2 x_2^0 - x_0^2 x_1^1 x_2^0.$$

Vidimo da u eksponentu svakog člana dolazi permutacija p brojeva 0, 1, 2, a da je pred dotičnim članom znak $(-1)^{ip}$, tj.

$$\det V_3 \begin{bmatrix} x_0 \\ x_1 \\ x_2 \end{bmatrix} = \sum_{p \in I3!} (-1)^{ip}\, x_0^{p_0} x_1^{p_1} x_2^{p_2}.$$

Zaključak je *općenit za svako n*, a ne samo za $n = 3$.

To je također jedan put kako se može *pristupiti uvođenju determinanata*. Tu se vidi opet kako broj 0 može imati važnu ulogu.

12. DETERMINANTA MATRICA PORETKA (ω, ω)

Ako imamo kvadratnu matricu a beskonačnog stupnja:

$$a = \begin{bmatrix} a_{11} & a_{12} & \cdots \\ a_{21} & a_{22} & \cdots \\ \cdot & & \\ \cdot & & \\ \cdot & & \end{bmatrix} \tag{1}$$

tada se pripadna determinanta uvodi *graničnim postupkom*: Definira se

$$\det a = \lim_{n\to\infty} \begin{vmatrix} a_{11} & a_{12} & a_{1n} \\ \cdot\cdot\cdot\cdot\cdot\cdot & & \\ \cdot\cdot\cdot\cdot\cdot\cdot\cdot & & \\ a_{n1} & a_{n2} & a_{nn} \end{vmatrix},$$

ukoliko je ovaj limes određen (može on biti $+\infty$ kao i $-\infty$).

Npr. za δ-matricu: $\delta_i^k = \begin{matrix} 1 \text{ za } i=k \\ 0 \text{ za } i\neq k \end{matrix}$

imamo

$$\det \delta = \lim \det 1_k = 1.$$

Za svaku dijagonalnu beskonačnu matricu imamo

$$\det \operatorname{diag} [a_{11}, a_{22}, \ldots] = \prod_{n=1}^{\infty} a_{nn}.$$

13. GEOMETRIJSKO ZNAČENJE DETERMINANTE KONAČNOG REDA

13.1. Uvodna razmatranja. Polazimo od bilo koje kvadratne matrice a tipa (n, n); dokazat ćemo da $\det a$ ima značenje volumena kvadra od n dimenzija u euklidskom koordinatnom prostoru od n dimenzija. Stvar je prirodno proširenje onog što smo naučili u pogl. 9, § 1.10 za slučaj $n=2$. Dokaz ćemo provesti induktivno. Premda bi razmatranja ovog paragrafa trebalo staviti u poglavlje 13, § 2 u kojem se govori o elementarnim razmatranjima o geometrijskim vektorima, ipak zbog cjelovitosti stvar stavljamo u poglavlje o determinantama jer čitalac zna toliko o vektorima (v. također 13 § 4.7.2).

13.2. Pojam kvadra. Očigledno paralelogram kojemu su OA_1, OA_2 susjedne stranice sastavljen je od svih tačaka Euklidovog prostora za koje je radijus-vektor $\overrightarrow{OT}$ linearna kombinacija radijus-vektora $\overrightarrow{OA_1}$, $\overrightarrow{OA_2}$ a s koeficijentima iz odreska $R[0, 1]$ realnih brojeva koji su $\geqq 0$ i $\leqq 1$ tj.

$$\overrightarrow{OT} = x_1 \overrightarrow{OA_1} + x_2 \overrightarrow{OA_2}.$$

Analogno u koordinatnom prostoru R^n od n dimenzija (npr. za $n=3,4$) i bilo kojih m radijus-vektora $\overrightarrow{OA_1}$, $\overrightarrow{OA_2}, \ldots,$ $\overrightarrow{OA_m}$ definiramo:

13.2.1. Definicija kvadra. *Paralelepiped ili kvadar s bridovima* (*ivicama*) $\overrightarrow{OA_1}, \overrightarrow{OA_2}, \ldots, \overrightarrow{OA_m}$ *jest skup* $K(O, A_1, \ldots, A_m)$ *svih tačaka* T *prostora* R^n *za koje vrijedi*

$$\overrightarrow{OT}=x_1\cdot\overrightarrow{OA_1}+x_2\cdot\overrightarrow{OA_2}+\cdots+x_m\cdot\overrightarrow{OA_m} \text{ i } x_\mu\in R[0,\ 1],\ \mu=1,\ 2,\ldots,\ m.$$

13.2.2. Definicija volumena kvadra. Volum ili n-dimenzionalnu mjeru μ_n paralelepipeda ili *kvadra* $K(O, A_1, A_2, \ldots, A_n)$ definiramo kao produkt $(n-1)$-dimenzijalne mjere „baze" $K'_n=K_{n-1}$ $(O, A_1, A_2, \ldots, A_{n-1})$ i razdaljine $A'_n A_n$ te baze i tačke A_n; pri tom nam A'_n označuje ortogonalnu projekciju od A_n na pomenutu bazu K'_n. (v. 13 § 4.7.2).

13.3. *Matrica* a *i njeni vektori* $a_{.\nu}$ *i pripadni kvadar.*

Teorem. *Neka je* $a=[a_{.1}, a_{.2}, \ldots, a_{.n}]$ *kvadratna matrica poretka* (n, n); *ona dakle ima* n *redaka* $a_{n'}$. *i* n *stupaca* $a_{.n'}$. *Shvatimo stupce* $a_{.n'}$ $(n'=1, 2, \ldots, n)$ *kao radijus-vektore* $\overrightarrow{OA_{n'}}$ *u prostoru* R^n. *Promatrajmo kvadar* K *što ga određuju ti radijus-vektori* $a_{.n'}$; *tada* $\det a$ *označuje* μ_n *toga kvadra* K.

Zapravo ćemo dokazati da je $\det(a^T a)=\mu_n{}^2$ što zbog $\det a^T=\det a$ (isp. 11, § 5.1) znači da je $(\det a)^2=(\mu_n)^2$ i da je apsolutna vrijednost od $\det a$ jednaka apsolutnoj vrijednosti mjere μ_n.

13.4. Dokaz da je $\det(a^T a)=\mu_n{}^2$.

Ako u prostoru R^n imamo bilo koji vektor $\vec{v}$ s komponentama $v_1, v_2, \ldots, v_n$,

tada je $v^T\vec{v}=[v_1,\ v_2, \ldots,\ v_n]\cdot\begin{bmatrix} v_1 \\ v_2 \\ \cdot \\ \cdot \\ \cdot \\ v_n \end{bmatrix}=v_1^2+v_2^2+\cdots v_n{}^2=$ kvadrat

dužine toga vektora $\vec{v}$. Dakle je teorem istinit za jednodimenzionalni kvadar. Pretpostavimo da je teorem istinit za svaki kvadar koji je određen sa manje od n vektorâ; dokažimo da je teorem istinit i za svaki kvadar K određen sa n vektorâ.

Sa A_n' označili smo projekciju tačke A_n na bazu $OA_1A_2\cdots A_{n-1}$; imamo

$$a_{.n}=\overrightarrow{OA_n}=\overrightarrow{OA'_n}+\overrightarrow{A'_nA_n}; \tag{1}$$

vektor $\overrightarrow{A_n'A_n}=\vec{v}$ okomit je na $a_{.1}, a_{.2}, \ldots, a_{.n-1}$ tj. skalarni produkt od $\vec{v}$ i $a_{.k}$ je 0 za $k=1, 2, \ldots, n-1$:

$$a_{.k}\circ\vec{v}=0 \text{ za } k=1, \ldots, n-1. \tag{2}$$

S druge strane, vektor $\overrightarrow{OA'}_n$ je linearna kombinacija vektorâ $a_{.1}, \ldots, a_{.n-1}$ tj. postoji niz brojeva $\lambda_i \in R$ za koje je

$$\overrightarrow{OA'}_n = \lambda_1 \cdot \overrightarrow{OA}_1 + \cdots + \lambda_{n-1} \cdot \overrightarrow{OA}_{n-1}. \tag{3}$$

Rástavi (1) i (3) daju

$$\det a = \det [a_{.1},\ a_{.2}, \ldots,\ a_{.n-1},\ a_{.n}] = \det [a_{.1}\ a_{.2} \cdots a_{.n-1}\ \overrightarrow{OA'}_n + \overrightarrow{A'_n A_n}]$$

$$= \det [b,\ \overrightarrow{OA}_n + \overrightarrow{A'_n A_n}],\ \text{gdje je}\ b = [a_{.1}\ a_{.2} \cdots a_{.n-1}].$$

Prema aditivnom svojstvu determinante posljednji izraz za $\det a$ postaje

$$\det a = \det [b,\ \overrightarrow{OA'}_n] + \det [b,\ \overrightarrow{A'_n A_n}]. \tag{4}$$

No zbog (3) imamo

$$\det [b,\ \overrightarrow{OA'}_n] = \det [b, \sum_{i=1}^{n-1} \lambda_i \cdot \overrightarrow{OA}_i] =$$

(zbog linearnosti operatora det; isp. § 3)

$$= \sum_{i=1}^{n-1} \lambda_i \det [b,\ \overrightarrow{OA}_i] = 0,$$

jer kvadratna matrica $[b,\ \overrightarrow{OA}_i]$ ima i-ti i n-ti stupac jednak.

Prema tome, formula (4) postaje

$$\det a = \det [b,\ \vec{v}],\ \text{gdje je}\ \vec{v} = \overrightarrow{A'_n A_n}. \tag{5}$$

Iz ove jednakosti izlazi

$$\det a^T = \det [b,\ \vec{v}]^T. \tag{6}$$

Izmnožimo međusobno jednadžbe (5), (6) i primijenimo svojstvo distributivnosti od *det* prema množenju matrica; izlazi

$$\det (a^T\ a) = \det [b,\ \vec{v}]^T\ [b,\ \vec{v}]. \tag{7}$$

No, produkt matrice $[b\ \vec{v}]^T$ i matrice $[b\ \vec{v}]$ je matrica

$$c = \begin{bmatrix} b^T b & 0 \\ 0 & \vec{v}^T \vec{v} \end{bmatrix} \tag{8}$$

kojoj je $c_{n\,n} = \vec{v}^T \vec{v} = \overrightarrow{A'_n A_n} \circ \overrightarrow{A'_n A_n} = \overline{A'_n A_n}^2$; matrica $b^T b$ je podmatrica produkta c i dobije se tako da se u c precrta n-ti tj. posljednji redak i n-ti stupac; na preostalim poljima matrice c dolaze 0 (prema formulama (2)).

Iz (7) i (8) dobijemo

$$\det(a^T a) = \det\begin{bmatrix} b^T b, & 0 \\ 0 & \overline{A_n' A_n}^2 \end{bmatrix} =$$

(razviti determinantu po posljednjem stupcu!)

$$= \det(b^T b) \cdot \overline{A'_n A_n}^2. \quad \text{Dakle je}$$

$$\det(a^T a) = \det(b^T b) \cdot \overline{A'_n A_n}^2. \tag{9}$$

No, $\det a^T = \det a$; s druge strane, prema pretpostavci $\det(b^T b)$ znači kvadrat mjere μ_{n-1} baze B; prema tome, (9) postaje

$$(\det a)^2 = \text{kvadrat baze} \cdot \text{kvadrat visine} = (\text{baza} \cdot \text{visina})^2 = (\mu_n)^2.$$

Dakle je

$$(\det a)^2 = \mu_n^2, \text{ za čim smo i išli.}$$

Na analogan način dokazujemo

—→ **13.5.** Teorem. *Za svaku realnu matricu a poretka* (s, n) *gdje su* s, n *prirodni brojevi predstavlja broj* $\det(a^T a)$ *kvadrat n-dimenzionalnog volumena kvadra što ga određuju radijus-vektori* $a_{.1}, a_{.2}, \ldots, a_{.n}$ *u Euklidovu koordinatnom prostoru* R^s *s ortonormiranom bazom.*

13.6. O predznaku determinante. Malo prije smo u nizu vektorâ $\overrightarrow{OA_\nu}$ $(\nu = 1, 2, \ldots, n)$ istaknuli posljednji vektor $\overrightarrow{OA_n}$, uklonili ga i promatrali bazu K'_n kao kvadar od preostalih vektora. Ako umjesto $\nu = n$ promatramo bilo koji broj ν u nizu $1, 2, \ldots, n$, dobit ćemo analogno kvadar K'_ν koji određuju vektori $\overrightarrow{OA_i}$ $(i = 1, 2, \ldots, \nu-1, \nu+1, \ldots n)$; uzmemo li K_ν' kao bazu, tada će visina biti $\overline{A_\nu A_\nu'}$. Međutim, ovaj slučaj svodi se na prethodni slučaj: dovoljno je provesti transpoziciju vektorâ $\overrightarrow{OA_\nu}$ i $\overrightarrow{OA_n}$; time doduše determinanta prijeđe u suprotnu vrijednost, no kvadrat determinante ostaje nepromijenjen i opet znači kvadrat volumena V paralelepipeda K_n kojem je baza K_ν' a visina $\overline{A_\nu' A_\nu}$.

Inače, ako je $V \neq 0$ te ako je orijentacija n-torke vektorâ $\overrightarrow{OA_1}, \ldots, \overrightarrow{OA_n}$ ista kao i orijentacija osnovnih n koordinatnih vektora, onda je $VK_n > 0$; i obrnuto, ako je $\det[\overrightarrow{OA_1}, \ldots, \overrightarrow{OA_n}] < 0$, bit će orijentacija n-torke vektorâ $\overrightarrow{OA_1}, \ldots, \overrightarrow{OA_n}$ protivna orijentaciji prostora R^n pomoću njegovih osnovnih specijalnih vektorâ koji stoje u stupcima jedinične matrice poretka (n, n).

13.7. *Poopćenje Pitagorina teorema.* Dovedemo li teorem 13.5 u vezu s teoremom 9.9.1. dolazimo do

⟶ **T e o r e m a (Poopćen Pitagorin teorem):** ***Kvadrat n-dimenzionalne mjere*** $\mu_n K$ ***paralelepipeda ili kvadra K koji određuju vektori*** $b_{.\nu}$ ***matrice*** $b_{(s,n)}$, ***za slučaj*** $s > n$, ***jednak je sumi kvadratâ n-dimenzionalnih mjera svih projekcijâ*** K_n ***što se dobijaju projicirajući ortogonalno kvadar K na sve n-dimenzionalne koordinatne prostore*** $\left(\text{***ima ih***}\ \binom{s}{n}\right)$.

Slučaj $n=1$, $s=2$ odnosno $n=1$, $s=3$ daje Pitagorin teorem o kvadratu dijagonale kvadrata odnosno kocke.

13.8. H a d a m a r d o v t e o r e m.[1] (isp. § 14.21). *Za svaku kvadratnu matricu a s realnim vrijednostima vrijedi*

$$\text{(H)} \qquad \det a \leq r_1 r_2 \cdot \cdots r_n \text{ gdje je } r_\nu = +(a_{1\nu}^2 + a_{2\nu}^2 + \cdots + a_{n\nu}^2)^{1/2}$$
$$(\nu = 1,\ 2, \ldots,\ n).$$

Kada se zna da det a predstavlja mjerni broj za volumen kvadra što ga određuju radijus-vektori $a_{.1}$, $a_{.2}, \ldots,$ $a_{.n}$ i da je r_ν dužina tog vektora, onda je prethodna Hadamardova nejednakost očigledna jer iskazuje da je volumen kvadra, kod kojega su zadane veličine bridova, maksimalan onda ako su mu osnovni bridovi dva po dva međusobno okomita. Naime, izraz det a tj. $(H)_1$ predstavlja volumen kvadra bridovâ $a_{.1}$, $a_{.2}, \ldots$; sa druge strane predstavlja $(H)_2$ volumen onog kvadra kad su bridovi međusobno okomiti i po redu jednaki r_1, $r_2, \ldots,$ r_n.

14. Zadaci o determinantama (opredjeliteljima) i njihovim izračunavanjima

Gledaj opet zadatke u pogl. 9 § 1,11, § 3.5, § 4.7; te pogl. 11. § 8.8 i § 10.8. Posebno ispitaj koji su od tih promatranih opredjelitelja singularni a koji regularni.

1. Provjeri:

$$1)\ \begin{vmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & a^2 & b^2 \\ 1 & a^2 & 0 & c^2 \\ 1 & b^2 & c^2 & 0 \end{vmatrix} = -(a+b+c)(b+c-a)+(c+a-b)(a+b-c)$$

$$2)\ \begin{vmatrix} x & a & b & c \\ a & x & 0 & 0 \\ b & 0 & x & 0 \\ c & 0 & 0 & x \end{vmatrix} = x^2(x^2-a^2-b^2-c^2).$$

2. Napiši nekoliko 1) skalarnih; 2) dijagonalnih; 3) dijadskih; 4) trokutnih kvadratnih matrica pa im odredi determinantu.

---

[1] J. Hadamard [Adamard] (1865—1963), vrlo poznat francuski matematičar.

3. U kvadratnoj matrici

$$a=\begin{bmatrix} 5 & 3 & -2 & 4 & 6 \\ 1 & 2 & 3 & 2 & 1 \\ 3 & 4 & 5 & -7 & 2 \\ 4 & 5 & 2 & -7 & 3 \\ 1 & 2 & 3 & 6 & 8 \end{bmatrix}$$

odredi: 1) podmatrice a_3^4, $a_{1\,3}^{5\,4}$, $a_{1\,3\,5}^{2\,4\,5}$ te njihove algebarske minore i algebarske komplemente; 2) nađi det a razvijajući po prva dva stupca; u drugi redić uvesti svuda 0 osim na polje (2, 1); 4) oko polja (1, 1) provesti kondenzaciju stupaca; 5) oko polja (1, 1) provesti kondenzaciju (zgušnjavanje) redaka.

4. Nađi Vandermondeovu matricu i determinantu koje pripadaju vektoru

1) $[2, 3]^T$; 2) $[3, -2, 4]^T$; 3) $[1, 1, 1, 1]^T$; 4) $[a, a+h, a+2h, a+3h]^T$; 5) $[a, a^2, a^3, a^4]^T$; 6) $[1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}]^T$, gdje je $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ (isp. zad. 21.1).

4'. Neka je $v=[a, b, c, d]^T$ provjeri: 1) $\det[\vec{1}, \vec{v}, \vec{v^2}, \vec{v^3}]=(b-a)(c-a)(d-a)(c-b)(d-b)(d-c)$; 2) $\det[\vec{1}, \vec{v}, \vec{v^2}, \vec{v^4}]=(a+b+c+d)(a-b)(a-c)(a-d)(b-c)(b-d)(c-d)$; 3) $\det[1, v, v^3, v^4]=(ab+ac+ad+bd+cd)(a-b)(a-c)(a-d)\cdot(b-c)(b-d)(c-d)$;

4) $\det[\vec{1}, \vec{v^2}, \vec{v^3}, \vec{v^4}]=(abc+abd+acd+bcd)(a-b)(a-c)(a-d)(b-c)(b-d)(c-d)$.

5. Dokaži $(V_n(x_1\, x_2 \cdots x_n))^2 \equiv \begin{vmatrix} 1 & x_1 & x_1^2 \cdots x_1^{n-1} \\ 1 & x_2 & x_2^2 \cdots x_2^{n-1} \\ \cdot & & \\ \cdot & & \\ \cdot & & \\ 1 & x_n & x_n^2 \cdots x_n^{n-1} \end{vmatrix}^2 =$

$$= \begin{vmatrix} s_0 & s_1 & s_2 \cdots s_{n-1} \\ s_1 & s_2 & \cdots s_n \\ s_2 & s_3 & \cdots \cdot \\ & & \cdot \\ & & \cdot \\ s_{n-1} & s_n & \cdots s_{2(n-1)} \end{vmatrix} = \prod_{i<k=1}^{n} (x_i - x_k)^2 \text{ gdje je } s_k = x_1^k + x_2^k + \cdots x_n^k.$$

6. *Cikličke determinante.* To su determinante kod kojih je svaki redić ciklička permutacija svojeg prethodnika. Prema tome, za cikličku determinantu imamo $c_{(k+1)}=c_{k2}$, $c_{k3}\ldots$.

Dijagonala je konstanta 0.

Za neki niz ν neka $\gamma\nu$ označuje cikličku determinantu u kojoj je taj niz ν prvi redić.

1) Dokaži da produkt dviju cikličkih determinanata istog reda daje opet cikličku determinantu (ne praveći pitanja od faktora ± 1).

2) Dokaži da je: $\gamma\left(\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n}\right) = 0$

za neparno n, $= (-1)^{\frac{n}{2}} 2^n$ za parno n.

7. Dokaži: 1) $\begin{vmatrix} 1 & 1 & \cdots & 1 \\ \binom{m}{1} & \binom{m+1}{1} & \cdots & \binom{m+n}{1} \\ \binom{m+1}{2} & \binom{m+1}{2} & \cdots & \binom{m+n+1}{2} \\ \cdots & \cdots & \cdots & \cdots \\ \binom{m+n-1}{n} & \binom{m+n}{n} & \cdots & \binom{m+2n+1}{n} \end{vmatrix} = 1;$

2) Napisati matricu a poretka $1+r$ za koju je $a_{ik} = \binom{m+i-1}{p+k-1}$ $(i,\ k = 1,\ 2, \ldots,\ r+1)$ i dokazati da je

$$\det a = \frac{\binom{m+r}{r+1}\binom{m+r-1}{r+1} \cdots \binom{m+r-p+1}{r+1}}{\binom{p+r}{r+1}\binom{p+r-1}{r+1} \cdots \binom{r+1}{r+1}};$$

obraditi posebno slučaj $m = 4,\ p = 3,\ r = 3$.

3) $\begin{vmatrix} \binom{m}{1} & 1 & 0 & \cdots & 0 \\ \binom{m}{2} & \binom{m}{1} & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & & 0 \\ \cdot & \cdot & \cdot & & \vdots \\ \cdot & \cdot & \cdot & & 1 \\ \binom{m}{k} & \binom{m}{k-1} & \binom{m}{k-2} & \cdots & \binom{m}{1} \end{vmatrix} = \binom{m+k-1}{k}$

4) $$\begin{vmatrix} \frac{1}{1!} & 1 & 0 & \cdots & 0 \\ \frac{1}{2!} & \frac{1}{1!} & 1 & & \vdots \\ \vdots & \frac{1}{2!} & \frac{1}{1!} & & 0 \\ \frac{1}{n!} & \frac{1}{(n-1)!} & \frac{1}{(n-2)!} & \cdots & \frac{1}{1!} \end{vmatrix} = \left(\frac{1}{n!}\right)$$

8. (*Gauss-Chiò-ov postupak*). Obrazac (2) u § 11.4. dokazati i tako da matricu a pomnožimo sa

$$\begin{bmatrix} a_{11} & -a_{12} & \cdots & -a_{1n} \\ & & & \\ & a_{11} & & \\ & & & \\ & & & a_{11} \end{bmatrix}$$

Na osnovu gornjeg obrasca izračunati vrijednost zadane determinante

$$\text{npr.} \quad \begin{vmatrix} 3 & 5 & -2 & 7 \\ 4 & -1 & 5 & 6 \\ 8 & 4 & 0 & 3 \\ 2 & 1 & 4 & 5 \end{vmatrix}.$$

9. (*Voigtov obrazac*). Dokaži

$$\begin{vmatrix} a+b\,i, & c+d\,i, \ldots \\ a_1+b_1\,i, & c_1+d_1\,i, \ldots \\ \cdots & \cdots \end{vmatrix} \cdot \begin{vmatrix} a-b\,i, & c-d\,i, \ldots \\ a_1-b_1\,i, & c_1-d\,i, \ldots \\ \cdots & \cdots \end{vmatrix} =$$

$$= \begin{vmatrix} a & b & c & d & \cdots \\ -b & a & -d & c & \cdots \\ a_1 & b_1 & c_1 & d_1 & \cdots \\ -b_1 & a_1 & -d_1 & c_1 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{vmatrix};$$

matrice prve i druge determinante međusobno su konjugirane. Uočite vezu

$$a+b\,i \Leftrightarrow \begin{bmatrix} a & b \\ -b & a \end{bmatrix}.$$

10. Neka je $$A=\begin{vmatrix} a_1 & b_1 \\ a_2 & a_2 \end{vmatrix}, \qquad B=\begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix},$$

$$C=\begin{vmatrix} Ax_1 & Ay_1 & Az_1 \\ Ax_2 & Ay_2 & Az_2 \\ Ax_3 & Ay_3 & Az_3 \end{vmatrix}=\begin{vmatrix} a_1x_1 & b_1x_1 & a_1y_1 & b_1y_1 & a_1z_1 & b_1z_1 \\ a_2x_1 & b_2x_1 & a_2y_1 & b_2y_1 & a_2z_1 & b_2z_1 \\ a_1x_2 & b_1x_2 & a_1y_2 & b_1y_2 & a_1z_2 & b_1z_2 \\ a_2x_2 & b_2x_2 & a_2y_2 & b_2y_2 & a_2z_2 & b_2z_2 \\ a_1x_3 & b_1x_3 & a_1y_3 & b_1y_3 & a_1z_3 & b_1z_3 \\ a_2x_3 & b_2x_3 & a_2y_3 & b_2y_3 & a_2z_3 & b_2z_3 \end{vmatrix}.$$

Dokazati da je $C=A^3B^2$. Općenito, neka su a i b kvadratne matrice reda (α, α) odnosno (β, β); tada je određena matrica

$$C=\begin{bmatrix} ab_{11} & ab_{12} & \cdots & ab_{1\beta} \\ ab_{21} & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ ab_{\beta 1} & \cdot & \cdots & ab_{\beta\beta} \end{bmatrix};$$

ona je kvadratna s oblasti $(\alpha\beta, \alpha\beta)$; dokazati da je

$$\det c=(\det a)^{\beta}(\det b)^{\alpha}.$$

11. Neka je a kvadratna matrica reda n; neka je a_{ik} kvadratna matrica reda m s vrijednostima a_{ikrs} $(r, s=1, 2, \ldots, m)$; time se dobije matrica B s komponentama a_{ikrs} $(i, k \in 1(n), r, s \in 1(m))$; neka je C matrica koja se dobije tako da se a_{ik} u razvoju $\det a$ zamijeni matricom $[a_{ikrs}]_{r,s}$ reda m; dokaži da je $\det B=\det C$ ukoliko su kljetke a_{ik} komutativne matrice. Ilustriraj stvar na jednostavnom primjeru.

12. 1) $$\begin{vmatrix} \operatorname{coses} x & 1 & & & \\ 1 & 2\operatorname{cosec} x & 1 & & \\ & 1 & \cdot & & \\ & & & \cdot & \\ & & & & 2\operatorname{cosec} x \end{vmatrix}=\frac{1}{2}\left(\operatorname{tg}^n\frac{x}{2}+\operatorname{ctg}^n\frac{x}{2}\right);$$

2) $$\begin{vmatrix} \cos\alpha & 1 & & & \\ 1 & 2\cos\alpha & 1 & & \\ & 1 & \cdot & \cdot & \\ & & \cdot & \cdot & \cdot \\ & & & 1 & 2\cos\alpha \end{vmatrix}=\cos n\alpha;$$

3) $$\begin{vmatrix} 2\cos\alpha & 1 & & & \\ 1 & 2\cos\alpha & 1 & & \\ & 1 & \cdot & \cdot & \\ & & \cdot & \cdot & \cdot \\ & & & 1 & 2\cos\alpha \end{vmatrix} = \frac{\sin(n+1)\alpha}{\sin\alpha}$$

13. 1) Dokaži da tačke (x_1, y_1), (x_2, y_2), (x_3, y_3) Euklidske ravnine određuju trokut kojemu je ploština $P = \begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_2 & y_2 & 1 \end{vmatrix}$.

2) Ako su a, b, c dužine stranica trokuta, tada je

$$16\,P^2 = -\begin{vmatrix} 0 & a & b & c \\ a & 0 & c & b \\ b & c & 0 & a \\ c & b & a & 0 \end{vmatrix} = (a+b+c)(a+b-c)(b+c-a)(c+a-b).$$

3) Pravci $A\,x + B\,y + C = 0$
$A'\,x + B'\,y + C' = 0$
$A''x + B''y + C'' = 0$ određuju trokut za koji je

$$2\,P = \frac{\begin{vmatrix} A & B & C \\ A' & B' & C' \\ A'' & B'' & C'' \end{vmatrix}^2}{\begin{vmatrix} A & B \\ A' & B' \end{vmatrix} \cdot \begin{vmatrix} A' & B' \\ A'' & B'' \end{vmatrix} \cdot \begin{vmatrix} A'' & B'' \\ A & B \end{vmatrix}}.$$

4) Za trokut sa stranicama x, y, z upisan u elipsu $a^2x^2 + a^2y^2 = a^2b^2$ vrijedi $4\,P = ab \cdot \frac{x}{x'}\frac{y}{y'}\frac{z}{z'}$; tu su x', y', z', poluprečnici elipse koji su paralelni sa stranicom x odnosno y odnosno z.

5) Za ploštine P, P' trokuta A_1, A_2, A_3 i trokuta A_1', A_2', A_3' vrijedi

$$-16\;PP' = \begin{vmatrix} 0 & 1 & 1 & 1 \\ 1 & & & \\ 1 & & d^2_{ik} & \\ 1 & & & \end{vmatrix}, \text{ gdje je } d_{ik} = \overline{A_i\,A'_k}.$$

14. 1. 1) Tačke (x_i, y_i), $(i = 1, 2, 3)$ određuju kružnicu

$$\begin{vmatrix} x^2+y^2 & x & y & 1 \\ x_i^2+y_i^2 & x_i & y_i & 1 \\ \cdot & \cdot & \cdot & \cdot \end{vmatrix} = (i = 1, 2, 3).$$

1. 2) Četiri tačke T_1, T_2, T_3, T_4 leže na istoj kružnici onda i samo onda ako je

$$(\det [(1-\delta_{ik})\,\overline{T_i\,T_k}^2]=0.$$

Ispisati tu matricu i tu determinantu.

2. 1) Četiri tačke $(x_i,\ y_i,\ z_i)$ određuju loptu [1]

$$\begin{vmatrix} x^2+y^2+z^2, & x, & y, & z, & 1 \\ \cdot & \cdot & \cdot & \cdot & \\ x_i^2+y_i^2+z_i^2 & x_i, & y_i, & z_i & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix} = 0\ (i=1,\ 2,\ 3,\ 4)$$

2. 2) Pet tačaka T_5, leže na istoj lopti onda i samo onda ako je $\det\left[(1-\delta_{ik})\,\overline{T_i\,T_k}^2\right]=0$; ispiši tu matricu i determinantu.

2. 3) Poopći na prostore od n dimenzija.

15. *Sinus trijedra.* Zadane su zrake OA_1, OA_2, OA_3 i pripadni kutovi $\alpha_1=\sphericalangle A_2OA_3$, $\alpha_2=\sphericalangle A_3OA_1$, $\gamma=\sphericalangle A_1OA_2$. Dokaži da pripadni jedinični kvadar ima volumen V za koji je $V^2=|\cos(A_iOA_k)|=\Delta$. Dokaži da tetraeder $OA_1\,A_2\,A_3$ ima zapreminu $\frac{1}{6}\overline{OA_1}\cdot\overline{OA_2}\cdot\overline{OA_3}\cdot\Delta^{1/2}$; izraz Δ^2 zove Staudt sinusom triedra po analogiji kako je građena gornja formula za sadržinu tetraedra i formula $\frac{1}{2}\,ab\sin\gamma$ za ploštinu trokuta.

16. *Kubna jednadžba i determinante.*

Najprije polinom x^3-1 ima nula-mjesta: 1, J, J^2 gdje je

$$J=-\frac{1}{2}+\frac{i}{2}\,3^{1/2}.$$

Promatrajmo kubni polinom

$$k(x)=\begin{vmatrix} x & a & b \\ b & x & a \\ a & b & x \end{vmatrix}=x^3-3\,abx+(a^3+b^3);$$

pripadna matrica je građena jednostavno: dijagonala je konstanta x, a redići su građeni jednostavno pomoću cikličkih permutacija.

Očigledno je $k=|k_{.1}+k_{.2}\,z+k_{.3}\,z^2,\ k_{.2},\ k_{.3}|$; to vrijedi za svaki broj z pa i specijalno za $z\in\{1,\ J,\ J^2\}$; ako u posljednjoj determinanti drugi redić pomnožimo za z^2, a treći sa z, značit će to da se determinanta množi sa z^3 dakle sa 1 pa se zato ni ne mijenja; no time

[1] Razlikujemo kuglu i loptu koja je omeđenje kugle!

prvi stupac postaje $x+az+bz^2$ pa taj izraz možemo izlučiti i dobiti

$$k=(x+az+bz^2)\begin{vmatrix} 1 & a & az^2 \\ 1 & xz^2 & az^2 \\ 1 & bz & xz \end{vmatrix}.$$

Drugim riječima $k(x)$ je djeljivo sa $x+az+bz^2$ za $z=1$, J, J^2; time se dobije faktorizacija

$$k(x)=(x+a+b)(x+aJ+bJ^2)(x+aJ^2+bJ).$$

Prema tome *polinom* $x^3-3abx+a^3+b^3$ *ima brojeve* $-a$ $-b$, $-aJ$ $-bJ^2$, $-aJ^2$ $-bJ$ *kao svoja nula-mjesta.*

Ako imamo kubni reducirani izraz x^3+px+q, tada se on svodi na posebni oblik (1) pomoću

$$-3ab=p,\quad a^3+b^3=q;$$

odatle se pomoću zadanih veličina p, q odrede parametri a, b.

Riješi na taj način kubne jednadžbe iz poglavlja 5, § 6.9.

17. 1) Promatraj beskonačnu matricu b za koju je $b_{ii}=1$, $b_{ik}=i^{-2}\cdot k^{-2}$ za $i\neq k$; dokaži da je $\det b$ određen broj.

2) Neka za niz $\vec{v}=[v_1, v_2\cdots]^T$ vrijedi $|v_n|<q<1/2$ skoro za svako n; tada je $\det[\vec{1}, \vec{v}, \vec{v}^2, \ldots]=0$; tu $\vec{1}$ označuje beskonačan niz od samih jedinica ispisanih u jedan stupac.

18. *Pridružena matrica* (взаимная матрица) kvadratne matrice a ili *komatrica* nastaje tako da se umjesto a_{ik} piše kofaktor fa_{ik}; možemo je označiti sa fa. Dokazati:

1) $\det a\cdot\det(fa)=(\det a)^n$;

2) $f(fa)=(\det a)^{n-2}\cdot a$; specijalno $f(fa)=a$ za $n=2$;

3) $f(ab)=fa\cdot fb$.

4) Algebarski komplement m-og reda matrice fa jednak je produktu $(\det a)^{m-1}$ i dopunbenog minora odgovarajućeg minora u matrici a.

19. Prisjedinjena (asocirana) matrica ili adjunkta matrice x, simbolički Ax ili x^Γ jest matrica za koju je $(Ax)_{ij}=fx_{ji}$ (pazi na redoslijed indeksa!). To znači da se Ax dobije iz x tako da se svaka komponenta x_{ij} zamijeni sa fx_{ji}, gdje je fx_{ji} algebarski komplement od x_{ji}. (v. pogl. 12. § 4.2). Dokaži ovo:

1) $x\cdot Ax=Ax\cdot x=\operatorname{diag}(\det x)$.

2) $A(Ax)=(\det x)^{n-2}x$, specijalno $A(Ax)=x$, ako je oblast matrice x jednaka (2, 2).

3) $A(xy)=Ay\cdot Ax$.

20. *Kroneckerov* ili *direktni produkt* (Kroneker). Neka su a, b dvije matrice oblasti (k, n); neka je (1) $w_1\ w_2, \ldots, w_{kn}$ niz bez ponavljanja svih uređenih dvojki (k', n'); tada se pod direktnim ili Kronekerovim produktom razumijeva matrica $a \times b = c$ oblasti (k, n) za koju je $(a \times b)_{ij} = a_{w_i}\ b_{w_j}$ (imajmo na umu da za svako $i, j = 1, 2, \ldots, k \cdot n$ oznaka a_{w_i} odnosno b_{w_j} stoji za posve određenu komponentu matrice a odn. matrice b; zato c_{ij} prolazi umnoščima svakog $a_{k'n'}$ sa svakim b_{rs}). Dokazati:

1) $(a+b) \times c = a \times c + b \times c$;

2) $(a \times (b+c) = a \times b + a \times c$;

3) $(ab \times (cd) = (a \times c)\,(b \times d)$;

4) $\det (a \times b) = (\det a)^{D_1 b}\ \det b^{D_1 a}$.

21. (Isp. § 13.8.) Neka je kvadratna matrica a poretka (n, n), n je prirodan broj; 1) ako su a_{ik} kompleksni brojevi kojima je apsolutna vrijednost $\leq M$, tada je $|\det a| \leq M^n n^{1/2}$; nađite supremum svih takvih brojeva $\det a$ i dokažite da je on upravo $M^n n^{1/2}$ (isp. zad. 4.6); 2) ako je $0 \leq a_{ik}$, tada je $|\det a| \leq M^n 2^{-n} (n+1)^{\frac{(n+1)}{2}}$; 3) ako je $-1 \leq a \leq 1$, tada 2^{n-1} dijeli broj $S_n = \sup |\det a|$; naći S_n za $n = 1, 2, 3, 4, 5$.

22. Dokaži:

$$\det_{(n,n)} (a+b)_{(n,n)} = \sum_p \det [c_{\cdot p_1} c_{\cdot p_2} \cdots c_{\cdot p_n}];$$

tu p prolazi svim preslikavanjima množine $1\,(n)$ tako da bude

$$c_{\cdot p_\nu} \in \{a_{\cdot \nu},\ b_{\cdot \nu}\} \text{ za svako } \nu \in 1\,(n).$$

23. Dokaži: neka je a određena (n, n)-matrica; neka je b isto kao i b' proizvoljna (ν, n)-podmatrica od a; pritom su ν, n prirodni brojevi i $\nu < n$; tada svakoj kombinaciji $K = \{k_1 < k_2 < \cdots < k_\nu\} \subset \{1, 2, \ldots, n\}$ odgovara determinanta $a_K^{D_1 b}$ i njen kofaktor $f a_K^{D_1 b}$ kao i $f a_K^{D_1 b'}$; u § 8.6. (opći Laplaceov teorem) smo dokazali da je

$$\sum_K a_K^{D_1 b} f a_K^{D_1 b} = \det a;\ \text{dokaži da}$$

$$D_1 b \neq D_1 b' \Rightarrow \sum_K (\det a_K^{D_1 b})\, f a_K^{D_1 b'} = 0.$$

24. Dokaži $\det (ab)^{i_1 i_2 \cdots i_\nu}_{j_1 j_2 \cdots j_\nu} = \sum_K \det a_K^{i_1 i_2 \cdots i_\nu} \det b^K_{j_1 j_2 \cdots j_\nu}$ (oznaka kao u zadatku 23).

Literatura: Anđelić [1], Faddejev-Sominski [1], Gavrilović [1], Kowalewski [1], Krečmar [1], Mitrinović [1], Mitrinović—Mihailović [1], Muir [1], Obreškov [1]—[3], Proskurjakov [1].

POGLAVLJE 12.

CRAMEROV TEOREM. INVERZIJA MATRICA

U ovom poglavlju upoznat ćemo se pobliže s Cramerovim teoremom o rješavanju sistema od n linearnih jednadžbi po n nepoznanica (broj nepoznatih veličina jednak je broju zadanih jednadžbi) i to odmah primijeniti da nađemo inverznu vrijednost a^{-1} regularnih kvadratnih matrica a. Oba su problema od osnovne teoretske i praktične vrijednosti.

1. POSTAVLJANJE PROBLEMA

Promatrajmo n linearnih jednadžbi za n veličina $x_1, \cdots, x_{n-1}, x_n$:

$$(1)\qquad \overbrace{\left.\begin{array}{l} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \cdots\cdots\cdots\cdots + a_{2n}x_n = b_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n1}x_1 \cdots\cdots\cdots\cdots\cdots a_{nn}x_n = b_n. \end{array}\right\}}^{n} n$$

Tu se pojavljuju matrice

$$a = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}, \quad x = \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{bmatrix}, \quad b = \begin{bmatrix} b_1 \\ b_2 \\ \cdot \\ \cdot \\ \cdot \\ b_n \end{bmatrix},$$

te matrica $[a, b] = [a_{\cdot 1}, \cdots, a_{\cdot n}, b]$. Matrica a zove se *matrica sistema* (1); $[a, b]$ se zove *proširena matrica sistema* (1).

Sam sistem (1) možemo pisati matrično ovako:

$$(2)\qquad ax = b.$$

Odmah se vidi koliko je matrični način pisanja ekonomičniji i pregledniji.

1.1. *Problem je ovaj: zadano je a, b; treba naći x.* U toj oznaci odmah se postavlja mnogo *općenitiji problem: ako su a, b zadane bilo kakve dvije matrice, pokušajte odrediti matricu x iz veze* (2).

2. CRAMEROV TEOREM

Teorem (G. Cramer, 1750)

2.1. *Iz skupa jednadžbi* **(1)** *za svako* $\nu \in \{1, 2, \ldots, n\}$ *izlazi*

$$\det a \cdot x_\nu = b_1 fa_{1\nu} + b_2 fa_{2\nu} + \cdots + b_n fa_{n\nu} = \det a(\nu); \tag{3}$$

pri tom je $fa_{i\nu} = \det(a \setminus a_{i\nu}) \cdot (-1)^{i+\nu}$, *tj.* $fa_{i\nu}$ *je kofaktor od* $a_{i\nu}$ *u matrici a; nadalje je* $a(\nu)$ *matrica koja iz a nastaje kad joj stupac* $a_{.\nu}$ *zamijenimo stupcem b sistema* (*1*).

Ako je $\det a \neq 0$, *tada je:*

$$x_\nu = \frac{1}{\det a} \sum_{i=1}^{n} b_i fb_{i\nu} \qquad (\nu = 1, 2, \ldots, n) \tag{4}$$

***jedno jedino rješenje sustava* (1).**

2.1.1. Primjedba. *Iz sistema* (1) *proizlazi sistem* (1*) *bez obzira na to da li matrica* $[a, b]$ *zavisi ili ne zavisi od veličinâ* x_ν.

2.1.2. Dokaz Cramerova teorema. Pomnožimo n jednadžbi (1) po redu kofaktorima $fa_{11}, fa_{21}, \cdots, fa_{n1}$ prvog stupca matrice a i zbrojimo tako dobivenih n jednadžbi. Izlazi

$$\begin{aligned}(5_1)\qquad &(a_{11} fa_{11} + a_{21} fa_{21} + \cdots + a_{\nu 1} fa_{\nu 1} + \cdots) x_1 + (a_{12} fa_{11} + \cdots + \\ &+ a_{\nu 2} f_{\nu 1} + \cdots) x_2 + \cdots = b_1 fa_{11} + b_2 fa_{21} + \cdots + b_\nu fa_{\nu 1} + \cdots +,\end{aligned}$$

tj.
$$\sum_{\mu=1}^{n} \left(\sum_{\nu=1}^{n} a_{\nu\mu} fa_{\nu_1} \right) x_\mu = \sum_{\nu} b_\nu fa_{\nu_1}.$$

Prema Laplaceovu pravilu (pogl. 11, § 7.8) koeficijent od x_1 tu je $= \det a$; po istom pravilu koeficijenti ostalih nepoznanica u (5_1) jesu $= 0$; izraz na desnoj strani u (3_1) jest $\det a(1)$, gdje $a(1)$ označuje matricu koja iz matrice a nastaje tako da se stupac $a_{.1}$ uz x_1 u (1) zamijeni stupcem

$$b = \begin{bmatrix} b_1 \\ \cdot \\ \cdot \\ \cdot \\ b_{n-1} \\ b_n \end{bmatrix}.$$

Na taj način jednadžba (3_1) postaje

$$\det a \cdot x_1 = \sum_{i=1}^{n} b_i fa_{i1} = \det a(1). \tag{6_1}$$

Na sličan način (kako?) — shvatite tu 1 kao varijabilan indeks — dobiva se poput (6_1) ovaj sistem jednadžbi:

$$\det a \cdot x_\nu = \sum_{\nu=1}^{n} b_i fa_{i\nu} = \det a(\nu), \tag{6_\nu}$$

gdje je $\nu = 1, 2, \cdots, n$. Time je Cramerov teorem dokazan.

Ako je $\det a \neq 0$, tada je jasno da (3)$\Rightarrow$(4). No, ako pri tom veličine a_{ij}, b_i $(i, j = 1, 2, \cdots, n)$ ne zavise od $x_1, x_2, \cdots x_n$, onda je jasno da su sistemi (3) i (4) međusobno ravnovaljani (ekvivalentni).

Dokažimo još da pri $\det a \neq 0$ veličine (4) zadovoljavaju (1). Stvarno, neka je $k \in \{1, 2, \cdots, n\}$; uvrstimo (4) u lijevu stranu k-te jednačine u (1); imamo

$$\sum_{\nu=1}^{n} a_{k\nu} x_\nu = \sum_{\nu=1}^{n} a_{k\nu} \sum_{j=1}^{n} \frac{b_j f a_{j\nu}}{\det a} = \sum_{j=1}^{n} b_j \frac{\sum_{\nu=1}^{n} a_{k\nu} f a_{j\nu}}{\det a} =$$

(prema Laplace-ovu pravilu 11 § 7.8.)

$$= \sum_{j=1}^{n} b_j \frac{\delta_{kj} \det a}{\det a} = \sum_{j=1}^{n} b_j \delta_{kj} = b_k .$$

Time je Cramerov stavak 2.1. potpuno dokazan.

2.3. Primjer. Zadane su jednadžbe

$$\begin{aligned} x - 2y &= 1 \\ 3x + 4y - z &= 2 \\ -2x + 3z &= -3. \end{aligned} \tag{5}$$

Matrica sistema glasi:

$$a = \begin{bmatrix} 1 & -2 & 0 \\ 3 & 4 & -1 \\ -2 & 0 & 3 \end{bmatrix}, \tag{6}$$

pa je $\det a = 1 \cdot 4 \cdot 3 + (-2 \cdot -2 \cdot -1) - (-2 \cdot 3 \cdot 3) = 26.$

Prema Crameru je

$$26x = \det a(x) = \begin{vmatrix} 1 & -2 & 0 \\ 2 & 4 & -1 \\ -3 & 0 & 3 \end{vmatrix} = (\text{razvijte po trećem retku}) =$$

$$= -3 \cdot 2 + 3 \cdot 8 = 18,$$

tj. $$x = 18/26 = 9/13.$$

$$26y = \det a(y) = \begin{vmatrix} 1 & 1 & 0 \\ 3 & 2 & -1 \\ -2 & -3 & 3 \end{vmatrix} = (\text{razvijte po prvom retku}) = 3 + 7 = 10.$$

$$26z = \det a(z) = \begin{vmatrix} 1 & -2 & 1 \\ 3 & 4 & 2 \\ -2 & 0 & -3 \end{vmatrix} = -14.$$

Traženo je rješenje $x = 9/13$, $y = 5/13$, $z = -7/13$.

3. Specijalan slučaj kad desne strane jednadžbi čine istaknut **jedinični niz.**

3.1. Definicija. *Niz je diadski i jedinični* ako mu je jedan član $=1$, a svi drugi $=0$.

3.1.1. Primjer. Zamijenimo desne strane u primjeru 2.3. po redu jediničnim nizovima 1, 0, 0: zatim 0, 1, 0 i najzad, 0, 0, 1. Prvi slučaj daje sistem

$$\begin{aligned} x-2y &= 1 \\ 3x+4y-z &= 0 \\ -2x+4z &= 0. \end{aligned}$$

Koristeći se podacima iz primjera 2.3. (*determinanta je ista*), imamo

$$26x=\begin{vmatrix} 1 & -2 & 0 \\ 0 & 4 & -1 \\ 0 & 0 & 3 \end{vmatrix} = (\text{razvijajući po prvom stupcu}) = fa_{11}$$

$$(=\text{komplement od } a_{11}) = 12, \quad \text{tj.} \quad 26x = fa_{11} = 12.$$

Isto tako:

$$26y=\begin{vmatrix} 1 & 1 & 0 \\ 3 & 0 & -1 \\ -2 & 0 & 3 \end{vmatrix} = fa_{12} = -7,$$

$$26z=\begin{vmatrix} 1 & -2 & 1 \\ 3 & 4 & 0 \\ -2 & 0 & 0 \end{vmatrix} = fa_{13} = 8.$$

Označujući sa $x_{.1}$ traženi vektor

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix}, \text{ izlazi da je } 26x_{.1} = \begin{bmatrix} fa_{11} \\ fa_{12} \\ fa_{13} \end{bmatrix}.$$

Drugim riječima, iz $ax_{.1} = 1_{.1}$ izlazi u našem primjeru:

$$\det a \cdot x_{.1} = \begin{bmatrix} fa_{11} \\ fa_{12} \\ fa_{13} \end{bmatrix} = fa_{1.},$$

pri tom $fa_{1.}$ označuje *redak algebarskih komplemenata što u matrici a* pripadaju elementima njenog retka $a_{1.}$.

Promatrajmo sada slučaj kad desna strana glasi

$$1_{.2} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix};$$

označujući nepoznanice sa $x_{\cdot 2}$, tj. sa x_{12}, x_{22}, x_{32}, imamo po Crameru:

$$\det a \cdot x_{12} = fa_{21} = 6,\ \det a \cdot x_{22} = fa_{22} = 3,\ \det a \cdot x_{32} = fa_{23} = -4.$$

Drugim riječima, sistem $ax_{\cdot 2} = 1_{\cdot 2}$ ima rješenje

$$x_{\cdot 2} = \frac{1}{26}\begin{bmatrix} 6 \\ 3 \\ -4 \end{bmatrix} = \frac{1}{\det a}\begin{bmatrix} fa_{21} \\ fa_{22} \\ fa_{23} \end{bmatrix} \quad \text{tj.} \quad x_{\cdot 2} = \frac{1}{\det a} fa_{2\cdot}.$$

Analogno iz $ax_{\cdot 3} = 1_{\cdot 3} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$ izlazi $x_{\cdot 3} = \frac{1}{\det a} fa_{3\cdot} = \frac{1}{\det a}\begin{bmatrix} fa_{31} \\ fa_{32} \\ fa_{33} \end{bmatrix} =$

$$= \frac{1}{26}\begin{bmatrix} -2 \\ 1 \\ 10 \end{bmatrix} = \begin{bmatrix} -1/13 \\ 1/26 \\ 5/13 \end{bmatrix}.$$

3.2. Na taj smo način za matricu

$$a = \begin{bmatrix} 1 & -2 & 0 \\ 3 & 4 & -1 \\ -2 & 0 & 3 \end{bmatrix}$$

promatrali tri sistema jednadžbi s *jednom te istom matricom a*, a s desnim stranama $1_{\cdot 2}$, tj.

$$1_{\cdot 1} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad 1_{\cdot 2} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad 1_{\cdot 3} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

Rješenja smo označavali po redu sa

$$x_{\cdot 1} = \begin{bmatrix} x_{11} \\ x_{21} \\ x_{31} \end{bmatrix}, \quad x_{\cdot 2} = \begin{bmatrix} x_{12} \\ x_{22} \\ x_{32} \end{bmatrix}, \quad x_{\cdot 3} = \begin{bmatrix} x_{13} \\ x_{23} \\ x_{33} \end{bmatrix}.$$

Tako dobijemo i matrice

$$[1_{\cdot 1},\ 1_{\cdot 2},\ 1_{\cdot 3}] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \frac{1}{26}\begin{bmatrix} 12 & 6 & -2 \\ -7 & 3 & 1 \\ 8 & -4 & 10 \end{bmatrix} = \begin{bmatrix} x_{11} & x_{12} & x_{13} \\ x_{12} & x_{22} & x_{23} \\ x_{13} & x_{23} & x_{33} \end{bmatrix} =$$

$$(7) \qquad = [x_{\cdot 1}, x_{\cdot 2}, x_{\cdot 3}] = x = \frac{1}{\det a}\begin{bmatrix} fa_{11} & fa_{21} & fa_{31} \\ fa_{12} & fa_{22} & fa_{32} \\ fa_{13} & fa_{23} & fa_{33} \end{bmatrix} = \frac{1}{\det a} f(a)^T.$$

3.3. Lako se provjeri da za gornje matrice a, x u (6) i (7) vrijedi:

(8) $$ax = \textit{jedinična matrica} = \operatorname{diag}(1).$$

To znači da dobivena matrica $(7)_2$ zadovoljava relaciju (8). Označimo li sa fa matricu čiji su elementi fa_{ik}, tada je $(7)_2 = \frac{1}{\det a}(fa)^T$, gdje a^T označuje transponat od a (zamjena odgovarajućih redaka i stupaca). Drugim riječima *za* naš *primjer* matrice a iz (6) vrijedi:

(9) $$a \cdot \frac{(fa)^T}{\det a} = \operatorname{diag}(1).$$

Odmah ćemo se uvjeriti da *ta formula vrijedi* za ***svaku regularnu kvadratnu konačnu matricu*** i time ćemo doći do jednog *osnovnog matematičkog teorema linearne algebre*. Prirodno je faktor od a u (9) nazvati *inverzna matrica od* a i označiti ga sa a^{-1}.

4.1. Definicija. Za kvadratnu matricu a neka fa označuje matricu koja iz a nastaje tako da joj se *svaka vrijednost* zamijeni *algebarskim komplementom*,

tj. po definiciji

$$(fa)_{ik} = fa_{ik},$$

gdje kao obično fa_{ik} označuje produkt od $(-1)^{i+k}$ i determinante koja se iz matrice a dobije brisanjem retka $a_{i.}$ i stupca $a_{.k}$; tj. $fa_{ik} = (-1)^{i+k} \det(a \setminus a_{ik})$.

Npr.

$$f\begin{bmatrix} 3 & 4 \\ 5 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -5 \\ -4 & 3 \end{bmatrix}.$$

$$f\begin{bmatrix} 3 & 4 \\ 5 & 1 \end{bmatrix}^T = \begin{bmatrix} 1 & -4 \\ -5 & 3 \end{bmatrix}.$$

Vidi se da je $(fa)^T = f(a^T)$. Sjetimo se da $(a^T)_{ik} = a_{ki}$.

4.2. Definicija adjunkte (v. pogl. 11, § 14,19) *Adjunkta zadane kvadratne matrice* a zove se *matrica* fa^T. Možemo je označiti sa Aa ili a^r. Drugim riječima, ako u matrici a svaku vrijednost zamijenimo pripadnim algebarskim komplementom, dobijemo određenu matricu fa. Transponat te matrice zove se adjunkta Aa matrice a; dakle je

$$(Aa)_{ik} = fa_{ki}$$

(imajte na umu obrnut red indeksa na lijevoj i na desnoj strani!).

Npr. $$A\begin{bmatrix} 3 & 5 \\ -1 & 4 \end{bmatrix} = f\begin{bmatrix} 3 & 5 \\ -1 & 4 \end{bmatrix}^T = f\begin{bmatrix} 3 & -1 \\ 5 & 4 \end{bmatrix} = \begin{bmatrix} 4 & -5 \\ 1 & 3 \end{bmatrix}.$$

Isto tako, za matricu

$$a=\begin{bmatrix} 1 & -2 & 0 \\ 3 & 4 & -1 \\ -2 & 0 & 3 \end{bmatrix} \text{ prelaz } a_{ik}\to fa_{ik} \text{ daje:}$$

$$a\to fa=\begin{bmatrix} 12 & -7 & 8 \\ 6 & 3 & -4 \\ -2 & 1 & 10 \end{bmatrix};$$

transponat od te matrice je Aa, tj.

$$Aa=(fa)^T=\begin{bmatrix} 12 & 6 & -2 \\ -7 & 3 & 1 \\ 8 & -4 & 10 \end{bmatrix}.$$

⟶ **4.3.** Teorem. *Za svaku konačnu kvadratnu matricu a vrijedi*

$$a\,(fa)^T=(fa)^T\,a=diag\,(det\,a).$$

Dokaz se sastoji u neposrednoj primjeni Laplaceovog teorema o determinantama. Nađimo, npr., produkt $a\,(fa)^T$; nađimo (ik)-vrijednost toga produkta: $(fa^T)_{ik}=$(po definiciji množenja)$=$redak $a_i.$ puta stupac $(fa^T)_{.k}$; no *k-stupac* od fa^T je *k-redak* u fa; dakle je:

$$(afa^T)_{ik}=a_{i.}\circ fa_{k.}=\text{(osnovni Laplaceov teorem)}=$$

$$=\det a\cdot\delta_i^k,\quad \text{gdje}\quad \delta_i^k=\begin{cases}1 & \text{za} \quad i=k.\\ 0 & \text{za} \quad i\neq k.\end{cases}$$

To upravo znači da je afa^T dijagonalna matrica sa svim elementima na dijagonali jednakim $\det a$.

4.4. Teorem. *Za svaku regularnu konačnu matricu a* vrijedi

$$a\cdot\frac{fa^T}{\det a}=\frac{fa^T}{\det a}\cdot a=diag\ (1).$$

Ovaj teorem izlazi iz relacije u prethodnom teoremu dijeleći je sa $\det a$. Teorem 4.4. osigurava egzistenciju inverzne matrice za *kvadratnu nesingularnu matricu*, tj. za matricu za koju je $\det a\neq 0$.

4.5. Iz $a\cdot Aa=\operatorname{diag}(\det a)$ izlazi $\det Aa=(\det a)^{n-1}$. Zaista, navedena jednakost omogućava da zaključimo da veza $\det a=0$ daje vezu $\det Aa=0$. U protivnom bi bilo $\det Aa\neq 0$, tj. postojala bi matrica $(Aa)^{-1}$. Množenjem ishodne jednakosti sa $(Aa)^{-1}$ dobivamo $a=\operatorname{diag}(\det a)\cdot(Aa)^{-1}=0$, što je nemoguće jer veza $a=0$ znači da su svi matrični elementi matrice a jednaki 0, pa dakle i $Aa=0$. Ako je pak a nesingularna matrica, tada prema Binet-Cauchyjevu teoremu imamo:

$$\det(a\cdot Aa)=\det\operatorname{diag}(\det a),\qquad \text{tj.}$$

$$\det a\cdot\det Aa=(\det a)^n.$$

Kako je $\det a\neq 0$, to je $\det Aa=(\det a)^{n-1}$.

5. INVERZIJA MEĐU MATRICAMA

5.0. Priprema. Problem inverzije zadane matrice a, tj. pronalaženje matrice x, za koju će biti $ax = xa = \mathrm{diag}(1, 1 \cdots 1)$ od osnovne je *praktične i teoretske vrijednosti*[1]. Problem je u vezi s rješavanjem linearnih sistema kojima je a matrica. *Teoretski* stvar se teoremom potpuno rješava za kvadratne matrice; *praktički* stvar još nije riješena, specijalno za (n, n)-matrice s velikim n. U novije vrijeme učinjen je u tom pogledu znatan napredak primjenom brzometnih računskih strojeva.

Problemom inverzije nekvadratnih matrica bavili su se N. Bjerhammar, M. Stojaković i dr.

⟶ **5.1.** Definicija. *Inverzna ili recipročna matrica zadane kvadratne* (n, n)*-matrice* a je *svaka matrica* x za koju je

$$(1_d) \qquad ax = 1_n \quad \text{i}$$

$$(1_l) \qquad xa = 1_n$$

gdje 1_n označuje *jediničnu* matricu. Inverzna matrica od a označuje se sa a^{-1} ili ^{-}a. Dakle je po definiciji:

$$(2) \qquad aa^{-1} = 1_n \text{ kao i } a^{-1}a = 1_n.$$

Odatle se odmah očitava da je $(a^{-1})^{-1} = a$.

5.1.1. Definicija. Ako je $ab = 1_n$, tada se kaže da je b *desni inverz ili desni reciprok od* a i pišemo $b = a_d^{-1}$, odnosno da je a *lijevi inverz* ili *lijevi reciprok od* b i pišemo $a = b_l^{-1}$.

5.1.2. Odmah ćemo dokazati da za matrice a **konačnog** poretka desni reciprok od a ujedno je i lijevi reciprok od a, pa se podudara s recipročnom matricom a^{-1}; i dualno: lijevi reciprok od a ujedno je i desni reciprok od a i podudara se sa a^{-1}; tada je a^{-1} **jednoznačno** određena matrica (stvar je mnogo zamršenija ako je oblast matrice beskonačna! Isp. § 6.5).

Prema teoremu 4.4. matrica $\dfrac{fa^T}{\det a}$ je *jedno značenje* za a^{-1}; međutim, odmah ćemo dokazati da a^{-1} *nema drugih značenja.*

Stvarno, neka za kvadratnu matricu a vrijedi relacija (1_d), pri čemu je n prirodan broj.

Odatle izlazi da je i x kvadratna matrica i $\mathrm{Dom}\, x = \mathrm{Dom}\, a$.

Iz (1_d) izlazi

$$\det(ax) = 1.$$

---

[1] Principijelno, naše je stanovište da se uz *svaki proces* ima promatrati i *obrnut proces*. Zato uz svaku zadanu matricu a treba promatrati i *antimatricu* ^{-}a kao protupreslikavanje onog preslikavanja što ga kao operator definira matrica a. Specijalno, za regularne kvadratne matrice a bilo bi opravdanije definirati a^{-1} pomoću $a^{-1}a = 1_n$, jer se funkcije slažu (komponiraju) pišući ih zdesna nalijevo. No, iz praktičnih razloga, ipak na ovom mjestu definiramo pomoću relacije $a^{-1}a = aa^{-1} = 1_n$, jer su skalarne jednadžbe za vrijednosti od a^{-1} više u skladu s uobičajenim pisanjem linearnih sistema. A prema već dokazanom teoremu 4.4. naslućujemo da je desni inverz od a ujedno i lijevi *inverz od a.*

Primjenom osnovnog Binet-Cauchyjeva teorema (pogl. 11, § 9) imamo dalje

$$\det a \cdot \det x = 1. \tag{2}$$

To znači da je $\det a \neq 0$: matrica a je *regularna*. Zato možemo promatrati i matricu $fa^T/\det a$, s kojom smo se već upoznali. Množeći (1_d) sprijeda matricom $\dfrac{fa^T}{\det a}$, dobijemo:

$$\frac{fa^T}{\det a} ax = \frac{fa^T}{\det a} \cdot 1_n$$

$$\left(\frac{fa^T}{\det a} \cdot a \right) x = \frac{fa^T}{\det a}$$

(po teorému 4.4)

$$1_n \cdot x = \frac{fa^T}{\det a}, \quad \text{tj.}$$

$$ax = 1 \Rightarrow x = \frac{fa^T}{\det a}. \tag{3}$$

Na osnovu toga, teoremom 4.4. osigurano je da iz $ax = 1$ proizlazi

$$xa = 1, x = \frac{f(a)^T}{\det a} \text{ te}$$

$$a^{-1} = \frac{f(a^T)}{\det a}. \tag{4}$$

Slično se dokazuje da iz (1_l) izlazi (1_d) i (4).

Najzad, iz relacije (2), (3) i (4) proizlazi

$$\det a \cdot \det a^{-1} = 1, \quad \text{tj.}$$

$$\det a^{-1} = (\det a)^{-1} = 1/\det a. \tag{5}$$

Skupljajući gornje rezultate, dobivamo ovaj

⟶ **5.2. Osnovni teorem o inverziji kvadratnih matrica.** ***Neka je a kvadratna matrica konačna poretka*** (n, n); ***regularnost matrice a, tj. nejednakost*** $\det a \neq 0$, ***potreban je i dovoljan uslov da postoji inverzna matrica*** a^{-1} ***kao rješenje jednadžbi*** $ax = 1 = xa$. ***Iz*** $\det a \neq 0$ ***nužno proizlazi***

$$a^{-1} = \frac{1}{\det a} fa^T; \quad \text{te}$$

$$\det a^{-1} = (\det a)^{-1}.$$

Iz $ax = 1_n$ ***nužno proizlazi*** $x = a^{-1}$; ***isto tako iz*** $ya = 1_n$ ***nužno izlazi*** $y = a^{-1}$ (isp. § 5.1.2).

5.3. Inverz produkta. Teorem. *Za kvadratne nesingularne matrice a, b istog konačnog poretka vrijedi* $(ab)^{-1} = b^{-1}a^{-1}$: *inverzija produkta je distributivna, ali* ***obrnutim*** *redom. Analogno za tri i više faktora* a_k, *vrijedi:*

$$(a_1 a_2 \cdot \cdot a_k)^{-1} = a_k^{-1} \cdot \cdot \cdot a_3^{-1} a_2^{-1} a_1^{-1}.$$

Stvarno, po definiciji imamo $(ab)(ab)^{-1} = 1_n$. Množeći to sprijeda najprije sa a^{-1} pa onda sa b^{-1}, dolazi se do iskazanog teorema za matrice a i b. Induktivno se teorem dokaže za slučaj $3, 4, \cdots$ faktora. Specijalno, kad su svi faktori međusobno jednaki, gornji teorem prelazi u:

5.4. Lema. $(a^2)^{-1} = (a^{-1})^2$ i općenito $(a^k)^{-1} = (a^{-1})^k$, tj.

$$(a^k)^{-1} = (a^{-1})^k \tag{1}$$

za svaki prirodni broj $k = 1, 2, \cdots$

Pri tom važi ova definicija:

5.5. Cijele potencije regularnih konačnih matrica. Definicija. Za kvadratnu matricu reda n stavljamo $a^0 = 1_n$, $a^1 = a$ $a^2 = a \cdot a, \cdots$, za prirodni broj k stavljamo $a^{k+1} = a(a^k)$. Ako je *a regularna* kvadratna matrica, onda stavljamo $a^{-k} = (a^{-1})^k$ za svaki prirodni broj k.

5.6. Teorem. *Za svaku kvadratnu nesingularnu konačnu matricu a vrijedi*

$$a^k \cdot a^l = a^{k+l}, \quad (a^k)^l = a^{kl},$$

gdje su k, l proizvoljni cijeli brojevi; specijalno:

$$(a^{-1})^{-1} = a \text{ i } (a^{-2})^{-3} = a^6.$$

Teorem se izvodi iz gornje leme 5.4. Zadovoljimo se da dokažemo ovu relaciju još za slučaj $k = -2$, $l = -3$, jer se analogno obrađuje opći slučaj $k < 0$, $l < 0$. No, $(a^{-2})^{-3} =$ (po definiciji) $= [(a^{-1})^2]^{-3} =$ (po obrascu (1)) $= \{[(a^2)^{-1}]^{-1}\}^3 = \{a^2\}^3 = a^2 \cdot a^2 \cdot a^2 =$ (zbog asocijacije) $= a^6 = a^{2 \cdot 3} = a^{-2 \cdot -3}$.

5.7. Operator inverzije prema *T*-operatoru i *-operatoru.

Teorem. $(a^{-1})^* = (a^*)^{-1}$; specijalno $(a^{-1})^T = (a^T)^{-1}$; pri tom $x \to x^T$ znači transponiranje matrice x; a x^* znači $\overline{x^T}$ (uzeti konjugiranu ili spregnutu matricu od x^T).

Stvarno,

$$(a^{-1})^* = \left(\frac{1}{\det a} Aa\right)^* = (Aa)^* \left(\frac{1}{\det a}\right)^* = Aa^* \frac{1}{\det a^*}$$

(to se lako vidi); dalje je to

$$= \frac{1}{\det a^*} Aa^* = (a^*)^{-1}.$$

6. DIJELJENJE MATRICA. LINEARNA MATRIČNA JEDNADŽBA

6.1. Matrična jednadžba $ax = b$. Naučili smo rješavati matrične jednadžbe $ax = 1_n$ (isp. § 5.2); rješenje je $x = a^{-1} = fa^T/\det a$ (ukoliko je $\det a \neq 0$). Na sličan se način rješava matrična jednadžba $ax = b$ ako je $\det a \neq 0$. Množenjem sa a^{-1} sprijeda izlazi

$$a^{-1}(ax) = a^{-1}b \text{ ili}$$

$$(a^{-1}a)x = a^{-1}b, \text{ tj.}$$

$x = a^{-1}b$ · jer je $a^{-1}a = I$ po definiciji 5.1.

6.2. Matrična jednadžba $xa=b$. Isto tako iz $xa=b$ izlazi

$$x=ba^{-1}.$$

U općem je slučaju $a^{-1}b \neq ba^{-1}$. Matrica $a^{-1}b, ba^{-1}$ mogu se zvati *lijevi i desni kvocijent matrica* b i a. Na taj je način jasno da imamo *dva obrata množenja*: *lijevo dijeljenje i desno dijeljenje*.

6.3. Cramerov teorem i inverzija matrica. Znamo da se sistem linearnih jednadžbi može pisati i matrično $ax=b$ (a je matrica sistema, x je stupac od nepoznanica, b je stupac desnih strana). Tad je $x=a^{-1}b$. Drugim riječima, poznavanje inverza a^{-1} matrice a omogućuje nam da *neposredno riješimo svaki linearni sistem s tom matricom a*: dovoljno je a^{-1} *pomnožiti stupcem desnih strana jednadžbi*. U tome je *velika praktična i teorijska važnost invertiranja* matrica.

6.4. Što je s matričnom jednadžbom $ax=b$ ako je a neregularna kvadratna ili nekvadratna matrica? Ubuduće ćemo obrađivati neke slučajeve takvih jednadžbi! Imajmo uvijek na umu jednadžbe oblika $ax=b$ i pratimo kako se razvija naše znanje o njima!

6.5. Zadaci o inverziji matrica. 1. Nađi a^T, fa, fa^T, a^{-1} za matricu a

$$1)\begin{bmatrix}1&0\\0&1\end{bmatrix};\quad 2)\begin{bmatrix}\cos\alpha&\sin\alpha\\-\sin\alpha&\cos\alpha\end{bmatrix};\quad 3)\begin{bmatrix}3&4&5\\5&3&0\end{bmatrix};$$

$$4)\begin{bmatrix}3&5&4\\2&1&2\\0&3&5\end{bmatrix};\quad 5)\begin{bmatrix}1&0&0\\0&x&u\\0&v&y\end{bmatrix};\quad 6)\begin{bmatrix}x&0&u\\0&1&0\\v&0&y\end{bmatrix};$$

$$7)\begin{bmatrix}x&u&0\\v&y&0\\0&0&1\end{bmatrix};\quad 8)\begin{bmatrix}3&-5&4\\2&1&5\\8&-9&13\end{bmatrix};\quad 9)\begin{bmatrix}2&1&0\\1&1&2\end{bmatrix}.$$

Za koje je slučajeve u navedenim primjerima a^{-1} određeno?

1_d. Nađi desni inverz matrice a iz prethodnog zadatka; 1_l. Nađi lijevi inverz matrice a iz zadatka 1.

2. Odredi x i y iz $ax=b$, $ya=b$ ako a i b znače ove matrice:

$$1)\begin{bmatrix}3&5\\4&2\end{bmatrix};\ \begin{bmatrix}3&4\\5&2\end{bmatrix};\quad 2)\begin{bmatrix}4&1&2\\5&3&5\\6&1&7\end{bmatrix},\ \begin{bmatrix}2&2&2\\3&3&2\\4&4&4\end{bmatrix};$$

$$3)\ a=\begin{bmatrix}5&7&2\\4&7&3\\3&2&4\end{bmatrix}\quad b=\begin{bmatrix}1\\2\\3\end{bmatrix},\ \begin{bmatrix}1&1\\2&2\\3&3\end{bmatrix},\ \begin{bmatrix}1&1&1\\2&2&2\\3&3&3\end{bmatrix},\cdots$$

3. Ako se zna rješenje x iz $ax=b$, riješi $by=a$.

4. Za matrice a i b iz zadatka 2 nađi rješenje jednadžbe $a^{-1}xa=b$' ukoliko rješenje postoji.

5. Može li postojati obratna matrica m^{-1} matrice m za koju zaključak $mx=my \Rightarrow x=y$ nije ispravan? Npr. $m=S$, gdje je $S_{ii-1}=1$ $(i=2,3,\cdots)$, a inače $S_{ik}=0$ te $x=(0,0,0,\cdots)^T$, $y=[1,0,\cdots]^T$.

6. Ako matrica $I+x$ ima svoju recipročnu vrijednost pa ako je $(I+x)^{-1}=I+y$, tada je $x+y+xy=[0]$. Dokaži!

7. Ako je produkt aa^T regularna matrica, tada je $a^T(aa^T)^{-1}$ jedan desni inverz a_d^{-1} od a; dokaži to. Nađi bar jedan lijevi inverz od a. Pri tom a može biti i nekvadratna, odnosno singularna matrica. Navedi primjere.

8. Promatraj ovu matricu x:

$$\frac{1}{3}\begin{bmatrix} 2 & 1 & -1 \\ 1 & 2 & 1 \\ -1 & 1 & 2 \end{bmatrix}, \qquad \frac{2}{21}\begin{bmatrix} 17 & 8 & -2 \\ 8 & 5 & 4 \\ -2 & 4 & 20 \end{bmatrix},$$

$$\frac{1}{116}\begin{bmatrix} 79 & 8 & 49 & -17 & 13 \\ 8 & 108 & -20 & -12 & 16 \\ 49 & -20 & 37 & -1 & 11 \\ -17 & -12 & -1 & 69 & 53 \\ 13 & 16 & 11 & 53 & 55 \end{bmatrix};$$

uvjeri se da vrijedi $x^2=x$ i uopće $x^n=x$ za svaki prirodni broj n!

Pokušaj naći još koje rješenje jednadžbe $x^2=x$ (npr. da bude $\mathrm{Dom}\, x=(4,4)$). Rješenja jednadžbe $x^2=x$ zovu se *idempotentne matrice.*

9. 1) Neka je matrica a takva da je a^Ta regularno; stavimo

$$a_l^{(0)}=a(a^Ta)^{-1}a^T;$$

uvjeri se da je $a_l^{(0)}$ kvadratna matrica i da zadovoljava $x^2=x$; kao i $xa=a$; promatraj slučaj

$$a=\begin{bmatrix} 1 & 1 \\ 2 & 3 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 1 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & -1 & 1 \\ 1 & 2 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

2) Za $x=a_l^{(0)}$ nađi $x(x-I)$, $(x-I)(x+I)$, $(x-I)^n$ za $n=2,3,\cdots$

3) Ako je aa^T regularna matrica, nađi: $x=a_d^{(0)}=a^T(aa^T)^{-1}a$, x^2, $(x-I)x$, x^n.

Bjerhammar naziva matrice $a_l^{(0)}$, $a_d^{(0)}$ *izvanrednim jediničnim matricama.*

Literatura: Anđelić [3], Blanuša [1], Denis-Papin, Kaufmann [1], Gantmaher [1], Križanič [1], Kurepa Svetozar [1], Lichnerowicz [1], Mac Duffee [1], Mal'cev [1], Zurmuhl [1].

POGLAVLJE 13.

SISTEM HOMOGENIH LINEARNIH JEDNADŽBI. VEKTORSKI PROSTORI. LINEARNA ZAVISNOST I LINEARNA NEZAVISNOST

0. POSTAVLJANJE PROBLEMA. UVODNA RAZMATRANJA

Dosad smo riješili jednadžbu $ax=b$ svaki put kad je a kvadratna konačna i regularna matrica, dakle $\det a \neq 0$ (ovaj uvjet regularnosti za slučaj da je a broj postaje $a \neq 0$). Jednadžba ima rješenje $x=a^{-1}b$. Sad ćemo uslov regularnosti *zabaciti*, ali ćemo staviti *ograničenja na matricu* b i pretpostaviti da je ona *nula-vektor* $\vec{0}$.

0.1. Prema tome, problem glasi:

Riješiti jednadžbu

(1) $$a\vec{x}=\vec{0};$$

ili eksplicitno: *naći niz* $x=(x_{n'})_{n'}$ od n članova $x_{n'}$ tako da bude *zadovoljen sistem* S_0 *ovih* k ***homogenih*** *jednadžbi*:[1]:

(S_0)
$$k\begin{cases} a_{11}x_1 + \cdots + a_{1\nu}x_\nu + \cdots = 0 \\ a_{21}x_1 + \cdots + a_{2\nu}x_\nu + \cdots = 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{i1}x_1 + \cdots + a_{i\nu}x_\nu + \cdots = 0, \\ \underbrace{\cdots\cdots\cdots\cdots\cdots\cdots}_{n}\cdots \end{cases}$$

odnosno

(S_0)
$$\sum_\nu a_{i\nu}x_\nu = 0 \qquad (i=1,2,\cdots k);$$

ili pomoću skalarnog produkta:

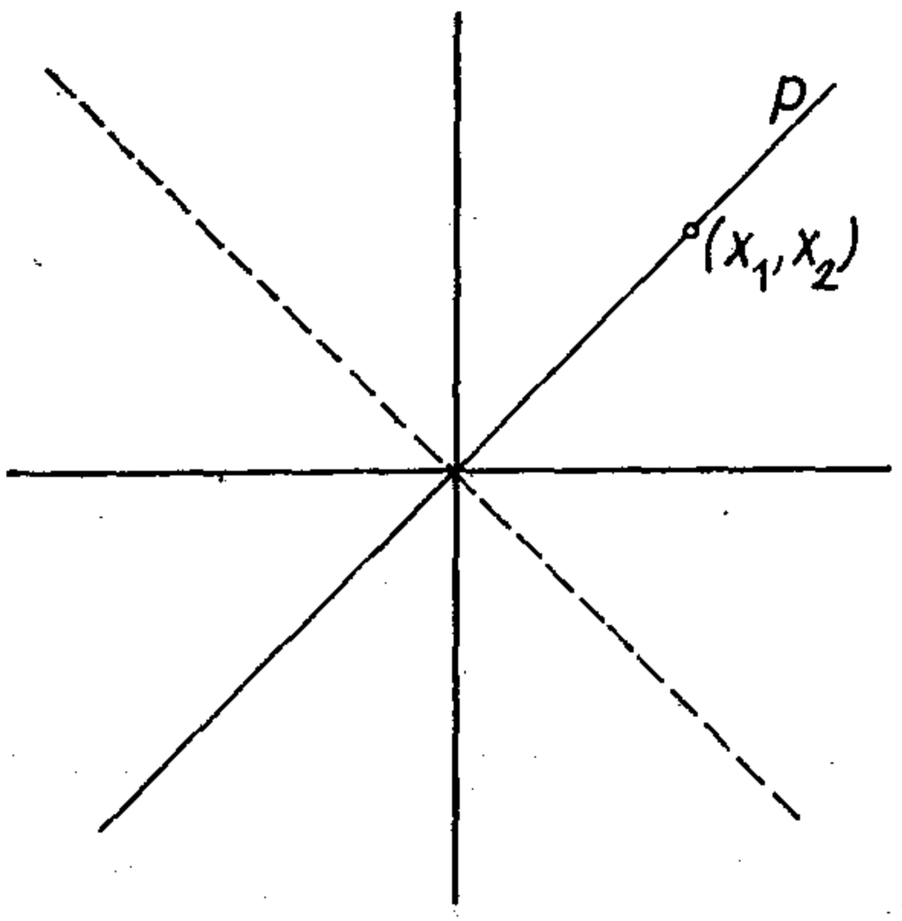
(1) $$a_{i\cdot}\circ\vec{x}=\vec{0}.$$

Pri tom su k i n prirodni brojevi; i, odnosno ν prolazi intervalom od prvih k, odnosno n prirodnih brojeva.

---

[1] Indeks 0 u S_0 podsjeća nas da imamo posla s homogenim sistemom jednadžbi (desne su strane jednake nuli).

0.2. Sistem (S_0), odnosno jednadžba (1) imaju uvijek rješenje, i to bar *nula-rješenje*. Ali je od interesa promatrati »*prostor*« $N(ax)$ ***svih*** rješenja jednadžbe (1) odnosno sistema (S_0). Naime, govori se o *prostoru rješenja jednadžbe* (1), *odnosno sistema* (S_0), *jer to pomaže prostornom gledanju i omogućava prostornu interpretaciju;* a ujedno ćemo tako vidjeti da u *algebri radimo s prostorima od proizvoljnog broja dimenzija.*



Sl. 13.0.3.

0.3. Tako npr. ako je $a=[3,-4]$, tada sistem (S_0) glasi

$$3x_1-4x_2=0;$$

ta jednadžba u koordinatnom prostoru R^2 od dvije dimenzije označuje pravulju p kroz ishodište (0, 0), i to kao množinu ***svih tačaka*** (x_1, x_2) *kojima pripadni radijus-vektor* $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ *stoji okomito na zadanom radijus-vektoru* $a=\begin{bmatrix} 3 \\ -4 \end{bmatrix}$.

Sva rješenja $x=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ „ispunjavaju“ tu pravulju p; svakoj tački $(x_1, x_2)\in p$ odgovara *pripadni radijus-vektor* $\vec{x}=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ ***kao rješenje;*** i obratno: *svakom rješenju* odgovara na pravulji p ona *tačka* (x_1, x_2) kojoj je $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ radijus-vektor.

0.4. Slučaj $k=1$ i $n=3$; dakle, imamo jednadžbu

$$a_{11}x_1+a_{12}x_2+a_{13}x_3=0.$$

Tada, radeći u trodimenzionalnom prostoru R^3 svih uređenih trojki, imamo analogno tri koordinatne međusobno okomite osi—nosioce brojeva x_1, x_2, x_3, pa se traže sve „tačke“ (x_1, x_2, x_3) kojima pripadni radijus-vektor $\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$ stoji okomito na zadanom radijus-vektoru $a^T=\begin{bmatrix} a_{11} \\ a_{12} \\ a_{13} \end{bmatrix}$.

Rješenje će „ispuniti“ čitavu ravninu kroz koordinatni početak i koja je okomita na zadanom nizu a (jer zadana jednadžba $a\circ\vec{x}=\vec{0}$ upravo znači da je $a\perp\vec{x}$).

0.5. P r i m j e r. Zadan je sistem jednadžbi:

$$\begin{aligned} 2x_1 - 3x_2 + 5x_3 &= 0 \\ 4x_1 - 6x_2 + 10x_3 &= 0; \end{aligned} \qquad \text{(2)}$$

riješite ga!

Očigledno, skup (2) jednadžbi reducira se na „podsistem“

$$2x_1 - 3x_2 + 5x_3 = 0. \qquad \text{(3)}$$

No, ovdje su rješenja radijus-vektori koji su okomiti na radijus-vektoru $\begin{bmatrix} 2 \\ -3 \\ 5 \end{bmatrix}$; rješenja čine „ravninu“, dakle „dvodimenzionalni prostor“; to znači da se sva rješenja mogu dobiti iz dva „nezavisna“ rješenja. Stvarno, iz (3) izlazi:

$$x_1 = 3/2x_2 - 5/2\, x_3. \qquad \text{(4)}$$

Pri tom su x_2, x_3 *proizvoljni*, tj. za svako x_2, x_3 niz

$$x = (3/2\, x_2 - 5/2\, x_3, x_2, x_3) \qquad \text{(5)}$$

daje jedno rješenje za (3), dakle i za zadani sistem (2).

Specijalno, za $x_2 = 1, \quad x_3 = 0$

$x_2 = 0, \quad x_3 = 1$

dobivamo ova dva rješenja:

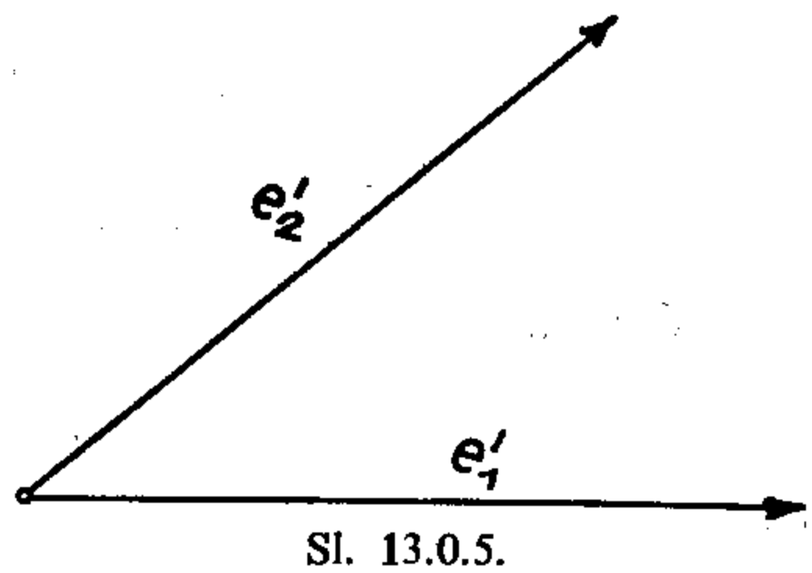
$$\begin{aligned} e_1 &= (\ 3/2, \quad 1, \quad 0) \\ e_2 &= (-5/2, \quad 0, \quad 1). \end{aligned} \qquad \text{(6)}$$

Opće rješenje (5) prikazuje se „linearno“ pomoću ova *dva specijalna rješenja* e_1, e_2 u (6); naime, očigledno je

$$x_1 e_1 + x_2 e_2 = x_1 \cdot (3/2,\ 1,\ 0) + x_2(-5/2,\ 0,\ 1) =$$

$$= (3/2\, x_1, x_1,\ 0) + (-5/2\, x_2, 0, x_2) - (3/2\, x_1 - 5/2\, x_2, x_1, x_2).$$

A to je upravo opće rješenje (5).



Sl. 13.0.5.

S druge strane, vektori e_1, e_2 ne mogu se izraziti linearno jedan pomoću drugoga. I najzad, treće svojstvo: *bilo koja dva nezavisna rješenja* sistema (2) čine „bazu“ rješenja u tom smislu da se *svako rješenje može pomoću njih izraziti kao linearan spoj.* Geometrijski je to jasno: *u ravnini određenoj radijus-vektorima* e_1, e_2 *možemo uzeti* bilo koja dva „nezavisna“ radijus-vektora e'_1, e'_2 (tj. koji ne padaju u istu pravulju) i upotrijebiti ih kao koordinatnu bazu: svaka tačka t ravnine određuje potpuno određenu uređenu dvojku (t_1, t_2) brojeva t_1, t_2, za koje je $\overrightarrow{0\,t} = t_1 \cdot e'_1 + t_2 e'_2$.

0.6. Taj način izražavanja prenosi se na prostore $R^4, R^5, \cdots$ od 4,5,$\cdots$ dimenzija. Za tijelo R realnih brojeva i prirodni broj n mi *definiramo* R^{In} ili R^n kao »*prostor*« *svih nizova po n članova iz R*, pri čemu na prirodan način uvodimo: *zbrajanje u* R^n i množenje cx za $c\in R$ i $x\in R^n$. Naime, za nizove $x, y\in R^n$ definiramo $x+y$ kao sumu nizova x i y, tj. $(x+y)_{n'}, = x_{n'} + y_{n'}$ (*zbrajaju se odgovarajući članovi*; npr. $[2, 5, 7, 4]+[3, -2, 8, -4]=[5, 3, 15, 0]$). Isto tako, za svaki broj $c\in R$ i svaki niz $x\in R^n$ definiramo cx kao niz $cx_{n'}$; npr. $5\cdot[3, -2, 4, 7, 9]=[15, -10, 20, 35, 45]$.

0.7. Eto, ta jednostavna ideja bit će nam vodilja u ovom poglavlju i ona će nas dovesti do vanredno važnih pojmova: *linearne nezavisnosti nizova, vektorâ, vektorskih prostora te do pojma ranga matrice. Razmatranja u ovom poglavlju od bitne su važnosti.*

0.8. Skup svih rješenja homogenog sistema (S_0), odnosno matrične jednadžbe (1) pokazat će se kao »*vektorski prostor*« od $d=n-r$ dimenzija, u kojem svakih r nezavisnih rješenja određuju prostor svih rješenja; pri tom je r rang matrice a, tj. *maksimalni stupanj regularne podmatrice u a* (to je *glavni teorem o sistemima homogenih jednadžbi* (S_0); d je tzv. *defekt matrice a*).

1. O PROSTORU SVIH RJEŠENJA HOMOGENOG SISTEMA S_0

1.1. Zasad osim *nula-rješenja* ne znamo nikojeg eventualnog drugog člana „prostora“ $N(ax)$ svih rješenja jednadžbe $\vec{ax}=\vec{0}$ (v. § 0.1)[1]; no ipak za *skup* $N(ax)$ možemo odmah ustanoviti da posjeduje stanovitu strukturu. Naime, u $N(ax)$ možemo *provoditi* ***zbrajanja (sabiranja)*** i da pri tom vrijede uobičajena pravila:

G_1: $u, v\in N(ax)$, tada je $u+v\in N(ax)$, tj. suma dvaju rješenja opet je rješenje.

Dokaz:

$$\begin{array}{lll} u\in N(ax) & \text{znači} & au=\vec{0} \\ & & + \\ \underline{v\in N(ax)} & \text{znači} & \underline{av=\vec{0}} \end{array}$$

$$au+av=\vec{0}+\vec{0},$$

$$a(u+v)=\vec{0}, \quad \text{dakle } u+v\in N(ax).$$

G_2: Nadalje je za *zbrajanje* u $N(ax)$ zadovoljen *zakon asocijacije*:

$$(u+v)+t=u+(v+t).$$

Ta u, v, t su ipak nizovi, dakle specijalne matrice.

---

[1] Slovo N je uzeto kao prvo slovo riječi nula: $N(ax)$ je skup nula-mjestâ pri preslikavanju $\vec{x}\to\vec{ax}$.

G_3: Skup $N(ax)$ sadrži „neutralni“ element, tj. jedan član — to je $\vec{0}$ — za koji je

$$u+\vec{0}=\vec{0}+u=u \quad \text{za svako} \quad u\in N(ax).$$

G_4: Iz $u\in N(ax)$ izlazi $-u\in N(ax)$ te $u+(-u)=\vec{0}=-u+u$.

Kratko se kaže: $N(ax)$ *je »aditivna grupa«*, misleći pri tom da su upravo ispunjeni gornji „grupovni aksiomi“ G_1, G_2, G_3, G_4. K tome je $N(ax)$ *komutativna* aditivna grupa u tom smislu da je $u+v=v+u$ za svako $u, v\in N(ax)$.

Osim gornjeg *internog zbrajanja*, zbrajanja unutar $N(ax)$, postoji i množenje članova c iz tijela R realnih brojeva i članova u iz „prostora“ $N(ax)$; pri tom važe ovi uslovi:

P_1: Iz $c\in R$, $u\in N(ax)$ izlazi $cu\,(=uc)\in N(ax)$.

P_2: Iz $c, d\in R$ i $u\in N(ax)$ izlazi $(c+d)u=cu+du$.

P_3: Iz $c\in R$, i $u, v\in N(ax)$ izlazi $c(u+v)=cu+cv$.

P_4: Iz $c, d\in R$ i $u\in N(ax)$ izlazi $c(du)=(cd)u$.

P_5: $1u=u$ za svako $u\in N(ax)$.

P_6: $0u=\vec{0}$ za svako $u\in N(ax)$.

1.2. Umjesto da se nabrajaju sva svojstva množine $N(ax)$ iskazana u § 1.1, kraće se govori ovako:

»$N(ax)$ je vektorski prostor nad tijelom R«. Ta rečenica stoji, dakle, umjesto gornjeg teksta u § 1.1. da je $N(ax)$ aditivna komutativna grupa koja dopušta množenje članovima iz R i da pri tom vrijede pravila P_1—P_6.

Dokazali smo, dakle, da vrijedi

1.3. Teorem. *Za svaku matricu a s vrijednostima u tijelu R[1] skup $N(ax)$ svih rješenja jednadžbe $ax=\vec{0}$ je određen vektorski prostor nad tijelom R.*

Rješenja jednadžbe (0.1) odnosno sistema (S_0) zvat ćemo i vektorima, nizovima i sl.

1.4. Primjer. Promatrajmo sistem (S_0) jednadžbi

$$\begin{aligned}
&2x_0+3x_1-5x_2-4x_3+x_4-\ \ x_5+5x_6=0\\
&-2x_0-3x_1+5x_2+4x_3-x_4+\ \ x_5-5x_6=0\\
&2x_0-3x_1+\ \ x_2+\ \ x_3+x_4+\ \ x_5+\ \ x_6=0\\
&2x_0+3x_1+7x_2+6x_3+x_4+3x_5-3x_6=0.
\end{aligned} \tag{1}$$

[1] R je *tijelo* realnih brojeva; riječ *»tijelo«* treba da nas podsjeti na prve četiri računske operacije unutar R.

Kakav je pripadni prostor $N(ax)$ rješenja? Tu je

$$a=\begin{bmatrix} 2 & 3 & -5 & -4 & 1 & -1 & 5 \\ . & . & . & . & . & . & . \end{bmatrix}$$ matrica napisanog sistema.

1.4.1. No, ako pogledamo napisane 4 jednadžbe, vidimo da je druga jednadžba j_2 zavisna od prve jednadžbe j_1 jer je $j_2=-j_1$; posljednja, četvrta jednadžba j_4 zavisna je od prve i treće (naime, $j_4=-j_1+2j_3$); drugim riječima, ako vrijedi j_1 i j_3, vrijedit će automatski i j_2 i j_4, dakle i čitav zadani sistem (S_0). Jednadžbe j_1, j_3 ne svode se jedna na drugu; sistem (S_{00}) jednadžbi:

$$\begin{aligned} 2x_0+3x_1-5x_2-4x_3+x_4-x_5+5x_6&=0 \\ 2x_0+3x_1+\ x_2+\ x_3+x_4+x_4+\ x_6&=0 \end{aligned} \tag{2}$$

je *nezavisan*; pripadni „prostor“ **rješenja** je isti kao prostor $N(ax)$ rješenjâ polaznog sistema (S_0).

1.4.2. No, (S_{00}) je lako riješiti: izrazit ćemo dvije „nepoznanice“ pomoću ostalih, recimo x_4, x_5 pomoću x_0, x_1, x_2, x_6. Izlazi:

$$\begin{aligned} x_4&=-2x_0-3x_1+2x_2+3/2\,x_3-3x_6 \\ x_5&=\qquad\qquad -3x_2-5/2\,x_3+2x_6. \end{aligned}$$

„Prostor“ $N(ax)$ svih rješenja sastoji se upravo od svih nizova

$$\begin{aligned} x=(x_0, x_1, x_2, x_3, &-2x_0-3x_1+2x_2+3/2\,x_3-3x_6, \\ &-3x_2-5/2\,x_3+2x_6, x_6), \end{aligned} \tag{3}$$

pri čemu su x_0, x_1, x_2, x_3, x_6 proizvoljni članovi iz R; prostor $N(ax)$ ima, dakle, 5 »*slobodnih parametara*«.

1.4.3. Među rješenjima ima ih 5 pomoću kojih se ostala rješenja izgrađuju; evo tih 5 rješenja:

$$\begin{aligned} e_1&=(1,\ 0,\ 0,\ 0,-2,\ 0,\ 0) \\ e_2&=(0,\ 1,\ 0,\ 0,-3,\ 0,\ 0) \\ e_3&=(0,\ 0,\ 1,\ 0,+2,-3,\ 0) \\ e_4&=(0,\ 0,\ 0,\ 1,3/2,-5/2,\ 0) \\ e_7&=(0,\ 0,\ 0,\ 0,-3,\ 2,\ 1). \end{aligned} \tag{4}$$

Oznaka e_i u vezi je s vrijednosti $x_i=1$ i $x_k=0$ za $k\in\{1,2,3,4,7\}\setminus\{i\}$.

Vidi se da je opće rješenje x u (3) linearan spoj tih 5 rješenja u (4), naime:

$$x=x_0e_1+x_1e_2+x_2e_3+x_3e_4+x_6e_7.$$

1.4.4. Ispitajmo još može li se koje od 5 rješenja napisanih u (4) izraziti pomoću ostalih rješenja iz (4). Može li se npr. rješenje e_1 izraziti pomoću preostalih rješenja

$$e_2, e_3, e_4, e_7, \quad \text{tj. je li } e_1 = \lambda_2 e_2 + \lambda_3 e_3 + \lambda_4 e_4 + \lambda_7 e_7?$$

Ne može, jer bi ta jednakost imala za posljedicu analognu jednakost za svaku komponentu, specijalno za prvu komponentu, tj. moralo bi biti

$$1 = \lambda_2 \cdot 0 + \lambda_3 \cdot 0 + \lambda_4 \cdot 0 + \lambda_7 \cdot 0,$$

što je nemoguće. Slično, e_i se ne može izraziti linearno pomoću ostalih, jer je i-komponenta od e_i jednako 1, dok su i-komponente ostalih rješenja $= 0$.

1.4.5. Dakle, 5 rješenja (vektorâ) iz (4) zbilja čine *nezavisan* skup rješenja zadanog sistema (S_0) i pomoću njih se izgrađuje, linearno, *svako rješenje sistema* (S_0); kraće se kaže da rješenja (4) čine *bazu rješenjâ ili vektorâ u prostoru* $N(ax)$ svih rješenja; zato taj prostor $N(ax)$ ima 5 „dimenzija".

1.4.6. U općem slučaju, kad bi jednadžbe (1) bile međusobno linearno „nezavisne", prostor $N(ax)$ imao bi „tek" $3 = 7 - 4$ dimenzija (4 „nepoznanice" izražavaju se pomoću ostalih $7 - 4$ nepoznanica).

1.5. Zadaci. 1. Napiši konkretan linearan homogen sistem od 3 jednadžbe s 3 nepoznanice. — Riješi taj sistem.

2. Promatraj sistem $ax = 0$, ako a označuje matricu:

1) $[2 \quad 3]$; 2) $\begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$; 3) $\begin{bmatrix} 2 & 3 \\ 4 & 5 \\ 6 & 7 \end{bmatrix}$; 4) $\underset{(4,4)}{I-} \begin{bmatrix} 2 & 1 & & \\ & 2 & 1 & \\ & & 2 & 1 \\ & & & 2 \end{bmatrix}$. Nađi x.

3. Neka je $a = \begin{bmatrix} 3 & -4 \\ 8 & 5 \end{bmatrix}$; ako je $a \cdot x = 0$, $ay = 0$, onda je $a \cdot [x, y] = [0, 0]$, i obrnuto. Poopći.

2. ELEMENTARNI PRIMJER VEKTORA IZ GEOMETRIJE

2.0. Gornji način *izražavanja pomoću vektora*, a pogotovu ono što će još slijediti, bazirano je na razmatranjima elementarne matematike o vektorima. Radi potpune jasnoće izložimo i taj slučaj, da poslije budemo svjesniji toga kako u algebri nesvjesno radimo s „prostorima" od 4, 5, $\cdots$ dimenzija i s „vektorima" iz takvih prostora.

2.1. Najjednostavniji *slučaj vektora* dobije se kad se promatraju *usmjereni segmenti* (*odresci*), odnosno uređene dvojke tačaka prostora: *svaku uređenu dvojku tačaka, odnosno svaki orijentirani segment kod kojeg razlikujemo jedan smjer od protivnog smjera* zovemo *vektor*. Ako su A, B krajevi odreska, onda ćemo

pripadna dva vektora označavati sa $\overrightarrow{AB}$ i $\overrightarrow{BA}$; strelica počinje na početnoj ili prvoj tački, a završava na završnoj tački usmjerenog segmenta. Veza između $\overrightarrow{AB}$, $\overrightarrow{BA}$ iskazuje se jednakošću

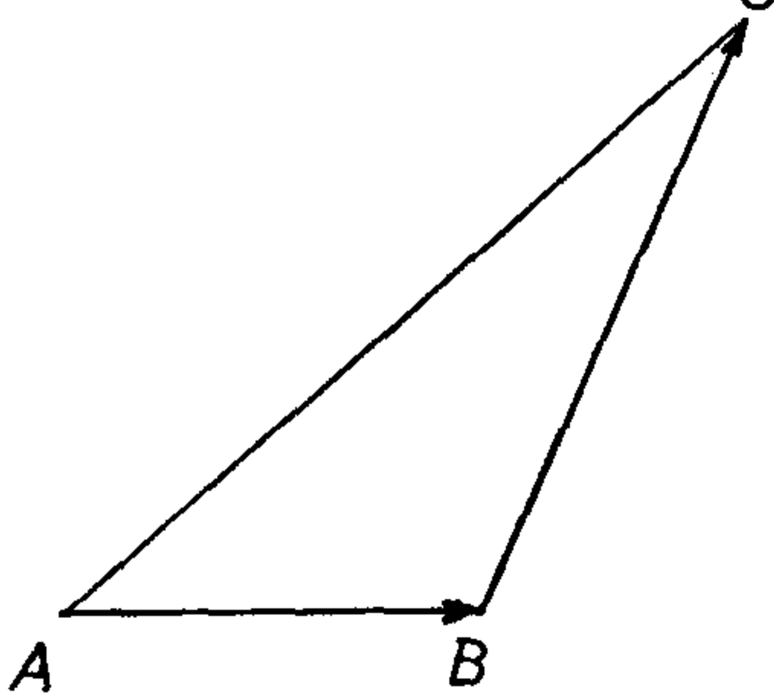
$$\overrightarrow{BA} = -\overrightarrow{AB}.$$

2.2. Uzimamo kao gotovu stvar da se *svaki* vektor v može *nanijeti* počev od bilo koje tačke A, tj. da za svaki vektor v i *svaku* tačku A postoji jedna jedina tačka T tako da bude $\overrightarrow{AT} = v$.

2.3. Ako je koja tačka O istaknuta, onda se vektor $\overrightarrow{OT}$ zove *radijus-vektor* ili *vektor položaja tačke T.*

2.4. *Nula-vektor.* Za svaku tačku A definira se vektor $\overrightarrow{AA}$ i kaže da je $\overrightarrow{TT} = \overrightarrow{AA}$ za svaku tačku T. Vektor $\overrightarrow{AA}$ zove se *nula-vektor* i označuje sa $\vec{0}$ (ili 0 ako nema zabune).[1)]

2.5. Iz iskustva znamo da često *imamo posla s usmjerenim odrescima i veličinama* (sila, put, brzina, akceleracija itd.).



Sl. 13.2.5.

Iskustvo nam daje povoda da *sumu* dvaju vektora *definiramo* ovako:

$$\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC},$$

tj. ako drugi vektor ima početak u svršetku prvog vektora, onda je suma prvog i drugog vektora opet vektor: početak mu je u početku prvog vektora, a svršetak u svršetku drugog vektora.

2.6. Definicija sume. Ako su $\overrightarrow{AB}$, $\overrightarrow{CD}$ zadani vektori, tada se suma $\overrightarrow{AB} + \overrightarrow{CD}$ definira ovako:

$$\overrightarrow{AB} + \overrightarrow{CD} = \overrightarrow{AB} + \overrightarrow{BD'}, \quad \text{gdje je} \quad \overrightarrow{BD'} = \overrightarrow{CD}.$$

2.7. Oznaka. *Geometrijske vektore* označujemo kao odreske snabdjevene *strelicom.* Ako ne može biti zabune, označivat ćemo ih i bez strelica. Brojeve ćemo odsad zvati i *skalarima.* Na taj način imat ćemo *skalare i vektore.*[2)]

[1)] Također se sjetimo nula-vektorâ 0, $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$, $\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, $\cdots$ te transponiranih vektora 0, [0, 0], [0, 0, 0], $\cdots$ koji dolaze u teoriji matrica i linearnih jednadžbi.

[2)] Poslije ćemo vidjeti da i brojeve možemo shvatiti kao posebne vektore (§ 3.6). Prema tome, vektori poopćavaju brojeve.

2.8. Oduzimanje vektora. *Oduzimanje* vektora *svodi se* na *zbrajanje* vektora: po definiciji, *oduzeti* vektor a znači dodati *suprotni* vektor $-a$:

$$b-a=b+(-a).$$

2.9. *Svojstva G_1-G_4 zbrajanja vektora.* Pozivajući se na elementarnu geometriju, lako se vidi da skup S svih vektora (koji su na zadanom pravcu, odnosno ravnini, odnosno prostoru) čine *aditivnu grupu* u tom smislu da vrijede ovi aksiomi:

G_1: Ako je $u\in S$ i $v\in S$, tada je $u+v\in S$.

G_2: Vrijedi zakon asocijacije: $(u+v)+t=u+(v+t)$.

G_3: Postoji neutralni element, tj. takav član $z\in S$ da bude $u+z=z+u=u$ za *svako* $u\in S$ (z se može označiti sa $\vec{0}$ ili 0).

G_4: Za svako $u\in S$ postoji određeno „$-u$“ sa svojstvom $u+(-u)=-u+u=0$.

Naravno da iz $u\in S$, $v\in S$ izlazi $v-u\in S$, jer je $v-u=v+(-u)$, no $-u\in S$ po zakonu G_4; dakle je $v\in S$ i $-u\in S$, pa po zakonu G_1 imamo također $v-u\in S$.

Osim toga se vidi da je grupa S *komutativna*, tj. da je $u+v=v+u$ za svako $u\in S$ i svako $v\in S$.

2.10. Množenje brojeva i vektora. Svojstva P_1-P_5. Također znamo da vektore možemo množiti realnim brojevima i da pri tom vrijede ovi zakoni:

P_1: Iz $c\in R$, $u\in S$ izlazi $cu\in S$[1].

P_2: (zakon distribucije prema zbrajanju skalara):

$$(a+b)x=ax+bx \quad \text{za bilo koje} \quad a,b\in R \text{ i } x\in S.$$

P_3 (*zakon distribucije prema zbrajanju vektora*):

$$a(u+v)=au+av \quad \text{za svako} \quad a\in R \text{ i } u,v\in S.$$

P_4 (*zakon asocijacije za množenje skalarima*):

$$c(du)=(cd)u \quad \text{za svako} \quad c,d\in R \quad \text{i } \textit{svako } u\in S.$$

P_5: $1u=u$ za svako $u\in S$.

2.11. *Kraće se kaže da je skup S jedan vektorski ili linearni prostor nad tijelom R realnih brojeva,* a to upravo znači da unutar S imamo komutativnu operaciju zbrajanja, te da R i S možemo komutativno množiti i da pri tom

---

[1] S R označujemo množinu svih realnih brojeva.

vrijede zakoni G_1-G_4, P_1-P_5 (zakoni komutacije glase: $u+v=v+u$, $au=ua$ za svako $u, v\in S$ i $a\in R$).

Praksa, naime, pokazuje da se često srećemo s „vektorskim" prostorima S *nad* R, u tom smislu da se radi o skupu S i operacijama $+, \cdot$ u gornjem smislu.

2.12. Teorem. U svakom vektorskom prostoru $(S, +, \cdot)$ je

(1) $$\mathbf{0\cdot u=\vec{0}=u\cdot 0} \quad \textbf{za svako } \mathbf{u}\in S,$$

(2) $$\vec{0}\,c=\vec{0}=c\,\vec{0} \quad \textbf{za svaki skalar } c\in R \textbf{ (v. 32 § 3.1.1).}$$

Dokaz. Svakako je

(3) $$c+0=c;$$

odatle množeći zdesna sa u:

$$c+0=c\Rightarrow (c+0)\,u=cu\Rightarrow$$

$$cu+0\,u=cu\Rightarrow$$

$$-(cu)+(cu+0\,u)=-(cu)+cu\Rightarrow$$

$$(-(cu)+cu)+0\,u=\vec{0}\Rightarrow$$

$$\vec{0}+0\,u=\vec{0}\Rightarrow$$

$$0\,u=\vec{0}.$$

Slično, množeći (3) sa lijeve strane sa u izlazi $u\,0=\vec{0}$.

Ako umjesto (3) pođemo od $u+\vec{0}=u$, tada množeći tu jednakost sa c sa lijeve strane, odnosno sa desne strane, dobije se traženi identitet (2).

3. VEKTORSKI ILI LINEARNI PROSTORI. VEKTORI. NEKOLIKO DEFINICIJA

Na osnovu razmatranja u prethodnom paragrafu uvodimo ovu osnovnu definiciju:

⟶ **3.1.** Definicija. *Svaka množina* $V=\{x, y, z, \cdots\}$ *u kojoj je definirano komutativno zbrajanje sa svojstvima* G_1-G_4 *i množenje s članovima tijela* R[1] *sa svojstvima* P_1-P_5 *zove se vektorski ili linearni prostor nad tijelom* R. *Svaki član vektorskog prostora nad* R *zove se* ***vektor nad tijelom*** R. (v. 26 § 1.1).

3.2. Primjedba. *Vektor* smo definirali u odnosu na zadan vektorski prostor kao *cjelinu*. Prema tome, kada kažemo: *vektor*, *vektorski prostor*, to

---

[1] R je tijelo realnih brojeva.

onda u stvari znači da se radi o elementu nekog skupa, koji, doduše, ima *neka ograničenja* ali to nipošto ne treba da bude vezano sa suviše *jakim ograničenjima*, kao što je *usmjeren odrezak ili slično*. Međutim, dobro je i korisno, i često se može, pokušati *geometrijski* ili mehanički interpretirati pojedine vektorske prostore. Razlog da se govori o „prostorima" baš i leži u toj mogućnosti, zornosti, očiglednosti (korist asocijacija!).

Velika mogućnost generaliziranja postoji i u tom da se u definiciji 3.1 tijelo R realnih brojeva može nadomjestiti kakvim drugim tijelom k, npr. tijelom kompleksnih brojeva, tijelom racionalnih funkcija, itd; time se dobije *vektorski prostor V(k) nad tijelom k.*

3.3. Primjeri vektorskih prostora i vektorâ. — 3.3.1. Primjer. Dokaži da za svaku pravulju p i svaku točku $0 \in p$, usmjereni pravocrtni segmenti oblika $\overrightarrow{OT}$, gdje je $T \in p$, čine vektorski prostor; $\overrightarrow{OT}$ je vektor. Zbrajanje i množenj kao obično.

3.3.2. Isto vrijedi za skup svih $\overrightarrow{AB}$ kad $A \in p$, $B \in p$.

3.3.3. Isto vrijedi ako p označuje bilo koju ravninu R^2.

3.3.4. Isto vrijedi ako p označuje „obični" prostor R^3 od tri dimenzije.

3.3.5. Skup tročlanih nizova (x_1, x_2, x_3) odnosno (x_0, x_1, x_2) realnih brojeva jest određen vektorski prostor R^3, pri čemu se adicija i množenje brojem definira na uobičajeni način:

$$(x_0, x_1, x_2) + (y_0, y_1, y_2) = (x_0 + y_0, x_1 + y_1, x_2 + y_2)$$

$$a \cdot (x_0, x_1, x_2) = (ax_0, ax_1, ax_2).$$

3.3.6. Poopćenje na prostor R^n odnosno R^{In} je očigledno; pri tom n označuje bilo koji redni broj (konačan ili beskonačan); In je množina svih realnih brojeva $0, 1, 2, \cdots$ koji su $< n$.

3.3.7. Ako promatramo bilo koji sistem od k *homogenih* linearnih jednadžbi

$$\sum_{\nu} a_{i\nu} x_\nu = 0 \qquad (i = 1, 2, \cdots, k)$$

s kompleksnim koeficijentima $a_{i\nu}$ i nepoznanicama x_ν, tada skup svih rješenja tih jednadžbi obrazuje određen „vektorski prostor" $N(ax)$ nad tijelom $R(i)$ kompleksnih brojeva (isp. § 1).

3.3.8. Sva rješenja diferencijalne jednadžbe $y'' + y = 0$ čine vektorski prostor; tu su *vektori* funkcije oblika $a \cos x + b \sin x$, gdje su a, b proizvoljni brojevi.

3.3.9. Rješenja diferencijalne jednadžbe

$$\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + \frac{\partial^2 u}{\partial z^2} = 0$$

obrazuje vektorski prostor; elementi su mu određene funkcije.

3.3.10. *Vektorski prostor* R^M (M zadana bilo koja množina). Ako je M bilo koji skup, neka R^M označuje skup *svih jednoznačnih funkcija* iz M prema R; skup R^M postaje određenim vektorskim prostorom čim u njenu definiramo *zbrajanje* na uobičajeni način:

$$f+g \quad \text{za} \quad f\in R^M,\ d\in R^M \quad \text{znači funkciju}$$

$$x\to fx+gx \quad \text{za svako} \quad x\in M, \text{ tj.}$$

$$(f+g)\,x=fx+gx.$$

Nadalje, za svako $a\in R$ i za svako $f\in R^M$ definiramo produkt af ili fa po obrascu

$$(af)\,x=a(fx) \quad \text{za svako} \quad x\in M.$$

Primjer za $M=R$, [0, 1] itd.

3.3.11. Skup svih matrica određene oblasti (k, n), s vrijednostima u tijelu R (odnosno $R(x)$), čine vektorski prostor nad tijelom R (odnosno $R(x)$).

Prema tome, i svaka matrica *m s realnim vrijednostima jest određen vektor u odnosu na neke druge matrice, koje zajedno sa m čine stanovitu organsku cjelinu prema zahtjevima* G_1—G_4, P_1—P_5.

3.3.12. Skup svih linearnih (homogenih) jednadžbi zadanih nepoznanica, koje iz zadanóg skupa jednadžbi nastaju množeći ih članovima iz R i zbrajajući jednadžbe *kao što je uobičajeno, jest određen vektorski prostor.* Prema tome, i *jednadžbe se mogu shvatiti kao vektori.*

3.3.13. Skup svih 1) rotacija oko 0, 2) translacijâ čine određen prostor. Pri tom se radi o kretanjima ravnine u samu sebe; ako je riječ o kretanjima u prostoru R^3, onda rotacije oko O ne čine vektorski prostor; translacije čine prostor.

3.4. Važna napomena. Gornji primjeri pokazuju kako *vektorski prostori i vektori mogu biti vrlo raznorodni.* Specijalno treba naglasiti da *vektori iz jednog prostora ne moraju imati nikakve veze s vektorima kojeg drugog prostora,* pa zato *ne mora postojati ni njihova suma.* Imajmo na umu da su pojedine stvari naglašene kao vektori tek u odnosu prema nekoj cjelini V (prema određenom vektorskom *prostoru) u vezi s nekim tijelom* $R, R(i), \ldots$ *i* prema operacijama unutar V (zbrajanje) i između V i R (množenje!).

Vidimo ovo: *ako se množina V zove linearni vektorski prostor, onda su u njoj definirane dvije operacije: zbrajanje elemenata i množenje elemenata s elementima nekog »tijela« i da te dvije operacije imaju uobičajena svojstva zbrajanja i množenja.* Zato se često kraće govori da su u V uvedene operacije zbrajanja elemenata i množenje, s uobičajenim svojstvima, a pri tom se misli da te operacije zadovoljavaju navedene aksiome G_1—G_4, P_1—P_5.

3.5. Naglašujemo da za tako *opće vektore* još nemamo operacije „množenja“ vektorâ (uz operaciju zbrajanja i oduzimanja); to će biti uvedeno tek u *nekim vektorskim prostorima* koje ćemo zvati *algebrama.*

3.6. Primijetimo da je i samo tijelo R realnih brojeva određen vektorski prostor, pa su dakle realni brojevi ujedno određeni vektori.

3.7. Vektorski prostor što ga određuju zadani vektori. — 3.7.1. Prostor Rx ili $L(R,\{x\})$ za određen vektor x sastoji se od svih cx, pri čemu c prolazi tijelom R. Npr. $\overrightarrow{ROE}$ za zadane tačke O, E sastoji se od svih $\overrightarrow{OT}$, pri čemu je T na pravulji određenoj tačkama O i E. Kaže se da se svaki vektor iz Rx može *linearno* izraziti (prikazati) pomoću x. Za nula-vektor $\vec{0}$ je $R\vec{0}=\{\vec{0}\}$.

3.7.2. Za dva vektora x_1, x_2 nekog vektorskog prostora V nad R određeni su potprostori Rx_1, Rx_2 kao i njihova „suma“

$$(*) \qquad Rx_1+Rx_2,$$

tj. skup svih y_1+y_2, pri čemu je $y_{2'}\in Rx_{2'}$.

Rx_1+Rx_2 je određen vektorski prostor, i to potprostor od V jer ga V sadrži kao dio, i to kao svoj organiziran dio: zbrajanje u (*) je upravo kao u V. Kaže se da vektori x_1, x_2 *razapinju ili određuju vektorski prostor* Rx_1+Rx_2 kao skup svih linearnih kombinacija $a_1x_1+a_2x_2$; pri tom $a_1\in R$, $a_2\in R$. Govori se da se svaki član iz $X=Rx_1+Rx_2$ može *linearno izraziti* pomoću vektorâ x_1, x_2. Također se kaže da vektori x_1, x_2 čine *bazu* (*osnovu*) prostora (*), specijalno ako se jedan ne može izraziti drugim.

3.7.3. Definicija. Ako je M neka množina vektorâ nekog vektorskog prostora V nad R, neka RM ili $L(R;M)$ označuje skup svih vektora oblika a_1x_1, $a_1x_1+a_2x_2$, $a_1x_1+a_2x_2+a_3x_3, \cdots$, pri čemu su $a_1, a_2, \cdots$ u R, a $x_1, x_2, \cdots$ su uzeti iz M. Kaže se da M *određuje ili razapinje* $L(R,M)$.

3.8. Zadaci. Je li skup u zadacima 1—4 vektorski prostor nad tijelom R realnih brojeva:

1. 1) samo tijelo R; 2) skup $R(0,\cdot)$ realnih brojeva >0; 3) skup $R(i)$ kompleksnih brojeva; 4) skup Q racionalnih brojeva; 5) skup D cijelih brojeva?

2. Skup svih $\overrightarrow{AB}$ kad $\overrightarrow{AB}$ znači: 1) proizvoljan pravocrtan odrezak iz zadane ravnine; 2) u jednoj poluravnini; 3) unutar zadane kugle?

3. Skup pozitivnih realnih brojeva u kojem unutrašnje „zbrajanje“ znači množenje, a mješovito množenje znači obično potenciranje?

4. Skup svih jednadžbi oblika $a_{11}x_1+a_{12}x_2=0$

$$a_{21}x_1+a_{22}x_2=0, \quad \text{pri čemu su } a_{ik}\in R?$$

5. Promatraj „vektore“ u, v u ovim zadacima 1—10. i odredi:

1) $u+v$; 2) $u-v$; 3) $-u+2v$; 4) $u+2v-5u+6v$;

5) $-3(u+v)+(u-3v)$, pri čemu u, v imaju ovo značenje:

1) $\begin{bmatrix}3\\4\end{bmatrix}, \begin{bmatrix}7\\x\end{bmatrix}$; 2) $(0,1,2),(3,4,5)$; 3) $(3,4,\cos^2x),(7,2,\sin^2x)$;

4) $5i+2j-3k,\ 3i-3j+7k.$

5) $\left|1-3\sqrt{2}+3\sqrt[3]{2},\ 5+7\sqrt[3]{2}-2\sqrt{2}.\right.$

6) Funkcije $1+3x^2-x^5$, $6+x+4x^5$ s oblasti R.

7) Funkcije $\cos x$, $\sin x$ definirane u R.

8) Matrice $\begin{bmatrix} 3 & -2 & 0{,}5 \\ 0{,}4 & 0{,}23 & 3{,}4 \\ 7{,}2 & 5{,}04 & 2{,}3 \end{bmatrix}$, $\begin{bmatrix} 0 & 0 & 3 \\ 1 & 0 & 5 \\ 7,2 & 3,4 & -5{,}2 \end{bmatrix}$.

9) Nizovi $\cos \omega' x$, $\sin \omega' x$; pri tom ω' prolazi beskonačnim cifarskim intervalom $I\omega' = \{0, 1, 2, \cdots\}$; nadalje, $x \in R$.

10) $\int_0^x \cos^2 t\, dt$, $\int_0^x \sin^2 t\, dt$.

4. LINEARNA ZAVISNOST VEKTORA. LINEARNA NEZAVISNOST VEKTORA

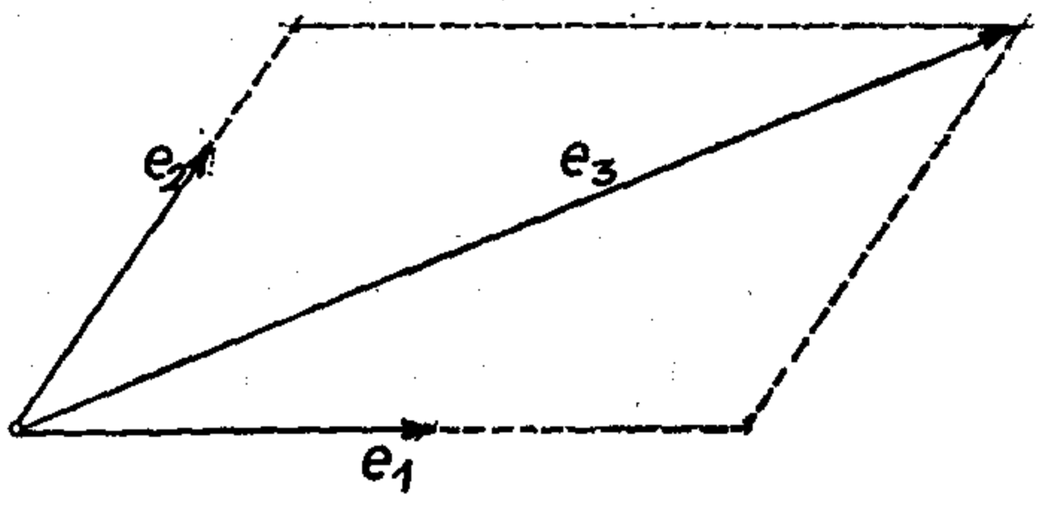
4.0. Priprema. Promatramo li na zadanoj pravulji p bilo koji vektor $\vec{e}$ koji je $\neq \vec{0}$, tada se **svaki** *drugi vektor* $\vec{v}$ s pravulje p može izraziti pomoću $\vec{e}$ u obliku $c\vec{e}$, tj. $\vec{v} = c\vec{e}$, odnosno $\vec{v} - c\vec{e} = \vec{0}$ gdje je c određen broj.

Specijalno, za $\vec{v} = \vec{0}$ imamo $c = 0$. Ako je $c \neq 0$, tada se i $\vec{e}$ može izraziti pomoću $\vec{v}$. *Bilo koja dva vektora na pravulji međusobno su vezana linearno.*

Naprotiv, u ravnini imamo i parova nezavisnih vektora: svaki par e_1, e_2 vektorâ koji zatvaraju oštar kut međusobno su nezavisni linearno, tj. jedan se ne može izraziti linearno pomoću drugoga, odnosno: nula-veza

$$\lambda_1 e_1 + \lambda_2 e_2 = \vec{0}, \qquad \lambda_2 . \in R$$

ima nužno za posljedicu $\lambda_1 = \lambda_2 = 0$. Naprotiv, ako je e_3 bilo koji treći vektor u ravnini, onda se nula-veza



Sl. 13.4.0.

$$\lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3 = \vec{0}$$

uz uslov $\lambda_3 . \in R$ može ostvariti i netrivijalno (tako npr. na slici je

$$e_3 = 2\,e_1 + 1{,}5\,e_2 \quad \text{tj.} \quad 2\,e_1 + 1{,}5\,e_2 - e_3 = \vec{0}).$$

Primjer s jednadžbama i nizovima. Jednadžbe

$$2x_0 + 3x_1 = 4, \quad 4x_0 + 6x_1 = 8$$

međusobno su zavisne; „pripadni“ nizovi

$$2, \quad 3, \quad 4$$
$$4, \quad 6, \quad 8$$

također; naprotiv, jednadžbe $2x+y=1$, $4x+y=5$ ne zavise međusobno linearno; isto vrijedi za dva niza 2, 1, 1 i 4, 1, 5.

Imajući na umu ta svakidašnja i elementarna razmatranja i, osim toga, znajući kako je raznovrstan i općenit pojam vektora (isp. § 3), prelazimo na preciziranje linearne zavisnosti (nezavisnosti) vektorâ i dokazivanje nekih osnovnih stvari o „dimenziji" vektorskih prostora.

Neka slika jednostavnih gornjih primjera služi kao oslonac i vodilja u općim razmatranjima.

Rang matrice kao zajednički maksimalni broj linearno nezavisnih njenih stupaca, odnosno redaka, odnosno kao maksimalni stupanj regularnih submatrica, osnovni je pojam u algebri. Druga je osnovna činjenica *istobrojnost svakog para bazâ* u svakom vektorskom *prostoru* (teorem 4.6.1.) i izomorfizam između V_k i V_n za $k=n<\infty$ (teorem 4.6.1).

4.1. Definicija linearne nezavisnosti[1]**.** Zadani konačni niz od s vektora[2] $v_{s'}$ je *linearno nezavisan ili slobodan* ako iz veza

$$\sum_{s'} \lambda_{s'} x_{s'} = 0, \quad \lambda_{s'} \in R \tag{1}$$

nužno izlazi

$$\lambda_{s'} = 0 \quad \text{za svako} \quad s' = 1, 2, \cdots, s. \tag{2}$$

Ako su veze (1) moguće i bez uslova (2), kaže se da su vektori $v_{s'}$, tj. vektori $v_1, v_2, \cdots, v_s$, *linearno zavisni*; pri tom je s prirodan broj.

4.1.1. Kaže se da je zadani *beskonačni skup M* vektorâ linearno nezavisan ako mu je svaki *konačni dio linearno nezavisan*. Beskonačni skup vektora je *linearno zavisan* ako mu je bar jedan konačan podskup linearno zavisan.

4.2. P r i m j e r i. — **4.2.1.** Je su li stupci matrice $a=\begin{bmatrix} 3 & 0 \\ 0 & 5 \end{bmatrix}$ linearno zavisni ili nezavisni?

Imamo stupce $a_{\cdot 1}=\begin{bmatrix} 3 \\ 0 \end{bmatrix}$, $a_{\cdot 2}=\begin{bmatrix} 0 \\ 5 \end{bmatrix}$; treba ispitati veze

$$\lambda_1 a_{\cdot 1} + \lambda_2 a_{\cdot 2} = \vec{0}, \qquad \lambda_{2'} \in R. \tag{3}$$

$$\lambda_1 \begin{bmatrix} 3 \\ 0 \end{bmatrix} + \lambda_2 \begin{bmatrix} 0 \\ 5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix},$$

$$\begin{bmatrix} \lambda_1 \cdot 3 \\ \lambda_1 \cdot 0 \end{bmatrix} + \begin{bmatrix} \lambda_2 \cdot 0 \\ \lambda_2 \cdot 5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix},$$

$$\begin{bmatrix} 3\lambda_1 + 0 \\ 0 + 5\lambda_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

---

[1] Rus.: зависимость, независимость; franc.: dépendance-indépedance: njem.: Abhängigkeit-Unabhängigkeit.

[2] Vektori $v_1, \cdots, v_s$ su izvađeni iz nekog vektorskog prostora V nad tijelom R ili generiraju neki vektorski prostor nad R.

Odatle izlazi:

$$3\lambda_1 = 0, \quad 5\lambda_2 = 0, \quad \text{tj.}$$

$$\lambda_1 = 0 \quad \text{i} \quad \lambda_2 = 0. \tag{4}$$

Dakle (3) $\Rightarrow$ (4): stupci su linearno nezavisni.

4.2.1.1. Analogno: Stupci (réci) u svakoj dijagonalnoj matrici bez 0 na dijagonali međusobno su linearno nezavisni. Dokaži!

4.2.2. Jesu li nizovi

$$\begin{aligned} f_0 &= 2, \quad 3, \quad 5, \quad 4 \\ f_1 &= 3, \quad -4, \quad 2, \quad 3 \\ f_2 &= 5, \quad -3, \quad 4, \quad 2 \end{aligned} \tag{1}$$

linearno zavisni ili nezavisni?

Treba riješiti jednadžbu

$$x_0 f_0 + x_1 f_1 + x_2 f_2 = \text{nula-niz} = (0,\ 0,\ 0,\ 0). \tag{2}$$

No, formirajući linearni spoj, imamo po redu:

$$x_0 f_0 + x_1 f_1 + x_2 f_2 = x_0(2,\ 3,\ 5,\ 4) + x_1(3,\ -4,\ 2,\ 3) + x_2(5,\ -3,\ 4,\ 2) =$$

$$= (2x_0, 3x_0, 5x_0, 4x_0) + (3x_1, -4x_1, 2x_1, 3x_1) + (5x_2, -3x_2, 4x_2, 2x_2) =$$

$$= (\text{sumacija nizova!}) =$$

$$= (2x_0 + 3x_1 + 5x_2,\ 3x_0 - 4x_1 - 3x_2,\ 5x_0 + 2x_1 + 4x_2,\ 4x_0 + 3x_1 + 2x_2).$$

Na taj način jednadžba (2) postaje

$$\begin{aligned} &(2x_0 + 3x_1 + 5x_2,\ 3x_0 - 4x_1 - 3x_2,\ 5x_0 + 2x_1 + 4x_2, \\ &4x_0 + 3x_1 + 2x_2) = (0,\ 0,\ 0,\ 0). \end{aligned} \tag{3}$$

Odatle, izjednačenjem odgovarajućih članova u nizu $(3)_1$ i u nizu $(3)_2$, izlazi ovaj sistem jednadžbi:

$$\begin{aligned} 2x_0 + 3x_1 + 5x_2 &= 0 \\ 3x_0 - 4x_1 - 3x_2 &= 0 \\ 5x_0 + 2x_1 + 4x_2 &= 0 \\ 4x_0 + 3x_1 + 2x_2 &= 0. \end{aligned} \tag{4}$$

Lako se uvjerimo da odatle *nužno* izlazi $x_0 = x_1 = x_2 = 0$. To znači da jednadžba (2) ima trivijalno rješenje kao jedino rješenje. A to po definiciji znači da su nizovi (1) linearno nezavisni.

4.2.2.1. Primjedba. Treba uočiti kako ispitivanje *linearne zavisnosti nizova* (1) dovodi do razmatranja *sistema homogenih* jednadžbi (4) i da je matrica toga sistema (4) upravo matrica sačinjena od zadanih nizova (1) kao svojih **stupaca,** tj. matrica sistema (1) je $[f_0, f_1, f_2]$. *Ta je veza bitna.*

4.2.3. Primjer. Jesu li *jednadžbe*

$$2x+3y+5z=4$$
$$3x-4y+2z=3$$
$$5x-3y+4z=2$$

linearno zavisne ili nezavisne?

Treba pogledati proširenu matricu tih jednadžbi i usporediti je sa zadatkom 4.2.2. Jednadžbe su nezavisne! Provedite formalan dokaz!

4.2.4. Primjer. Jesu li tri funkcije: $x\to 1$, $x\to x$, $x\to x^2$, koje su definirane u intervalu $R[0, 1]$ realnih brojeva, linearno zavisne ili nezavisne?

Da odgovorimo na pitanje, treba promatrati pripadni nula-spoj:

$$\lambda_0\cdot 1+\lambda_1\cdot x+\lambda_2\cdot x^2=\vec{0};$$

to znači da treba biti

$$\lambda_0+\lambda_1 x+\lambda_2 x^2=0 \tag{1}$$

za **svako** $0\leq x\leqq 1$; pri tom su $\lambda_0, \lambda_1, \lambda_2$ **fiksni** brojevi. No, kako su λ fiksni brojevi, jednadžba (1) je algebarska. Ako je $\lambda_2\neq 0$, tada on ima samo jedno ili dva rješenja, naime brojeve oblika

$$\frac{-\lambda_1+(\lambda_1{}^2-4\lambda_0\lambda_2)^{1/2}}{2\lambda_2}.$$

A to znači da su spomenute tri potencija-funkcije 1, x, x^2 s domenom $R[0, 1]$ linearno nezavisne.

4.3. Što znači da zadan skup M određuje i razapinje zadani prostor V? Dimenzija.

4.3.1. Razapinjanje. Za zadani skup M vektorâ neka $L(R, M)$ označuje skup svih vektora oblika

$$\lambda_1 x_1,\ \lambda_1 x_1+\lambda_2 x_2,\ \lambda_1 x_1+\lambda_2 x_2+\lambda_3 x_3,\ \cdots,$$

pri čemu su $\lambda_1, \lambda_2, \cdots\in R$, $x_1, x_2, \cdots\in M$; primijetimo da i u sumi dolazi najviše konačno mnogo brojeva $\lambda_{n'}$ različitih od nule. Kaže se da M, odnosno *vektori iz* M, *razapinju* (*određuju*) *prostor* $L(R, M)$.

4.3.2. Pojam dimenzije. Minimalni glavni (kardinalni) broj množine M, za koju je $L(R, M)=V$ (zadani prostor V), zove se *dimenzija prostora* V; označuje se sa $\dim V$. Ili općenitije: za svaki neprazni skup $S\neq\{\vec{0}\}$ iz vektorskog prostora definiramo $\dim S$ kao *minimalni kardinalni broj* množina M sa svojstvom $L(R, M)\supset S$.

Npr. funkcije u R: $x\to 2$, $x\to x^3$, $x\to x^4$ razapinju prostor $L(R, \{2, x^3, x^4\})$ polinomâ $\lambda_3\cdot 2+\lambda_3\cdot x^3+\lambda_4 x^4$; kako su te funkcije linearno nezavisne (isp. primjer 4.2.4), dimenzija je prostora $=3$.

4.4. Baza zadanog vektorskog prostora V. — 4.4.1. Definicija. *Svaki normalno dobro uređeni skup B linearno nezavisnih vektora za koje je $L(R, B)=V$ zove se baza prostora V.*

Prema tome, kod baze se traži troje:

1) Baza je „normalno dobro uređen“ skup tako da se zna njen prvi element B_1, pa drugi element B_2 (ukoliko ga ima), itd. i k tome da nijedan početni komad niza ne bude istobrojan s čitavim nizom (to je potrebno spomenuti za prostore s beskonačno mnogo dimenzija, da se ne dogodi da bazu zapišemo npr. ovako: $B_1, B_2, \ldots, B_n, B_{n+1}, \ldots, B_\omega$).

2) *U bazi nema linearno zavisnih vektora* (zato nula-vektor nije u B jer je nula-vektor zavisan od svakog vektora).

3) *Svaki član $v \in V$ može se prikazati pomoću konačno mnogo članova* $x_0(v), x_1(v) \ldots$ iz baze B u tom smislu da je $v = v_0 x_0(v) + v_1 x_1(v) + \ldots$; pri tom su $v_0(v), v_1(v), \ldots \in R$.

Ako je baza B konačna i ima n članova, označujemo ih po redu:

$$B_1, B_2, \ldots, B_{n-1}, B_n \text{ i pišemo } B = \{B_{n'}\}_{n'} \text{ ili } \{B_{n'}\}$$

znajući da n' prelazi intervalom $1\,(n)$.

⟶ 4.4.2. Jednoznačnost izražavanja vektora pomoću zadane baze.
Teorem. ***Neka je V vektorski prostor nad tijelom R; ako je B baza u V, tada za svaki član $v \in V$, $v \neq \vec{0}$, postoji potpuno određeno preslikavanje baze B u R: $x \to v_x (x \in B)$ sa svojstvom da je $v_x \neq 0$ na konačnom dijelu baze B izvan kojeg je $v_x = 0$ i da je***

$$v = \sum_{x \in B} v_x x. \tag{1}$$

Specijalno, ako je baza B konačna i $B = \{B_{n'}\}_{n'}$, tada je potpuno određen niz (a ne skup) $v_{n'} \in R$ sa svojstvom

$$v = \sum v_{n'} B_{n'};$$

v_x (odnosno $v_{n'}$) zove se koordinata od v u smjeru $x \in B$ (odnosno u smjeru $B_{n'}$).
Specijalno za nula-vektor $\vec{0}$ iz V imamo

$$\vec{0} = \sum_{x \in B} 0 \cdot x.$$

Dokaz. Prema definiciji baze B, vrijedi $V = L(R, B)$; to znači da za svako $v \in V$, $v \neq \vec{0}$ postoji preslikavanje $x \to v_x \in R$ od B u R sa svojstvom da vrijedi (1) i da bude $v_x = 0$ svuda osim eventualno na konačnom dijelu od B, gdje je $v_x \neq 0$. Pa pretpostavimo da je također i $x \to v'_x$ preslikavanje od B u R s analognim svojstvom da je $v_x' \neq 0$ tek na konačnom ili pustom dijelu baze B. Tada je $\vec{0} = v - v' = \sum_{x \in B} v_x x - \sum_{x \in B} v'_x x$. No, ako je M množina svih $x \in B$ u kojima bar jedan od članova v_x, v'_x nije $= 0$, onda je M konačno i očigledno je gornja razlika $= \sum_{m \in M} (v_m - v'_m)\, m$, odakle je $\vec{0} = \sum_{m \in M} (v_m - v'_m)\, m$. Kako je M konačni dio baze B, M je *nezavisno*, pa posljednja jednakost ima za posljedicu $0 = v_m - v'_m$ za svako $m \in M$, što zbog $v_x = v'_x = 0$ za $x \in B \setminus M$ znači da je zaista $v_x = v'_x$ za svako $x \in B$.

4.5. Istobrojnost različitih baza u prostoru. Ravnina je dvodimenzionalna; *svaka baza* u njoj ima po *dva* člana; u prostoru R^{I3} *svaka* baza ima po *tri* člana, tj. ako su B, B' bilo koje *dvije* baze u običnom prostoru, onda skupovi B, B' imaju jednak broj članova. *Jedna od osnovnih činjenica o vektorskim prostorima koja zadire u algebru, geometriju itd. sastoji se u tom da isti iskaz važi za* ***svaki*** *vektorski prostor nad tijelom realnih ili kompleksnih brojeva.*

—→ 4.5.1. Teorem. (osnovni teorem o istobrojnosti baza). ***Neka je V bilo koji prostor (nad tijelom R ili R (i)); ako je $\dim V < \infty$, tada su bilo koje dvije baze prostora V istobrojne: one imaju isti broj članova. Svakih $n = \dim V$ linearno nezavisnih članova iz V čine bazu prostora pa se svaki član iz V na jednoznačan način prikazuje kao njihov linearan spoj.***

To je zaista fundamentalan teorem!

Dokaz. Čitalac može, pri dokazu, uvijek imati u mislima npr. ravninu umjesto V. Pa neka V ima upravo n dimenzijâ, dakle $\dim V = n \in N$. Tada po definiciji broja $\dim V$ postoji jedna baza $e = \{e_{n'}\}_{n'}$ upravo od n članova. Neka je $B = \{B_{s'}\}_{s'}$ bilo koja baza *istog* prostora V; s je broj članova u B; dakle je $s \geq \dim V$, tj. $s \geq n$. Treba dokazati da je $s = n$. To ćemo dokazati *postepenim smjenjivanjem* članova iz e članovima iz B.

Promatrajmo niz od $n+1$ člana:

$$\underbrace{e_1, e_2, \ldots, e_{n'}, \ldots, e_n}_{\text{baza } e}, \underbrace{B_1}_{\text{prvi član baze } B}. \tag{1}$$

Uklonimo iz tog niza *prvi* član x koji *zavisi linearno od preostalih članova niza* (1); vrijedi $x \in e$, i preostalih n članova *opet je jedna baza* e' u kojoj je i član B_1 iz baze B. Stvarno, kako je e baza, to za vektor[1] B_1 imamo rastav

$$B_1 = \sum_{n'} B_{1n'} \cdot e_{n'}; \tag{2}$$

kako je B_1 član jedne baze, naime baze B, to je $B_1 \neq \vec{0}$; znači da je bar jedna komponenta $B_{1n'} \neq 0$.

Neka je k prvi broj $\leq n$ za koji je $B_{1k} \neq 0$; tada iz rastava (2) možemo izraziti vektor e_k pomoću članova iz $e \setminus \{e_k\} \cup \{B_1\}$; dakle

$$e_k = B_k - \sum_r \frac{B_{1r}}{B_{1k}} e_r \qquad (r \leq n,\ r \neq k). \tag{3}$$

Dakle je e_k izbačeni vektor x. Dokažimo još da preostali članovi u (1) čine bazu, tj. da zamjenom u bazi e vektora e_k s vektorom B_1 dobijemo opet bazu. Stvar izlazi neposredno iz (3). Naime, kako je za proizvoljan vektor v iz V na snazi rastav

$$v = \sum_{n'} v_{n'} e_{n'}, \tag{4}$$

to unošenjem izraza $(3)_2$ za vektor e_k u (4) dobijemo rastav vektora v po vektoru B_1 i vektorima $e_{n'} \neq e_k$.

---

[1] U konkretnom slučaju „vektor" B_1 može biti geometrijski vektor, niz, jednadžba, funkcija, matrica, ...

Time smo dokazali da vrijedi ova:

4.5.1.2. Lema. *Neka je e bilo koja baza prostora V* i $x \in e$; *neka je v neki član* $\neq \vec{0}$ *iz V, sa svojstvom da v u smjeru x ima komponentu* $\neq 0$; *tada je skup* $e \setminus \{x\} \cup \{v\}$ *opet baza u prostoru.*

Dovršimo gornji dokaz. Izbacivanjem prvog zavisnog člana u (1) dobije se iz (1) određen niz e' od n članova; pripišimo tome nizu naredni član B_2 baze B; u nastalom nizu od $n+1$ člana provedimo isto razmatranje kao maloprije: izbacimo *prvi zavisni* član! Preostaje određen niz e'' od n članova sa B_1, B_2 kao dva posljednja člana, itd. Poslije n koračaja doću ćemo istim postupkom do određenog niza $e^{(n)}$ koji je upravo n-člani niz $(B_{n'})_{n'}$; taj niz $e^{(n)} = (B_{n'})_{n'}$ kao i nizovi $e^{(i)}$ kod drugih koračaja čini bazu. To znači da je $n = s$, jer bi inače bilo $n < s$ pa bi npr. član B_{n+1} baze B zavisio linearno od članova $B_1, \ldots, B_n$ jer ovi članovi tvore bazu $e^{(n)}$ prostora V; međutim, svi vektori svake baze linearno su nezavisni; zato B_{n+1} ne postoji pa je zaista $n = s$.

Istobrojnost baza je dokazana.

Idemo dalje! Pa neka je M bilo koja množina od $n = \dim V$ linearno nezavisnih vektora; tada je M baza u V; u obrnutom slučaju skup $V \setminus L(R, M)$, bio bi pun tj. neprazan; izabirući iz njega neki član i dovodeći ga u M, dobili bismo skup $M' \supsetneq M$; i skup M' je nezavisan, a ima već $n+1$ član; očigledno se proces može nastaviti, pa ako M' još nije baza, možemo M' proširiti i doći najzad do neke baze $S \supset M'$. No, baza S imala bi bar $n+1$ član, protivno dokazanoj istobrcjnosti baza.

Posljednji dio rečenice u teoremu 4.5.1. sadržan je u teoremu 4.4.2.

Time je osnovni teorem 4.5.1. potpuno dokazan.

4.5.1.3. Primjer. U § 1.4. riješili smo niz od 4 linearne homogene jednadžbe sa 7 nepoznanica i dokazali da sva rješenja čine prostor od 5 dimenzija. Pet „vektora", tj. 5 rješenja navedenih tamo pod šifrom (4), obrazovali su bazu. A sada znamo da ***svakih*** 5 *nezavisnih rješenja čine bazu i da svaka baza ima upravo* 5 *članova.*

To je *znatno preciziranje u savladavanju stvarnosti*!

4.5.2. Teorem o izgradnji baze. *Neka je* (1) $M = v_1, \ldots v_m$ *bilo koji niz od m linearno nezavisnih vektora prostora V; ako je* $m < \dim V$, *tada postoji baza e prostora koja proširuje skup M, a dobije se tako da se nizu* (1) *priklopi bilo koji niz od* $n-m$ *članova iz V koji su linearno nezavisni od vektora* (1), *tj. leže u* $V \setminus LM$, *a također su linearno nezavisni međusobno.*

Dokaz. Kako je $m < \dim V$, postoji bar jedan vektor $v_{m+1} \in V$ koji je nezavisan od M, tj. $v_{m+1} \in V \setminus LM$; radeći dalje sa $M_1 = v_1, v_2, \ldots, v_m, v_{m+1}$ kao što smo upravo radili sa M, pa ako je $m+1 < \dim V$, doći ćemo na sličan način do $v_{m+2} \in V \setminus LM_1$ itd.; nakon $n-m$ koračaju doći ćemo tako do niza $v_1, v_2, \ldots v_m, v_{m+1}, v_{m+2}, \ldots, v_n$ od n linearno nezavisnih vektora prostora V od n dimenzija; taj n-člani niz čini bazu prostora V (v. teor. 4.5.1.).

4.6. Izomorfizam vektorskih prostora. — 4.6.0. Priprava. Bili smo iznenađeni saznanjem na kako se *raznovrstan način* mogu pojaviti vektorski prostori, a time i vektori (isp. primjere u § 3.3). Sad ćemo, međutim, spoznati

drugu stranu medalje. Kao što se *pojedini broj* može pojaviti u *raznim* situacijama (npr. broj 2 kao dva oka, dva oraha, dvije dužine, itd.), tako se i pojedini *vektorski prostor* može pojaviti u naoko *raznim*, no *sličnim* vidovima. Tako ćemo npr. vidjeti da je svaki vektorski prostor dimenzije 2 (nad tijelom R) „sličan" ili „izomorfan" s prostorom R^2 svih dvočlanih nizova u R.

Zaključak je općenit.

—→ **4.6.1.** Teorem. *Neka su V, V' dva vektorska prostora nad tijelom R; ako je* $\dim V = \dim V' = n < \infty$, *tada su prostori V, V' izomorfni, tj, postoji tolikovanje* t[1] (*bijekcija*): $x \to tx$ prostora V na V' s *ova dva svojstva*:

L_1 $\qquad t(x+y) = tx + ty$ za svako $x, y \in V$

L_2 $\qquad t(\lambda x) = \lambda tx$ za svako $\lambda \in R$ i $x \in V$.

Specijalno, oba prostora V, V' izomorfna su s prostorom R^n svih n-članih nizova s vrijednostima u R (tj. R^n je skup svih jednoznačnih funkcija od $1(n)$ ka R, pri čemu je adiranje u R^n i množenje između elemenata iz R i onih iz R^n definirano na svagdašnji način)[2].

4.6.2. Sam teorem možemo ilustrirati „prostorom" rješenjâ npr. jednadžbe $2x - 3y + 5z = 0$. Prostor rješenja izomorfan je s ravninom (pa ta zadana jednadžba je slika ravnine!).

4.6.3. Dokaz teorema **4.6.1.** Neka je e baza u V a e' u V'; kako je $\dim V = \dim V' = n$, to prema teoremu 4.5.1. baze e, e' imaju svaka po n elemenata; pa neka je $e = \{e_\nu\}_\nu$, $e' = \{e'_\nu\}_\nu$; tu $\nu \in 1(n)$. Definirajmo sada funkciju t od e na e' zahtjevom $te_\nu = e'_\nu$. *Proširimo t* s baze e na čitav prostor V na *prirodan način*: neka je $v \in V$; tada je, prema teoremu o jednoznačnosti 4.4.2 moguće na *jedan jedini* način pisati

$$v = \sum_\nu v_\nu e_\nu .$$

Definirajmo tv relacijom

$$t\left(\sum_\nu v_\nu e_\nu\right) = \sum_\nu v_\nu t e_\nu .$$

Time je t definirano na *jednoznačan* način u čitavu prostoru V; no t je i *jednolisno*: ako je $v \neq u$ u V, tada je $tv \neq tu$; stvarno, iz $v \neq u$ izlazi $v_k \neq u_k$ za bar jedno $k \leq n$; dakle je i $v_k e'_k \neq u_k e'_k$ tj. $v_k te_k \neq u_k te_k$, dakle i $tv \neq tu$.

Dokažimo da su ispunjeni uslovi L_1 i L_2.

Pa neka je $x, y \in V$; tada je

$$x = \sum_\nu x_\nu e_\nu ,\ y = \sum_\nu y_\nu e_\nu ; \quad \text{odatle} \quad (x+y) = \sum_\nu (x_\nu + y_\nu)\, e_\nu ;$$

po definiciji (1) imamo odatle

$$f(x+y) = t \Sigma (x_\nu + y_\nu) e_\nu = \Sigma (x_\nu + y_\nu)\, te_\nu = \Sigma (x_\nu + y_\nu)\, e'_\nu = \Sigma x_\nu e'_\nu + \Sigma y_\nu e'_\nu =$$

$$= \Sigma x_\nu te_\nu + \Sigma y_\nu te_\nu = t \Sigma x_\nu e_\nu + t \Sigma y_\nu e_\nu = tx + ty .$$

---

[1] tj. obostrano jednoznačno preslikavanje.
[2] Možemo reći da je R^n „obični euklidski prostor od n dimenzijâ" nad tijelom R.

Analogno:

$$t(\lambda x) = t(\lambda \Sigma x_\nu e_\nu) = t \Sigma \lambda x_\nu e_\nu = \Sigma \lambda\ x_\nu t e_\nu = \lambda \Sigma x_\nu t e_\nu =$$
$$= \lambda t \Sigma x_\nu e_\nu = \lambda tx, \quad \text{tj.} \quad t(\lambda x) = \lambda tx$$
$$\text{za svako } \lambda \in R \text{ i svako } x \in V.$$

Time je izomorfizam prostorâ V, V' dokazan.

Još se radi o onom dodatku za prostor R^n; ovaj prostor ima n dimenzija, jer su redići e_ν jedinične matrice 1_n nezavisni članovi u R^n, u jednu ruku; u drugu ruku, za svaki član $x = (x_\nu) \in R^n$ očigledno je

$$x = x_1(1, 0, 0, \cdots) + x_2(0, 1, 0, \cdots) + \cdots =$$
$$= \sum x_\nu e_\nu, \quad \text{tj.} \quad L(R, \{e_\nu\}_\nu) = R^n.$$

Dakle redovi (odnosno stupci) matrice 1_n obrazuju bazu prostora R^n.

Teorem 4.6.1. je potpuno dokazan.

4.6.4. O homogeno-linearnim preslikavanjima vektorskih prostora.

Linearno preslikavanje t linearnog prostora u linearan prostor je svako preslikavanje t za koje vrijede gornji uslovi L_1 i L_2.

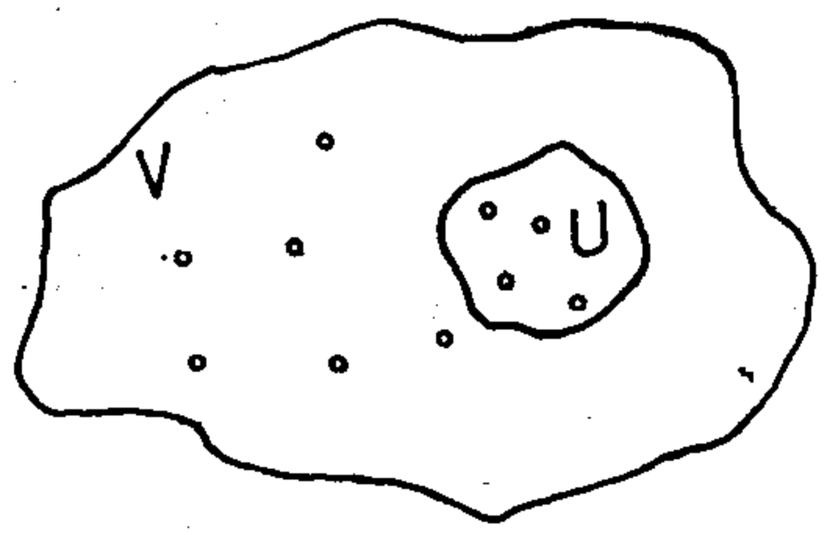
U toku dokazivanja u 4.6.3. dokazali smo i ovaj rezultat:

L e m a. *Linearno preslikavanje vektorskog prostora V potpuno je određeno poznavajući njegove vrijednosti u jednoj bazi prostora.*

4.6.5. Primjedba o osnovnom teoremu o istobrojnosti baza. Kako je taj teorem „istinit" za euklidske prostore R^n, to iz izomorfije prostora R^n i prostora V, za koji je $\dim V = n$, izlazi da je teorem o istobrojnosti baza istinit i za V.

4.7. Osnovni teorem o vektorskom prostoru, bazama, potprostoru i njegovu komplementu. — 4.7.0. Ideja vodilja. Neka su p i q dvije pravulje (pravca) koje se sijeku; neka nam njihovo sjecište služi kao nula (0) za računanje; ravnina R^2 što je određuju pravulje p i q izlazi kao množina svih suma $p' + q'$; svaka tačka ravnine predočena je na jedan jedini način u tom obliku.

Kaže se da je ravnina R^2 direktna suma pravuljâ p i q i piše $R^2 = p + q$.



Sl. 13.4.7. Članovi baze V i podbaze U markirani su tačkicama

4.7.1. Osnovni teorem o vektorskim prostorima, podbazama i potprostorima. ***Neka je $V = V_n(K)$ proizvoljan vektorski prostor nad tijelom K, i***

(1) $$e = (e_1\ e_2\ \ldots\ e_n)$$

proizvoljna baza toga prostora; svaki podskup e° od e razapinje određen podprostor $U = Le^\circ$ prostora V; posebno, ako je e° pravi podskup od e, tada prostor Le°

što ga rađa e° i prostor $U' = LCe^\circ$ što ga rađa skup $Ce^\circ = e \setminus e^\circ$ imaju svojstvo da je svako $v \in V$ predočivo na jedan jedini način u obliku

(2) $$v = v_u + v_{u'} \quad \textit{pri čemu} \quad v_u \in U, \quad v_{u'} \in U'.$$

2. Kaže se da je V *direktna suma prostorâ* U, U' i piše

(3) $$V = U \dot{+} U';$$

kaže se također da je U' *direktni komplement potprostora* U *u odnosu na prostor* V. Vrijedi

(4) $$U \cap U' = \{\vec{0}\} \text{ te } (4') \quad \dim V = \dim U + \dim U'.$$

D o k a z. Neposredno se provjerava da je Le° određen vektorski prostor i da je $\dim Le^\circ = ke^\circ$ (= broj članova u e°).

Isto tako

$$\dim LCe^\circ = k(e \setminus e^\circ) = ke - ke^\circ = \dim V - \dim Le^\circ.$$

Za zadanu bazu (1) prostora V, i za svako $v \in V$ imamo posve određen rastav

(5) $$v = v^1 e_1 + v^2 e_2 + \cdots + v^n e_n,$$

gdje su $v^\nu \in K$ članovi tela K; neka e° kao podniz od niza e glasi

(6) $$e^\circ = e_{i_1} e_{i_1} \cdots e_{i_m};$$

neka preostatak niza e glasi

(7) $$e_{j_1} \cdots e_{j_r};$$

tada, na osnovu zakona obrtanja i združivanja, iz (5) izlazi

(8) $$v = (v^{i_1} e_{i_1} + v^{i_2} e_{i_2} + \cdots + v^{i_m} e_{i_m}) + (v^{j_1} e_{j_1} + \cdots v^{j_r} e_{j_r}).$$

Vektor u prvoj zagradi je član u prostoru Le°; vektor u drugoj zagradi je član prostora LCe°; oba ta vektora određena su jednoznačno jer su jednoznačno određeni: rastav (5) i e° kao podniz (6) te Ce° kao podniz (7).

Nula-vektor $\vec{0}$ je svakako zajednički član od Le° *i* Ce°, međutim, to je i jedini zajednički član tih dvaju prostora. Stvarno, iz $v \in Le^\circ \cap LCe^\circ$ izlazi zbog $v \in Le^\circ$ prikaz

$$v = \sum_{\mu=1}^{m} x^\mu e_{i_\mu}$$

u bazi (6), *a* zbog $v \in LCe^\circ$ izlazi prikaz

$$v = \sum_{\rho=1}^{r} y^\rho e_{i_\rho} \text{ u bazi (7).}$$

Iz jednakosti

$$\sum_{\mu} x^\mu e_{i_\mu} = \sum_{\rho} y^\rho e_{i_\rho} \text{ odnosno}$$

$$\sum x^\mu e_{i_\mu} - \sum y^\rho e_{i_\rho} = \vec{0} \text{ i činjenice da su } e_{i_\mu}, e_{i_\rho}$$

članovi baze e samog prostora V *izlazi (zbog linearne nezavisnosti članova* baze) da su koeficijenti $=0$, tj.

$$x^{\mu}=0=y^{\rho} \text{ pri } \mu\in 1(m),\ \rho\in 1(r).$$

A to upravo znači da je $v=\vec{0}$, što se tvrdi relacijom (4).

Na sličan se način dokazuje

4.7.2. Teorem. ***Neka je vektorski prostor $V=V_n(K)$ dimenzije $n<\infty$; neka je V direktna suma svojih potprostora U_1, U_2 u smislu da je svaki $v\in V$ predočiv na jedincat način kao***

$$v=v_{u_1}+v_{u_2} \text{ pri } v_{u_i}\in U_i \ (i=1,2);$$

ako je $e^{(i)}$ vektorska baza u prostoru U_i $(i=1,2)$, tada je $e^{(1)}\cup e^{(2)}$ vektorska baza samog prostora $V=U_1+U_2$:

$$L(e^{(1)}\cup e^{(2)})=V; \text{ posebno je}$$

$$\dim V=\dim U_1+\dim U_2.$$

(kaže se također da je v_{u_1} projekcija na potprostor U_1 vektora $\vec{v}$ u smjeru potprostora U_2).

Kao poseban slučaj teorema 4.7.2. imamo

4.7.3. Teorem. *Neka je $V=V_n(K)$ proizvoljan prostor konačne dimenzije: neka je e vektorska baza prostora V, a U potprostor od V. Ako baza e ima izvan U najviše $\dim V-\dim U$ članova tj. ako je*

$$k((V\setminus U)\cap e)\leq \dim V-\dim U, \tag{1}$$

tada je $e\cap U$ baza potprostora U; posebno je tada

$$L(e\cap U)=U,\ \dim U=k(e\cap U) \tag{2}$$

$$\dim V=k(e\cap U)+k(e\cap(V\setminus U). \tag{3}$$

Naime iz identiteta

(4) $e=(e\cap U)\cup(e\setminus(V\setminus U))$ i mimoilaznosti (disjunktnosti) tih dvaju sastojaka izlazi

$$(V=)\,Le=L(e\cap U)+L(e\cap(V\setminus U)), \text{ a odatle}$$

(5) $\dim V=\dim L(e\cap U)+\dim L(e\cap(V\setminus U))$ i dalje obrazac (3).

Iz (1), (4) i očigledne relacije $\dim L(e\cap U)\leq \dim U$ izlazi tražena jednakost (2).

Primjedba. Bez *uslova* (1) zaključak (2) ne mora stajati: dovoljno je posmatrati euklidski prostor $V=R^3$, bazu $e=(e_1, e_2, e_3)$ i potprostor-pravulju U kroz O na kojoj ne leži ni jedan od vektora e_1, e_2, e_3; tada je $e\cap U=\varnothing$ pa $e\cap U$ *nije baza od* U.

4.8. *Zadaci o vektorskim prostorima.* Zadani su ovi „vektori"; jesu li i kako su međusobno linearno zavisni ili uopće nisu međusobno linearno zavisni:

0. brojevi 3, 4?
1. kompleksni brojevi $1+2i,\ 1-3i$?
2. kompleksni brojevi $3-2i,\ 4+5i,\ -3-i$?

3. jednadžbe
$$2x-3y+4=0$$
$$-3x+2y-2=0$$
$$2x-8y+12=0?$$

4. jednadžbe
$$2x-3y+4z=0$$
$$-3x+2y-2z=0$$
$$2x-8y+12z=0?$$

5. polinomi
$$2x^2-3x^5+4x^9$$
$$-3x^2+2x^5-2x^9$$
$$2x^2-8x^5+12x^9?$$

6. polinomi
$$2x-3y+4z$$
$$-3x+2y-2z$$
$$2x-8y+12z?$$

7. redići matrice
$$\begin{bmatrix} 2 & -3 & 4 \\ -3 & 2 & -2 \\ 2 & -8 & 12 \end{bmatrix}?$$

8. stupci matrice iz zad. 7?

9. funkcije $\cos \pi x$, $\sin \pi y$ definirane u skupu:

   1) R; 2) Q; 3) D; 4) $I3=\{0, 1, 2\}$; 5) $I2$?

10. funkcije x, x^2, x^3 definirane u skupovima iz zadatka 9?

11. matrice $a=\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ i $b=\begin{bmatrix} 3 & 4 \\ 1 & 2 \end{bmatrix}$?

12. matrice $\begin{bmatrix} 2 & 3 \\ -3 & 2 \end{bmatrix}, \begin{bmatrix} 5 & 4 \\ -4 & 5 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$?

13. matrice $a=\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, a^T, fa, fa^T?

14. matrice $a=\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$?

    Kako bi glasilo odgovarajuće pitanje i odgovor ako je matrica a poretka 2×3, odnosno $k \times m$?

15. nizovi
$$0, 1, 2, 3, 4, \ldots$$
$$0, 2, 4, 6, 8, \ldots?$$

16. stupci matrice $\begin{bmatrix} 0 & 1 & 2 & 3 \cdots \\ 0 & 1 & 4 & 9 \cdots \end{bmatrix}$?

17. Odredi vektorski prostor što ga razapinju vektori u zadatku $17^{\cdot} = 0, 1, 2, \cdots, 16$. Navedi 5 članova toga prostora.

18. Koliko ima neizomorfnih prostora iz zadatka 17? Navedi ih.

19. Odredi bazu u prostoru iz zadatka $17^{\cdot} = 0, 1, \cdots, 16$.

20. 1) Čine li svi cijeli algebarski polinomi u varijabli x s realnim koeficijentima određen vektorski prostor $R[x]$? 2) Da li je $\{1, x, x^2, \cdots x^n, \cdots\}$ baza u $R[x]$? 3) Isto pitanje za $\{x, x^3, x^5, \cdots\}$. 4) Kolika je dimenzija vektorskog prostora $L(R, \{1, x, x^2, x^3, \cdots\})$ odnosno $L(R, \{x, x^3, x^5, \cdots\})$ što ga razapinju „vektori" $1, x, x^2, \cdots$ odnosno „vektori" $x, x^3, x^5, \cdots$ A jesu li ta dva prostora izomorfna?

21. Neka V označuje prostor 1) realnih brojeva; 2) kompleksnih brojeva; 3) radijus-vektorâ u prostoru R^3; 4) realnih polinomâ u odnosu na x; 5) svih realnih neprekidnih funkcija s oblasti $R[a, b]$; 6) svih realnih neprekidnih funkcija u $R[a, b]$ koje su 0 u $\frac{1}{2}(a+b)$. Je li množenje sa $\alpha)$ 2, $\beta)$ $2x$, $\gamma)$ x^2, $\delta)$ $2x^2$ homogeno linearno preslikavanje prostora V?

5. OSNOVNI TEOREM O LINEARNOJ NEZAVISNOSTI STUPACA, ODNOSNO REDAKA U MATRICAMA. M-PODMATRICE. RANG MATRICE

5.0. P r i p r e m a. Kod ***svake*** matrice imamo određen skup stupaca i određen skup redaka. Nastaje pitanje o *maksimalnom* broju *nezavisnih redaka* matrice i o *pronalaženju takvih* redaka. Naime, time se rješava problem o *maksimalnom podsistemu nezavisnih linearnih jednadžbi* kojima je matrica jednaka sa zadanom matricom. Ili, što je isto: *kolika je dimenzija prostora što ga razapinju* (*određuju*) *redići* (*réci*) *matrice*? **Osnovna je spoznaja ova:** dimenzija prostora $R_1(a)$ što ga razapinju reci konačne matrice ista je kolika i dimenzija prostora $R_2(a)$ što ga razapinju stupci matrice i jednaka je ***maksimalnom stupnju regularne*** podmatrice zadane konačne matrice.

Tako npr. za

$$a = \begin{bmatrix} 3 & 5 & 4 & 2 & 4 \\ 3 & 1 & 2 & 0 & 5 \end{bmatrix} \text{ imamo } \dim R_1 a = \dim R_2 a = 2.$$

5.1. Osnovni pojam: M — submatrica Ma. Za *svaku* matricu a neka Ma označuje *bilo koju regularnu kvadratnu submatricu od a maksimalnog stupnja*; Ma se zove *M-submatrica od a* (veliko slovo M nas podsjeća da se radi o nekim maksimalnim podmatricama).

Uvođenje matrice Ma uz a vrlo pojednostavnjuje izlaganje.

Npr. za

$$a=\begin{bmatrix}3 & 1 & 2 & 4 & 5\\ 2 & 2 & 2 & 3 & 10\end{bmatrix}$$ imamo $Ma=\begin{bmatrix}3 & 1\\ 2 & 2\end{bmatrix}$, $Ma=\begin{bmatrix}3 & 2\\ 2 & 2\end{bmatrix}$;

također je $Ma=\begin{bmatrix}3 & 4\\ 2 & 3\end{bmatrix}$, $Ma=\begin{bmatrix}3 & 5\\ 2 & 10\end{bmatrix}$; nije $Ma=\begin{bmatrix}1 & 5\\ 2 & 10\end{bmatrix}$.

Ako je a beskonačna matrica, tada Ma ne mora postojati.

—→ **5.2. Definicija ranga *ra* matrice *a*.** Rang matrice a je supremum brojeva ν sa svojstvom da je neka (ν, ν)-podmatrica regularna (isp. pogl. 21. § 4.4). Rang matrice a označit ćemo sa ra, r_a ili naprosto sa r. Specijalno, ako u matrici a nema ni jedne regularne submatrice, tj. ako su sve vrijednosti $a_{ik}=0$, stavljamo $r_a=0$.

Npr. $r\begin{bmatrix}3 & 4 & 5 & 7 & 8\\ 6 & 8 & 10 & 14 & 16\end{bmatrix}=1$ jer je npr. $[3]=3$ regularna submatrica, a sve su submatrice višeg reda singularne, tj. [3] je jedna M-podmatrica.

Naravno, ako matrica ima konačno redaka ili konačno mnogo stupaca tada ona ima jednu M-podmatricu poretka (r, r).

5.3. Defekt matrice. Defekt ili nulost matrice a poretka (k, n) jest razlika n-r; označuje se sa da, odnosno d, def, dakle simbolički: $da=D_2\,a-r_a$, $\text{def}=D_2-r$ (isp. 26 § 4.3.1). Npr.

$$d\begin{bmatrix}1 & 2 & 3 & 4\cdots\\ 2 & 3 & 4 & 5\cdots\end{bmatrix}=\infty.$$

5.4. Znak $m_1 a$ za matricu a označuje *maksimalan broj linearno nezavisnih redaka matrice a.* Npr.

$$m_1\begin{bmatrix}1 & 2\\ 3 & 4\\ 5 & 6\\ \cdots & \cdots\end{bmatrix}=2 \text{ (dokaži to!).}$$

5.5. Znak $m_2 a$ za matricu a označuje *maksimalan broj*[1] *linearno nezavisnih stupaca matrice a.*

Npr. $m_2[1 \quad 2 \quad 3 \quad 4 \quad 5\cdots]=1.$

—→ **5.5.0. Osnovni teorem o nezavisnosti redaka (stupaca) i rangu matrica.** ***Za svaku matricu a koja je konačna bar u jednom smjeru brojevi $m_1 a$, $m_2 a$, ra su jednaki:***

(*r*) $$m_1 a = m_2 a = ra.$$

Za svaku podmatricu Ma od a, odgovarajućih $m_1 a$ redaka (stupaca) matrice a je linearno nezavisno. Drugim riječima, ako je matrica a poretka

---

[1] Umjesto izraza „maksimalan broj" bolje bi i ispravnije bilo svuda govoriti "supremum". Naravno radi li se o matricama konačne oblasti, ta su dva načina izražavanja ekvivalentna.

(k, n) pa ako je bar jedan od brojeva k, n konačan, tada je maksimalni broj njenih nezavisnih redaka jednak maksimalnom broju njenih nezavisnih stupaca, odnosno maksimalnom stupnju regularne podmatrice.

Tako npr. ako je $ra=3$, onda znamo da matrica a ima *bar jednu* regularnu podmatricu oblasti (3, 3), dok su *sve* kvadratne podmatrice stupnja >3 singularne; nadalje, ako je oblast matrice a konačna, onda znajmo da u matrici *postoje* 3 nezavisna retka (stupca), no da su *svaka* 4 retka (stupca) međusobno zavisna.

⟶ **5.5.1.** Korolar. *U svakoj matrici s konačnom oblasti maksimalni broj nezavisnih stupaca jednak je maksimalnom broju nezavisnih redaka:* $m_2=m_1$. *Drugim riječima, dimenzija prostora što ga određuju (razapinju) stupci konačne matrice ista je kolika i dimenzija prostora što ga razapinju redići te matrice a, ta je dimenzija jednaka ra.*

5.6. Dokaz osnovnog teorema 5.5. Dokaz jednakostî (*r*) proizaći će iz ovih relacija:

$$m_1 a = ra,\ ra = ra^T,\ ra^T = m_1 a^T,\ m_1 a^T = m_2 a.$$

Druga jednakost je neposredna posljedica jednakosti $\det a = \det a^T$ za svaku kvadratnu matricu a (v. pogl. 11, teorem 5.1); četvrta je očigledna; treća izlazi iz prve. Treba, dakle, još dokazati prvu jednakost; ona će biti dokazana time što ćemo dokazati da u njoj umjesto znaka = možemo pisati i $\leq$ i $\geq$.

5.6.1. Lema. $m_1 a \geq ra$.

Stvarno, neka je K proizvoljna kvadratna submatrica matrice a; pa neka je $\mathrm{st}\, K > m_1$; onda to znači da je K izvađena iz $\mathrm{st}\, K$ redaka matrice a; kako u a ima najviše m_1 nezavisnih redaka, znači to da je bar jedan redak u K linearna kombinacija preostalih redaka iz K; zato je (v. pogl. 11, teorem 10.6) nužno $\det K = 0$. Dakle je *svaka* kvadratna submatrica stupnja $>m_1$ nužno singularna; znači da za sve regularne kvadratne submatrice x mora biti $rx \leq m_1 a$, pa dakle i supremum $rx \leq m_1 a$, tj. $ra \leq m_1 a$.

5.6.2. Osnovna lema. $m_1 a \leq ra$.

Ta osnovna lema izlazi neposredoo iz ove činjenice:

⟶ **5.6.3. Lema.** *Neka je l prirodan broj; ako je l redaka (stupaca) bilo kakve matrice a linearno nezavisno, tada matrica tih redaka (stupaca) obuhvata jednu regularnu podmatricu stupnja (l, l).*

Dokaz. *Pretpostavimo* da tvrdnja 5.6.3. *nije tačna*, nego da, naprotiv, postoji l linearno nezavisnih redaka u matrici a i da njihova matrica f ne sadrži ni jedne regularne podmatrice stupnja (l, l). tj. da je $r(f) < l$. Pa neka je tada b jedna regularna podmatrica u f stupnja $r(f)$. Prema osnovnom teoremu 10.3. iz pogl. 11. izlazilo bi da su *svi* drugi redići matrice f — njih $l - r(f)$ na broju — linearno zavisni od $r(f)$ redaka iz kojih je izvučena matrica b — protivno pretpostavci da je svih l redaka matrice f linearno nezavisno. Slično se dokazuje i onaj dio leme o stupcima.

Time je lema 5.6.3 dokazana.

Odatle izlazi i lema 5.6.2, jer bi njena negacija dovela do relacije $m_1 a > ra$, koja je u suprotnosti s dokazanom lemom 5.6.3. Linearna nezavisnost stupaca

(redaka) svake M-podmatrice Ma, a time i odgovarajuće submatrice $a_1 Ma$ (odnosno $a_2 Ma$), (isporedi pogl. 10, § 2.8) proizlazi iz teorema 10.5. o determinantama u poglavlju 11.

Time je, najzad, osnovni teorem 5.5. potpuno dokazan.

—→ **5.7.** Teorem. *Za svaku matricu konačne oblasti prostor što ga određuju réci matrice izomorfan je s prostorom što ga određuju stupci te matrice. Dimenzija tih prostora jednaka je maksimalnom stupnju regularnih submatrica.*

Taj je teorem posljedica teorema 5.5. i teorema 4.6.1. o izomorfiji.

Sadržinu teorema 5.7. objasnite živo na kojoj posebnoj matrici kao npr. na

$$\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}, \quad \begin{bmatrix} 2 & 1 & 2 \\ 3 & 4 & 6 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \end{bmatrix}, \text{ itd.}$$

6. OSNOVNI TEOREMI O LINEARNOJ NEZAVISNOSTI NIZOVA

U praksi imamo specijalno često posla s ispitivanjem zavisnosti ili nezavisnosti *nizova*. Gornji osnovni teorem ima za posljedicu naredna tri teorema, kojima se često služimo.

6.1. Teorem. *Dva jednako duga niza po bar dva člana zavisna* (*nezavisna*) *su linearno onda i samo onda ako je jedan proporcionalan* (*nije proporcionalan*) *drugome*, tj. ako jedan izlazi (ne izlazi) iz drugoga množenjem sa stanovitom konstantom.

Tako su npr. nizovi $2, \quad 3, \ldots$

$1, \quad 2, \ldots$

nezavisni bez obzira na to kako glase dalji članovi i koliko ih ima. Stvarno, neka su $f = f_0, f_1, \ldots; g = g_0, g_1, \ldots$ dva zavisna jednako duga niza po bar dva člana. To znači da je svaka podmatrica stupnja 2 iz f, g singularna.

Posebno je

$$\begin{vmatrix} f_0 & f_1 \\ g_0 & g_1 \end{vmatrix} = 0;$$

odatle $f_0 g_1 = f_1 g_0$; odatle se zaključuje da je $f_0 = g_0 \lambda, f_1 = g_1 \lambda$ za neki broj λ; slično $f_2 = g_2 \lambda$ te $f_3 = g_3 \lambda$, itd.

—→ **6.2.** Teorem. *Da zadanih k nizova $f_{k'}$ po n članova $f_{k'n'}$ uz pretpostavku da je bar jedan od brojeva k, n konačan bude linearno nezavisno, nužno je i dovoljno da pripadna matrica $[f_{k'n'}]$ članova $f_{k'n'}$ sadrži jednu regularnu kvadratnu submatricu oblasti (k, k) (dakle je nužno broj nizova manji ili najviše jednak dužini n nizova).*

Taj teorem izlazi iz teorema 5.0. za slučaj da je $m_1 f = k$, tj. da su svi promatrani nizovi međusobno linearno nezavisni.

6.3. Teorem. *Da zadanih k nizova $f_{k'}$ po n članova uz pretpostavku da je bar jedan od brojeva k, n konačan bude međusobno linearno zavisno, nužno je i dovoljno da svaka kvadratna submatrica stupnja k bude singularna* (isp. teorem 10.2. u pogl. 11).

7. HOMOGENI LINEARNI SISTEMI I NEZAVISNOST NIZOVA

Na primjeru 4.2.2. vidjeli smo kako je ispitivanje linearne nezavisnosti nizova

$$f_0 = 2, \quad 3, \quad 5, \quad 4$$
$$f_1 = 3, \quad -4, \quad 2, \quad 3$$
$$f_2 = 5, \quad -3, \quad 4, \quad 2$$

ekvivalentno s pitanjem da li homogeni linearni sistem s matricom $[f_0, f_1, f_2]$ ima *jedino* trivijalno rješenje kao svoje rješenje.

Zaključak je općenit pa ga možemo izreći kao

7.1. Teorem. *Ako su stupci matrice homogenog linearnog sistema međusobno linearno nezavisni (zavisni), tada taj sistem homogenih jednadžbi osim trivijalnog rješenja nema (ima i) drugih rješenja; i obrnuto: ako homogen sistem linearnih jednadžbi osim trivijalnog rješenja nema (ima i) drugih rješenja, tada stupci matrice nisu (jesu) međusobno linearno zavisni.*

Na osnovu te organske veze o nizovima kao stupcima matrice homogenih sistema, a koja je izražena teoremom 7.1, možemo osnovne teoreme 6.1, 6.2. izreći za homogene linearne sisteme. Tako dobivamo ova dva korisna teorema:

7.2. Teorem. *Da zadani sistem homogenih linearnih jednadžbi nema, osim trivijalnog rješenja, nikojeg drugog rješenja, nužno je i dovoljno da matrica sistema sadrži jednu regularnu kvadratnu podmatricu kojoj je duljina jednaka broju nepoznanica.*

7.3. Teorem. *Da zadani sistem homogenih linearnih jednadžbi s n nepoznanica ima bar jedno netrivijalno rješenje, nužno je i dovoljno da matrica sistema ne sadrži ni jedne regularne submatrice stupnja n.*

⟶ 7.4. Linearna nezavisnost homogenih linearnih funkcija.

Teorem: ***Zadano je k linearnih homogenih funkcija***

(1) $$a_{i1}x_1 + \cdots + a_{in}x_n \ (i = 1, 2 \cdots, k) \text{ ili kraće } a_{k'} \circ \vec{x};$$

maksimalan broj tih funkcija koje su međusobno linearno nezavisne jednak je rangu $r(a)$ ***matrice*** $a = [a_{k'n'}]$ ***koeficijenata zadanih funkcijâ*** **(1).**

8. OSNOVNI REZULTATI O SISTEMIMA HOMOGENIH LINEARNIH JEDNADŽBI

8.0. Sad možemo *izreći* i *brzo dokazati* osnovne rezultate o *sistemima homogenih jednadžbi*, odnosno, o *matričnoj jednadžbi* $a\vec{x} = \vec{0}$.

Neka je

$$a = [a_{k'n'}] = \begin{bmatrix} a_{11} & a_{12} & a_{13} \cdots a_{1n'} \cdots \\ a_{21} & \cdots\cdots\cdots\cdots \\ \cdot & \\ \cdot & \\ a_{k'1} & \cdots\cdots\cdots a_{k'n'} \cdots \\ \cdots\cdots & \cdots\cdots \end{bmatrix}$$

matrica od k redaka i n stupaca; pri tom pretpostavljamo da su k, n prirodni brojevi ili n može biti i beskonačno.

Sistem S_0 homogenih linearnih jednadžbi s matricom a:

$$(S_0) \qquad \sum_{n'} a_{k'n'} x_{n'} = 0 \qquad (k' \in 1\,(k),\ n' \in 1\,(n))$$

znači isto što i matrična jednadžba

$$(1) \qquad \underset{(k,\,n)\,(n,\,1)}{a\vec{x}} = \underset{(k,\,1)}{\vec{0}}, \text{ gdje je } \underset{(n,\,1)}{\vec{x}} = \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ x_{n'} \\ \cdot \end{bmatrix}, \quad \underset{(k,\,1)}{\vec{0}} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \end{bmatrix}.$$

Neka je ra rang matrice a, tj. maksimalni stupanj regularnih submatricâ matrice a.

⟶ **8.1. Teorem o nezavisnosti jednadžbi.** *Da jednadžbe zadanog sistema homogenih linearnih jednadžbi budu linearno nezavisne, nužno je i dovoljno da rang matrice bude jednak broju jednadžbi:* $ra = k = k_1 a$.

⟶ **8.2. Teorem o reduciranim podsistemima.** ***Bilo koji podsistem od*** $r\,a$ ***jednadžbi s regularnom podmatricom stupnja*** $r\,a$ ***predstavlja reducirani podsistem jednadžbi u tom smislu da je to maksimalan skup linearno nezavisnih jednadžbi u sistemu. Svaki reducirani podsistem je ekvivalentan sa samim sistemom*** S**: oba imaju jedna te ista rješenja.**

Svi reducirani podsistemi međusobno su ekvivalentni.

⟶ **8.3.** *Skup svih rješenja od* (1) *obrazuje vektorski prostor od* $n\text{-}r\,(a) = def\,a$ *dimenzija.*

⟶ **8.4.** *Ako je* $n = r\,(a)$, *tada osim trivijalnog rješenja* $\vec{x} = \vec{0}$ *jednadžba* (1) *nema nikakva drugoga; i obrnuto.*

⟶ **8.5. (Fundamentalni skup ili baza rješenja).** ***Ako je*** $n > r\,(a)$, ***tada bilo kojih*** $d\,(:= n - r)$ ***nezavisnih rješenja reduciranog sistema, odnosno rješenja kojima matrica sadrži regularnu podmatricu*** [1] ***stupnja*** $d\,(a) = n - r$, ***čine bazu ili fundamentalni skup rješenja u tom smislu da se svako drugo rješenje sistema, odnosno jednadžbe*** (1) ***izražava linearno pomoću tih*** d ***rješenja.***

8.6. *Vektorski prostor tih rješenja izomorfan je s euklidskim prostorom* R^{Id} *od* $d = n - r$ *dimenzija.*

Broj d zove se »*defekt*« ili *nulitet* (*nulost*) *matrice a.*

U toku dokazivanja govorit ćemo na *jeziku jednadžbi*, a u zagradi ćemo naznačiti *matričnu* terminologiju pozivajući se na već dokazane činjenice o matricama.

---

[1] Broj $r\,(a)$ se može odrediti topovskom eliminacijom iz pogl. 8, § 2.6; broj zaokruženih članova je upravo $r\,(a)$ (dokaz u pogl. 15).

8.7. Dokaz teorema. 8.1. Ako je *svih* zadanih k jednadžbi (redaka) linearno nezavisno, onda prema osnovnom teoremu 5.5.0 vrijedi $k = r(a)$; i obratno ako je $k = r(a)$, svih k jednadžbi (redaka) je prema teoremu 5.5.0 linearno nezavisno.

8.8. Dokaz teorema 8.2. Prema osnovnom teoremu 5.5.0. maksimalni broj $m_1 a$ nezavisnih jednadžbi (redaka) jednak je rangu $r(a)$ matrice a. Prema teoremu 8.1. *bilo kojih* $r(a)$ jednadžbi (redaka) s regularnom podmatricom stupnja $r(a)$ predstavlja nezavisan sistem jednadžbi (redaka); to je, dakle, maksimalan nezavisan podsistem, pa je *svaka* eventualna *preostala* jednadžba (redak) linearan spoj tih $r(a)$ nezavisnih. Zato tih $r(a)$ nezavisnih jednadžbi predstavlja *reducirani podsistem*, jer su *sve druge* jednadžbe zadovoljene rješenjima tih $r(a)$ nezavisnih, bez obzira na to o kojim se nezavisnima jednadžbama — njih $r(a)$ na broju — radi!

8.9. Rješavanje reduciranog sistema (dokaz teorema 8.3; 8.4). Posebno je pitanje kako se dolazi do reduciranog podsistema. O tome će biti govora kasnije, u poglavlju 15.3.3. Ovdje je važno da vidimo kako se reducirani sistem rješava, jer se rješenja reduciranog podsistema podudaraju s rješenjima samog sistema.

8.9.1. Radi se o rješavanju $r\,(=r(a))$ nezavisnih jednadžbi, tj. o r jednadžbi s jednom regularnom podmatricom stupnja r. *Opći se slučaj* obrađuje upravo onako kao *poseban primjer* 1.4. Jasno je da, bez ograničenja, možemo uzeti da je podmatrica c stupnja r u lijevom gornjem uglu regularna, tj. da je

$$c_{ij} = a_{ij} \text{ za } i,j = 1, 2, \ldots r \text{ i da je } \det c \neq 0.$$

8.9.2. Ako je $n = r$, tada osim trivijalnog rješenja drugog nema: prema Cramerovu je pravilu

$$\det c \cdot x_{r'} = \det c\,(x_{r'}) = 0; \tag{1}$$

pri tom $c(x_{r'})$ označuje matricu koja iz matrice c nastaje kad se njen stupac $c_{r'}$ zamijeni nulama, što stoje na desnoj strani sistema. Iz (1) zbog $\det c \neq 0$ izlazi $x_{r'} = 0$ za $r' = 1, 2, \ldots, r$.

8.9.3. Ostaje slučaj $r < n$ (relacija $r > n$ nije moguća). Radi se, dakle, o sistemu jednadžbi koje možemo pisati ovako:

$$\sum_{r'} a_{ir'} x_{r'} = -a_{ir+1} x_{r+1} - a_{ir+2} x_{r+2} - \cdots - a_{in} x_n \quad (i = 1, 2, \ldots, r). \tag{2}$$

Odatle prema Cramerovu pravilu izražavamo r veličina $x_{r'}$ pomoću preostalih $n-r$ veličina $x_{r+1}, \ldots, x_n$, **koje su proizvoljne.**

Važno je imati na umu da se tih $n-r$ veličina proizvoljno mogu uzeti u osnovnom tijelu s kojim radimo i odakle su uzeti npr. koeficijenti

$$a_{ij} \quad \text{pri} \quad i,j = 1, 2, \ldots, r.$$

8.9.4. Specijalno je jednostavno te proizvoljne veličine $x_{r+1}, \ldots, x_n$ odabrati tako *da jedna jedina od njih bude* $= 1$, *a sve druge* 0, stavljajući po redu tako da se njihov niz podudara po redu sa svakim stupcem, odnosno retkom jedinične tablice:

$$I_{(n-r,\,n-r)} = \begin{bmatrix} 1 & & & 0 \\ & \cdot & & \\ & & \cdot & \\ & & & 1 \\ & & & & 1 \\ 0 & & & & & \cdot \\ & & & & & & \cdot \end{bmatrix}_{d=n-r}.$$

Kao i na specijalnom primjeru 1.4, vidi se da se na taj način dobije d rješenja sistema (2), od kojih se *svako drugo* rješenje izgrađuje linearno (formalan dokaz nalazi se malo niže u § 8.9.7). K tome je tih d rješenja linearno nezavisno, jer im tablica sadrži regularnu podmatricu stupnja d, npr. baš pomenutu jediničnu matricu I_d (vidi obrazac (4) u primjeru 1.4). To znači da sva rješenja zaista obrazuju vektorski prostor od d dimenzija (d je defekt matrice a). Time smo ujedno već dokazali i teoreme 8.3. i 8.4.

8.9.5. *Dokažimo teorem* 8.5. No, ako d rješenja reduciranog podsistema sadrži regularnu matricu stupnja d, onda su prema teoremu 5.5.0. ta rješenja linearno nezavisna. Imamo, dakle, posla s d nezavisnih rješenja, tj. onoliko kolika je i dimenzija prostora svih rješenja (teorem 8.3); to prema teoremu 4.5.1. o istobrojnosti baza znači da tih d rješenja čine bazu.

8.9.6. Najzad, teorem 8.6. je posljedica teorema u pogl. 13, § 4.6.1. o izomorfizmu vektorskih prostora, koji imaju isti konačan broj dimenzija.

Time su osnovni teoremi 8.1—8.6. o homogenim linearnim jednadžbama potpuno dokazani.

8.9.7. Formalan dokaz pasusa 8.9.4. Radilo se o rješavanju reduciranog sistema (2).

Nađimo, npr., x_1 jer se analogno određuju i druge veličine $x_{r'}$. Prema Cramerovu teoremu imamo:

$$\det [a_{r'r''}] \cdot x_1 = \begin{vmatrix} -\sum_{d'} a_{1\,r+d'}\, x_{r+d'}, & a_{12}, & \ldots, & a_{1r}\, a_{1r} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ -\sum_{d'} a_{r'\,r+d'}\, x_{r+d'}, & a_{r'2}, & \ldots & a_{r'r}\, a_{r'r} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \end{vmatrix}.$$

Stavljajući $d' = (n-r)'$ tj. $d' = 1, \ldots, d-1, d$, i služeći se aditivnim svojstvom determinanata (pogl. 11, § 3.2), postaje gornja jednadžba (stupci osim prvoga ostaju nepromijenjeni):

$$(\det c)\, x_1 = \sum_{d'} \begin{vmatrix} -a_{1\,r+d'}\, x_{r+d'}, \ldots \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ -a_{r'\,r+d'}\, x_{r+d'}, \ \cdot \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \end{vmatrix}.$$

Odatle

$$x_1 = -\sum_{d'} x_{r+d'} (\det c)^{-1} \cdot \begin{vmatrix} a_{1r+d'} & a_{12} & \cdots & a_{1r} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ a_{rr+d'} & a_{r2} & \cdots & a_{rr} \end{vmatrix}. \tag{3}$$

Time je x_1 izraženo pomoću proizvoljnih d veličina $x_{r+1}, \ldots, x_n$. Ujedno vidimo ovo: koeficijent od $x_{r+d'}$ iza znaka Σ upravo je ono rješenje $x_1^{(d')}$ za x_1 koje se dobije uzimajući

$$x_{r+d'} = 1, \; x_{r+t} = 0 \quad \text{za preostale} \quad t \in \{1, 2, \ldots, d\} \; \text{i} \; t \neq d'. \tag{4}$$

Na taj način obrazac (3) postaje

$$x_1 = \sum_{d'} x_{r+d'} x_1^{(d')}.$$

Analogno:

$$x_{r'} = \sum_{d'=1}^{d} x_{r+d'} x_{r'}^{(d')} \quad \text{za} \quad r' = 1, 2, \ldots, r. \tag{5}$$

Tako vidimo da je $x_{r'}$ linearni spoj od $x_{r'}^{(d')}$; stavimo li prema (4) također $x_{r+d'}^{(d')} = 1$, $x_{r+t}^{(d')} = 0$ za $d' \neq t = 1, 2, \ldots, d$, tada je svaki od d nizova $(x_{n'}^{d'})_{n'}$ jedno rješenje jednadžbi (2); osim toga i za njih očigledno vrijedi, formalno, obrazac (5) pišući n' umjesto r':

$$x_n = \sum_{d'} x_{r+d'} x_{n'}^{(d')}, \quad d = n - r. \tag{6}$$

Riječima: pomoću gornjih specijalnih d rješenjâ (vektorâ)

$$\overrightarrow{x^{(d')}} = \begin{bmatrix} x_1^{(d')} \\ \cdot \\ \cdot \\ \cdot \\ x_{n'}^{(d')} \\ \cdot \\ \cdot \end{bmatrix} = -\det c \begin{bmatrix} C_{1r+d'} \\ \cdot \\ \cdot \\ \cdot \\ C_{rr+d'} \\ (I_d)_{.d'} \end{bmatrix}$$

(C_{ij} je determinanta matrice koja iz c nastaje kad umjesto $c_{.j}$ pišemo $[a_{r'j}]$)

opće se rješenje $\vec{x}$ homogenog sistema (2) izgrađuje kao njihov linearni spoj:

$$\vec{x} = \sum_{d'} c_{d.} \overrightarrow{x^{(d')}},$$

pri čemu je $c_{d'}$ proizvoljan niz od d članova iz tijela R (sjetimo se da je $d = n - r$ defekt matrice a).

8.9.8. Još jedan način kako se rješava (reducirani) homogeni sistem — Frobeniusova metoda[1].

Prvi korak. *Odredi se rang $r(a)$ matrice a* ili, što je isto: *odredi se maksimalan broj linearno nezavisnih jednadžbi u sistemu*, tj. odredi se $r_1(a)$ jednadžbi s jednom regularnom podmatricom stupnja $r(a)$. Tako se nađe jedan

[1] G. Frobenius (1849—1917), njemački matematičar

reduciran podsistem i u tom podsistemu S_{00} jedna regularna podmatrica c stupnja $r(a)$. Od interesa je da ta podmatrica bude što jednostavnija. Inače, do takvih $r(a)$ jednadžbi možemo doći topovskom eliminacijom iz pogl. 9, § 2,6; to su one jednadžbe kod kojih su *zaokruženi topovski koeficijenti* (dokaz toga iznijet ćemo u pogl. 15, § 2.4).

Drugi korak. *Ispiše se matrica reduciranog podsistema; ona je poretka* $(r(a), n)$ *te se matrica nadopuni na matricu* $a(c)$ *poretka* (n, n) *tako da u njoj komplement uočene podmatrice* c *bude* ***jedinična matrica*** I_d od $d = n - r$ redaka; *na preostala mjesta matrice* $a(c)$ *stavimo* 0.

Ilustracija. Tako je npr. reducirani podsistem u primjeru 1.4. bio

$$2x_0 + 3x_1 - 5x_2 - 4x_3 + x_4 - x_5 + 5x_6 = 0$$
$$2x_0 + 3x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 0.$$

U toj matrici a možemo uzeti $c = M$-podmatrica =

$$= a \begin{matrix} 1 & 2 \\ 5 & 6 \end{matrix} = \begin{bmatrix} a_{15} & a_{16} \\ a_{25} & a_{26} \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}.$$

Tada je

$$a\underset{(n,\,n}{(c)} = \left|\begin{array}{ccccc|c} 2 & 3 & -5 & -4 & \boxed{\begin{matrix} 1 & -1 \\ 1 & 1 \end{matrix}} & 5 \\ 2 & 3 & 1 & 1 & & 1 \\ 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & & 1 \end{array}\right|$$

Jedinice se stavljaju po redu po jedna u svaki od pripisanih d redaka; nepopunjena mjesta su 0.

Matrica $a(c)$ je regularna (n, n)-matrica: determinanta joj je $= \det c$ ili $-\det c$. Razvijajući, naime, $\det a(c)$ po pripisanim recima, razvoj je jednak $\det c \cdot 1$ ili $\det c \cdot -1$.

Treći korak. Za (n, n)-matricu $a(c)$ i svaki njen pripisani redak $a(c)_{r+d'}$. nađe se redak

$$(\star) \qquad a(c)^{\Gamma}_{r+d'}, \quad (d' = 1, 2, \ldots, n-r)$$

odgovarajućih algebarskih komplemenata ili kofaktora. Tih d nizova (⋆) *komplemenata čine bazu svih rješenjâ reduciranog sistema.*

(*i*) U prvom redu, *ti su algebarski komplementi* (⋆) *rješenja reduciranog sistema*: prema Laplaceu, unutrašnji ili skalarni produkt niza (⋆) algebarskih komplemenata svakog *pripisanog* retka d' i svakog retka $a_{r'}$ kao *stranog* retka iznosi 0 tj. $a_{r'.} \circ a(c)^{\Gamma}_{r+d'.} = 0$; to znači da ti komplementi zadovoljavaju jednadžbu rednog broja r' za $r' = 1, 2, \ldots, r$ (imajmo na umu da je $a_{r'.} = a(c)_{r'}$). Dakle: zaista *dobivamo d rješenja* (⋆).

(*ii*) *Tih d rješenja* (*) *je linearno nezavisno.*
Da to ispitamo, promatrajmo njihov nula-spoj:

$$\sum_{d'} \lambda_{d'} \cdot a(c)^{\mathrm{r}}_{r+d'\cdot} = \vec{0}. \tag{1}$$

Odatle, množeći skalarno retkom $a(c)_{r+e}$ za svako $e = 1, \ldots, d$, izlazi

$$\sum_{e=1}^{d} \lambda_{d'}\, a(c)_{r+e\cdot} \circ a(c)^{\mathrm{r}}_{r+d'\cdot} = 0. \tag{2}$$

No, naznačeni skalarni produkt po Laplaceu je $\delta^{d'}_{e} \cdot \det a(c)$, dakle je $=0$ za $e \neq d'$ i $=1$ za $e = d'$. Tako se veza (2) svodi na jednakost $\lambda_{d'} \cdot \det a(c) = 0$, odakle zbog $\det a(c) \neq 0$ izlazi $\lambda_{d'} = 0$ za svako $d' \in 1, 2, \ldots, d$. To prema (1) znači da je svih d rješenja (*) međusobno linearno nezavisno.

(*iii*) *Svako rješenje reduciranog homogenog sistema jest linearni spoj gornjih d rješenja* (*). To izlazi iz teorema 8.3, na osnovu upravo dokazane nezavisnosti d rješenja (*).

8.10. Čest slučaj: Broj nepoznanica za 1 veći od broja jednadžbi: $n = k + 1$.
U tom slučaju matrica $a(c)$ ima bar jedan pripisan redić (ima upravo jedan pripisan redić ako je $r(a) = k = n-1$). Algebarski komplementi komponenata tog pripisanog redića mogu se razlikovati jedino u predznaku od niza determinanata što pripadaju podmatricama $a \setminus a_{\cdot n'}$; pri tom $a \setminus a_{\cdot n'}$ označuje matricu što se dobije iz a ispuštanjem njena stupca $a_{n'}$. Zato vrijedi:

Teorem. *Niz* $\xi_{n'} = (-1)^{n'+1} \det(a \setminus a_{n'})$ *čini rješenje promatranog skupa od k jednadžbi s* $n = k + 1$ *nepoznanicom. Ako je k tome bar jedno* $\xi_{n'} \neq 0$ *onda je opće rješenje proporcionalno s rješenjem* $\xi_{n'}$ *pa se obično zapisuje u obliku produženog razmjera* $\xi_1 : \xi_2 : \xi_3 : \ldots : \xi_{n'}$.

Tako npr. opće rješenje jednadžbi

$$2x - 3y + 4z = 0$$
$$2x + y - z = 0$$

glasi

$$x : y : z = \begin{vmatrix} -3 & 4 \\ 1 & -1 \end{vmatrix} : -\begin{vmatrix} 2 & 4 \\ 2 & -1 \end{vmatrix} : \begin{vmatrix} 2 & -3 \\ 2 & 1 \end{vmatrix} = -1 : 10 : 8,$$

tj. $$x = -\lambda, \quad y = 10\lambda, \quad z = 8\lambda \ (\lambda \text{ proizvoljno}).$$

8.11. Stavak. *Neka je V vektorski prostor dimenzije n (prirodan broj); tada je* $\vec{0}$ *jedini član iz V koji je okomit na svakom* $v \in V$, *tj.*

$$vx = 0 \text{ za svako } v \in V \text{ povlači } \vec{x} = \vec{0}.$$

Stavak 8.11 drukčije je izrečen stavak 8.4. Dokažimo 8.11 i neposredno. Ako naime odaberemo neku koordinatnu bazu $e = (e_1 \ldots, e_n)$, tada u odnosu na e_ν vektori x i ex dobivaju zapise $[x_1, x_2, \ldots, x_n]^T$ i $[0 \ldots 1, \ldots]^T$ pa se posebno jednakost $e_\nu x = 0$ ispisuje kao

$$1.\ x_\nu = 0, \quad \text{tj.} \quad x_\nu = 0 \quad \text{za svako } \nu \in \{1, \ldots, n\}.$$

8.12. Stavak. *Neka je V vektorski prostor dimenzije $n\in\{1, 2, \ldots, \}$ nad tijelom $R(i)$ kompleksnih brojeva; tada je $\vec{0}$ jedini član $x\in V$ koji je hermitski okomit na svaki član $v\in V$, tj. za koji je $v\ominus x=0$.*

Dokaz je kao u § 8.11.

9. Zadaci o linearnoj zavisnosti i skupovima homogenih linearnih jednadžbi.

1. Da li ova dva vektora čine vektorsku bazu u ravnini: 1) (0, 1), (1, 0), 2) (3, 4), (6, 8); 3) (2, 5), (−2, −5); 4) (3, 5), (−3, 5); 5) (3, 5), (3, −5); 6) (−3, 5), (−3, −5)?
2. Promatraj vektore $e_1=(0, 1, 1)$, $e_2=(1, 0, 1)$, $e_3=(1, 1, 0)$; $v=(1, 1, 1)$; dokaži da vektori e_1, e_2, e_3 čine bazu pa u njoj izrazi v.
3. Isto pitanje za vektore $e_1=(-2, 3, 5)$, $e_2=(-2, -3, 5)$, $e_3=(-2, -3, -5)$, $v=(3, 4, -6)$.
4. Isto pitanje za $e_1=(3, 4, 2)$, $e_2=(2, 4, 1)$, $e_3=(1, -3, 2)$, $v_1=(2, 1, 0)$, $v_2=(3, 2. 4)$, $v_3=(1, 2, 5)$, Da li v_1, v_2, v_3 čine bazu?
5. Odredi prostor što ga razapinju vektori $u=(3, 2, 1)$, $v=(2, 5, 4)$, $w=(1, -2, 3)$, $z=(5, 0, -4)$.
6. Odredi dimenziju i bar dvije baze prostora svih polinomâ a_0+a_1x+ $+a_2x^2+\cdots$ stupnja: 1) ≤ 1, 2) ≤ 2, 3) ≤ 3, 4) $\leq n$, 5) $<\omega$.
7. S kojim je euklidskim prostorom izomorfan prostor iz zad. 5? Odredi izomorfiju!
8. Da li svi vektori (x_1, x_2, x_3) čine vektorski prostor ako je ispunjen jedan od ovih uslova: 1) $x_1+x_2+x_3=0$, 2) $x_1+x_2+x_3=1$, 3) $x_1^2+x_2^2+x_3^2=1$, 4) $x_1+x_2=5$, 5) $x_1x_2x_3=1$, 6) $x_1=0$, 7) $x_1x_2=0$?
9. 1) Da li sve matrice s oblasti (n, n) čine vektorski prostor? 2) A ako su simetrične? 3) A ako su kososimetrične? Odredi bazu i dimenziju.
10. Neka su x, y, z linearno nezavisni vektori; odredi dimenziju prostora što ga određuju ovi vektori: 1) $2x, -y, -z$; 2) $x+y, y+z, z+x$; 3) $x-y, y-z, z-x$; 4) $2x-3y, 3x+2y-6z, -x-y-z$; 5) $2x+3y+4z, -2x+3y+4z, 2x-3y+4z, 2x+3y-4z, -2x-3y+4z, -2x+3y-4z, 2x-3y-4z, -2x-3y-4z$.
11. Odredi prostor što ga određuju nizovi zapisani kao 1) redići, 2) stupci u matrici $a=\begin{bmatrix}1 & 2 & 3\\ 0 & 1 & 2\\ 3 & 2 & 1\end{bmatrix}$; izrazi jedne pomoću drugih.

    Isto pitanje za proizvoljnu matricu koju zadaj sam.
12. Dokaži: 1) Ako su vektorski prostori V, V' izomorfni, imaju oni jednaku dimenziju; 2) ako je i izomorfizam prostora V na prostor V', tada baza e prostora V prelazi u bazu ie prostora $iV=V'$.

13. Odredi najveći broj linearno nezavisnih: 1) redaka u matrici

$$a=\begin{bmatrix} 2 & 0 & 3 & 4 \\ 20 & 4 & 26 & 44 \\ 0 & -2 & 2 & -2 \\ 10 & 2 & 13 & 22 \\ 8 & 4 & 8 & 20 \end{bmatrix};$$

2) stupaca u matrici a; 3), 4) linearnih homogenih jednadžbi kojima su koeficijenti redići matrice odnosno stupci matrice a. 5) Odredi prostor svih rješenja svih jednadžbi, iz 3); 6) odredi prostor svih rješenja iz jednadžbi 4); 7) izrazi nizove u redićima pomoću nizova u stupcima, i dualno; 8) odredi bar jednu M-podmatricu od a.

14. Primijeni Frobeniusovu metodu na slijedeći skup jednadžbi:

1)
$$\begin{aligned} x_1+2x_2+3x_3-4x_4-6x_5&=0\\ -4x_1+x_2-3x_3+5x_4-6x_5&=0\\ -2x_1+5x_2+3x_3-3x_4-18x_5&=0; \end{aligned}$$

2)
$$\begin{aligned} 2x_1+3x_2-6x_3-7x_4&=0\\ x_1-x_2-x_3-x_4&=0. \end{aligned}$$

15. Promatraj nizove: 1) 1, −1, 1, −1, 1 2) 1, −1, 1, −1, 1
2, 3, 4, 5, 6 1, 1, −1, 0, 0
3) 2 −2 2 −2 2
3 −3 3 −3 3
5 −5 5 −5 5;

koji od tih nizova zadovoljavaju jednadžbama iz zad. 14.1)? Koje od tih triju skupina nizova čine fundamentalni sistem rješenja? Navedi još koju bazu rješenja!

16. Riješi: 1)
$$\begin{aligned} 2x+3y-4z&=0\\ 5x-2y+z&=0 \end{aligned}$$
2)
$$\begin{aligned} 2x+3y-4z+5t&=0\\ x-y+z+t&=0\\ 3x+y-z-2t&=0. \end{aligned}$$

17. Za koje λ ima sistem 1)
$$\begin{aligned} 2\lambda x-y&=0\\ x-2\lambda y&=0 \end{aligned}$$
2)
$$\begin{aligned} 3x+2\lambda y-3z&=0\\ 2x+3y+\lambda&=0\\ 3\lambda x+2y-3z&=0 \end{aligned}$$
neko rješenje $\neq\vec{0}$?

18. Riješi: 1)
$$\begin{aligned} 2x-26y-4z&=0\\ -3x-24y-3z&=0 \end{aligned}$$
2)
$$\begin{aligned} 3x_1+5x_2-3x_3-4x_4&=0\\ 6x_1-7x_2+4x_3+5x_4&=0\\ 18x_1+4x_2+6x_3-2x_4&=0. \end{aligned}$$

Literatura: Vidjeti literaturu u poglavljima 8—12.

POGLAVLJE 14.

OPĆI SISTEMI LINEARNIH JEDNADŽBI. LINEARNA MATRIČNA JEDNADŽBA S JEDNOM NEPOZNATOM MATRICOM

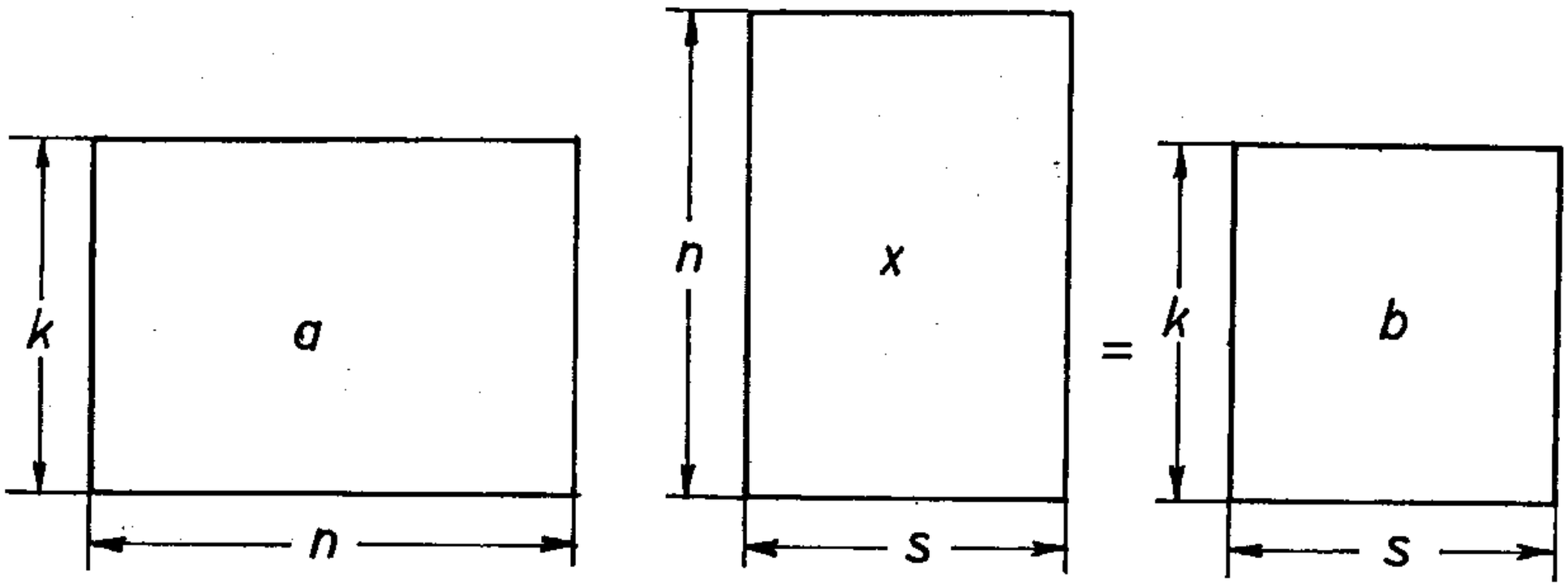
0. UVOD I GLAVNI REZULTATI

0.1. Ako je $a=[a_{k'n'}]$ matrica poretka (k, n), tada ćemo promatrati jednadžbu oblika

$$a\,x=b; \tag{1}$$

pri tom je b poznata, x nepoznata matrica. Naravno broj redaka od x jednak je n (broj stupaca od a); broj stupaca od x jednak je broju s redaka od b; dakle je x poretka (n, s), b je tipa (k, s). Shematski:

$$\underset{(k,n)}{a}\quad \underset{(n,s)}{x}=\underset{(k,s)}{b}$$



Matrična jednakost (1) stoji umjesto ks ovih »*skalarnih jednadžbi*«

$$\sum_{n'} a_{k'n'}\,x_{n's'}=b_{k's'}. \tag{1$_{k'}$}$$

Pri tom, ako ne kažemo drukčije, za svaki redni broj m, m' prolazi svim rednim brojevima 1, 2, ... množine $1\,(m)$; specijalno, brojevi k, n, s ne moraju biti konačni. Ako je npr. $n=\omega$, onda ω' prolazi svim prirodnim brojevima 1, 2, ... Jedanput više vidimo kako je pregledniji matrični način pisanja.

U specijalnom slučaju, kad su b, x vektori, tj. matrice poretka $(n, 1)$, možemo pisati i

(2) $$a\vec{x}=\vec{b}$$

ili eksplicitno: imamo ovaj sistem S od k jednadžbi:

S $$\sum_{n'} a_{k'n'}\, x_{n'} = b_{k'}.$$

Slučaj $b_{k'}=0$ obradili smo u prethodnom poglavlju 13. *Sadašnji slučaj svodi se stvarno na prethodni.* I čitavo je dokazivanje analogno onom što smo radili u „homogenom" slučaju u prošlom poglavlju. Razlika je jedino u tome što *jednadžba* (2), *odnosno sistem S, ne mora imati rješenja.* Uostalom, to već znamo iz *elementarne matematike,* jer npr. jednadžba $0\cdot x=1$ nema rješenja (među brojevima).

Rezultat ovog poglavlja sastoji se u ova dva teorema:

—→ **0.2.** Teorem. Kao što npr. pravulja $3x+2y=5$ kao skup rješenja te jednadžbe nastaje translacijom za $\begin{bmatrix} 0 \\ 5/2 \end{bmatrix}$ iz pravulje $3x+2y=0$, tako i u općem slučaju:

Skup svih rješenja od $ax=b$ nastaje »translacijom« za ξ iz skupa svih rješenja pripadne homogene jednadžbe $ax=0$ ili preglednije ispisujući ispod svake matrice njen poredak:

$$\underset{(k,n)}{a}\quad \underset{(n,s)}{x} = \underset{(k,s)}{b} \quad \Rightarrow x=\xi+\text{opće rješenje jednadžbe } ax=0;$$

pri tom je — ukoliko postoji — ξ jedno, inače bilo koje, rješenje polazne jednadžbe (1), *dakle je $a\xi=b$.*

Drugim riječima:

Ako matrična jednadžba $ax=b$ dopušta neko rješenje, npr. ξ, tada se opće rješenje te jednadžbe $ax=b$ dobije kao suma spomenutog rješenja ξ i općeg rješenja pripadne homogene jednadžbe

$$\underset{(k,n)\,(n,s)}{ax} = \underset{(k,s)}{0}.$$

—→ **0.3. Teorem o egzistenciji (Capelli — Kronecker).** ***Ako matrična jednadžba $ax=b$ ima neko rješenje, onda je $ra=r[a, b]$.*** **I obratno:** ***ako je $ra=r[a, b]$, tada postoji neka matrica x za koju vrijedi*** (1).

Pri tom za svaku matricu y, ry znači rang te matrice y, tj. supremum stupnjeva regularnih podmatrica u y; naravno, $[a, b]$ je matrica koja se dobije produžavanjem tablice a tablicom b kao stupcima.

Npr., ako je

$$a=\begin{bmatrix} 2 & 3 & 4 \\ 1 & 5 & 3 \end{bmatrix},\quad b=\begin{bmatrix} 7 & 3 \\ 2 & 4 \end{bmatrix},\quad \text{tada je } [a, b]=\begin{bmatrix} 2 & 3 & 4 & 7 & 3 \\ 1 & 5 & 3 & 2 & 4 \end{bmatrix}.$$

0.4. Matrica a zove se *matrica jednadžbe* $ax=b$, odnosno odgovarajućeg sistema (1); matrica $[a, b]$ zove se *proširena matrica* jednadžbe $ax=b$, odnosno odgovarajućeg sistema jednadžbi (1).

1. ILUSTRACIONI PRIMJERI

1.0. Primjer. Riješi sistem jednadžbi

$$\begin{aligned} x_0 + 2x_1 - 3x_2 &= 4 \\ 3x_0 + 9x_1 - x_2 - x_3 &= 3 \\ 5x_0 + 6x_1 + 2x_2 + x_3 &= 0 \\ 3x_0 - x_1 + 2x_3 &= 1 \\ 12x_0 + 16x_1 - 2x_2 + 2x_3 &= 8. \end{aligned} \tag{1}$$

1.0.1. Matrice sistema jesu:

$$a = \begin{bmatrix} 1 & 2 & -3 & 0 \\ 3 & 9 & -1 & -1 \\ 5 & 6 & 2 & 1 \\ 3 & -1 & 0 & 2 \\ 11 & 16 & -2 & 2 \end{bmatrix}, \qquad [a, b] = \begin{bmatrix} & 4 \\ & 3 \\ a & 0 \\ & 1 \\ & 8 \end{bmatrix}. \tag{2}$$

1.0.2. Postavlja se pitanje o *reduciranom podsistemu* jednadžbi (1). Stvar se rješava *isto kao i kod homogenog sistema: treba naći rang proširene matrice.* To ćemo pitanje obraditi sistematski kasnije, u poglavlju 15. Ovdje ipak vidimo da je posljednja jednadžba j_5 suma jednadžbi $j_{4'}$. Ili, što je analogno, redak $[a\,b]_5$ je suma redaka $[a\,b]_{4'}$. Zato se jednadžba j_5, odnosno redak $[a\,b]_5$ mogu brisati. Također se vidi da je $j_2 = j_1 + j_3 - j_4$; dakle se može brisati j_2. Preostaje još sistem

$$\begin{matrix} j_1 \\ j_3 \\ j_4. \end{matrix} \tag{3}$$

To znači da je rang polazne matrice $[a, b]$ ili 3 ili <3. No rang je upravo 3, jer je npr.

$$\det \begin{bmatrix} 1 & -3 & 0 \\ 5 & 2 & 1 \\ 3 & 0 & 2 \end{bmatrix} = 25, \quad \text{tj.} \quad \det a^{1\,3\,4}_{1\,2\,4} \neq 0 \quad (\text{također je } \det a^{1\,2\,3}_{1\,2\,3} \neq 0;$$

no u izabranoj podmatrici c stupci su jednostavniji). To znači da je $r\,a = r\,[a, b]$ $(= 3)$: sistem je moguć (prema teoremu 0.3).

1.0.3. *Nalaženje reduciranog podsistema.* To znači da (3) predstavlja reduciran podsistem polaznog sistema (1); on je konzistentan, jer mu obje matrice imaju isti rang: 3. Eksplicitno, taj ćemo reducirani sistem (3) napisati tako da odvojimo na jednu stranu veličine uz uočenu regularnu podmatricu c. Tako dobivamo ovaj

1.0.4. *Pripravljen oblik reduciranog podsistema.*

(4.)

$$\begin{aligned} x_0 - 3x_2 &= 4 - 2x_1 \\ 5x_0 + 2x_2 + x_3 &= -6x_1 \\ 3x_0 + 2x_3 &= 1 + x_1 \end{aligned}$$ ili matrično (4) $$\begin{bmatrix} 1 & -3 & 0 \\ 5 & 2 & 1 \\ 3 & 0 & 2 \end{bmatrix} \begin{bmatrix} x_0 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 4-2x_1 \\ -6x_1 \\ 1+x_1 \end{bmatrix}.$$

1.0.5. Sistem (4.), odnosno matričnu jednadžbu (4) znamo „riješiti", tj. naći uočene veličine x_0, x_2, x_3. Sistem (4.) možemo riješiti po Cramerovu teoremu; matričnu jednadžbu (4.) možemo riješiti množenjem te jednadžbe sprijeda sa c^{-1}, tj. inverzom „koeficijenta" c.

Radimo, radi vježbe, na oba načina.

1.0.6. U oba slučaja potrebna je determinanta

$$\det c = \begin{vmatrix} 1 & -3 & 0 \\ 5 & 2 & 1 \\ 3 & 0 & 2 \end{vmatrix} =$$

$=$ (razvijanje po prvom retku) $= 4 + -3 \cdot -7 = 25$, tj.

(5) $$\det c = 25.$$

1.0.7. Nađimo x_0 iz sistema (4) po Cramerovu teoremu:

$$x_0 = \frac{1}{25} \begin{vmatrix} 4-2x_1 & -3 & 0 \\ -6x_1 & 2 & 1 \\ 1+x_1 & 0 & 2 \end{vmatrix}.$$

Odatle, prema linearnom svojstvu determinanata, imamo

$$x_0 = \frac{1}{25} \left(\begin{vmatrix} 4 & -3 & 0 \\ 0 & 2 & 1 \\ 1 & 0 & 2 \end{vmatrix} + x_1 \begin{vmatrix} -2 & -3 & 0 \\ -6 & 2 & 1 \\ 1 & 0 & 2 \end{vmatrix} \right).$$

No, prva je determinanta $= 13$, a druga (razvij po trećem retku) $-3 - 44 = -47$.

Dakle je

(7) $$x_0 = \frac{1}{25}(13 - 47x_1).$$

Slično bismo našli

(8) $$x_2 = \frac{1}{25}(-29 + x_1)$$

(9) $$x_3 = \frac{1}{25}(-7 + 83x_1).$$

Niz x_0, x_1, x_2, x_3, za koji vrijedi (6), (7), (8), (9) uz proizvoljno x_1, jest opće rješenje reduciranog sistema (4.), a time i polaznog sistema (1).

To rješenje možemo pisati i u obliku:

$$\text{(10)}\qquad \begin{aligned} x_0 &= 13/25 - 47\lambda \\ x_1 &= \qquad\quad 25\lambda \\ x_2 &= -29/25 + \lambda \\ x_3 &= -7/25 + 83\lambda \end{aligned}$$

(λ proizvoljno u R, odnosno $R(i)$, odnosno u tijelu Q racionalnih brojeva, već prema tome kako se traži).

1.0.8. Iz (10) vidimo da je opće rješenje suma partikularnog rješenja

$$13/25,\quad 0,\quad -29/25,\quad -7/25$$

(koji se iz reduciranog sistema dobije stavljajući $\lambda = 0$) te općeg rješenja

$$-47\lambda,\quad 25\lambda,\quad \lambda,\quad 83\lambda$$

homogenog sistema što pripada sistemu (4). To i odgovara slovu teorema 0.2.

1.0.9. Matrični način rješavanja reduciranog sistema. Nađimo komatricu od A, tj. matricu Ac svih algebarskih komplemenata u c.

$$Ac = \begin{bmatrix} 4 & -7 & -6 \\ 6 & 2 & -9 \\ -3 & -1 & 17 \end{bmatrix}.$$ Tako je npr. to $-7 = (-1)^{1+2} \cdot \begin{vmatrix} 5 & 1 \\ 3 & 2 \end{vmatrix}$.

$$\text{(11)}\qquad c^{-1} = \frac{1}{\det c} Ac^T = \frac{1}{25} \begin{bmatrix} 4 & 6 & -3 \\ -7 & 2 & -1 \\ -6 & -9 & 17 \end{bmatrix}.$$

Pomnožimo li sprijeda matričnu jednadžbu (4) sa c^{-1}, dobivamo traženo rješenje

$$\begin{bmatrix} x_0 \\ x_2 \\ x_3 \end{bmatrix} = c^{-1} \begin{bmatrix} 4-2x_1 \\ -6x_1 \\ -1+x_1 \end{bmatrix} = \frac{1}{25} \begin{bmatrix} 4 & 6 & -3 \\ -7 & 2 & -1 \\ -6 & -9 & 17 \end{bmatrix} \cdot \begin{bmatrix} 4-2x_1 \\ -6x_1 \\ 1+83x_1 \end{bmatrix} =$$

$$= (\text{množeći te matrice}) =$$

$$= \frac{1}{25} \begin{bmatrix} 4 & (4-2x_1)+6 & (-6x_1)-3 & (1+x_1) \\ -7 & (4-2x_1)+2\cdot(-6x_1)-1\cdot(1+x_1) \\ -6\cdot(4-2x_1)-9\cdot & -6x_1+17\cdot(1+x_1) \end{bmatrix} = \frac{1}{25} \begin{bmatrix} 13-47x_1 \\ -29+x_1 \\ -7+83x_1 \end{bmatrix}.$$

Dakle je

$$\text{(12)}\qquad \begin{bmatrix} x_0 \\ x_2 \\ x_3 \end{bmatrix} = \frac{1}{25} \begin{bmatrix} 13-47x_1 \\ -29+x_1 \\ -7+83x_1 \end{bmatrix}.$$

Stavljajući $x_1 = \mu$, dobivamo ovo opće rješenje jednadžbi (1):

$$\begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} = \frac{1}{25} \begin{bmatrix} 13 - 47\,\mu \\ \mu \\ -29 + \mu \\ -7 + 83\,\mu \end{bmatrix};$$

ono se može pisati i u obliku:

$$\begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} = \frac{1}{25} \begin{bmatrix} 13 \\ 0 \\ -29 \\ -7 \end{bmatrix} + \frac{\mu}{25} \begin{bmatrix} -47 \\ 1 \\ 1 \\ 83 \end{bmatrix}, \text{ odnosno}$$

$$\begin{aligned} x_0 &= 13/25 - 47\,\mu/25 \\ x_1 &= \mu/25 \\ x_2 &= (-29 + \mu)/25 \\ x_3 &= (-7 + 83\,\mu)/25. \end{aligned} \tag{13}$$

Vidimo da smo došli do istog rješenja kao maloprije: rješenja (10) i (13) su ista (dovoljno je staviti $\mu = 25\,\lambda$).

1.0.10. Pokus za rješenja (12) i jednadžbu (4).

$$(4)_1 = \begin{bmatrix} 1 & -3 & 0 \\ 5 & 2 & 1 \\ 3 & 0 & 2 \end{bmatrix} \cdot \frac{1}{25} \begin{bmatrix} 13 - 47\,x_1 \\ -29 + x_1 \\ -7 + 83\,x_1 \end{bmatrix} =$$

$$= \frac{1}{25} \begin{bmatrix} 1 & (13 - 47\,x_1) - 3 \cdot (-29 + x_1) \\ 5 & (13 - 47\,x_1) + 2 \cdot (-29 + x_1) + 1\,(-7 + 83\,x_1) \\ 3 \cdot (13 - 47\,x_1) + 0 & (-29 + x_1) + 2\,(-7 + 83\,x_1) \end{bmatrix} =$$

$$= \frac{1}{25} \begin{bmatrix} 13 + 87 - 50\,x_1 \\ 65 - 58 - 7 \quad -235\,x_1 + 2\,y_1 + 83\,x_1 \\ 39 - 14 - 141\,x_1 + 166\,x_1 \end{bmatrix} =$$

$$= \frac{1}{25} \begin{bmatrix} 100 - 50\,x_1 \\ 150\,x_1 \\ 35 + 25\,x_1 \end{bmatrix} = \begin{bmatrix} 4 - 2\,x_1 \\ 6\,x_1 \\ 1 + x_1 \end{bmatrix} = (4)_2.$$

Dakle, matrica (12) zbilja zadovoljava (4); to ujedno znači da je napravljena proba za rješenja (13) s obzirom na sistem (4) i da je proba dala ispravan rezultat. Dakle je (13) zaista opće rješenje reduciranog sistema (4), a time i polaznog sistema (1).

1.1. Riješi $ax=b$ ako je

$$a=\begin{bmatrix} 2 & 3 & -5 & -4 & 1 & -1 & 5 \\ -2 & -3 & 8 & 4 & -1 & 1 & -5 \\ 2 & 3 & 1 & 1 & 1 & 1 & 1 \\ 2 & 3 & 7 & 6 & -1 & 3 & 3 \end{bmatrix}, \quad b=\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

U pogl. 13, § 1.4. ustanovili smo da je rang matrice a jednak 2, tj. $ra=2$; no rang proširene matrice je >2, jer joj je npr. podmatrica

$$[a, b]^{1\,2\,3}_{5\,6\,8} \text{ regularna: } \begin{vmatrix} 1 & -1 & 1 \\ -1 & 1 & 0 \\ 1 & 1 & 0 \end{vmatrix} = -2.$$

Zato prema teoremu 0.3. zadana jednadžba $ax=b$ nema rješenja.

2. DOKAZI TEOREMA 0.2. i 0.3.

2.0. Dokaz teorema 0.2.

2.0.0. Dokaz se može prepustiti kao vježba: tako je prost. Stvarno, pretpostavimo da postoji bar jedno rješenje zadane jednadžbe

$$ax=b; \tag{1}$$

pa neka je onda ξ jedno rješenje te jednadžbe, dakle

$$a\xi=b. \tag{2}$$

Oduzmemo li tu jednadžbu od zadane jednadžbe $ax=b$, izlazi

$$ax-a\xi=b-b$$

$$a(x-\xi)=\underset{(k,s)}{0}. \tag{3}$$

Prema tome, razlika

$$y=x-\xi \tag{4}$$

zadovoljava homogenu jednadžbu

$$ay=\underset{(k,s)}{0}, \tag{1_0}$$

što pripada zadanoj jednadžbi (1).

Obrnuto, iz (1_0) i (2) zbrajanjem izlazi

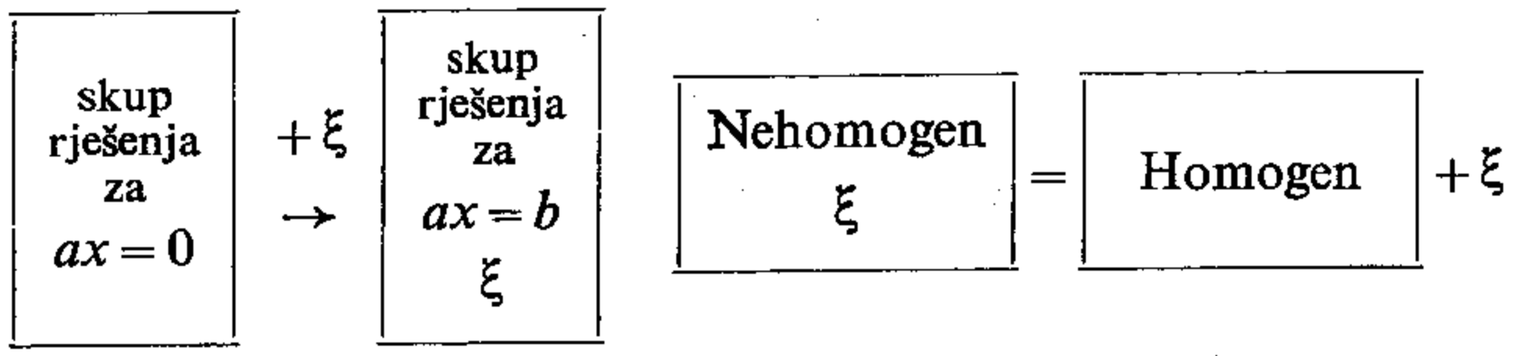
$$ay+a\xi=\underset{(k,s)}{0}+b$$

$$a(y+\xi)=b. \tag{5}$$

Jednadžba (3) kaže ovo: *razlika* $x-\xi$ *svakog rješenja polazne jednadžbe i bilo kojeg rješenja te jednadžbe zadovoljava homogenu jednadžbu* (1_0); dualno, jednadžba (5) kaže: *suma svakog rješenja homogene jednadžbe i proizvoljnog rješenja* ξ *zadane jednadžbe rješenje je zadane jednadžbe.*

Slikovito možemo reći: skup rješenja jednadžbe (1) nastaje svakom translacijom za ξ iz množine rješenja jednadžbe (1_0); pri tom ξ zadovoljava (1).

Shematski:



Formalno možemo to strogo definirati.

2.0.1. Oznaka za skup rješenja. Za jednadžbu ili sistem S jednadžbi neka $s\,S$ označuje skup svih rješenja sistema S (s je početno slovo lat. riječi solutio = rješenje).

Npr. $s\,(3\,x=6)=\{2\}$, $s\,(0\cdot x=1)=$ prazan skup.

Tada za teorem 0.2. imamo ovaj iskaz:

⟶ **2.0.2. Teorem. Ako je skup** $s\,(ax=b)$ **neprazan, tada je**

(b) $$s\,(ax=b)=s\,(ax=0)+\xi \text{ za svako } \xi\in s\,(ax=b).$$

Pri tom, naravno, $s\,(ax=b)+\xi$ naznačuje skup svih suma oblika

$$y+\xi, \quad \text{gdje je } y\in s\,(ax=b).$$

2.0.3. Primjedba. Gornja veza između *nehomogenog slučaja* ili *slučaja sa »smetnjama«* i *homogenog slučaja* (»*smetnje su* 0«) vrlo je česta u matematici i njenim primjenama.

2.1. Dokaz teorema 0.3. (isp. također pogl. 15, § 3.11). Teorem je glasio ovako:

2.1.0. (Teorem o egzistenciji). *Ako matrična jednadžba* $ax=b$ *ima neko rješenje, onda je* $ra=r\,[a, b]$; *i obrnuto, ako je* $ra=r\,[a, b]$, *tada jednadžba* $ax=b$ *ima neko rješenje.*

2.1.1. Nužnost. Naravno, $ra\leq r\,[a, b]$. Treba dokazati i dual: $ra\geq r\,[a, b]$. To će izaći iz ove činjenice: postojanje jednadžbe (1) ima za posljedicu ovaj zaključak: *ako svaka kvadratna podmatrica reda* h *u* a *ima determinantu* $=0$, *tada to vrijedi i za svaku kvadratnu podmatricu* m *reda* h *iz* $[a, b]$.

Pa neka je $m\subset[a, b]$, $\operatorname{st} m=h$. Treba dokazati da je

(7) $$\det m=0.$$

Prema pretpostavci, relacija (7) vrijedi ako je $m \subset a$. Zato možemo pretpostaviti da m ima bar jedan stupac iz b; radi jednostavnosti pretpostavimo da podmatrica m ima samo jedan stupac iz b; to je onda nužno posljednji stupac $m_{.h}$. Dakle je $m_{.h}$ podstupac jednog stupca u b, recimo baš od prvog podstupca $b_{.1}$. No, pretpostavljena jednadžba $ax = b$ kaže da je $b_{.1} = ax_{.1}$ (tako se množe matrice!), tj.

$$b_{.1} = \begin{bmatrix} \sum_{\nu} a_{1\nu} x_{\nu 1} \\ \cdots\cdots \\ \sum_{\nu} a_{k\nu} x_{\nu 1} \end{bmatrix}.$$

Na taj način, ispisujući u $\det m$ samo njen posljednji stupac, imamo:

$$\det m = \begin{vmatrix} \cdots \sum_{\nu} a_{1\nu} x_{\nu 1} \\ \cdots\cdots\cdots \\ \cdots \sum_{\nu} a_{k\nu} x_{\nu 1} \end{vmatrix} =$$

$=$(linearni karakter $\det m$ prema posljednjem stupcu, v. pogl. 11, teorem 4.4.1)$=$

$$= \sum_{\nu} \begin{vmatrix} \cdots a_{1\nu} \\ \cdot \\ \cdot \\ \cdot \\ \cdots a_{k\nu} \end{vmatrix} x_{\nu 1} = 0,$$

jer su sve determinante iz $\sum$ jednako 0. Promatrajmo, naime, matricu

$$z = \begin{bmatrix} \cdots a_{1\nu} \\ \cdot \\ \cdot \\ \cdot \\ \cdots k_{k\nu} \end{bmatrix}$$

i specijalno njen posljednji stupac $z_{.h}$.

P r v i s l u č a j: stupac $z_{.h}$ jednak je jednom od preostalih stupaca matrice z, odnosno matrice m (jer prvih $h-1$ stupaca imaju one iste!). Tad je, naravno, $\det z = 0$ (dva jednaka stupca u z).

D r u g i s l u č a j je negacija prvog: posljednji stupac u z nije isti s nikojim od preostalih stupaca u z. Ako je poredak stupaca u z isti kao poredak odgovarajućih stupaca u a, onda je $z \subset a$, pa je prema pretpostavci $\det z = 0$; ako pak nije $z \subset a$, onda premještanjem stupca $z_{.h}$ na odgovarajuće mjesto kao u a nastaje iz z potpuno određena matrica μ, za koju je $\mu \subset a$, dakle i $\det \mu = 0$ jer je $\operatorname{st} \mu = h$. No, $\det \mu$ se samo u predznaku može razlikovati od broja $\det z$ (μ nastaje iz z transpozicijom stupaca); dakle je

$$\det z = \pm \det \mu = \pm 0 = 0.$$

Time je, najzad, relacija (7) dokazana. Doduše, mi smo ispitivali jedino slučaj kad m ima samo jedan podstupac od b; no preostali slučajevi, kad m ima

2, 3, ... podstupca od b, obrađuje se slično. Tako npr. ako je *svaki* stupac $m_{\cdot k'}$ od m podstupac od $b_{\cdot k'}$ i tada je gornje zaključivanje na snazi, samo što je pisanje zamršenije.

Treba imati na umu da je

$$b_{\cdot i_{k'}} = ax_{\cdot i_{k'}}, \quad \text{dakle}$$

$$m_{l i_{k'}} = \sum_{\nu} a_{l\nu} x_{\nu t_{k'}}$$

za svako $l \in 1(h)$; primjenjujući distributivnost u $\det m$ s obzirom na njene stupce, zaključuje se, kao i maloprije, da je $\det m = 0$.

2.1.2. *Uslov je dovoljan: ako je* $ra = r[a, b]$, tada postoji neka matrica x za koju je $ax = b$. Dokaz ćemo svesti na naše znanje o homogenim jednadžbama i osnovni teorem iz pogl. 11, § 10.3. o determinantama.

Radi kratkoće stavimo $r = ra$; dakle također, zbog pretpostavke

$$ra = r[a, b], \qquad \text{imamo} \qquad r = r[a, b].$$

Pa neka je c, $c \subset a$, regularna kvadratna podmatrica dužine r. Radi jednostavnosti pisanja i izražavanja možemo pretpostaviti da je c smješteno u gornjem lijevom uglu u a, tj. da je $c_{\cdot r'} \subset a_{\cdot r'}$, $c_{r'\cdot} \subset a_{r'\cdot}$. (inače se transpozicijama redaka i stupaca u a može uvijek ostvariti ta nebitna pretpostavka). No, prema pretpostavci vrijedi $r[a, b] = ra = r = \mathrm{st}\, a$, $\det c \neq 0$; naravno, $c \subset [a, b]$. I sada dolazi primjena osnovnog teorema iz pogl. 11, § 10.3. o determinantama.

Prema tome teoremu svaki stupac matrice $[a, b]$ je linearan spoj onih r stupaca matrice $[a, c]$ iz kojih je izvađena matrica c; no $c \subset a$; dakle je svaki stupac $b_{\cdot r'}$ od b linearna kombinacija od r stupaca matrice a, pa, i pogotovu od svih n stupaca matrice a; to znači da postoji niz $(\lambda_{\nu, s'})_{\nu}$ sa svojstvom

$$\sum_{\nu} \lambda_{\nu s'} a_{\cdot \nu} = b_{\cdot s'}, \qquad \text{dakle}$$

$$\sum_{\nu} a_{k'\nu} \lambda_{\nu s'} = b_{k's'}.$$

To upravo znači da je $a\lambda = b$, gdje je $\lambda = [\lambda_{\nu s'}]$. Time je nađeno rješenje $x = \lambda$ zadane jednadžbe $ax = b$.

3. KAKO SE RJEŠAVA JEDNADŽBA $ax = b$, ODNOSNO PRIPADNI SISTEM SKALARNIH JEDNADŽBI?

3.0. Polazimo od matrične jednadžbe

(1) $$ax = b,$$

odnosno od sistema jednadžbi

(1) $$\sum_{\nu} a_{k'\nu} x_{\nu s'} = b_{k's'} \ (\nu \in 1(n)).$$

Poznato je $a = [a_{k'n'}]$, $b = [b_{k's'}]$; traži se $x = [x_{n's'}]$; znači da su oblasti a, x, b po redu (k, n), (n, s), (k, s).

3.1. Prvi korak: **Egzistencija.** Odredi se rang matrice a i rang $r[a, b]$ (sistematsko određivanje ranga matrica uzeto je na posebnom mjestu u pogl. 15); inače se $r(a)$, odnosno reduciranı sistem, vrlo zgodno određuje topovskim postupkom iz pogl. 8, § 2.6; onaj sistem jednadžbi sa zaokruženim ili topovskim dijelovima upravo je jedan reducirani sistem).

Ako je $ra < r[a\ b]$, rješenja nema, i stvar je gotova.

Ako je $ra = r[a, b]$, rješenje postoji (teorem 0.3), pa ga treba naći.

3.2. Slučaj kad je a regularna kvadratna konačna matrica. Ako je $\det a \neq 0$, tj. ako je $ra = \mathrm{st}\, a$, tada je automatski $r[a, b] = ra$. U tom slučaju treba naći a^{-1} kao $\frac{1}{\det a} f a^T$ pa rješenje x glasi $x = a^{-1} b$ (isp. pogl. 12, § 5.2).

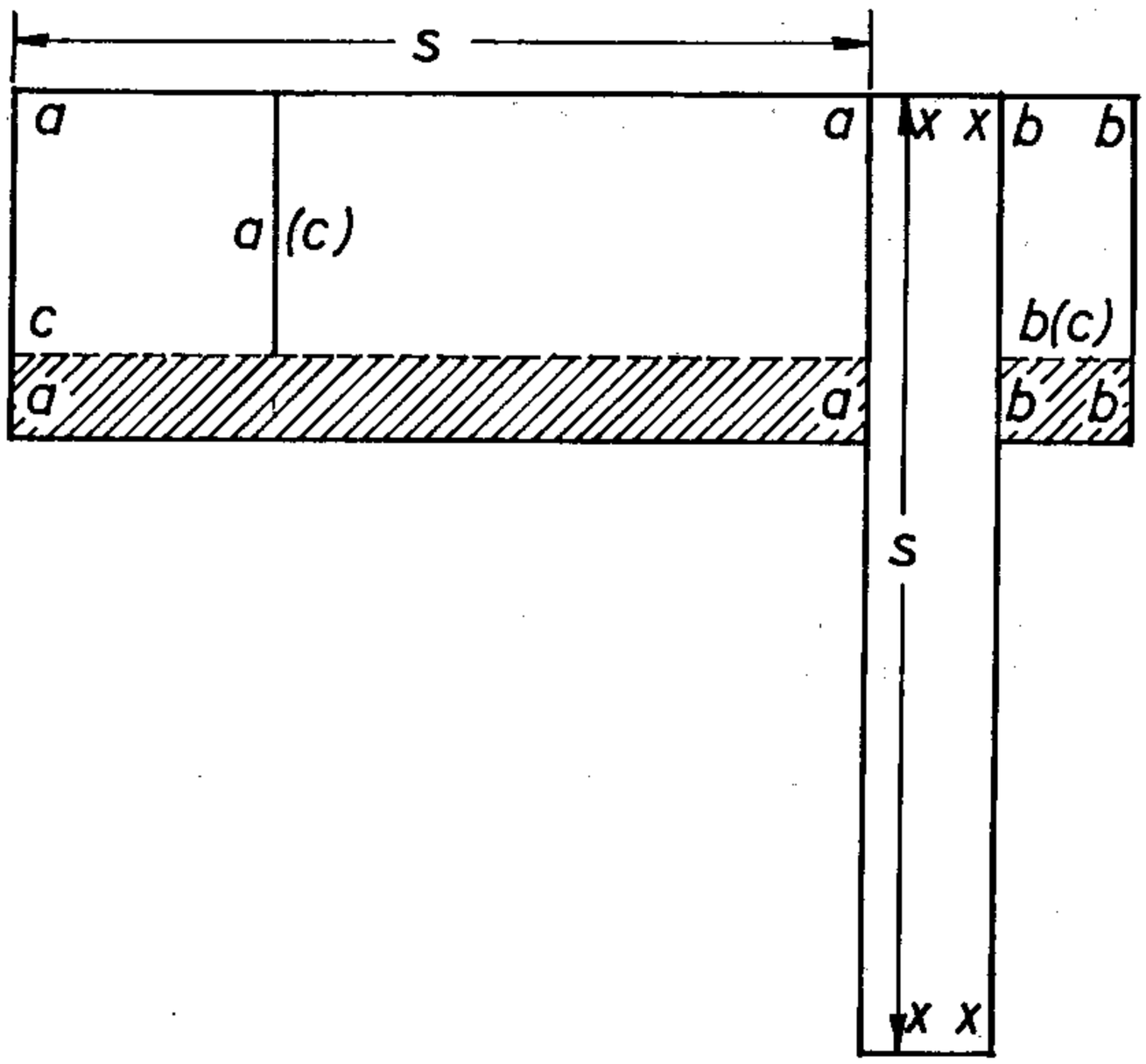
3.3. *Matrice* c, $a(c)$, $b(c)$, $[a, b]$ (c). Kad se ustanovilo da je $ra = r[a, b]$ i da je taj broj r prirodni broj,[1)] onda se odredi jedna što jednostavnija regularna podmatrica $c \subset a$ reda r. Pripadni redići matrice a obrazuju određenu matricu — označimo je sa $a(c)$. Odgovarajući redići u $[a, b]$ i b obrazuju podmatrice, označimo ih sa $[a, b]c$, $b(c)$. Radi jednostavnosti pisanja, govorenja i skiciranja možemo pretpostaviti da je c u gornjem lijevom uglu matrice a. Tom nebitnom pretpostavkom koristili smo se u više navrata.

3.4. Reducirani podsistem. Reducirana jednadžba.

Jednadžba

$$a(c)\, x = b(c) \tag{2}$$

zove se *reducirana jednadžba* što pripada *polaznoj jednadžbi*;



Sl. 14.3.4. Dio koji nije isjenčan predstavlja podjednadžbu $a(c)\, x = b(c)$.

[1)] Slučaj kad je r beskonačno predstavlja posebnu studiju.

sistem

$$\sum_{n'} a(c)_{r'n'} x_{n's'} = b(c)_{r's'} \tag{2}$$

zove se *reducirani podsistem zadanog sistema* (1).

Na slici 14.3.4. je shematski predstavljena zadana jednadžba $ax = b$ te reducirana »*podjednadžba*« $a(c)\,x = b(c)$ time što smo isjenčili ono što ne spada toj „podjednadžbi".

3.5. Teorem. *Reducirani podsistem ima ista rješenja koja i sam zadani sistem*; ili ovako matrično: *ako je* $a(c)\,x = b(c)$, tada je $ax = b$. Dokažimo to.

Prema pretpostavci je $a(c)\,x = b(c)$, tj.

$$a(c)_{r'}.\,x = b(c)_{r'}.. \tag{3}$$

Treba dokazati da je onda također $ax = b$, tj.

$$a_{k'}.\,x = b_{k'}. \tag{4}$$

(naime a, b imaju po k redaka).

No, za rangove matrica c, $a(c)$, $[a, b]$, $[a(c),\ b(c)]$ znamo da je jedan te isti broj r = stupanj od c. Prema osnovnom teoremu o linearnoj zavisnosti (v. pogl. 11, § 10.3) znači to da je svaki redak $[a, b]_{k'}.$ matrice $[a, b]$ linearna kombinacija od r redaka $[a(c),\ b(c)]_{r'}.$ matrice $[a(c),\ b(c)]$. Postoji, dakle, r brojeva $(\lambda_{r'}^{k'})_{r'}$ za koje je

$$[a, b]_{k'}. = \sum_{r'} \lambda_{r'}^{k'} [a(c),\ b(c)]_{r'}.. \tag{5}$$

Odatle specijalno izlaze odgovarajuće veze za matrice a i b:

$$a_{k'}. = \sum_{r'} \lambda_{r'}^{k'} a(c)_{r'}. \tag{6}$$

$$b_{k'}. = \sum_{r'} \lambda_{r'}^{k'} b(c)_{r'}. \tag{7}$$

Imajmo na umu cilj (4); pomnožimo zato (6) zdesna matricom x; zbog distributivnog svojstva matričnog množenja, dobivamo:

$$a_{k'}.\,x = \sum_{r'} (\lambda_{r'}^{k'} a(c)_{r'}.)\,x = \sum_{r'} \lambda_{r'}^{k'} (a(c)_{r'}.\,x) =$$

(zbog pretpostavke (3)) $= \sum_{r'} \lambda_{r'}^{k'} b(c)_{r'} =$ (prema 7) $= b_{k'}.$

Dobili smo, dakle, jednakost $a_{k'}.\,x = b_{k'}.$, za čim smo i išli

Time je dokazano da se pri rješavanju linearnih sistema možemo ograničiti na rješavanje kojega god reduciranog podsistema, jer su rješenja samog sistema ista kao za reducirani podsistem.

4. RJEŠAVANJE REDUCIRANOG SISTEMA

4.0. Ako smo već našli reducirani podsistem, odnosno reduciranu jednadžbu $a(c)\,x = b(c)$, onda to treba i riješiti.

Korisno služi ovaj teorem:

4.1. Teorem o partikularnom rješenju. *Neka je* $ax = b$. *Neka je* c *bilo koja regularna podmatrica od* a *reda* $r = ra$ (rang od a) = rang od $[a, b]$; neka je $b(c)$ *matrica što je čine oni redići matrice* b *što odgovaraju redićima matrice* a *iz kojih je* c *izvađeno. Tada je određena i matrica* $c^{-1}\,b(c) = u$. *Neka je* ξ *ona nadmatrica matrice* $u = c^{-1}\,b(c)$ *koja se iz* u *dobije tako da se* u *nju uvedu nula-redići što odgovaraju stupcima matrice* $a(c)$ *koji leže izvan* c. *Tada vrijedi* $a\xi = b$, *tj.* ξ *je jedno partikularno rješenje polazne jednadžbe.*

Konstrukcija je jasna (isp. primjer u 4.3). Dokaz da je $a\xi = b$ je prost. Naime, očigledno je $a(c)_{r'.} \circ \xi_{.s'} = c_{r'.} \circ u_{s'.}$; to znači da je $a(c)_{r'.} \circ \xi_{s'.} = b(c)_{r's'}$, tj. $a(c)\,\xi = b(c)$. Drugim riječima, ξ zadovoljava reduciranu jednadžbu, a po § 3.5 zadovoljava time i samu jednadžbu $ax = b$.

4.2. Uzmimo *jednostavan slučaj da je* b *tipa* $n \times 1$, tj. stupac (vektor). Tada je riječ o r jednadžbi po n nepoznanica x_ν:

$$\sum_\nu a_{r'\nu}\, x_\nu = b_{r'}. \tag{8}$$

Te se jednadžbe rješe s obzirom na veličine uz matricu c; kako smo uzeli da je $c_{ij} = a_{ij}$, možemo lako provesti razdvajanje i dobiti

$$\sum_{r'} a_{ir'}\, x_{r'} = -a_{i\,r+1}\, x_{r+1} - \cdots - a_{in}\, x_n + b_i, \quad (i = 1,\ 2,\ \ldots\ r). \tag{8_0}$$

Odatle se uočenih r veličina $x_{r'}$ uz koje je matrica c izrazi pomoću preostalih $d\,(= n - r)$ veličina $x_{r+d'}$ koje su proizvoljne; tako se dobije traženo rješenje. Specijalno, uzme li se da za svih tih d veličina vrijedi $x_{r+d'} = 0$, dobije se određeno partikularno rješenje reduciranog sistema, a time i cijelog sistema. Pišemo li (8_0) matrično

$$c\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{bmatrix} = \begin{bmatrix} \sum -a_{1\,r+d'}\, x_{r+d'} + b_1 \\ \cdots\cdots\cdots \\ \sum -a_{r\,r+d'}\, x_{r+d'} + b_r \end{bmatrix};$$

ada množeći sa c^{-1}, izlazi

$$\begin{bmatrix} x_1 \\ \vdots \\ x_r \end{bmatrix} = c^{-1} \cdot \begin{bmatrix} \sum -a_{1\,r+d'}\, x_{r+d'} + b_1 \\ \cdots\cdots\cdots \\ \sum -a_{r\,r+d'}\, x_{r+d'} + b_r \end{bmatrix},$$

pa to smatramo traženim rješenjem sistema (8).

Sasvim je tako i u općem slučaju kad je $\mathrm{Dom}\, b = (k, s)$.

4.3. Primjer. Riješi $ax=b$ ako je

$$a=\begin{bmatrix} 1 & 2 & -3 & 0 \\ 3 & 9 & -1 & -1 \\ 5 & 6 & 2 & 1 \\ 3 & -1 & 0 & 2 \\ 12 & 16 & -2 & 2 \end{bmatrix} \qquad b=\begin{bmatrix} 4 & 0 \\ 3 & -1 \\ 0 & 3 \\ 1 & 4 \\ 8 & 6 \end{bmatrix}.$$

U § 1.0. riješili smo jednadžbu $ay=b_{.1}$; time smo dobili početni stupac $x_{.1}$ tražene matrice x. Analogno bismo riješili jednadžbu $au=b_{.2}$ i dobili naredni stupac $x_{.2}$ traženog rješenja x; time tražena matrica x glasi $x=[y, u]$. Reducirana jednadžba bila bi, npr., ova:

$$\begin{matrix} & & \vartheta & \\ & & & \end{matrix}$$

$$\begin{bmatrix} 1 & 2 & -3 & 0 \\ 5 & 6 & 2 & 1 \\ 3 & -1 & 0 & 2 \end{bmatrix} \cdot x = \begin{bmatrix} 4 & 0 \\ 0 & 3 \\ 1 & 4 \end{bmatrix}; \tag{9}$$

uočena matrica c ne sadrži naznačenog, drugog, stupca iznad kojeg je stavljen znak ϑ. Ako u $a(c)$ ispustimo sve stupce izvan c, prelazi reducirana jednadžba u $cu=b(c)$; odatle $u=c^{-1}b(c)$; u našem slučaju

$$\begin{bmatrix} 1 & -3 & 0 \\ 5 & 2 & 1 \\ 3 & 0 & 2 \end{bmatrix} u = \begin{bmatrix} 4 & 0 \\ 0 & 3 \\ 1 & 4 \end{bmatrix}.$$

Odatle

$$u=c^{-1}\begin{bmatrix} 4 & 0 \\ 0 & 3 \\ 1 & 4 \end{bmatrix},$$

tj. (v. § 1.0.9, formula (11) za c^{-1}):

$$u=\frac{1}{25}\begin{bmatrix} 4 & 6 & -3 \\ -7 & 2 & -1 \\ -6 & -9 & 17 \end{bmatrix} \cdot \begin{bmatrix} 4 & 0 \\ 0 & 3 \\ 1 & 4 \end{bmatrix}.$$

Izmnožimo to; izlazi

$$u=\frac{1}{25}\begin{bmatrix} 13 & 6 \\ -29 & 2 \\ -7 & 41 \end{bmatrix}.$$

Iz te matrice u možemo lako naći partikularno rješenje ξ polazne jednadžbe, i to kao onu nadmatricu od u koja se dobije uvođenjer odgovarajućih

redaka s vrijednostima 0 za svaki stupac u $a(c)$ izvan c. Kako je u našem primjeru stupac $a(c).2$ izvan c, znači da će biti redak $\xi_2. = [0, 0]$; dakle je

$$\xi = \frac{1}{25}\begin{bmatrix} 13 & 6 \\ 0 & 0 \\ -29 & 2 \\ -7 & 41 \end{bmatrix}.$$

Provjerimo da li ξ zadovoljava jednadžbu $ax = b$. Imamo po redu:

$$a\xi = \begin{bmatrix} 1 & 2 & -3 & 0 \\ 3 & 9 & -1 & -1 \\ 5 & 6 & 2 & 1 \\ 3 & -1 & 0 & 2 \\ 12 & 16 & -2 & 2 \end{bmatrix} \cdot \frac{1}{25}\begin{bmatrix} 13 & 6 \\ 0 & 0 \\ -29 & 2 \\ -7 & 41 \end{bmatrix} = \frac{1}{25}\begin{bmatrix} 100 & 0 \\ 75 & -25 \\ 0 & 75 \\ 25 & 100 \\ 200 & 150 \end{bmatrix} = \begin{bmatrix} 4 & 0 \\ 3 & -1 \\ 0 & 3 \\ 1 & 4 \\ 8 & 6 \end{bmatrix}.$$

Stvar je u redu.

Kao što smo vidjeli, zaključak je općenit.

5. Zadaci o sistemima linearnih jednadžbi i linearnim matričnim jednadžbama s jednom nepoznatom.

1. Riješi ove jednadžbe:

1) $\begin{aligned} 2x+3y-4z &= 5 \\ -3x-2y+4z &= -5 \\ x+y+2z &= 2 \\ 2y-z &= 2 \end{aligned}$

2) $\begin{aligned} 2x+3y-4z &= 5 \\ -3x-2y+z &= -5 \\ -x+y-3z &= 2 \end{aligned}$

3) $\begin{aligned} 2x+3y-4z &= 5 \\ 4x+6y-8z &= 10 \end{aligned}$

4) $\begin{aligned} 2x+3y-4z &= 5 \\ 2x+3y-24z &= 0 \end{aligned}$

5) $\begin{aligned} 2x+3y-4z &= m \\ -3x-2y+z &= -5 \\ x+y+2z &= 0 \end{aligned}$

6) $\begin{aligned} 2x+3y-4z &= m \\ -3x-2y+z &= n \\ x+y+2z &= 0 \end{aligned}$

7) $\begin{aligned} 2x+3y-4z &= m \\ -3x-3y+z &= n \\ x+y+2z &= p \end{aligned}$

8) $\begin{aligned} \lambda x+3y-4z &= m \\ -3x-\lambda y+z &= n \\ x+y+\lambda z &= p. \end{aligned}$

2. Odredi brojeve a, b, c tako da stupci matrice

$$\begin{bmatrix} 3 & 2 & 2 \\ 4 & 4 & 3 \\ 5 & 1 & 2 \end{bmatrix}$$

zadovoljavaju uslovu $ax + by + cz = 1$.

3. Odrediti a, b, c, d te a', b', c', d' tako da jednadžbe

$$ax+by+cz=d$$

$$a'x+b'y+c'z=d'$$

budu zadovoljene od strane nizova:

1) (2, 3, 4), (2, 6, 1); 2) (0, 0, 0), (1, 2, 3); 3 (−2, 4, 1), (0, 1, 0).

4. Koji se algebarski polinom stupnja 2 $a(x)=a_0+a_1x+ax^2$, $a_2\neq 0$, poništava u tačkama

1) 0, 1, 2? 2) −3, 4, 5? 3) 0, $2-3i$, $2+3i$? 4) 1, −1, i?

5. Odredi algebarski polinom $a(x)$ stupnja 3 za koji je $a(1)=2$,

$a(2)=3$, $a(-1)=4$, $a(-2)=2$.

6. Odredi bar jedan sistem linearnih nezavisnih jednadžbi kojemu zadovoljava niz $\xi=2, 3, 5, 4$, a opće rješenje pripadnog homogenog (jednorodnog) sistema ima za bazu nizove: 0, 0, 1, 2

3, 4, 0, 1.

7. Isto pitanje za niz 2, −3, 5, 2, 4 i nizove 0, 0, 1, 2, −1

3, 1, 0, 0, 2.

8. Zadana je matrica $m=\begin{bmatrix} 3, & 2, & 4, & 5, & 0 \\ 3, & 1, & 2, & 3, & 4 \\ 2, & 1, & 1, & 2, & 1 \end{bmatrix}$; nađi bar jedan homogeni sistem jednadžbi kojemu zadovoljavaju 1) stupci, 2) redići matrice m.

9. Riješi $ax=b$ za ove matrice a, b:

1) $\begin{bmatrix} 2 & 3 \\ -2 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 4 \\ 5 & 6 \end{bmatrix}$; 2) $\begin{bmatrix} 2 & 3 \\ -2 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 4 & 7 \\ 5 & 6 & 8 \end{bmatrix}$;

3) $\begin{bmatrix} 3 & 4 & 5 \\ -3 & 2 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$; 4) $\begin{bmatrix} 2 & 3 \\ 4 & 6 \end{bmatrix}, \begin{bmatrix} 3 & 5 & 8 \\ 4 & 6 & 9 \end{bmatrix}$;

5) $\begin{bmatrix} 2 & 3 \\ 4 & 6 \end{bmatrix}, \begin{bmatrix} 3 & 5 & 8 \\ 6 & 10 & 16 \end{bmatrix}$.

9.′ Isto pitanje za jednadžbu $xa=b$.

10. Riješi $axb=c$ za ove matrice a, b, c:

1) $\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}, \begin{bmatrix} -3 & 2 \\ 5 & -3 \end{bmatrix}, \begin{bmatrix} -2 & 4 \\ 4 & -1 \end{bmatrix}$;

2) $\begin{bmatrix} -3 & 2 \\ 5 & -3 \end{bmatrix}$, $\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}$, $\begin{bmatrix} -2 & 4 \\ 3 & -1 \end{bmatrix}$;

3) $\begin{bmatrix} 5 & 1 \\ 2 & 3 \end{bmatrix}$, $\begin{bmatrix} 3 & 4 \\ 7 & 1 \end{bmatrix}$, $\begin{bmatrix} 0 & 2 \\ 4 & 3 \end{bmatrix}$.

11. Riješi $axa = b$, ako a, b znače ove matrice: 1) [1, 1], [1, 1]; 2) [2, 0] [0, 0]; 3) $\begin{bmatrix} 3 \\ 4 \end{bmatrix}$, [2, 5]; 4) $\begin{bmatrix} 1 & 2 \\ -3 & 2 \end{bmatrix}$, $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$; 5) $\begin{bmatrix} 1 & 2 \\ 5 & 4 \end{bmatrix}$, $\begin{bmatrix} 3 & 2 \\ -1 & 1 \end{bmatrix}$.

12. Ima li matrična jednadžba $axa = I$ rješenje za svako zadano a?

12′. Isto pitanje zamijenjujući jediničnu matricu I matricom

1) [1, 1]; 2) [1, 0]; 3) $\begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix}$.

13. Ima li jednadžba $axa = b$ uvijek rješenje uz uslov da su a, b zadane matrice i da je $\mathrm{Dom}\, a = \mathrm{Dom}\, b$?

14. Zadana je jednadžba $ax = b$ uz uslov $\det(aa^T) \neq 0$;
stavimo $a_d^\circ = a^T (aa^T)^{-1} a$ (poglavlje 12, § 6.5.9); tada matrica $a_d^{-1} b + (I - a_d^\circ) m$ je rješenje jednadže $ax = b$; pri tom m znači svaku matricu suglasnog poretka $(D_2 a,\ D_2 b)$. Dokaži!

Zadaci iz geometrije.

15. Nađi nuždan i dovoljan uslov pa da tačke (x_i, y_i) leže na istoj pravulji

$$Ax + By + C = 0 \quad \text{i} \quad \text{to za}$$

1) $i = 1, 2, 3$; 2) $i = 1, 2, 3, 4$; 3) $i = 1, 2, 3, \ldots, n$.

15.^{a} (Dual od 15): nađi nuždan i dovoljan uslov pa da k pravuljâ

$$A_i x + B_i y + C_i = 0 \ (i = 1, 2, \ldots, k)$$

prolazi istom tačkom i to za: 1) $k = 2$, 2) $k = 3$, 3) $k = 4$, 4) $k = n$.

16. Odredi nuždan i dovoljan uslov pa da:
1) 3; 2) 4; 3) 5 tačaka (x_i, y_i) ravnine leže na istoj kružnici.

17. Zadane su 3 tačke (x_i, y_i); odredi: kružnicu koja ih sadrži kao i poluprečnik r i središte (p, q) te kružnice. Dokaži da su r, p, q racionalni brojevi, ako su brojevi x_i, y_i racionalni.

18. Odredi ravninu $Ax + By + Cz + D = 0$ u kojoj leže tačke:
1) (1, 0, 0), (0, 1, 0), (0, 0, 1); 2) (3, 4, 5), (−3, 4, 5), (2, 1, 3);
3) (1, 2, 3), (−1, −2, −3), (0, 0, 5) 4) (x_i, y_i, z_i), $(i = 1, 2, 3)$;
5) (x_i, y_i, z_i) $(i = 1, 2, 3, 4, 5)$.

19. Odredi nuždan i dovoljan uslov pa da jednadžbe

$$A_i x + B_i y + C_i z + D_i = 0 \quad (i = 1, 2, 3)$$

određuju 3 različne pravulje

1) kroz jednu tačku; 2) kao stranice trokuta?

20. Slično pitanje za prostor: Nađi nuždan i dovoljan uslov pa da 4 jednadžbe $A_i x + B_i y + C_i z + D_i = 0$ određuju 4 različne ravnine

1) koje imaju jednu tačku zajedničku; 2) koje nemaju nikoje zajedničke tačke ali nema ni paralelnih ravnina.

21. Promatraj jednadžbe

$$A_i x + B_i y + C_i z + D_i = 0 \quad (i = 1, 2); \quad \text{mogu li one}$$

1) biti bez rješenja; 2) imati jedno jedino rješenje?
Šta to znači geometrijski?

22. Šta je nužno i dovoljno pa da jednadžbe

$$A_i x + B_i y + C_i z + D_i = 0, \quad (i = 1, 2, \ldots, n)$$

imaju bar 2 različita rješenja? Geometrijska interpretacija!

23. Odredi krivulju drugog reda koja prolazi tačkama

$$(x_i, y_i) \quad (i = 1, 2, 3, 4, 5). \qquad \text{Konkretiziraj!}$$

POGLAVLJE 15.

RANG MATRICE

0. UVOD I PRIPRAVA

0.0. Dosad smo se služili rangom za matrice a koristeći se ovim glavnim svojstvom o linearnoj nezavisnosti: kod matrica, odnosno jednadžbi: broj r_a (kao maksimalni stupanj neke nesingularne podmatrice Ma u a) kazuje ujedno koliko matrica a ima nezavisnih redaka (stupaca), odnosno koliko u sistemu jednadžbi

$$\sum_{\nu=1}^{n} a_{k'\nu} x_\nu = 0 \quad (k' \in 1(k) = \{1, 2, \ldots, k\}) \tag{1}$$

ima linearno nezavisnih jednadžbi. Svakako, poznavanje bar jedne *regularne* submatrice $Ma \subset a$ *maksimalnog* reda mnogo je dragocjenije nego poznavanje pukog broja r_a koji kazuje koliko matrica Ma ima nezavisnih redaka ili stupaca. Stvarno, Ma nas dovodi do reducirane jednadžbe $a(Ma)\vec{x} = \vec{0}$ ekvivalentne sa $a\vec{x} = \vec{0}$, odnosno do reduciranog podsistema zadanog sistema (1).

0.1. No, *traženje* broja r_a dovodi nas i do *M-submatrica*, stanovitih matrica dovoljno čvrsto vezanih za a, tako da odatle možemo povući korisne zaključke i o samoj polaznoj matrici (odnosno sistemu jednadžbi u kojem se a pojavljuje). Pri tom mislimo specijalno na reduciranje matrica a na *T-matrice* (*topovsko reduciranje i eliminiranje*); a korist što je od takve redukcije imamo upoznali smo već u pogl. 8, § 2.6). *Rang svake T-matrice t upravo je jednak broju položaja takvih nezavisnih rubnih njenih topova ispod kojih nema nikojeg topa matrice, a drže pod paljbom svaki redak matrice u kojem se nalazi bar jedan top* (ovdje „top" matrice znači svaki njen element $\neq 0$). Permutacijom redaka prelazi svaka *T*-matrica u određenu $\overline{\diagdown|}$-matricu ($\overline{\diagdown|}$-matrice zovu se i *gornjotrokutne matrice*; kod njih su svi elementi *ispod* dijagonale jednaki 0; dualno su: $|\diagdown$-matrice ili *donjotrokutne matrice*; kod njih su komponente *iznad* glavne dijagonale jednake 0).

0.2. Nadalje ćemo u ovom poglavlju pobliže upoznati nekoliko svojstava ranga, specijalno *da se rang r_a matrice a ne mijenja pri vršenju tzv. elementarnih transformacija nad a* [*matrični odraz operacijâ kojima se svakodnevno služimo pri rješavanju jednadžbi* (množenja jednadžbi s brojevima $\neq 0$, zbrajanje jednadžbi)].

To će nas dovesti do saznanja da je *svaka matrica a »ekvivalentna« s normiranom matricom posebnog oblika*

$$k\left\{\underbrace{\begin{bmatrix} \underbrace{\begin{matrix}1 & & \\ & \ddots & \\ & & 1\end{matrix}}_{r} & \\ & \end{bmatrix}}_{n}\right. .$$

Zvuči čudnovato kad se čuje da se *svaka matrica a tipa* (k, n) *i ranga* r *može elementarno svesti na taj normalni oblik*, odnosno obratno, da se a iz tog normiranog oblika $\nu = \nu(k, n, r)$ može *rekonstruirati* relacijom $a = x \nu y$, gdje su x i y *regularne kvadratne matrice*. Dokazat ćemo, naime, da vrijedi ovaj

0.3. Glavni teorem o rangu i ekvivalenciji matrica. Za matrice a, b ova četiri suda (0)—(3) međusobno su logički ravnopravna:

$$\text{(0)} \qquad k_1 a\left\{\overbrace{\begin{bmatrix} \underbrace{\begin{matrix}1 & \\ \cdot & \\ & 1\end{matrix}}_{r_a} & \\ & 0 \end{bmatrix}}^{k_2 a}\right. = \left.\overbrace{\begin{bmatrix} \underbrace{\begin{matrix}1 & \\ \cdot & \\ \cdot & 1\end{matrix}}_{r_b} & \\ & \end{bmatrix}}^{k_2 b}\right\} k_1 b.$$

Pri tom $k_1 a$ (odnosno $k_2 a$) kazuje koliko a ima redaka (stupaca).

(1) Prvi sud: *Matrice a, b su istog poretka* (k, n) *i istog ranga.*

(2) Drugi sud: *Matrice a i b su ekvivalentne* $(a \sim b)$ *u tom smislu da se jedna iz druge može izvesti pomoću konačnog broja »elementarnih« transformacija.* (v. § 4.1. i § 6.0. definicija).

(3) Treći sud: *Matrična jednadžba* $x a y = b$ *dopušta neko rješenje* x, y *sa svojstvima* $\det x \neq 0$, $\det y \neq 0$ (*dakle su x i y regularne kvadratne matrice*).

0.4. Posebno, odatle izvire (zaključak (1) $\Leftrightarrow$ (3)) da se množenjem matrice s regularnom kvadratnom matricom rang ne mijenja.

0.5. Ako se još doda da je rang dijagonalne matrice jednak broju njenih topova na dijagonali, onda je već ukazano glavnim teoremom da ćemo, služeći se elementarnim transformacijama i množenjima, nastojati zadanu matricu a prevesti na što jednostavniji oblik (trokutni, dijagonalni, . . . , odnosno sa što više 0) — slično kao što smo npr. kod Gaussova algoritma nastojali da iz jednadžbi uklonimo što više nepoznanica.

0.6. Tako npr. ako u matrici vidimo da joj je jedan redak ρ jednak s drugim retkom ili da se može izraziti linearno pomoću ostalih redaka, može se čitav taj redak odmah nadomjestiti samim nulama — rang se tim prelazom ne mijenja!

0.7. Imajmo na umu *korist od poznavanja ranga matrica*; ta je korist iskazana u osnovnom teoremu o nezavisnosti unutar matrica (teorem 10.3. o matricama i osnovni teorem 5.5. u pogl. 11). Izrecimo taj teorem i ovom prilikom:

0.8. Ako matrica a ima konačan broj redaka ili stupaca (ili oboje), tada za svaku njenu M-podmatricu $M(a)$ (v. definiciju 2.1) pripadni redići (stupci) matrice a predstavljaju maksimalan broj linearno nezavisnih redaka (stupaca). Drugim riječima, broj ra pokazuje dimenziju prostora što ga razapinju reci (stupci) matrice a.

1. RANG I M-PODMATRICE NEKIH MATRICA

1.0. D e f i n i c i j a. M-podmatrica matrice a, simbolički Ma, jest bilo koja kvadratna regularna podmatrica maksimalne duljine.

1.1. D e f i n i c i j a. Rang ra matrice a je supremum duljinâ $k_2 x$ kvadratnih regularnih podmatrica x u a. Matricama s jedinim vrijednostima 0 pridjeljuje se 0 kao rang.

P r i m j e r. Očigledno je

$$r\left[\begin{array}{ccc|c} 3 & . & . & \\ 0 & 1 & . & \text{proizvoljno} \\ 0 & 0 & 3 & \\ \hline 0 & 0 & 0 & .. \end{array}\right] = 3.$$

Tu je odmah uokvirena M-matrica

$$\begin{bmatrix} 3 & . & . \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{bmatrix}.$$

Singularnost svake podmatrice x stupnja >3 proizlazi iz činjenice što x ima nužno 0-niz kao svoj četvrti redak (inače x može imati i ∞ mnogo redaka).

Najjednostavnije je rang ra i podmatricu Ma odrediti kad matrica a ima mnogo nulâ. U tom pogledu evo jednog vrlo korisnog teorema:

1.2. T e o r e m. *Ako matrica a u svakom stupcu ima najviše jednu vrijednost $\neq 0$, tada je rang ra jednak broju redaka u a koji nijesu $=\vec{0}$; ako se iz a uklone svi reci koji su 0 i svi stupci koji su 0, tada se u preostatku u lijevom kraju pojavljuje matrica Ma.*

Npr.
$$r\begin{bmatrix} 0 & \boxed{3} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \boxed{7} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \boxed{5} & 0 & 0 & 4 \end{bmatrix} = 3;\ \text{brisanjem} \Rightarrow$$

$$\begin{bmatrix} \boxed{\begin{matrix} 3 & 0 & 0 \\ 0 & 0 & 7 \\ 0 & 5 & 0 \end{matrix}} & \begin{matrix} 0 \\ 0 \\ 4 \end{matrix} \end{bmatrix};\ Ma \text{ je uokvireno.}$$

Dokaz teorema. Brisanjem svih konstantnih redaka i stupaca u a koji su 0 dobije se određena matrica b; u njoj svaki stupac ima jednu jedinu vrijednost $\neq 0$; ako nije $b_{11} \neq 0$, nego je $b_{i1} \neq 0$, tada se transpozicijama redaka $b_{i\cdot}, b_{i-1\cdot}, \ldots, b_{1\cdot}$ redak $b_{i\cdot}$ dovede da postane prvi redak. Npr. ako je

$$b = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 2 \\ 0 & 3 & 0 & 0 & 4 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 \end{bmatrix},\ \text{tada odatle izlazi} \begin{bmatrix} b_{1\cdot} \\ b_{3\cdot} \\ b_{2\cdot} \\ b_{4\cdot} \end{bmatrix},$$

$$\text{pa dalje} \begin{bmatrix} b_{3\cdot} \\ b_{1\cdot} \\ b_{2\cdot} \\ b_{4\cdot} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 \\ 0 & 3 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 \end{bmatrix} = d;$$

sad se u d promatra kofaktor f_{11} i na njemu, unutar d, vrši odgovarajući proces: to daje prelaz

$$d \to \begin{bmatrix} \boxed{\begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 4 \end{matrix}} & \begin{matrix} 0 & 0 \\ 4 & 0 \\ 0 & 2 \\ 0 & 0 \end{matrix} \end{bmatrix} = e;$$

vidimo ovo: uokvirena submatrica x poretka 4×4 na početku matrice e je trokutna; vrijednost determinante je $1 \cdot 3 \cdot 1 \cdot 4$, tj. $\det x \neq 0$. No, matrica e obrnutim nizom transpozicija dolazi natrag u matricu b; pri tom iz matrice x nastaje određena podmatrica y od b; naravno, $\det y = \det x$ ili $\det y = -\det x$; dakle je $\det y \neq 0$, tj. $y = Ma$. A za tim i idemo. Slično je u općem slučaju.

1.3. Lema. Rang matrice a koja je izvan dijagonale jednaka 0 jednak je broju nenultih vrijednosti na dijagonali. Brisanjem u a svih konstantnih redaka i stupaca koji su 0 dobiva se *jedina* M-podmatrica Ma matrice a.

Npr.
$$a=\begin{bmatrix} 0 & & & & 0 \\ & 1 & & & \\ & & 0 & & \\ & & & 0 & \\ 0 & & & & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & \\ & 2 \end{bmatrix} = Ma.$$

2. PREVOĐENJE MATRICE U TZV. T-OBLIK. DOKAZ OSNOVNOG TEOREMA

2.0. Već u pogl. 8., § 2.6. upoznali smo se s jednim praktičnim postupkom kako se rješavaju linearne jednadžbe. Ideja se sastoji u ovom: u prvoj jednadžbi u kojoj svi koeficijenti nisu $=0$ treba odabrati *top* (tj. jedan koeficijent $\neq 0$) i metodom protivno-jednakih koeficijenata ukloniti sve druge topove *ispod* izabranog. U tako dobivenim jednadžbama proces iterirati itd. Skup jednadžbi s „topovima“ ekvivalentan je sa skupom zadanih linearnih jednadžbi.

2.1. Opis postupka. Preneseno na matrice, to govori ovo: u zadanoj matrici promatrati *prvi redak* u kojem se nalazi bar jedan top[1]; *jednog od njih, t_1, izabrati, markirati i pomoću njega ukloniti svaki eventualni drugi top t ispod t_1, i to* ovom »*elementarnom*« *L-operacijom na recima: redak od t_1 pomnožiti sa $-t/t_1$ i rezultat dodati retku u kojem je top t.* U novonastaloj situaciji proces se iterira. Pogledati da li se u novoj matrici nalazi koji top *nezavisan* od t_1; ako se nalazi, izabrati i markirati jedan, t_2, iz *prvog mogućeg retka*, uništiti paljbom (operacija s *L-recima*) svaki eventualni top ispod t_2 itd.

Na taj se način dobije najzad određena matrica a_T i u njoj određen niz osobitih markiranih topova $t_1, t_2, \ldots$; ti su svi topovi na $\neq$ stupcima i $\neq$ recima (ne mogu se gađati međusobno), *svaki* redak u a_T *s bar jednim topom* sadrži i *jedan osobit*; najzad, *niže od osobitih topova nema nikojeg drugog topa. Broj tih osobitih topova, tj. broj markiranih mjesta, jest ra_T* (rang matrice a_T); najmanja podmatrica $\subset a_T$ kojoj oblast obuhvata sva ta osobita mjesta topova upravo je jedna M-podmatrica (podmatrica najobuhvatnijeg područja s determinantom $\neq 0$).

2.2. Definicija T-matrica i $\vdash$-matrice. Primjeri. — **2.2.0.** Kaže se da je zadana matrica a jedna *T-matrica* ako sadrži jedan podskup S topova s ovim svojstvima:[2]

---

[1] Top matrice je svaka njena vrijednost $\neq 0$. Radi slikovitosti zgodno se služiti riječju top. Izboru „osobitih topova“ u praksi će se ipak posvetiti malo više pažnje, npr. tako da retke međusobno uredimo, recimo da kao prvi redak nastupi onaj s najviše topova i s najizrazitijim topovima. Ili npr. da se najglomazniji topovi stave na dijagonalu ili da topovi budu 1, -1 itd.

[2] Znajmo da je S podfunkcija funkcije a.

(I) *Svaki redak matrice u kojem se nalazi bar jedan njen top sadrži i jedan top iz S.*

(II) *Ispod topova u S nema nijednog topa matrice.*

(III) *Topovi u S međusobno se ne gađaju* tj. bilo koja dva od njih smještena su u različitim recima i različitim stupcima matrice.

Nula-matrice smatramo *T*-matricama.

Transponati *T*-matrica zovu se $\vdash$*-matrice*.[1)]

Kraće možemo govoriti da je *S istaknut skup topova u promatranoj matrici a* ili, što je pravilnije: *S je istaknuta podfunkcija od a*. Istaknute topove možemo uokviriti i sl.

Evo primjera *T*-matrica:

$$\begin{bmatrix} \boxed{1} & & \\ & \boxed{1} & \\ & & \boxed{1} \end{bmatrix}, \begin{bmatrix} \boxed{3} & 1 & 0 \\ 0 & 0 & \boxed{2} \\ 0 & \boxed{4} & 0 \end{bmatrix}, \begin{bmatrix} 2 & \boxed{1} & 5 & 0 & 0 & 6 \\ \boxed{1} & 0 & \cdot & \cdot & \cdot & \cdot \end{bmatrix}, \begin{bmatrix} 0 & 0 & \boxed{1} & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \ldots$$

Evo primjera matrice koja nije *T*-tipa:

$$\begin{bmatrix} 1 & 1 \\ 2 & 3 \end{bmatrix},$$

i to iz razloga što u njenom prvom retku ne možemo izabrati istaknuti top (uslov 2!).

2.2.1. L e m a. Svaki redak, svaka dijagonalna matrica, svaka matrica bez topova ispod dijagonale — sve su to primjeri *T*-matrica, bez obzira na broj stupaca. Svaki stupac s posljednjim članom također je *T*-matrica. Npr.

$$\begin{bmatrix} 2 \\ 0 \\ 0 \\ \vdots \end{bmatrix} \text{ je } T\text{-matrica;}$$

transponat matrice [1, 2, 3, . . .] mnogosti N nije *T*-matrica.

2.3. Definicija L-postupka s matricom. — **2.3.0.** Izvršiti *elementaran ili jednočlan L-postupak na recima matrice* znači jednom *retku* matrice pribrojiti neki *drugi redak iste matrice pomnožen brojem*.[2)]

2.3.1. *Složen L-postupak s recima* jest onaj pri kojem se jednom retku matrice pribroji linearna kombinacija konačne množine drugih redaka matrice.

[1)] Nazivi *T-matrica* i $\vdash$*-matrica* u vezi su s početnim slovom riječi *top* ili *tvrđava* kao i posebnom građom tih matrica.

[2)] To je operacija koja odgovara svakidašnjem poslu s jednadžbama.

2.3.2. Analogno se definiraju elementarne i složene L-operacije sa *stupcima* matrice.

2.3.3. P r i m j e d b a. Slovo L u gornjem nazivu je početno slovo riječi »*linearan*«, odnosno »*linija*«.

Npr. za matricu

$$a=\begin{bmatrix} 3 & 4 & 5 & 8 \\ 5 & 1 & 4 & 2 \end{bmatrix}$$

daje L-operacija $a_2.-5/3\ a_1.$ matricu

$$\begin{bmatrix} 3 & 4 & 5 & 8 \\ 0 & -\frac{17}{3} & -\frac{13}{3} & -\frac{34}{3} \end{bmatrix}.$$

2.4. Osnovni teorem o prevođenju matrice u T-matrice.

⟶ 2.4.0. (a) Svaka matrica *a* koja ima konačno mnogo redaka može se pomoću konačno mnogo elementarnih L-operacija s récima (isp. definiciju 2.3) prevesti u jednu *T*-matricu a_T istog domena, tj. oblasti: Dom a_T = Dom *a*. To znači da postoji konačan niz matrica $A_0=a$, A_1, $A_2\ldots.$, $A_s=a_T$, u kojem svaki član A_l osim prvog izlazi iz prethodnog člana A_{l-1} jednom elementarnom *L*-operacijom L_{l-1} redaka matrice A_{l-1}.

(b) U svakom istaknutom skupu *S* topova u dobivenoj matrici a_T ima upravo $r(a_T)$ topova (gdje ra_T označuje rang matrice a_T).

(c) Polja što ih zauzimaju topovi iz *S* zajedno s poljima što ih tuku po dva topa iz *S* određuju jednu *M*-podmatricu Ma_T u a_T, tj. maksimalnog reda regularnu kvadratnu podmatricu u a_T.

(d) $ra=ra_T$ (matrice *a*, a_T imaju isti rang).

(e) Ako je *a* kvadratna konačna matrica duljine *n*, tada je

$$\det a=\det a_T.$$

(f) Ako je $k(S)<n$, onda je $\det a=0$. Ako je $k(S)=n$, onda je $\det a=(-1)^I \prod_{\dot{S}} \dot{S}$; pri tom naznačeni produkt kazuje rezultat izmnažanja svih markiranih topova u *S*; *I* označuje sumu indeksâ (tj. prvih i drugih indeksa) svih topova u S[1].

To je formulacija osnovnog teorema na slikovitom jeziku. Ta je formulacija lakša od strogo funkcionalne, koja glasi ovako:

---

[1] Ne gubimo s uma činjenicu da je svaka matrica određena funkcija na Descartesovu pravokutniku kojoj podfunkcije smatramo podmatricama samo onda ako su im domeni Descartesovi kvadri! Sjetimo se da je $D_1 T$ prva projekcija domena od *T*; $D_2 T$ je druga projekcija od Dom *T*.

2.4.0^{bis} Teorem;

(a) Svaka matrica a koja ima konačno mnogo redaka može se pomoću konačno mnogo elementarnih L-operacija s redićima (isp. definiciju 2.3) prevesti u jednu T-matricu a_T (definicija 2.2) istog domena: Dom a_T = Dom a. To znači da postoji konačan niz matrica: $A_0 = a$, $A_1, A_2, \ldots, A_s = a_T$, u kojem svaki član A_{l-1} osim prvog izlazi iz prethodnog jednom elementarnom L-operacijom L_{l-1} redaka matrice A_l.

(b) Za svaku odlikovanu potfunkciju S dobivene matrice a_T, tj. za svaku odlikovanu restrikciju $a_T \mid M$ funkcije a_T vrijedi $k \operatorname{Dom} S = kM = ra_T$ (k (Dom S) znači kardinalni broj oblasti funkcije S).

(c) Potfunkcija $a_T \mid D_1 S \times D_2 S$ je jedna M-podmatrica u a_T.

(d) $ra = ra_T$.

(e) Ako je a kvadratna konačna matrica duljine n, tada je $\det a = \det a_T$.

(f) Ako je $k(\operatorname{Dom} S) < n$, onda je $\det a = 0$. Ako je $k(\operatorname{Dom} S) = n$, onda je $\det a = (-1)^{\sum_{(i,j)} (i+j)} \prod_{(i,j)} (a_T)_{ij}$, pri čemu je $(i, j) \in \operatorname{Dom} S$.

Dokaz teorema svodi se na dokaz jednakosti Dom a = Dom a_T, jednakosti $ra = ra_T$ (v. § 2.4.4) i dokaz teorema 2.4.5. o T-matricama.

2.4.1. Ilustracija prevođenja a u a_T:

$$a = \left[\begin{array}{ccc} 5 & \boxed{-1} & 2 \\ 4 & -1 & 1 \\ -1 & 1 & 0 \\ 3 & -2 & 1 \end{array}\right] \Big| \cdot -1 \rightarrow \left[\begin{array}{ccc} 5 & \boxed{-1} & 2 \\ -1 & 0 & -1 \\ -1 & 1 & 0 \\ 3 & -2 & 1 \end{array}\right] \Big| \cdot 1 \Big| \cdot -2$$

(tu smo naznačili dva elementarna postupka)

$$\left[\begin{array}{ccc} 5 & \boxed{-1} & 2 \\ \boxed{-1} & 0 & -1 \\ 4 & 0 & 2 \\ -7 & 0 & -3 \end{array}\right] \Big| \cdot 4 \Big| \cdot -7 \rightarrow \left[\begin{array}{ccc} 5 & \boxed{-1} & 2 \\ \boxed{-1} & 0 & -1 \\ 0 & 0 & \boxed{-2} \\ 0 & 0 & 4 \end{array}\right] \Big| \cdot 2 \rightarrow$$

$$\rightarrow \left[\begin{array}{ccc} 5 & \boxed{-1} & 2 \\ \boxed{-1} & 0 & -1 \\ 0 & 0 & \boxed{-2} \\ 0 & 0 & 0 \end{array}\right] = a_T.$$ Dakle je $r(a_T) = 3 = r(a)$.

Označeni topovi razapinju u a_T podmatricu

$$Ma_T = \begin{bmatrix} 5 & \boxed{-1} & 2 \\ \boxed{-1} & 0 & -1 \\ 0 & 0 & \boxed{-2} \end{bmatrix}, \text{ kojoj je determinanta } 2.$$

2.4.2. *Opis puta od a do* a_T. To smo opisali u § 2.1, a vidi se i iz gornjeg primjera.

2.4.3. Lema. *Pri elementarnim L-transformacijama matrice oblast se i rang te matrice ne mijenjaju.*

2.4.3.0. Neka je, dakle, a matrica; neka b izlazi iz a elementarnom transformacijom. Treba dokazati da je $\mathrm{Dom}\, a = \mathrm{Dom}\, b$, te $ra = rb$. Prva je jednakost očigledna — uostalom, spomenut ćemo je u toku dokaza jednakosti $ra = rb$. Pa neka je c jedna regularna podmatrica u a stupnja $r = r(a)$. Prema osnovnom teoremu u pogl. 11, § 10.3, svaki redak u a je linearan spoj od onih r redaka iz kojih je uzeto c. A sada, kako b iz a nastaje jednostavnom L-operacijom: da se nekom određenom retku $a_i.$ doda $\lambda a_j.$, gdje je $i \neq j$, pa time dobije redak $b_i. = a_i. + \lambda a_j.$, svi su ostali redići u a i b zajednički, tj. $a_k'. = b_k'.$. Zato je specijalno $\mathrm{Dom}\, a = \mathrm{Dom}\, b$. No, kako su svi redići u a (dakle specijalno i redići $a_i.$, $a_j.$) linearni spojevi od spomenutih r redaka iz kojih je uzeto c, znači da će i svi reci od b biti linearni spojevi od istih r redaka; to prema teoremu 10.6 istog poglavlja 11. znači da je svaka submatrica u b stupnja $> r$ singularna, dakle $r(b) \leq r = r(a)$. Idući natrag od b ka a pomoću elementarne transformacije, znači da je također $r(a) \leq r(b)$. Te dvije relacije imaju za posljedicu traženu jednakost $r(a) = r(b)$. Tako je teorem dokazan.

2.4.3.1. Gornje zaključivanje pogotovu kazuje da je $\det a = \det b$.

2.4.4. $ra = ra_T$; $\mathrm{Dom}\, a = \mathrm{Dom}\, a_T$. Kako je zadana matrica a takva da postoji konačni niz matrica $A_0 = a, A_1, A_2, \ldots, A_s = a_T$, za koje svaki član nastaje iz prethodnoga pomoću L-transformacije, to primjenom gornje leme 2.4.3. izlazi $r A_0 = r A_1 = \cdots r A_s$, tj. $r A_0 = r A_s$, tj. $ra = ra_T$.

Iz istog razloga je $\mathrm{Dom}\, a = \mathrm{Dom}\, a_T$. Nadalje je iz istog razloga $\det a = \det a_T$, ako je a kvadratna konačna matrica. Time je dokazana važna jednakost $ra = ra_T$, te jednakost $\mathrm{Dom}\, a = \mathrm{Dom}\, a_T$ u osnovnom teoremu 2.4.0. kao i iskaz (e).

Sada prelazimo na dokaz onih svojstava podmatrice $a_T(T)$ o kojima se govori u teoremu 2.4.0. u iskazima (b), (c) i (f). U tu svrhu dokažimo ovaj teorem o T-matricama.

2.4.5. Teorem o rangu *M*-podmatrica za *T*-matrice. *Ako je u proizvoljna T-matrica, a T proizvoljan istaknut njen skup topova iz u, onda je*

(I) $u(T) = Mu$; *pri tom* $u(T)$ *označuje onu podmatricu od u »što je čine polja od T i polja što ih tuku po dva topa iz T« tj. za koju je*

$$Dom\, u(T) = D_1 T \times D_2 T;$$

Mu označuje jednu regularnu kvadratnu podmatricu maksimalne duljine uzetu iz *u*.

(ii) $ru = k(\mathrm{Dom}\, T)$ (=kardinalni broj svih polja u T).

Dokaz. 1. *$u(T)$ je određena kvadratna podmatrica duljine $k\,T$, gdje $k\,T$ kazuje broj topova (polja) iz T.*

Neka je, naime, X, odnosno Y skup svih prvih, odnosno drugih koordinata svih polja iz T; to znači da je X prva, a Y druga projekcija množine T. Za svako $x \in X$ postoji samo jedno $x' \in Y$, i obrnuto, za svako $y \in Y$ postoji samo jedno $\bar{y}$ za koje je $\bar{y} \in X$; i to zato jer u T nema raznih polja s istom prvom ili drugom koordinatom. Drugim riječima, pridruživanje $x \to x'$ je određeno *tolikovanje* od X na Y. Dakle, $kX = kY$. S druge strane, pridruživanje $x \to (x, x')$ je jedno tolikovanje od X na T, odnosno na skup polja od T; dakle je $kX = k\,\mathrm{Dom}\, T$. Imamo, dakle, $kX = kY = k\,\mathrm{Dom}\, T$. Najzad, $X \times Y$ je upravo $\mathrm{Dom}\, u(T)$ (domen od $u(T)$). To znači da je $u(T)$ jedna podmatrica tipa $kX \times kY$, tj. tipa $k\,\mathrm{Dom}\, T \times k\,\mathrm{Dom}\, T$, kvadratna podmatrica duljine $k\,\mathrm{Dom}\, T$; to je i trebalo dokazati.

2. *Nadalje je $u(T)$ također jedna T-matrica* (isp. definiciju § 2.2.0). To je očigledno, posebno zbog razloga što ni u u nema topova ispod T. Na taj je način matrica $u(T)$ određena kvadratna T-matrica.

3. *Matrica u (T) je regularna kvadratna matrica.*

Dokaz toga izdvajamo u posebnu tačku: teorema o T-determinantama u § 2.4.6. (vidi niže).

4. *Svaki redak x matrice u koji leži izvan podmatrice u (T) sastoji se od samih nula* (ukoliko izvan $u(T)$ uopće ima koji redak); drugim riječima, *precrtaju li se svi reci od u gdje ima elemenata od $u(T)$, preostatak je nula-matrica* (može biti i „prazno“).

Kad bi, naime, u nekom retku x od u ležao koji top, morao bi, po svojstvu (I) T-matricâ, jedan top od x biti u T, dakle i u $u(T)$; time redak x ne bi bio izvan $u(T)$-kontradikcija s definicijom retka x.

5. $u(T) = Mu$.

To znači da treba dokazati dvije tvrdnje: (1) *$u(T)$ je regularna kvadratna matrica.* To je dokazano pod tačkom 3.

(II) *Ako je b kvadratna submatrica od u za koju je* $\mathrm{st}\, b > \mathrm{st}\, u(T)$, *onda je* $\det b = 0$. Po definiciji, ako je $\mathrm{st}\, b > \mathrm{st}\, u(T)$, onda je $\det b = 0$. No, prema t. 1, $\mathrm{st}\, u(T) = k\,\mathrm{Dom}\, T$; zato relacija $\mathrm{st}\, b > \mathrm{st}\, u(T)$ znači da podmatrica b ima bar jedan redak u retku x matrice u koji je izvan podmatrice $u(T)$; to prema t. 4. znači da je jedan redak u b sastavljen od nula, dakle je $\det b = 0$.

6. $ru = k\,Dom\,T$.

Upravo dokazasmo u 5. da je $u(T) = Mu$; to znači da je $\mathrm{st}\, u(T) = \mathrm{st}\, M(u) = ru$; tj. $\mathrm{st}\, u(T) = ru$. No, prema 1, imamo $\mathrm{st}\, u(T) = k\,\mathrm{Dom}\, T$; dakle je $k\,\mathrm{Dom}\, T = ru$.

Time je teorem 2.4.5. o T-matricama dokazan (isp. ipak t. 3). Preostalo nam je (v. t. 3) da dokažemo još:

2.4.6. Teorem o *T*-determinantama.[1] *Neka je a kvadratna T-matrica konačnog poretka* (n, n); *to znači da je* $a=0$ *ili u a postoji bar jedna tzv. istaknuta potfunkcija T* (isp. § 2.2.0). *Ako je kardinalni broj domena T manji od n*, tj. $k\,D\,T<n$, *tada je* $\det a=0$; *i obratno. Ako je »broj* $k\,D\,T$ *topova u T« jednak broju n, tada je matrica a regularna* i $\det a=(-1)^I \prod_{x\in DT} T_x$; *pri tom je I suma svih brojeva i, j za koje je* $(i, j)\in DT$, *tj. za koje skup T topova tuče redak* $a_{i.}$ *i stupac* $a_{.j}$; *produkt naznačuje rezultat izmnažanja svih topova u T, tj. svih vrijednosti funkcije T.*

Dokaz. Prvi dio teorema je očigledan. Naime, ako je kardinalni broj $k\,D\,T$ množine $D\,T$ manji od broja n redaka matrice a, znači to da bar jedan redak r nema svojeg predstavnika u T; to znači da je r uopće bez topova, sve vrijednosti retka r su 0, pa je, dakle, $\det a=0$. Ako je pak $k\,D\,T=n$, označimo sa $a_{\nu s_\nu}$ onog topa iz T koji je u retku $a_{\nu.}$, tj. $(\nu, s_\nu)\in \mathrm{Dom}\,T$; to je sasvim određen top matrice a. Promatrajmo najgornji top t_1 u T, tj. top a_{1s_1}; on je jedini u čitavu stupcu $a_{.s_1}$; zato se Laplaceov razvoj za $\det a$ po tom stupcu reducira na produkt $a_{1s_1} f a_{1s_1}$, gdje je $f a_{1s_1}$ algebarski komplement od a_{1s_1} u a; dakle je $f a_{1s_1}=(-1)^{1+s_1}\cdot \det (a\setminus t_1)$; $a\setminus t_1$ nastaje iz a brisanjem retka i stupca u kojem je t_1.

No, iz istog razloga je $\det (a\setminus t_1)=(-1)^{2+s_2}\det [(a\setminus a_{1s_1}\setminus a_{2s_2})]$, itd. dok se ne dođe do izraza

$$\det a=(-1)^{1+s_1} a_{1s_1}\cdot (-1)^{2+s_2} a_{2s_2}\cdot \ldots =$$

$$=(-1)^{\Sigma(\nu+s_\nu)} \prod_\nu a_{\nu s_\nu}.$$

A to se i želi dokazati, jer je

$$\sum_\nu (\nu+s_\nu)=I, \qquad \prod a_{\nu s_\nu}=\prod_x T_x,\ x\in \mathrm{Dom}\,T \text{ (tu je } \nu=1, 2, \ldots, n).$$

Posebno izlazi ovo: ako je $k\,\mathrm{Dom}\,T=n$, onda je $\det a\neq 0$. Prema tome, ako je $\det a=0$, onda je nužno $k\,T<n$, pa je time dokazan i drugi dio prvog dijela teorema. Time je dokazano 2.4.6, dakle i 2.4.5.2; a to je još bilo preostalo pa da teorem 2.4.3.2 bude potpuno dokazan.

2.5. Zadaci o *M*-podmatricama, *T*-matricama i trokutnim matricama

1. Da li je podmatrica oblasti (3, 3) koja je smještena u lijevom gornjem uglu slijedeće matrice jedna *M*-podmatrica ili nije:

$$1)\begin{bmatrix} 1 & 0 & 0 & 5 \\ 0 & 1 & 0 & 6 \\ 0 & 0 & 1 & 7 \end{bmatrix}, \qquad 2)\begin{bmatrix} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 3 \\ 1 & 1 & 1 & 9 \end{bmatrix}, \qquad 3)\begin{bmatrix} 3 & 0 & 0 & 8 \\ 0 & 4 & 1 & 6 \\ 4 & 0 & 0 & 5 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

[1] Taj teorem izdvajamo na posebno mjesto jer je sam po sebi interesantan. Naravno, oznaka a za T-matricu u teoremu 2.4.6. nema veze s istim slovom u teoremu 2.4.0.

$$4)\begin{bmatrix} 0 & 2 & 4 & 7 & 3 \\ 1 & 4 & 8 & 8 & 4 \\ 2 & 5 & 10 & 9 & 2 \\ 3 & 6 & 12 & 0 & 6 \end{bmatrix}, \quad 5)\begin{bmatrix} 0 & 3 & 0 & 1 \\ 0 & 0 & 4 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 2 & 0 \end{bmatrix}, \quad 6)\begin{bmatrix} 0 & 0 & 5 & 0 \\ 0 & 2 & 0 & 4 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix},$$

$$7)\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \quad 8)\begin{bmatrix} 4 & 0 & 6 \\ 0 & 5 & 0 \\ 3 & 0 & 6 \end{bmatrix}?$$

2. Koja je od gornjih matrica tipa T, Ma, elementarna? Napišite nekoliko matrica tih svojstava!

3. Provedite prelaz $a \to a_T$ za matrice a iz zad. 1 (isp. § 2.4.1).

4. Odredite na dva načina vrijednost determinanata ovih matrica; i to: 1) izračunavajući neposredno i 2) svodeći matricu na $\diagdown$-oblik:

$$1)\begin{bmatrix} 2 & 5 & 7 \\ 3 & 0 & 4 \\ -2 & 3 & -5 \end{bmatrix}, \quad 2)\begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{bmatrix}, \quad 3)\begin{bmatrix} 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 5 \end{bmatrix},$$

$$4)\begin{bmatrix} 7 & 8 & 9 & 10 & 11 \\ -7 & 8 & -9 & 10 & -11 \\ 7 & -8 & 9 & -10 & 11 \\ -7 & 8 & -9 & -10 & 11 \\ 7 & 8 & 9 & -10 & -11 \end{bmatrix}, \quad 5)\begin{bmatrix} 0 & 1 & 0 & 2 & 0 \\ 1 & 2 & 3 & 4 & 5 \\ -1 & -3 & -7 & -9 & -11 \\ 4 & 10 & 14 & 18 & 22 \\ 5 & -5 & -10 & -15 & -20 \end{bmatrix},$$

$$6)\begin{bmatrix} 0 & 0 & -2 & 0 & 0 \\ 0 & 5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 \\ 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 7 & 0 \end{bmatrix}, \quad 7)\begin{bmatrix} 2 & -3 & 4 & 0 & 5 \\ 1 & 6 & 0 & 4 & -1 \\ 5 & 0 & 8 & 4 & 9 \\ 7 & 12 & 8 & 12 & 7 \\ 17 & 12 & 24 & 20 & 25 \end{bmatrix}.$$

5. Matrica je gornjotrokutna (donjotrokutna), ako su joj komponente ispod (iznad) glavne dijagonale jednake 0. 1) Da li je umnožak od dvije gornjotrokutne matrice opet gornjotrokutna matrica? 2) Dokaži da je obratna matrica od regularne gornjotrokutne matrice a opet gornjotrokutna matrica i da je diag $\diagdown^{-1} = (\text{diag}\ \diagdown)^{-1}$:

$$(a^{-1})_{ii} = (a_{ii})^{-1}, \quad (a^{-1})_{ik} = \frac{-\sum_{j=1}^{k-1} (a^{-1})_{ij}\, a_{jk}}{a_{kk}}, \quad (k = i+1,\ i+2, \ldots, n);$$

dualno, za donjotrokutnu regularnu matricu a imamo

$$(a^{-1})_{ik} = \frac{-\sum_{j=k}^{n} a_{ij}(a^{-1})_{jk}}{a_{ii}}, \quad (k = i+1,\ i+2, \ldots, n).$$

Pomoću tih rekurzivnih formula provodi se inverzija *trokutnih* matrica vrlo lako. 3) Ako je $\det a \neq 0$, da li je $a = dg$ tj. $a = \left|\diagdown\right| \cdot \left|\diagup\right|$ gdje je d ili $\left|\diagdown\right|$ donjotrokutna, g ili $\left|\diagup\right|$ gornjotrokutna matrica?

3. PRIMJENA OSNOVNOG TEOREMA O SVOĐENJU NA *T*-MATRICE. IZRAČUNAVANJE DETERMINANATA MATRICA. SISTEMI LINEARNIH JEDNADŽBI

3.0. Važnost osnovnog teorema 2.4.0. ne sastoji se samo u tome što nam on daje alat u ruke kojim ćemo odrediti, za zadanu matricu a, *njen rang ra kao broj kT poljâ na kojima je smješten istaknut skup T topova* u dobivenoj matrici a_T. *Važnost postupka je mnogo veća, pogotovu u vezi s rješavanjem linearnih sistema jednadžbi i izračunavanjem determinanata.*

3.1. Primjena osnovnog teorema na izračunavanje determinanata. Ako je a kvadratna konačna matrica, tada a i pripadna *T-matrica* a_T, do koje dolazimo iz a, imaju *istu determinantu*: $\det a = \det a_T$. No, prema teoremu o T-determinantama (§ 2.4.6) $\det a_T$ lako se izračuna. Uostalom, nije ni potrebno ići od a sve do a_T; ako u kojoj etapi (polaznoj ili kasnije) vidimo da etapna matrica e u kojem retku (stupcu) ima malo topova, jedan od njih, e_{ij}, odlikovat ćemo i pomoću toga topa e_{ij} ukloniti preostale topove iz dotične linije i onda odmah tada na etapnoj matrici e upotrijebiti Laplaceov razvoj po toj liniji (retku ili stupcu). Time se provela redukcija:

$$\det a = e_{ij}(-1)^{i+j} \det (e \diagdown e_{ij});$$

$e \diagdown e_{ij}$ se dobije iz e uklanjajući top e_{ij} i obje njegove linije.

3.2. Sistem linearnih jednadžbi. Neka je S zadan sistem linearnih jednadžbi (recimo s n nepoznatih veličina x_ν); neka $[a, b]$ označuje potpunu matricu sistema S; provodeći redukcije matrice a na matricu a_T onako kako je opisano u § 2.1. i vršeći čitav taj posao $a \to a_T$ unutar matrice $[a, b]$, prelazi i ova podmatrica b u posve određenu matricu; označimo je sa $b(a, a_T)$ da se vidi da *ta matrica zavisi i od b i od a i od* a_T. To je zamršena oznaka, no glavno je da sagledamo ideju; ideja je jednostavna: *vršenje L-operacijâ na lijevim stranama jednadžbe povlači za sobom vršenje odgovarajućih L-operacija i na desnim stranama* (i obrnuto).

3.3. Reducirani sistemi. Sistem S_T jednadžbi kojem je $[a_T, b(a, a_T)]$ potpuna matrica *ekvivalentan je s polaznim sistemom S.*

3.4. *Markirani skup T topova u* a_T *ukazuje po kojim ćemo nepoznanicama reducirani sistem* S_T *rješavati.*

Rješavat ćemo ga ovako:

3.4.0. Poći će se od ***najdonjeg topa*** *i iz dotične jednadžbe naći odgovarajuću nepoznanicu uz promatrani top, ne obaziruć se na preostale eventualne nepoznanice koje u toj jednadžbi stvarno dolaze: sve takve nepoznanice su potpuno slobodne.*

3.4.1. Zatim se s tom „nađenom" nepoznanicom polazi k narednom najnižem topu iz T, njegovoj nepoznanici, odredimo je iz te jednadžbe na sličan način kao što smo maloprije odredili onu nepoznanicu, itd., itd., sve dok ne dođemo do kraja.

3.5. *Dobiveno rješenje je opće rješenje reduciranog sistema S_T a time polaznog sistema S.*

3.6. *Sve nepoznate veličine koje nisu uz topove T sasvim su proizvoljne, dakle su i nezavisne jedne od drugih.*

3.6.1. Primjedba. Po gornjim smo obrascima rješavali primjere u specijalnim slučajevima počev već od pogl. 8, § 2.6. No, potpun dokaz za opći slučaj iznesen je tek u prošlom § 2, s primjedbom da još *uvidimo da su rješenja sistema S_T zaista i rješenja polaznog sistema S,* tj. da vidimo da je ispravna rečenica:

⟶ **3.7.** ***Svako rješenje reduciranog sistema S_T iz § 3.3. rješenje je i polaznog sistema S iz § 3.2.***

3.8. Dokažimo, dakle, još sud 3.7. Kao što je naznačeno u teoremu 2.4.0, prelaz od S na S_T[1] dobio se nizom elementarnih L-operacija s redićima matrice, odnosno s jednadžbama; obratan put dovodi nas od S_T do S: svaki koračaj od S prema S_T dozvoljava i povrat, tj. obrat. Tako npr. neka se jedan koračaj K od $[a, b]$ prema $[a, b(a, a_T)]$ sastojao u ovoj elementarnoj L-operaciji: „Iz etapne matrice e formiraj narednu matricu f tako da umjesto retka $e_{6.}$ dođe $e_{6.} + 5 \cdot e_{2.}$ kao redak."[2]

Tada će protivni koračaj ^{-}K glasiti ovako:

„Iz etapne matrice f formiraj narednu matricu e tako da umjesto retka $f_{6.}$ dođe $f_{6.} + (-5) \cdot f_{2.}$ kao redak." Simbolički možemo korak K označiti

$$e \xrightarrow[6,2]{5} f;$$

povratak tada glasi:

$$f \xrightarrow[6,2]{-5} e.$$

Dakle, uistinu iz $[a, b]_T$, odnosno iz sistema S_T jednadžbi dolazimo natrag do $[a, b]$, odnosno do sistema S. A to upravo i znači da su rješenja sistema S_T *ujedno i rješenja za sistem S.*

---

[1] U sistemu S_T treba ispisivati *sve koeficijente*, pa bili oni 0 ili $\neq 0$: dakle se ispisuju i nula-jednadžbe, tako da uvijek imamo posla sa k jednadžbi; k je broj redaka matrice $[a_T, b(a, a_T)]$.

[2] Dakle je redak $f_{6.} = e_{6.} + 5\, e_{2.}$, dok je $f_{k'.} = e_{k'.}$ za svaki drugi redak.

Uostalom, ako radimo sa sistemima linearnih jednadžbi, onda gornji propis *K* glasi ovako: „Iz etapnog sistema *e* jednadžbi formiraj naredni sistem *f* jednadžbi tako da umjesto jednadžbe e_6 dođe jednadžba $e_6 + 5 \cdot e_2$“ itd. Tada se očito vidi da se kod svake etape dolazi do ekvivalentnog sistema jednadžbi.

3.9. Svi gornji zaključci vrijede i za slučaj kad se uz *L-transformacije* redaka upotrebljavaju i *elementarne M-transformacije redaka*, tj. množenje jednog retka matrice brojem $\lambda \neq 0$ (isp. § 4.4).

3.10. Matrična jednadžba $ax = b$, (a, b su zadane matrice). *Čitav tekst iz tačaka* 3.2 — 3.9. *vrijedi i za općenitiji slučaj matrične jednadžbe* $ax = b$; *ona je ekvivalentna s matričnom jednadžbom* $a_T x = b\,(a, a_T)$.

3.11. Treba ukazati na ovo: *ako jednadžba* $ax = b$ *ima rješenje, onda je baza topova u* a_T *također baza u* $[a_T, b\,(a, a_T)]$ *i* $[a, b]_T$, *i obrnuto.*

Tada su, naime, svi reci u a_T (a time i u $[a_T, b\,(a, a_T)]$ koji su izvan redaka s istaknutim topovima zauzeti samim nulama.

Time se dobiva jednostavan *dokaz teorema* 0.3. *o koegzistenciji u pogl.* 14. *čak i za širi slučaj da je b proizvoljna zadana matrica* (isp. pogl. 14, § 2.1).

4. ELEMENTARNE TRANSFORMACIJE MATRICA

4.0. Priprava. U § 2. uzeli smo jednu vrstu elementarnih transformacija matrica (§ 2.3): zadanom retku (stupcu) neke matrice dodaj drugi koji redak te matrice množen nekim brojem. Vidjeli smo koliku korist imamo od upotrebe takvih transformacija (isp. osnovni teorem 2.4.0. i § 3). Sada uvodimo još dvije vrste elementarnih transformacija s ciljem da *u biranju »topova« pri redukciji imamo veću slobodu.* Zato će i redukcija pomoću takvih transformacija dovesti do *najjednostavnijih mogućih T-matrica*: *dijagonalnih, pa čak i takvih kojima su svi topovi* $= 1$.

4.1. *Definicija elementarnih transformacija L, M, Tr u odnosu na matrice.*

4.1.0. *L*-Transformacije. Ako umjesto jednog retka (stupca) neke matrice *a* stavimo u njoj sumu toga retka (stupca) i kratnika nekog drugog retka (stupca) matrice *a*, kaže se *da je na matrici a izvršena elementarna L-operacija, i to na recima* (*stupcima*).

4.1.1. *Tr*-operacije. Ako u zadanoj matrici *a* permutiramo međusobno dva njena retka (stupca), govori se tada o elementarnoj *Tr-operaciji matrice a*, i to na recima (stupcima).

Specijalno, ako dva *susjedna* retka (stupca) zamijene međusobno svoja mjesta, dobivamo određenu *Tr-operaciju.* Ako isti redak a_i. izvrši uzastopno nekoliko takvih elementarnih „susjednih“ transpozicija, recimo 3, i to prema gore, nastaje matrica za koju možemo reći da iz *a* nastaje *translacijom retka* a_i. za 3 prema gore. Slično za stupce. Npr. translacijom stupca $a_{.3}$ za 3 prema lijevo prelazi matrica *a* u $[a_{.3}\, a_{.1}\, a_{.2}\, a_{.4} \ldots]$.

4.1.2. ***M*-operacije.** Ako u zadanoj matrici a jedan njen redak (stupac) zamijenimo njegovim produktom s nekim brojem ili skalarom $\lambda \neq 0$, govori se o elementarnoj *M-operaciji matrice a, i to na recima* (*stupcima*).

4.1.3. Primjedba. *Nazivi L-, M-, Tr-operacije dolaze u vezi s riječima: linearan, množiti i transpozicija* (ili još bolje: translacija!)

4.2. *Upotreba elementarnih transformacija.* Elementarne transformacije upotrebljavamo zato da zadanu matricu svedemo na što jednostavniji oblik, a da pri tom bitna svojstva matrice ostaju sačuvana. O *L*-transformacijama bilo je dosta govora u §§ 2. i 3.

4.2.1. Elementarne transformacije i determinante. Posebno se elementarne transformacije *kvadratnih* matrica upotrebljavaju za izračunavanje determinanata. Naime, ako b nastaje iz a elementarnom transformacijom, vrlo je jednostavna veza između $\det a$ i $\det b$:

$$\det a = \det b \quad \text{za svaku elementarnu } L\text{-transformaciju}$$

$$\det a = -\det b \quad \text{za svaku elementarnu } Tr\text{-transformaciju}$$

$$\det a = \lambda^{-1} \det b \quad \text{za svaku elementarnu } M\text{-transformaciju.}$$

4.3. Bitna uloga *Tr*-transformacije. — **4.3.0.** *Uloga Tr-transformacije sastoji se u ovom: proizvoljna »figura« a_{ij}* ploče (matrice) a može se nizanjem *Tr*-operacija dovesti u *proizvoljno polje*, specijalno u početak (1, 1). Dovoljno je izvršiti „translaciju" retka $a_{i.}$ za i prema gore da postane početni redak, a onda translaciju stupca $a_{.j}$ za j da postane početni stupac. U novoj završnoj matrici z uočena vrijednost a_{ij} je sada z_{11}.

4.3.1. Praktična upotreba. Pri numeričkom rješavanju jednadžbi, npr. pri Gaussovu postupku (pogl. 8, § 2.7), bira se ključni koeficijent — top — na poseban način; *pomoću Tr-transformacija dovodi se top u početak* (1, 1).

Npr. dovedi *Tr*-transformacijama jedan top maksimalne apsolutne vrijednosti u matrici

$$a = \begin{bmatrix} 2 & 0 & 3 & 4 & 5 & 7 \\ 0 & 0 & 4 & -5 & \boxed{-10} & 8 \\ 3 & 2 & 4 & 5 & 8 & 9 \end{bmatrix} \text{ u početak (1, 1).}$$

Evo tog pretvaranja. Top je -10; prema topu -10 udešavamo:

$$\xrightarrow[\text{(ispisuj retke)}]{} \begin{bmatrix} 0 & 0 & 4 & -5 & \boxed{-10} & 8 \\ 2 & 0 & 3 & 4 & 5 & 7 \\ 3 & 2 & 4 & 5 & 8 & 9 \end{bmatrix} \longrightarrow$$

$$\xrightarrow[\text{(piši po stupcima)}]{} \begin{bmatrix} \boxed{-10} & 0 & 0 & 4 & -5 & 8 \\ 5 & 2 & 0 & 3 & 4 & 7 \\ 8 & 3 & 2 & 4 & 5 & 9 \end{bmatrix}.$$

4.3.2. Translacije i dijagonalne matrice. Ako su svi topovi matrice d na dijagonali (tj. d je dijagonalna matrica) pa ako na dijagonali ili uopće nula nema ili je nulâ (topova) konačno mnogo, tada se Tr-operacijom (translacijom) mogu svi topovi postaviti na *početni dio dijagonale*.

Npr.

$$\begin{bmatrix} 3 & & & & & & 0 \\ & 0 & & & & & \\ & & 3 & & & & \\ & & & 0 & & & \\ & & & & 3 & & \\ & & & & & 0 & \\ & & & & & & 0 \\ 0 & & & & & & \cdot \\ & & & & & & & \cdot \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & & & & & & 0 \\ & 3 & & & & & \\ & & 3 & & & & \\ & & & 0 & & & \\ & & & & 0 & & \\ & & & & & \cdot & \\ 0 & & & & & & \cdot \end{bmatrix}$$

To kod ove beskonačne dijagonalne matrice diag [0, 1 0 1 0 1 . . .] nije moguće!

4.3.3. Translacije i *T*-matrice. — 4.3.3.0. Zadatak. Zadana je *T*-matrica (isp. definiciju 2.2)

$$l = \begin{bmatrix} 4 & 7 & \boxed{2} & 4 & 1 & \\ 0 & 0 & 0 & 0 & 0 & \\ \boxed{3} & 5 & 0 & 5 & 2 & X \\ 0 & 0 & 0 & 0 & 0 & \\ 0 & 4 & 0 & 0 & \boxed{4} & \end{bmatrix}$$

sa svojom osobitom topovskom bazom (topovi baze su markirani). Translacijama prevedi l u T-matricu u tako da u njoj zadana topovska baza dođe na dijagonalu ili čak, ako je moguće, na početni dio dijagonale (X je proizvoljna podmatrica: prazna ili neprazna, ali uz uslov da su X_2. i X_4. bez topova (inače l ne mora biti *T*-matrica).

Rješavanje. Početni korak: **Najgornji top** dovedi u polje (1, 1); izlazi *T*-matrica (ispisuj po stupcima)

$$\begin{bmatrix} \boxed{2} & 4 & 7 & 4 & 1 & \\ 0 & 0 & 0 & 0 & 0 & \\ 0 & \boxed{3} & 5 & 5 & 2 & X \\ 0 & 0 & 0 & 0 & 0 & \\ 0 & 0 & 1 & 2 & \boxed{4} & \end{bmatrix}.$$

Najgornji top u preostatku baze dovedi u naredno polje (2, 2) dijagonale; izlazi (ispisuj po recima)

$$\left[\begin{array}{ccccc} \boxed{2} & 4 & 7 & 4 & 1 \\ 0 & \boxed{3} & 5 & 5 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & \boxed{4} \end{array}\right] X(1);$$

isto s preostatkom; izlazi tražena matrica

$$u=\left[\begin{array}{ccccc} \boxed{2} & 4 & 1 & 7 & 4 \\ 0 & \boxed{3} & 2 & 5 & 5 \\ 0 & 0 & \boxed{4} & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right] X(2).$$

Analogno se dokazuje:

4.3.4. Teorem. *Ako je T bilo kakva T-matrica, a A jedna njena istaknuta baza topova, tada se nizom Tr-operacija na recima može T prevesti u takvu T-matricu U da zadana baza A topova zauzme dijagonalan položaj i ostane baza u U; ako je A konačno, može se dalje pomoću Tr-operacija na stupcima doći do T-matrice u kojoj će baza A zauzeti cijelu dijagonalu ili njen početni komad. U svakoj etapi ostaje A i dalje baza.*

Kombinirajmo *L*-operacije i *Tr*-operacije; to znači da vrijedi i osnovni teorem 2.4.0. i teorem 4.3.4. Na taj način imamo

4.3.5. Teorem. *Svaka matrica a kojoj je broj redaka konačan može se konačnim nizom operacija, koje su bilo L-operacije s recima bilo operacije Tr, prevesti u jednu dijagonalnu T-matricu, tj. u* $\boxed{\ }$*-matricu* $\boxed{\ }a$. *Rang se pri tom ne mijenja:* $ra=r(\boxed{\ }a)$ *i jednak je broju topova na dijagonali dobivene matrice* $\boxed{\ }a$. *Pripadna najmanja podmatrica u* $\boxed{\ }a$ *nad tim topovima jest određena M-podmatrica dobivene matrice* $\boxed{\ }a$.

N. B. Imajmo pri tom na umu da *L*-operacije s recima i *Tr*-operacije odgovaraju svakidašnjim operacijama s linearnim jednadžbama kojima se rješenja time ne mijenjaju.

4.3.6. Teorem (*i*). *Svaka matrica a kojoj je oblast konačna može se pomoću konačno mnogo operacija tipa L, Tr vršenim na* **recima** *svesti na matricu u kojoj ispod* [*iznad*] *dijagonale koja izlazi iz gornjeg lijevog* [*donjeg desnog*] *vrha dolaze same* 0.

(*ii*) *Svaka matrica kojoj je oblast konačna može se pomoću konačno mnogo operacija tipa L, Tr i vršenim na* ***stupcima*** *svesti na matricu u kojoj desno* [*lijevo*] *od dijagonale koja polazi iz gornjeg lijevog* [*donjeg desnog*] *vrha stoje samo* 0.

D o k a z. Promatrajmo $a_{\cdot 1}$; ako je taj stupac $\neq \vec{0}$, možemo pretpostaviti da je $a_{11} \neq 0$; naime, ako je $a_{11} = 0$, pa ako je a_{i1} prvi top u $a_{\cdot 1}$, onda će transpozicijom retka $a_{1\cdot}$ i retka $a_{i\cdot}$ matrica a preći u matricu b u kojoj je polje (1, 1) jednako a_{i1} pa na toj matrici b možemo dalje raditi i svaki redak $b_{j\cdot}$ sa $j > 1$ zamijeniti sa $b_{j\cdot} - \frac{b_{1\cdot}}{b_{11}} b_{j1}$; time se dobije matrica

$$a' = \begin{bmatrix} b_{11} & b_{12} \cdots \\ 0 & c \\ 0 & \\ \cdot & \\ \cdot & \\ \cdot & \end{bmatrix}.$$

Sada se prelazi na analogno razmatranje matrice $a' \diagdown b_{11}$ (nastaje iz a' brisanjem prvog retka i prvog stupca) pa se ona prevede u matricu u kojoj se eventualni jedini top mora nalaziti u početnom polju itd. Isto tako ako je bilo $a_{\cdot 1} = \vec{0}$ prelazi se na razmatranje matrice $a \diagdown a_{11}$ itd.

Poslije najviše $k_1 a$ koraka dolazi se do željene matrice.

Analogno se dokazuje teorem (*i*) za tekst u [ ]: ulogu *prvog* stupca $a_{\cdot 1}$ preuzima sada *posljednji* stupac $a_{\cdot n}$; ulogu polja (1, 1) preuzima polje (k, n).

Slično se dokazuje teorem (*ii*).

4.3.7. Lako se provjeri da je

$$a' = \left|\diagdown\right|_1 \cdot a,$$

gdje matrica $\left|\diagdown\right|_1$ označuje onu koja iz jedinične matrice nastaje zamjenjujući joj prvi stupac sa

$$\left[1, \ -\frac{a_{21}}{a_{11}}, \ \frac{a_{31}}{a_{11}}, \ldots, \ -\frac{a_{k1}}{a_{11}}\right]^T.$$

Uopće se tako lako provjeri da konačnim nizom *L*-transformacija redaka dobijemo, polazeći od matrice a, određenu matricu oblika

$$\left|\diagdown\right|_m \cdots \left|\diagdown\right|_2 \left|\diagdown\right|_1 a, \quad \text{gdje su} \quad \left|\diagdown\right|_1, \ \left|\diagdown\right|_2, \ldots, \ \left|\diagdown\right|_m$$

donjotrokutaste matrice.

4.4. Bitna uloga *M*-transformacije matrica. — 4.4.0. *Uloga M-transformacije matrice a sastoji se u tome da se uočeni proizvoljni top T matrice a pretvori u proizvoljnu vrijednost* $v \neq 0$ (najčešće: „normiranje“: $v = 1$), *i to prema želji: množeći ili T-ov redak ili T-ov stupac brojem* $v T^{-1}$.

Npr. „normiraj“ top $2 = T$ u matrici

$$u = \begin{bmatrix} \boxed{2} & 8 & 12 & 4 \\ 6 & 8 & 12 & 0 \end{bmatrix}$$

množeći bilo njegov redak bilo njegov stupac sa T^{-1}. Množeći stupac, izlazi:

$$\begin{bmatrix} \boxed{1} & 8 & 12 & 4 \\ 3 & 8 & 12 & 0 \end{bmatrix};$$

množeći redak, izlazi:

$$\begin{bmatrix} \boxed{1} & 4 & 6 & 2 \\ 6 & 8 & 12 & 0 \end{bmatrix}.$$

4.4.1. Praktična upotreba *M*-transformacije. *Izabrani top $T = x_{ij}$ matrice x normira se na* 1 *množenjem njegova retka* (*čitaj*: *jednadžbe*), *odnosno stupca sa* T^{-1}. *U novonastaloj matrici u poništi se svaki željeni top t iz stupca $u_{.j}$ pomoću L-transformacije*: *retku od t dodaj redak* $-t \cdot u_{i}$..

4.4.2. Primjer. Dijagonalnu matricu

$$\begin{bmatrix} 3 & & & \\ & 0 & & \\ & & 4 & \\ & & & 0 \end{bmatrix}$$

prevedi u dijagonalnu matricu s normiranim topovima 1. Dovoljno je po redu svaki stupac (redak) u kojem je top pomnožiti recipročnom vrijednošću toga topa. Imamo, dakle, po redu:

$$\begin{bmatrix} 3 & & & \\ & 0 & & \\ & & 4 & \\ & & & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & & & \\ & 0 & & \\ & & 4 & \\ & & & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & & & \\ & 0 & & \\ & & 1 & \\ & & & 0 \end{bmatrix}.$$

Naravno, znak $\rightarrow$ ne može se zamijeniti znakom $=$.

Analogno se dokazuje:

4.4.3. *Svaka dijagonalna matrica sa n topova* $\neq 1$ *može se nizom od n elementarnih M-operacija svesti na dijagonalnu matricu u kojoj je svaki top* $= 1$.

Npr. za beskonačnu dijagonalnu matricu: diag: [1, 2, 3, . . .] potreban je beskonačan niz jednočlanih *M*-operacija pa da se svede na „normirani“ oblik: diag [1, 1, 1, . . .].

4.5. Zadaci o elementarnim transformacijama matrica i determinanata.

1. Ako je a bilo koja kvadratna matrica iz § 2.5 neka $a\,(2, 3)$ označuje matricu koja iz a nastaje tako da joj polje (2, 3) pomaknemo u položaj (1, 1). U kakvoj su vezi $\det a$, $\det a\,(2, 3)$?

2. Pođi od jedinične matrice $1_3 = e$ pa $e_{.3}$ pomnoži sa -2 i dodaj k $e_{.1}$; u rezultatu $e_{2.}$ pomnoži sa 2 i rezultat dodaj retku $e_{3.}$; dobivenu matricu pomnoži sa 2; nađi matricu koju na taj način dobijemo kao i pripadnu determinantu.

3. Ispitaj matrice I, J, K iz teorije kvaterniona te matrice $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \xi, \beta_1, \beta_2, \beta_k$ iz kvantne mehanike (pogl. 10, § 4.7.9, 4.7.10); pokaži kako se te matrice prikazuju u obliku $x\,I\,y$, gdje je I jedinična matrica oblasti (4,4). Odredi rang tih matrica.

4. Neka je

$$a = \begin{bmatrix} 2 & 4 & 5 & 6 \\ 3 & 2 & 2 & 1 \end{bmatrix}, \qquad b = \begin{bmatrix} 3 & 4 & 5 \\ 4 & 2 & 1 \\ 5 & 1 & 2 \\ 3 & 1 & 1 \end{bmatrix}.$$

Odredi rang ovih matrica: 1) a, b; 2) $a\,b$, 3) $c = \begin{bmatrix} a & & & \\ 0 & 0 & 1 & 0 \end{bmatrix}$,

4) bc, 5) $b + c^T$, 6) $[b_{.1}\, b_{.2}]\, a$, 7) $V[a_{1.}]^T$, 8) $V[a_{2.}]^T$
isp. pogl. 11, § 11.5).

5. Napiši nekoliko matrica ranga 2 i oblasti: 1) 2×2, 2) 3×3, 3) $n \times n$ za bilo koji redni broj $n \geq 2$, 4) 6×10, 5) $k \times n$ gdje su k, n redni brojevi > 1. 6) Ako je $N = [1, 2, \ldots]$, odredi rang matrice:
1) NN^T, 2) $N^T N$, 3) $[N^T, N^T]$.

5. KANONSKI OBLIK MATRICA

5.0. Pođemo li od kakve (konačne) matrice a, tada je možemo pomoću (konačnog) niza elementarnih *L-transformacija* dovesti do određene T-matrice a_T (osnovni teorem 2.4.0); svaka (konačna) T-matrica može se (konačnim) nizom elementarnih *Tr-transformacija* prevesti u *dijagonalni oblik* (v. § 4.3.3.1). Svaka se dijagonalna (konačna) matrica može (konačnim) nizom elementarnih *M-operacija* prevesti u dijagonalnu matricu bez topova $\neq 1$. Odatle neposredno zaključujemo ovo:

5.1. Teorem. *Svaka se konačna matrica može pomoću konačnog niza elementarnih transformacija svesti na kanonski normiran oblik, tj. na dijagonalnu matricu bez topova* $\neq 1$.

5.2. Teorem. *Svaka se matrica može* (konačnim ili beskonačnim) *nizom elementarnih operacija svesti na* $\diagdown|$*-oblik* (odnosno $|\diagdown$-oblik), tj. na oblik u kojem su sve vrijednosti ispod (iznad) dijagonale jednake 0.

5.3. Teorem. *Kod svake elementarne transformacije matrice ostaje rang matrice uščuvan.*

To smo u § 2.4.3. dokazali za L-transformacije. Za M-transformacije stvar je očigledna, jer ako matrica a' izlazi iz matrice a tako da u a redak (stupac) y zamijenimo sa λy, gdje je λ broj $\neq 0$, tada svakoj kvadratnoj submatrici x iz a odgovara kvadratna matrica x' u a'; očigledno je $\det x = \lambda_1^- \det x'$

ili $\det x = \det x'$, već prema tome da li se pri toj M-operaciji jedan redak u x množio sa λ ili se nije množio. No, u svakom slučaju, ako je x regularno (singularno), onda je to i x'. A to upravo znači da je rang od a jednak rangu od a'. Analogno se stvar zaključuje za Tr-transformacije.

Iz 5.1. i 5.3. zaključujemo da vrijedi:

5.4. Teorem. *Neka su matrice a, b konačne. Ako su one istog poretka i istog ranga, tada tim matricama pripada isti normirani dijagonalni oblik*

$$\begin{bmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & \ddots & & & \\ & & & & 1 & & \\ & & & & & 0 & \\ & & & & & & \ddots \end{bmatrix};$$

r jedinica na dijagonali

i obrnuto: *ako matricama a, b pripada isti normirani dijagonalni oblik* ν, *tada je* $\mathrm{Dom}\, a = \mathrm{Dom}\, b$, $ra = rb =$ broj jedinica u ν.

Dokažimo ovaj drugi dio.

Prema pretpostavci, a i b imaju isti normirani oblik ν; to znači da je $a \Leftrightarrow \nu$, $b \Leftrightarrow \nu$, gdje znak $x \sim y$ ili $x \Leftrightarrow y$ treba čitati: *polazeći od x dolazimo do y pomoću konačno mnogo elementarnih transformacija*. No, očigledno iz $b \Leftrightarrow \nu$ izlazi $\nu \Leftrightarrow b$ (dovoljno je stazu od b do ν prelaziti *natrag* korak po korak obrnutim redom od onog putovanja od b do ν). No, putovanjem $a \Leftrightarrow \nu$ pa putovanjem $\nu \Leftrightarrow b$ prešli smo stazu od a do b (preko ν), i to, naravno, u konačno mnogo koračaja. Dakle je $a \Leftrightarrow b$.

Radi kratkoće možemo znak $x \sim y$ čitati: *x ekvivalentno sa y*.

5.5. Zadaci. Navedi kanonske oblike matrica iz § 4.5.

6. EKVIVALENTNE MATRICE

6.0. Definicija. Konačna matrica *a ekvivalentna je* s matricom *b*, simbolički $a \sim b$, ako se počinjući sa a može pomoću ***konačno mnogo elementarnih operacija*** doći do matrice b.

6.1. U sadašnjoj oznaci možemo za matrice iz § 2.4.1. napisati:

$$a = \begin{bmatrix} 5 & -1 & 2 \\ 4 & -1 & 1 \\ -1 & 1 & 0 \\ 3 & -2 & 1 \end{bmatrix} \sim \begin{bmatrix} 5 & \boxed{-1} & 2 \\ \boxed{-1} & 0 & -1 \\ 0 & 0 & \boxed{-2} \\ 0 & 0 & 0 \end{bmatrix} = a_T$$

(tu je markiran odlikovani skup topova); dalje je (čitati po stupcima!)

$$a_T\sim\begin{bmatrix}\boxed{-1} & 5 & 2\\ 0 & \boxed{-1} & -1\\ 0 & 0 & \boxed{-2}\\ 0 & 0 & 0\end{bmatrix}$$

(istaknuti su topovi dovedeni na dijagonalu!)

Dalje:
$$\sim\begin{bmatrix}1 & 5 & 2\\ 0 & 1 & 1\\ 0 & 0 & 1\\ 0 & 0 & 0\end{bmatrix}$$

(množili smo prvi stupac sa -1, drugi redak sa -1 i treći redak sa -2^{-1}). Ovo je dalje: $\sim\mathrm{diag}\,[1\ \ 1\ \ 1\ \ 0]_3^4$. Dakle je

$$a\sim\mathrm{diag}\,[1\ \ 1\ \ 1\ \ 0]_3^4=\nu\,a;$$

gornji indeks ili eksponent 4 i donji indeks 3 ukazuju na broj k_1 redaka i broj k_2 stupaca.

6.2. Lema. Relacija ekvivalentnosti među matricama je *povratna* ili *refleksivna* ($a\sim a$), *simetrična* ili *obrtna* (iz $a\sim b$ izlazi $b\sim a$) te *prelazna* (iz $a\sim b$, $b\sim c$ izlazi $a\sim c$).

6.3. Teorem. **Ekvivalentnost matrica istog oblika i ranga.** *Ako su matrice a i b konačne, iste oblasti i istog ranga, tada je $a\sim b$; obrnuto: iz $a\sim b$ izlazi* $\mathrm{Dom}\,a=\mathrm{Dom}\,b$, $ra=rb$ (isp. § 5.4).

6.4. Teorem o normiranim matricama. *Ako je matrica x konačna, tada je*

$$x\sim\mathrm{diag}\,[\underbrace{1\ \ 1\cdots 1}_{r(x)}\ \ \underbrace{0\ \ 0\ \cdots\ 0}_{\mathrm{Min}\,\{k_1x-rx,\ k_2x-rx\}}]:$$

k_1x, k_2x je broj redaka, odnosno stupaca matrice x (isp. § 5.4). Takve dijagonalne matrice zovu se *normirane dijagonalne matrice*.

Na taj način možemo odmah napisati matricu zadane oblasti $k\times n$ i zadanog ranga r: to je matrica

$$I(k,n,r)=\underbrace{\begin{bmatrix}1 & & & & 0\\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & \\ & & & & \ddots\\ 0 & & & & 0\end{bmatrix}}_{n}\Bigg\}k.$$

$\underbrace{\qquad}_{r}$ jedinica na dijagonali

Sve druge matrice s istom oblasti i istog ranga izlaze iz te normirane matrice pomoću konačnog broja elementarnih transformacija.

7. ELEMENTARNE MATRICE

7.0. Definicija. *Elementarne matrice* jesu one koje iz *jediničnih matrica* nastaju bilo kojom *elementarnom transformacijom.*

7.1. Tako npr. ako u jediničnoj matrici diag [1, 1, 1] treći stupac $e_{.3}$ zamijenimo sumom $e_{.3}+4\,e_{.2}$, izlazi „elementarna matrica"

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix}.$$

Top 4 ima položaj (2, 3).

Izvršimo analognu operaciju u kojoj drugoj matrici x:

$$x \to [x_{.1},\ x_{.2},\ x_{.3}+4\,x_{.2}] = \begin{bmatrix} x_{11} & x_{12} & x_{13}+4\,x_{12} \\ x_{21} & x_{22} & x_{23}+4\,x_{22} \\ x_{31} & x_{32} & x_{33}+4\,x_{32} \end{bmatrix}.$$

Vidi se da je to upravo jednako produktu

$$x \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix}.$$

Za analognu operaciju s recima matrice x i jedinične matrice 1_3 bilo bi

$$x \to \begin{bmatrix} x_{1.} \\ x_{2.} \\ x_{3.}+\lambda x_{2.} \end{bmatrix}, \tag{1}$$

$$I \underset{(3,3)}{\to} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 4 & 1 \end{bmatrix}. \tag{2}$$

Vidi se da se iznos (proizvod) u (1) dobije iz proizvoda u (2) množeći ga zdesna sa x.

Tako vidimo kako se *L-operacija* na proizvoljnoj matrici x dobije *množeći rezultat analogne operacije sa I, i to sprijeda* ili *straga,* već prema tome da li se radi s recima ili stupcima.

7.2. Ista se stvar lako dokazuje i za ostala dva tipa elementarnih operacija: množenje retka (stupca) sa $\lambda \neq 0$ te transpozicija dvaju redaka (stupaca).

Npr. transpozicija prvih dvaju redaka u a dovodi do

$$b=\begin{bmatrix} a_{2\cdot} \\ a_{1\cdot} \\ \cdot \\ \cdot \end{bmatrix};$$

no odmah se vidi da je (čitaj po redićima!):

$$b=\begin{bmatrix} 0 & 1 & 0 & \cdot & \cdot \\ 1 & 0 & \cdot & \cdot & \cdot \\ \text{isto} & & & & \end{bmatrix}\cdot a.$$

Na taj način imamo:

⟶ **7.3. Teorem o prikazivanju rezultata elementarne transformacije kao produkt odgovarajuće elementarne matrice.** *Rezultat svake elementarne transformacije s recima* (*stupcima*) *matrice a dobije se tako da se matrica a pomnoži sprijeda* (straga) *odgovarajućom elementarnom matricom.* To simbolički možemo pisati:

$$t_{=}a=(t_{=}1)\cdot a$$

$$t_{\parallel}a=a\cdot(t_{\parallel}1);$$

$t_{=}x$ (odnosno $t_{\parallel}x$) označuje rezultat elementarne transformacije s recima (odnosno stupcima) matrice x.

7.4. Lema. **Svaka elementarna matrica x je regularna.** Naime, ako x nastaje iz jedinične matrice L-operacijom, onda je $\det x=\det(\text{jed.})=1$.

Ako x nastaje M-operacijom, onda je $\det x=\lambda$.

Ako x nastaje Tr-operacijom, onda je $\det x=-1$.

7.5. Iz 7.3. i 7.4. izlazi specijalno ovo: *ako b iz a nastaje elementarnom operacijom, onda je $b=xay$, gdje su x, y regularne matrice* (mogu biti $i=1$). Ako, nadalje, c nastaje iz b pomoću elementarne operacije, znači to da je isto tako $c=x'by'$, gdje su x', y' opet neke regularne matrice. Dakle je $c=x'(xay)y'=(x'x)a(yy')$. No, produkt regularnih matrica $x'x$, odnosno y, y' opet je regularna matrica; zato je, dakle, $c=XaY$, gdje su X, Y *regularne* (iako ne nužno elementarne) matrice. Provedemo li na rezultatu XaY novu elementarnu transformaciju, opet ćemo doći do produkta s tri faktora; srednji je a, a krajnji su regularne kvadratne matrice. Zaključujući tako postupno, dokazuje se ovo:

7.6. Teorem. *Ako je matrica a ekvivalentna s matricom b,* tj. *ako je $a\sim b$, onda je $xay=b$, pri čemu matričnu jednadžbu $xay=b$ zadovoljava bar jedan par* ***regularnih*** *matrica x i y.*

Vrijedi i obrat (isp. zaključak (3) ⇒ (2) u § 8.9; također § 8.10).

7.7. Svođenje matrice na trokutni odnosno trapezni oblik. Na osnovu razmatranja u §§ 4.3.6, 7.3. i 7.4. zaključujemo da vrijedi

⟶ Teorem. *Svakoj kvadratnoj matrici a kojoj je oblast konačna pripadaju regularne kvadratne matrice x, x′ za koje je*

$$xa = \text{◺} \quad \textit{odnosno} \quad x'a = \text{◹};$$

isto tako za neke regularne kvadratne matrice y, y′ matrica ay [*odnosno ay′*] *nema ispod* [*iznad*] *dijagonale nikoje vrijednosti* $\neq 0$.

Ako je a nekvadratna matrica konačne oblasti, tada postoje regularne kvadratne matrice x, x′ sa svojstvom da u matrici xa [*odnosno x′ a*] *ispod* [*iznad*] *dijagonale iz gornjeg lijevog* [*donjega desnog*] *vrha stoje same* 0; *isto tako za neke regularne kvadratne matrice y, y′ matrica ay* [*odnosno ay′*] *ima svojstvo da desno* [*lijevo*] *od dijagonale iz gornjeg lijevog* [*donjeg desnog*] *vrha stoje same* 0.

Bar jedna od matrica xa, x′ a, ay, ay′ je trokutasta ◺ *ili* ◹ (*preostatak je ili trokut ili pravokutan trapez; ovaj slučaj nastupa onda, ako je matrica a nekvadratna*).

U općem slučaju nijedna od matrica x, x', y, y' ne mora biti trokutasta, jer bi inače zaključili da se svaka matrica može prikazati kao produkt od dvije trokutaste matrice.

7.7.1. Ne može se svaka matrica pa ako je i kvadratna prikazati kao produkt od dvije trokutne matrice.

Tako npr. matrica $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ nije produkt od dvije trokutaste matrice; nijedna kvadratna regularna matrica a oblasti (n, n) za koju je $a_{11} = 0$, $a_{nn} = 0$ nije produkt dviju trokutnih matrica.

Pretpostavimo naprotiv da je $a = xy$ i da su x, y trokutaste matrice.

Najprije, matrica a nije trokutasta jer je regularna, a s druge strane kad bi bila trokutasta bilo bi $\det a = \prod a_{ii} = 0$ radi $a_{11} = 0$.

Iz relacije $a = xy$ proizlazi $\det a = \det x \det y$ dakle $\det x \neq 0$, $\det y \neq 0$.

Posebno je

$$x_{11} y_{11} \neq 0, \quad x_{nn} y_{nn} \neq 0. \tag{1}$$

Matrice x, y ne mogu biti obje donjotrokutaste niti obje gornjotrokutaste jer bi im inače produkt a bio donjotrokutasta, odnosno gornjotrokutasta matrica, protivno činjenici da a nije trokutasta matrica.

Dakle bi preostalo da bude

$$x = d, \qquad y = g$$

ili

$$x = g, \qquad y = d$$

pri čemu sa d i g označujemo proizvoljnu donjotrokutastu, odnosno gornjotrokutastu matricu. No, u prvom slučaju bilo bi

$$a_{11} = d_{1\cdot} g_{\cdot 1} = d_{11} g_{11} = x_{11} y_{11}$$

tj.

$$0 = x_{11} y_{11}; \quad \text{protivno sa (1);}$$

u drugom slučaju bilo bi

$$a_{nn} = g_{n\cdot}\, d_{\cdot n} = g_{nn}\, d_{nn} = x_{nn}\, y_{nn}$$

tj.

$$0 = x_{nn}\, y_{nn};$$ ovo je u protivnosti sa (1).

7.8. Zadaci o ravnopravnim ili ekvivalentnim matricama.

1. Da li su slijedeći parovi matrica ekvivalentni?

1) $\begin{bmatrix}1&0\\0&1\end{bmatrix}, \begin{bmatrix}0&1\\1&0\end{bmatrix}$; 2) a, a^T; 3) $a, \bar{a}$, 4) a, a^*;

5) $\begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix}, \begin{bmatrix}0&1&0\\0&0&0\\0&0&1\end{bmatrix}$; 6) $\begin{bmatrix}0&0&1\\1&0&0\\0&0&1\end{bmatrix}, \begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix}$;

7) $\begin{bmatrix}1&0&1\\0&1&0\\1&0&1\end{bmatrix}, \begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$; 8) $\begin{bmatrix}1&0&0\\1&0&0\\1&1&1\end{bmatrix}, \begin{bmatrix}0&0&0\\0&1&0\\0&0&1\end{bmatrix}$;

9) $\begin{bmatrix}1&1&1\\1&0&1\\1&1&1\end{bmatrix}, \begin{bmatrix}1&1&1\\1&1&1\\1&1&1\end{bmatrix}$; 10) $\begin{bmatrix}1&0\\0&1\end{bmatrix}, \begin{bmatrix}0&0&0\\0&1&0\\0&0&1\end{bmatrix}$,

2. U prethodnom zadatku odredi elementarne transformacije kojima se prva matrica prevodi u drugu, ukoliko su matrice ravnopravne.

3. Riješi jednadžbu $xay = b$ za ove matrice a, b: 1) $1_2, 1_2$;

2) $\begin{bmatrix}1&0\\0&1\end{bmatrix}, \begin{bmatrix}0&1\\1&0\end{bmatrix}$; 3) $\begin{bmatrix}2&4\\5&3\end{bmatrix}, \begin{bmatrix}1&3\\4&2\end{bmatrix}$; 4) $\begin{bmatrix}1&2&3\\4&5&6\\7&8&9\end{bmatrix}$,

$\begin{bmatrix}1&0&4\\5&2&7\\6&8&3\end{bmatrix}$; 5) $c = \begin{bmatrix}3&4&-2\\3&2&-1\\5&1&6\end{bmatrix}, \begin{bmatrix}1&0&0\\0&0&0\\0&0&0\end{bmatrix}$; 6) $c, \begin{bmatrix}0&0&0\\0&0&0\\0&0&0\end{bmatrix}$.

8. NEKOLIKO TEOREMA O RANGU MATRICA

8.0. Na ovom mjestu možemo skupiti nekoliko važnih činjenica o rangu $r(a)$ matrice a (a je proizvoljna matrica s konačnom oblasti).

8.1. Lema. *Rang matrice ne mijenja se elementarnim transformacijama matrice.*

8.2. Lema. *Rang dijagonalne matrice jednak je broju topova na dijagonali.*

8.3. Lema. *Rang T-matrice jednak je broju topova u svakom istaknutom skupu topova.*

8.4. Teorem (*i*) *Rang produkta dviju matrica ne premašuje rang nikojeg svojeg faktora*: $r(ab) \leq ra, rb$.

Teorem (*ii*) (Teorem o nulosti; Sylvester, 1884). Za kvadratne matrice konačna poretka vrijedi

$$\operatorname{Sup}\{\operatorname{Def} a, \operatorname{Def} b\} \leq \operatorname{Def}(ab) \leq \operatorname{Def} a + \operatorname{Def} b;$$

pri tom je

$$\operatorname{Def} a = k_1 a - r(a).$$

Teorem (*iii*). Za kvadratne konačne matrice a, b vrijedi

$$ra - \operatorname{Def} b,\ rb - \operatorname{Def} a \leq r(a \cdot b) \leq \inf\{r(a), r(b)\}. \tag{2}$$

Pri tom se može desiti da bude $r(ab) = 0$, premda je $r(a) > 0$, $r(b) > 0$.

Npr. za $a = \begin{bmatrix} 1_n & 0 \\ 0 & 0 \end{bmatrix}$, $b = \begin{bmatrix} 0 & 0 \\ 0 & 1_n \end{bmatrix}$, vrijedi

$$\operatorname{Dom} a = \operatorname{Dom} b = (2n, 2n) \quad r(ab) = 0.$$

Teorem (*IV*). Ako su a, b, c matrice konačnog istog poretka (n, n), tada vrijedi

$$r(ab) + r(bc) \leq r(b) + r(abc) \tag{3}$$ (Frobenius, 1911).

Dokaz teorema (*i*) se oslanja na Binet-Cauchyjev teorem (pogl. 11 o determinantama, § 9.9). Najprije primijetimo da je svaka kvadratna podmatrica m produkta ab produkt od s redaka iz a i s stupaca iz b, gdje je $s = k_1 m = k_2 m$ (broj redaka odnosno stupaca). To prema Binet-Cauchyjevu teoremu znači da je $\det m$ linearna kombinacija nekog broja kvadratnih podmatrica x, y za koje je $x \subset a$, $y \subset b$ te $k_1 x = k_2 y = k_1 m$. A to odmah ima za posljedicu ovo: ako je $s > ra, rb$, onda je $\det m = 0$, jer je $\det x = \det y = 0$. Q.E.D.

8.4.1. Dokažimo Frobeniusov teorem (*IV*) jer iz njega proizlaze (*ii*) i (*iii*).

Promatrajmo skup $N(ab)$ svih rješenja jednadžbe $(ab)\vec{x} = \vec{0}$; prema poglavlju 13. teor. 8.1. dimenzija prostora $N(ab)$ je jednaka defektu $\operatorname{Def}(ab)$ matrice ab tj. $\dim N(ab) = \operatorname{Def}(ab) = k_2(ab) - r(ab)$. Iz istog je razloga $\dim Nb = k_2 b - r(b)$. No, jasno je da je

$$N(b) \subset N(ab) \tag{4}$$

jer $\vec{x} \in N(b)$ znači $b\vec{x} = \vec{0}$ dakle je i $a(b\vec{x}) = \vec{0}$ tj. $(ab)\vec{x} = \vec{0}$; prema tome $\vec{x} \in N(ab)$. Iz (4) izlazi $\dim N(b) \leq \dim N(ab)$, dakle $\operatorname{Def}(b) \leq \operatorname{Def}(ab)$; odavde izlazi $k_2 b - r(b) \leq k_2(ab) - r(ab)$; kako je $k_2 b = k_2(ab)$ daje posljednja relacija ovo $-r(b) \leq -r(ab)$ tj.

$$r(ab) \leq r(b). \tag{5}$$

Iz (4) zaključujemo ovo: od $\mathrm{Det}\,(ab)=\mathrm{Dim}\,N\,(ab)$ linearno nezavisnih vektora koji određuju prostor $N\,(ab)$ imamo već $\mathrm{Def}\,b$ linearno nezavisnih vektora koji određuju njegov potprostor Nb pa zato još treba odabrati

$$\alpha=\mathrm{Def}\,(ab)-\mathrm{Def}\,b \tag{6}$$

linearno nezavisnih vektora u $N\,(ab)\setminus N\,(b)$ pa da ti vektori, $\mathrm{Def}\,b+\alpha$ na broju, čine bazu prostora $N\,(ab)$. Dakle je $\alpha\geq 0$, pa prema (6) imamo

$$0\leq\alpha=(k_2\,(ab)-r\,(ab))-(k_2\,b-rb)=r\,(b)-r\,(ab) \qquad \text{tj.}$$

$$0\leq\alpha=r\,(b)-r\,(ab). \tag{7}$$

Time smo dokazali da vrijedi ova lema.

8.4.2. L e m a. Prostor $N\,(ab)$ ima upravo $r\,(b)-r\,(ab)\geq 0$ linearno nezavisnih vektora koji s nekom bazom potprostora $N\,(b)$ čine bazu čitavog prostora $N\,(ab)$:

$$\dim N\,(ab)=\mathrm{Dim}\,Nb+(rb-r\,(ab)). \tag{8}$$

Posebno, ako su vektori $x_1, x_2, \ldots, x_p$ iz $N\,(ab)$, a vektori $bx_1, bx_2, \ldots, bx_p$ linearno nezavisni, onda je nužno,

$$\sum_{p'}\lambda_{p'}\,x_{p'}\in N\,(b)\ \Leftrightarrow\ \lambda_{p'}=0 \ \text{dakle} \tag{9}$$

$$p\leq r\,(b)-r\,(ab). \tag{10}$$

8.4.3. Promatrajmo sada produkt abc matrica a, b, c. Radi $abc=a\,(bc)$ daje lema 8.4.2. relaciju

$$\dim N\,(abc)=\dim N\,(bc)+q, \qquad \text{gdje je} \tag{11}$$

$$q=r\,(bc)-r\,(abc)\geq 0. \tag{12}$$

Jednakost (11) kazuje da se vektorska baza, e, prostora $N\,(bc)$ može proširiti u vektorsku bazu E prostora $N\,(abc)$ izborom novih q linearno nezavisnih vektora $v_{q'}$ iz $N\,(abc)$. Naravno

$$\sum\lambda_{q'}\,v_{q'}\in N\,(bc)\ \Leftrightarrow\ \lambda_{q'}=0. \tag{13}$$

Zbog toga su vektori $(bc)\,v_{q'}$ linearno nezavisni. Naime svaka 0-veza

$$\sum\lambda_{q'}\,(bc)\,v_{q'}=\vec{0} \quad \text{daje} \quad (bc)\sum\lambda_{q'}\,v_{q'}=\vec{0} \qquad \text{tj.}$$

$$\lambda_{q'}\,v_{q'}\in N\,(abc). \tag{14}$$

Ta jednakost sa (13) daje

$$\lambda_{q'}=0.$$

Dakle su vektori $(bc)\,v_{q'}$ linearno nezavisni. No, vektori $cv_{q'}$ leže u Na; zato prema lemi 8.4.2 vrijedi $q\leq r\,(b)-r\,(ab)$. Dakle prema (12):

$$r\,(bc)-r\,(abc)\leq r\,(b)-r\,(ab).$$

Odatle neposredno izlazi Frobeniusova relacija (3).

8.4.4. Stavi li se u (3) posebno $a=\boxed{0}$, dobije se $r(bc)\leq r(b)$ što zajedno sa (5) daje sadržaj teorema (*i*).

8.4.5. Relacije $b=I$ i (3) daju

$$r(a)+r(c)\leq n+r(ac));$$

odatle se lako dolazi do relacije (2).

Time je čitav teorem 8.4. dokazan.

8.5. Evo jednog poopćenja gornjeg teorema 8.4; ako se služimo vektorskim jezikom, teorem je vrlo zoran: *pođemo li od nekog skupa S vektora* (mogu biti, npr. stupci matrice), *pa u prostoru što ga oni razapinju uzmemo neki skup M vektora, tada dimenzija prostora što ga razapinju vektori množine M ne može biti veća od dimenzije prostora što ga razapinju vektori iz S.* Matrično, to ćemo izreći ovako (zapravo izričemo manje!):

8.6. Teorem. *Ako su stupci matrice x linearne kombinacije stupaca* (*redaka*) *matrice a, tada je* $r(x)\leq r(a)$.

Dokažimo taj teorem. Treba pokazati ovo: neka je d bilo koja kvadratna podmatrica u x za koju je $k_1 d>r(a)$ ($k_1 d$ je broj redaka od d); treba pokazati da je $\det d=0$. Ako je slučajno $d\subset a$, stvar je jasna; stvar ide odmah i onda (isti razlog!) ako je matrica d kakva linearna kombinacija matricâ $y\subset a$ jer su takve podmatrice y nužno dužine $=k_1 d$. No, $\det d$ je svakako linearna kombinacija od determinanata spomenutih matrica y. Da se to vidi, dovoljno je matricu d napisati i izraziti joj stupce kao linearne spojeve stupaca iz a, i onda se poslužiti aditivnim svojstvom determinanata. Dakle je $\det d=0$. A to znači da je zaista $rx\leq ra$.

Istaknimo ovaj poseban slučaj gornjeg teorema, jer se često javlja.

8.7. Teorem o obrubljivanju. *Ako matrica A nastaje iz matrice a tako da se matrica a obrubi jednim ili više stupaca koji su linearne kombinacije stupaca matrice a, tada je* $r(a)=r(A)$.

Gledajući stvar vektorski, taj teorem je pogotovu očigledan!

—→ **8.8. Teorem o rangu produkta s regularnom matricom.** *Rang matrice ne mijenja se množeći je regularnom matricom.*

Naime, neka je

$$b=ax, \tag{1}$$

gdje je x *regularna* matrica. Uslov $\det x\neq 0$ ima za posljedicu da postoji obratna matrica x^{-1} od x (pogl. 12, § 5.2). Množeći jednadžbu (1) zdesna sa x^{-1}, izlazi $bx^{-1}=a$. To prema teoremu 8.4. znači: *b kao faktor* od *a* ima rang $\geq ra$, tj.

$$rb\geq ra. \tag{2}$$

No, iz istog razloga, po relaciji (1) zaključujemo prema 8.4. da je

$$rb\leq ra. \tag{3}$$

Iz (2) i (3) izlazi tražena jednakost $ra = rb$.

⟶ **8.9. Osnovni teorem o ekvivalentnim konačnim matricama.** *Neka su x, y matrice s konačnim brojem redaka i stupaca. Tada su naredne četiri izreke međusobno logički ravnopravne:*

(0) $\nu a = \nu b$ (isp. § 5.4 i § 10).

(1) $\mathrm{Dom}\, a = \mathrm{Dom}\, b$ te $ra = rb$

(2) *Jednadžba $xay = b$ zadovoljena je bar jednim parom regularnih matrica x, y.*

(3) *Matrice a i b su ekvivalentne u tom smislu da jedna nastaje iz druge konačnim nizom uzastopnih elementarnih operacija L, M, Tr.* (isp. §§ 4.1., 7.0).

Smisao teorema je taj da svaki od ta četiri suda ima kao svoju logičku posljedicu svaki od preostalih.

Teorem je istinit jer je istinit svaki od zaključaka u ovom lancu:

$$3 \Rightarrow 2 \Rightarrow 1 \Rightarrow 0 \Rightarrow 3.$$

Zakjučak $3 \Rightarrow 2$ (tj. rečenica „Ako stoji (3), onda stoji i (2)“) dokazana je u § 7.6.

(2) $\Rightarrow$ (1) (v. § 8.8).

(1) $\Rightarrow$ (0) (očigledno!).

(0) $\Rightarrow$ (3). To se dokazuje slično dokazu uslovljavanja (0) $\Rightarrow$ (1) iz § 5.4.

U vezi s teoremom 8.9. možemo primijetiti kako u njemu dolaze do izražaja razna svojstva o matricama; sad se jedna a sad druga više pojavljuju i koriste, no prema teoremu 8.9. znamo da se pojavljuju sva ta svojstva ukoliko je osigurana jedna od četiri skupine (0), (1), (2), (3).

8.10. U vezi s rangom ra svake konačne matrice a imamo ovu shemu-teorem:

$$\underset{\text{regularne matrice}}{\overset{x\,a\,y}{\searrow\ \swarrow}} = \underbrace{\left[\begin{array}{ccc} 1 & & 0 \\ & \ddots & \\ & 1 & \\ & & \\ 0 & & 0 \end{array}\right]}_{r(a)} \Bigg\} \begin{array}{l} k_1 a = \text{broj redaka u } a. \\ \\ k_2 a = \text{broj stupaca u } a. \end{array}$$

Specijalno, *za svaku regularnu matricu dužine n postoje dvije regularne matrice x, y za koje je*

$$xay = \mathrm{diag}\left(\underbrace{1, 1 \cdots 1}_{n}\right).$$

9. KAKO ODREDITI RANG MATRICE?

9.0. Rang matrice određuje se na osnovu njegovih svojstava iz prethodnog paragrafa. Specijalno, upiremo prstom na teoreme 8.1, 8.6. i 8.7. Tako npr. iz teorema 8.1. saznajemo da se rang matrice ne mijenja prilikom elementarnih transformacija matrice.

Tim se svojstvom obilno koristimo za traženje ranga, kao što smo se već uvjerili u raznim prilikama (stvarno, rang smo uz put dobili prilikom pojednostavnjivanja matrice).

9.1. Još jedan način za određivanje ranga matrice. — 9.1.0. Teorem. *Zadana je matrica a i prirodni broj n. Ova dva suda* (0) i (1) *izviru jedan iz drugoga*:

(0) $ra = n$.

(1) *Matrica a sadrži jednu regularnu kvadratnu podmatricu b dužine n, no sve druge eventualne kvadratne podmatrice* $\supset b$ *dužine* $n+1$ *jesu singularne* (*dovoljno je pretpostaviti da ove podmatrice nastaju obrubljivanjem matrice b*).

Zaključak (0) $\Rightarrow$ (1) izvire neposredno iz definicije ranga. Mnogo je zanimljiviji obratan zaključak (1) $\Rightarrow$ (0). Ispravnost tog zaključka dokazana je u pogl. 11, teorem 10.3. o determinantama. Ilustrirajmo stvar na primjeru.

9.1.1. Odredi rang *ra* tablice

$$a=\begin{bmatrix} 2 & 0 & 0 & 4 & 5 & 3 \\ 0 & 0 & 3 & 4 & 1 & 2 \\ \boxed{\begin{matrix} 2 & 0 \\ 4 & 3 \end{matrix}} & & 3 & 8 & 6 & 5 \\ & & 1 & 2 & 5 & 3 \end{bmatrix}.$$

Uokvirena matrica

$$b=\begin{bmatrix} 2 & 0 \\ 4 & 3 \end{bmatrix}$$

je regularna; dužina joj je $k_1 b = 2$; dakle je $ra \geq 2$. Obrubimo li b odozgo retkom $a_{2.}$, a zdesna stupcem $a_{.3}$, dobije se matrica

$$c=\begin{bmatrix} 0 & 0 & 3 \\ \boxed{\begin{matrix} & b & \end{matrix}} & & 3 \\ & & 1 \end{bmatrix},$$

kojoj je determinanta 3. $\det b \neq 0$; dakle je $ra \geq 3$. Sva kvadratna obrubljenja matrice c jesu singularna, kao što se lako može provjeriti; dakle je $ra = 3$.

10. PREGLED NORMIRANIH MATRICA

Normirane matrice nastaju iz 0-matricâ tako da se neki početni komad dijagonale (može biti i prazan!) nadomjesti jedinicama. Tako npr. sve normirane matrice poretka 3×4 glase:

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Ako radi kratkoće normiranu matricu poretka (k_1, k_2) sa r jedinica označimo sa

$$1\,(k_1, k_2, r),$$

onda gornje četiri matrice nose oznake

$$1\,(3, 4, 0), \quad 1\,(3, 4, 1), \quad 1\,(3, 4, 2), \quad 1\,(3, 4, 3);$$

sve one „izviru" iz nula-matrice $1\,(3, 4, 0)$.

Sve nula-matrice možemo nanizati, svrstati u niz, tako da svaka nula-matrica s manjim produktom $k_1 \cdot k_2$ dođe ispred svake nula-matrice s većim produktom $k_1 \cdot k_2$; nula-matrice s istim produktom $k_1 k_2$ možemo svrstati po veličini broja k_1 (broj redaka). Evo početka niza svih nula-matrica:

$$[0] = 1\,(1, 1, 0), \quad [0, 0] = 1\,(1, 2, 0), \quad \begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1\,(2, 1, 0), \quad [0, 0, 0], \quad \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix},$$

$$[0, 0, 0, 0] = 1\,(1, 4, 0), \quad \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 1\,(2, 2, 0), \quad \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = 1\,(4, 1, 0), \quad 1\,(1, 5, 0),$$

$$1\,(5, 1, 0), \quad 1\,(1, 6, 0), \quad 1\,(2, 3, 0), \quad 1\,(3, 2, 0), \quad 1\,(6, 1, 0), \ldots$$

Ako neposredno poslije svakog člana tog niza nula-matrica ispišemo po redu i sve druge odgovarajuće normirane matrice, dobije se ovaj beskonačni niz ν *svih normiranih konačnih matrica*:

$$\nu\colon \quad [0], \ [1]; \quad 1\,(1, 2, 0), \quad 1\,(1, 2, 1); \quad 1\,(1, 3, 0), \quad 1\,(1, 3, 1),$$

$$1\,(3, 1, 0), \quad 1\,(3, 1, 1); \quad 1\,(1, 4, 0), \quad 1\,(1, 4, 1), \quad 1\,(2, 2, 0), \quad 1\,(2, 2, 1),$$

$$1\,(2, 2, 2), \quad 1\,(4, 1, 0), \quad 1\,(4, 1, 1); \ldots$$

Svaka konačna matrica x ekvivalentna je s jednim jedinim članom νx gornjeg niza. To znači da se konačnim brojem elementarnih transformacija može svaka matrica x prevesti u (dobiti iz) posve određen(og) član(a) gornjeg niza ν.

Tako je npr. drugi član niza $\nu_2 = [1]$; pomnoži mu li se redak s λ, izlazi svaki „top" $[\lambda] = \lambda$, tj. svaki član tijela R koji je $\neq 0$.

10.1. Zadaci o rangu matrica.

1. Promatraj matricu $a = \begin{bmatrix} 3 & 2 & 1 \\ 1 & 1 & 2 \\ 1 & 3 & 2 \end{bmatrix}$; odredi matrice:

   1) $b = [a_{.1}, 2\,a_{.2}, a_{.3}]$, 2) $c = [b_{.1} - 3\,b_{.2} + b_{.3}, b_{.2} - b_{.3}, b_{.3}]$,

   3) $d = [c_{.1}, c_{.2}, c_{.3} + 3\,b_{.1} - 2\,b_{.2}]$; prikaži matrice b, c, d u obliku produkta u smislu § 7.3.

2. Dualno od zad. 1.

3. Za prethodnu matricu a odredi ove matrice i njihov rang:
   1) $b=[2a_{.1}, a_{.2}, 3a_{.3}]$, 2) $c=[-a_{.1}, a_{.1}+a_{.2}, a_{.2}+a_{.3}, a_{.3}+a_{.1}]$,
   3) $d=[2a_{.3}, -2a_{.1}+2a_{.3}, 4a_{.1}-5a_{.3}]$, 4) $e^T=[a_{.1}, 2a_{.1}, 3a_{.1}, 6a_{.1}]$,
   5) $j=[a, b, c]$, 6) $g=[c, d, f, a, a]$, 7) $h=[a, a, f, g]$,
   8) $k=ab$, 9) bca.

4. Odredi rang matrica:
   1) $a-b$, 2) $3a+2b$, 3) $2ac$, 4) ge, 5) a^2, 6) a^n.

5. Može li biti $rx=2$, $r(x^2)=0$?

6. Postoji li matrica x za koju je $rx=4$, $r(xx^T)=3$?

7. Nabroji sve normirane matrice oblasti (3, 3) i za svaku od njih po dvije matrice koje su s njom ekvivalentne.

8. Koliko ima normiranih matrica oblasti (m, n) i ranga r?
   (Npr. $m=6$, $n=4$, $r=2$).

9. Odredi rang ovih matrica:

$$1)\ \begin{bmatrix} 2 & 3 \\ x & 5 \end{bmatrix}, \qquad 2)\ \begin{bmatrix} 4-x & 2\sqrt{5} & 0 \\ 2\sqrt{5} & 4-x & \sqrt{5} \\ 0 & \sqrt{5} & 4-x \end{bmatrix},$$

$$3)\ a_{ik}=\begin{cases} 1 & \text{za } i=k \\ n-1 & i\neq k, \end{cases} \operatorname{Dom} a=(n, n).$$

10. Neka je $M=\begin{bmatrix} a & -d & g & j & m & -p & -s & -v \\ b & e & -h & k & -n & q & -t & -w \\ c & f & i & -l & -o & -r & u & -z \end{bmatrix}$

(ispiši najprije slova a onda predznak $\pm$); ako su $a, b, c, \ldots,$ pozitivni realni brojevi, dokaži da je $rM_{7'}=r(M\setminus M_{.7'})=3$ za $7'=1, 2, \ldots, 7$.

11. Neka je a kvadratna (n, n)-matrica ranga r; pretpostavimo da su glavni minori $d_k=a_{12\ldots k}^{12\ldots k}$ $(k=1, 2, \ldots, r)$ regularni; dokaži da postoji rastav $a=dg$, gdje je d donjotrokutna, g gornjotrokutna matrica; imamo

$$d_{kk}\,g_{kk}=\frac{d_k}{d_{k-1}}\ (k=1, 2, \ldots, r;\ d_0=1),$$

$$d_{ik}=d_{kk}\,a\binom{12\ldots k-1\ i}{12\ldots k-1\ k}\cdot d_k^{-1}$$

$$g_{ki}=g_{kk}\,d_k^{-1}\,a\binom{12\ldots k-1\ k}{12\ldots k-1\ i}\ (i=k+1, \ldots, n;\ k=1, \ldots, r).$$

Ako je $r>n$, možemo staviti: $d_{.j}=\vec{0}$, $g_{j.}=$proizvoljno za $j=r+1, \ldots, n$, odnosno $d_{j.}=\vec{0}$, $g_{.j}=$proizvoljno za $r<j\leq n$.

12. Neka je a regularna kvadratna matrica reda n; kljetočna matrica $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ ima rang $ra = n$ onda i samo onda ako je $d = ca^{-1}b$. Dokaži!

13. 1) Promatrajmo kljetkastu matricu $m = \begin{bmatrix} a & b \\ -c & 0 \end{bmatrix}$ uz uslov $\det a \neq 0$; ako ta matrica prelazi u matricu $m' = \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix}$ i to služeći se elementarnim operacijama nad prvih n redića ili dodavanjem linearne kombinacije prvih n redića preostalim redićima, tada je nužno $d' = ca^{-1}b$; 2) specijalno, ako su b, c jedinične matrice, tada je $d' = a^{-1}$; drugim riječima, opisanim transformacijama prelazi

$$\begin{bmatrix} a & I \\ I_n & 0 \end{bmatrix} \text{ u } \begin{bmatrix} a' & b' \\ 0 & a^{-1} \end{bmatrix};$$

na taj se način dolazi do a^{-1} kao donjeg desnog ugla u dobivenoj matrici; 3) ako je b stupac, $c = 1_n$, tad je d' rješenje matrične jednadžbe $ax = b$; 4) isto tako, za gornji prelaz

$$\begin{bmatrix} a & b \\ I_n & 0 \end{bmatrix} \to \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix} \text{ vrijedi } ad' = b.$$

11. O OPĆOJ MATRIČNOJ LINEARNOJ JEDNADŽBI

11.0. Neka su zadane proizvoljne matrice a, b; radi se o tome da se riješi jednadžba

$$ax = b. \tag{1}$$

Ta je jednadžba ekvivalentna sa sistemom od $k_2 b$ jednadžbi

$$ax_{.s} = b_{.s} \quad \text{za} \quad s = 1, 2, \ldots k_2 b, \ (= \text{broj stupaca matrice } b).$$

No, takve smo jednadžbe apsolvirali u prethodnom poglavlju. Time bi i sadašnji problem: diskusija jednadžbe (1) bio riješen. Ipak, izložimo ukratko i sažeto stvar direktno na jednadžbi (1).

11.1. Promatra se matrica a i njena nadmatrica $[a, b]$. Tada se počev od $[a, b]$ vrši niz operacija tipa L (i Tr) *s recima, ali birajući topove uvijek u stupcima od* a, nikad u b, sve dok a ne pređe u T-matricu a_T: time i b, odnosno $[a, b]$ dolaze u određenu matricu $b(a, a_T)$, odnosno $(a_T, b(a, a_T))$; *polazna jednadžba ekvivalentna je dobivenoj reduciranoj jednadžbi*

$$a_T x = b(a, a_T) \quad \text{(ne plaši se te oznake } b(a, a_T)!). \tag{2}$$

11.2. Nadalje je

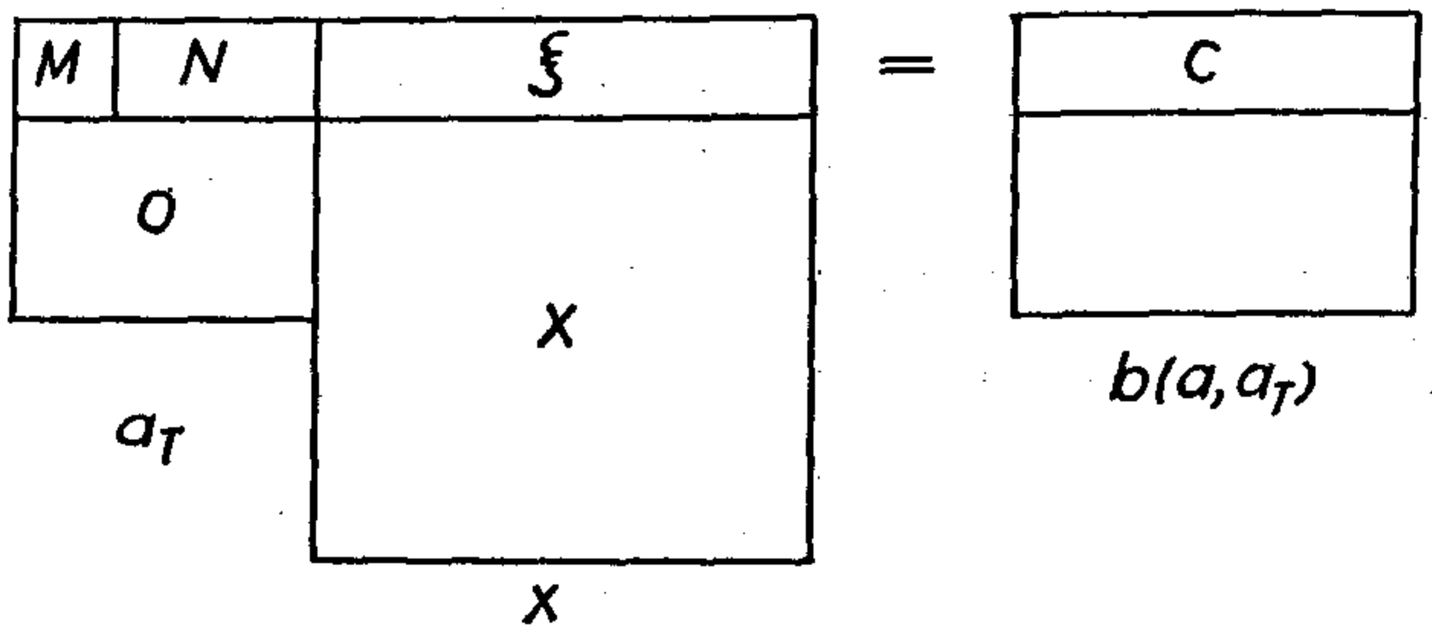
$$ra = ra_T; \quad r[a, b] = r[a_T, b(a, a_T)], \tag{3}$$

jer smo se služili elementarnim operacijama — a pri njima se rang ne mijenja.

No, problematika jednadžbe (2) je jednostavna:

11.3. *Ako je* $ra_T = r[a_T, b(a, a_T)]$, *tada jednadžba* (2) (dakle i (1)) *ima rješenje; nalazi se ovako*:

Radi jednostavnosti pretpostavimo da se svi odlikovani topovi nalaze u prvih r redaka i prvih r stupaca podmatrice a_T (znači da su svi ostali redići bez topova); tada se pripadna istaknuta regularna podmatrica M, u kojoj je smješteno svih tih r topova, nalazi u lijevom gornjem uglu matrice a_T. Sa sheme vidimo što su matrice N, ξ, X, c; tako je npr. c (odnosno ξ) matrica sastavljena od onih redaka zadane matrice $b(a, a_T)$ (tražene matrice x) koji odgovaraju recima matrice M (isp. § 3.2. u vezi s označivanjem $b(a, a_T)$).



Sl. 15.11.3.

Gornju shemu možemo pisati, simbolički, ovako:

$$\begin{bmatrix} M & N \\ 0 & \end{bmatrix} \begin{bmatrix} \xi \\ X \end{bmatrix} = \begin{bmatrix} c \\ 0 \end{bmatrix};$$

odatle izmnažanjem:

$$\begin{bmatrix} M\xi + NX \\ 0 \end{bmatrix} = \begin{bmatrix} c \\ 0 \end{bmatrix}.$$

Specijalno:

$$M\xi + NX = c;$$

$$M^{-1} \mid M\xi = c - NX$$

$$\xi = M^{-1}(c - NX). \tag{4}$$

11.4. *Relacijom* (4) *izraženo je traženo rješenje*

$$\begin{bmatrix} \xi \\ X \end{bmatrix} = x$$

reducirane jednadžbe (2); *pri tom je podmatrica* X *tražene matrice* x *proizvoljna*; nadalje je $k_1 X = da$, $k_2 X = k_2 b$ ($k_1 y$, $k_2 y$ označuju broj redaka, odnosno broj stupaca matrice y; $da = defekt\ a = k_2 a - ra$).

Prema tome, *u rješenju* x *matrične jednadžbe* (1) *dolazi proizvoljna podmatrica* X *dužine* $k_1 X = da$ *i širine* $k_2 X = k_2 b$.

11.5. Primjedba. Isti se postupak može provoditi odmah na polaznoj jednadžbi (1) ako je $ra = r[a, b]$ te ukoliko smo u a pronašli kakvu regularnu kvadratnu podmatricu M dužine ra.

11.6. Obrnuto, *ako jednadžba* $ax = b$ *postoji, tada je* $ra = r[a, b]$.

Naime, iz jednadžbe (1) izlazi $ax_{.s} = b_{.s}$ za svaki stupac $b_{.s}$ matrice b. To znači da je $a_{i.}\, x_{.s} = b_{is}$, tj. da je stupac $b_{.s}$ linearni spoj stupaca matrice a; drugim riječima, svaki stupac matrice $[a, b]$ jest linearni spoj stupaca matrice a; prema teoremu 8.6. izlazi odatle tražena jednakost $ra = r[a, b]$.

11.7. Zadaci o općoj matričnoj linearnoj jednadžbi

1. Zadane su matrice

$$a = \begin{bmatrix} 2 & 3 & 7 \\ 4 & 2 & 10 \\ 3 & 1 & 7 \end{bmatrix}, \qquad b = \begin{bmatrix} 1 & 2 \\ 3 & -2 \\ 1 & 5 \end{bmatrix};$$ riješi jednadžbu:

1) $ax = b$; 2) $ax = [b, b_{.2}]$; 3) $ax = [b_{.2}, b_{.1}, b_{.2}, b_{.1}]$;

4) $ax = [2\,b_{.1}, 3\,b_{.2}, 5\,b_{.1}, 6\,b_{.1}]$; 5) $ax = [\vec{0}, b_{.1}, b_{.2}, \vec{0}]$;

6) $ax = [a, b]$; 7) $ax = xa$.

2. Neka je e zadana matrica; ako iz $k_2 e = k_1 x$ slijedi $ex = xe$, onda je matrica e nužno jedinična. Dokaz!

3. Za kvadratne matrice a, 0 reda n riješi $ax = 0$; promatraj specijalno slučajeve $n = 1, 2, 3$.

4. Provjeri: matričnoj jednadžbi $ax = b$ pridruži proces

$$\begin{bmatrix} a & b \\ -1_n & 0 \end{bmatrix} \to \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix};$$

kod tog procesa vršimo na lijevoj strani elementarne operacije u prvih n redića, gdje je $\mathrm{Dom}\, a = (n, n)$; k preostalim redićima dopušteno je jedino dodavati linearne kombinacije prvih n redića; dokaži da je d' traženo rješenje.

5. Provjeriti:

$$\begin{bmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{bmatrix}^{-1} = \begin{bmatrix} \dfrac{bc}{(a-b)(a-c)} & \dfrac{ca}{(b-c)(b-a)} & \dfrac{ab}{(c-a)(c-b)} \\ \dfrac{-(b+c)}{(a-b)(a-c)} & \dfrac{-(c+a)}{(b-c)(b-a)} & \dfrac{-(a+b)}{(c-a)(c-b)} \\ (a-b)^{-1}(a-c)^{-1} & (b-c)^{-1}(b-a)^{-1} & (c-a)^{-1}(c-b)^{-1} \end{bmatrix}.$$

6. Dokazati 1) $\begin{bmatrix} I_n(k) & b \\ 0 & I_n \end{bmatrix}^{-1} = \begin{bmatrix} I_n & -b \\ 0 & I_n \end{bmatrix}$,

pri tom je b matrica kojoj je oblast (k, n);

2) $\begin{bmatrix} a & f & e \\ & b & d \\ & & c \end{bmatrix}^{-1} = \begin{bmatrix} a^{-1} & -a^{-1}fb^{-1} & x \\ & b^{-1} & -b^{-1}dc^{-1} \\ & & c^{-1} \end{bmatrix}$

gdje je $x = a^{-1}fb^{-1}dc^{-1} - a^{-1}ec^{-1}$; a, b, c, d, e, f su matrice; a, b, c su kvadratne i regularne matrice. Nađi $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}^{-1}$.

7. Gornjotrokutne pomoćne jedinične matrice oblasti (n, n) glase

$H = H(n)$, H^2, H^3, ..., H^{n-1}, pri čemu je $H_{ik} = \begin{matrix} 1 \\ 0 \end{matrix}$ za $\begin{matrix} i = k-1 \\ i \neq k-1 \end{matrix}$.

Nađi niz H^2, H^3, ... i dokaži da je

$H^r = 0$ za $r \geq n$ te $H^r_{ik} = \begin{matrix} 1 \\ 0 \end{matrix}$ za $\begin{matrix} i = k-r \\ i \neq k-r \end{matrix}$ za $r = 1, 2, \ldots, n-1$.

Donjotrokutne pomoćne jedinične matrice jesu $F = F(n)$, F^2, ..., F^{n-1}, pri čemu je $F_{ik} = \begin{matrix} 1 \\ 0 \end{matrix}$ za $\begin{matrix} i = k+1 \\ i \neq k+1 \end{matrix}$. Odredi niz F, F^2, F^3, ...

1) Provjerite $aH = [\vec{0}, a \setminus a_{.k_2 a}]$, pri čemu $[a \setminus a_{.k_2 a}]$ označuje matricu koja iz matrice a nastaje kad iz a uklonimo posljednji stupac;

$$aF = [a \setminus a_{.1}, \vec{0}];$$

2) Za svaki red $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots$ vrijedi

$$c(H) = c_0 I + c_1 H + c_2 H^2 + \cdots = \begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ & a_0 & \cdot & \\ & & \cdot & \cdot \\ & & & \cdot \ a_1 \\ 0 & & & a_0 \end{bmatrix}$$

(matricu čitaj po kosim crtama! Svaka je konstantna!)

$$c(F(n)) = c_0 F + c_1 F + c_2 F^2 + \cdots = \begin{bmatrix} a_0 & & & 0 \\ a_1 & a_0 & & \\ \cdot & a_1 & & \\ \cdot & & & \\ \cdot & & & \\ a_{n-1} & \cdots & a_1 & a_0 \end{bmatrix}$$

3) Dokaži da su matrice $H^T H$, $H H^T$ idempotentne tj. zadovoljavaju

$$x^2 = x \text{ i da je } H^i (H^T)^i + (H^T)^k H^k = I_n$$

za prirodne brojeve $i + k = n$.

4) Nađi $x+H$ i dokaži da je

$$(x+H)^r = \begin{bmatrix} x^r & \binom{r}{1}x^{r-1} & \dots & \binom{r}{n-1}x^{r-n+1} \\ & x^r & \binom{r}{1}x^{r-1} & \dots & \binom{r}{n-2}x^{r-n+2} \\ & & \dots\dots\dots\dots\dots & & \\ & & & x^r & \binom{r}{1}x^{r-1} \\ & & & & x^r \end{bmatrix}.$$

Dijagonala je konstanta x^r.

8. *Nilpotentne matrice.* To su matrice kojima je neka potencija jednaka nula-matrici; drugim riječima, to su prirodni korijeni nula-matricâ. Najmanji prirodni broj n za koji je $a^n = 0$ zove se indeks (nilpotentnosti) veličine a.

   1) Odrediti indeks nilpotentnosti matrica $H(n)$, $F(n)$ iz zadatka 7;

   2) Odredi neku (svaku) nilpotentnu matricu poretka (2, 2), (3, 3).

9. *Trag matrice* (*tr-funkcija*). Trag matrice a je veličina $tra = \sum a_{ii}$, tj. suma komponenata na dijagonali matrice. Dokazati: 1) Ako je matrica a dijagonalna i dijadska, tada je $tr\,a = r(a)$; 2) $tr(ab) = tr(ba) = \sum a_{ik} b_{ki}$; specijalno veličina $tr(a\,a^*) = tr(a^*\,a) = \sum_{i,k} a_{ik}\,\bar{a}_{ik} =$ zove se kvadrat norme $No\,a$ matrice a; stavlja se $No\,a$ ili $\|a\| = +(tr\,a\,a^*)^{1/2}$; 3) Za skalarnu matricu $a = \mathrm{diag}[c, c, \dots]$ vrijedi $tr\,a = n \cdot c$, $No(a) = n^{1/2}|c|$; 4) $No(ab) \leq No(a)\,No(b)$.

10. Neka je *Qu* skup matrica oblika $\zeta = \begin{bmatrix} z & -Z^* \\ Z & z^* \end{bmatrix}$, pri čemu su z, Z bilo koji kompleksni brojevi; 1) da li je matrica ζ normalna?

    2) Je li umnožak svake dvojke članova iz *Qu* opet član u *Qu*? Što je nužno i dovoljno pa da determinanta toga produkta bude 0?

    3) Je li ikoji član u *Qu* nilpotentan?

    4) Nađi ζ^*, ζ^{-1}.

Literatura: Isto kao u poglavljima: 10, 12 i 13.

POGLAVLJE 16.

KVADRATNE FORME, HERMITSKE I BILINEARNE FORME

U ovom poglavlju upoznat ćemo se s jednom vrstom jednostavnih, ali važnih funkcija: *homogeni polinomi stupnja* 2 zadanih veličina $x_1, x_2, \ldots$; shvatimo li ove veličine kao komponente vektora $\vec{x}$ pisan kao stupac, tada je *kvadratna forma skalarni produkt* $\vec{x} \circ a\vec{x}$ *vektora* $\vec{x}$ *i pridružena vektora* $a\vec{x}$, pri čemu je a proizvoljna matrica. Vidjet ćemo kako je *matrica važno i pogodno sredstvo* za pregledno izučavanje kvadratnih formi. Takvi polinomi dolaze u teoriji i primjenama (krivulje i površine 2. stupnja, izraz za kvadrat daljine, za energiju, itd.).

Podsjet. Ako je a kvadratna matrica, a x i y matrice kojima je jedna „dimenzija" $= 1$ (reci ili stupci), tada matrični produkt $x \cdot a \cdot y$ postoji jedino onda ako je x redak, a y stupac; specijalno, $x\,a\,x$ ne postoji (osim ako je a skalar). Zato je ili $x^T a\,x$ ili $x\,a\,x^T$ na snazi (u prvom slučaju je x zapisan kao stupac pa je x^T redak).

1. PRIMJERI I DEFINICIJA KVADRATNIH FORMI

1.1. Neka je x, y, z proizvoljan niz od tri realna broja. Tada je $2x^2 + 3xy + 4z^2$ određen realan broj; zavisnost ovog izraza od (x, y, z) je očigledna; izraz $2x^2 + 3xy + 4z^2$ je određen polinom s obzirom na x, y, z, i to *polinom stupnja* 2; čak je to i *homogen* polinom stupnja 2 jer je *svaki* član stupnja 2.

1.2. Kvadratne forme veličina x, y jesu npr. x^2, xy, $3x^2$, $-2y^2$, $x^2 + y^2$, $3x^2 + 5xy + 6y^2$. Ova posljednja ima tri člana. Više ih ne može ni biti u *reduciranom* obliku. Naime, monomi u odnosu na x, y su oblika x^2 ili xy ili y^2 pomnoženo koeficijentima. Monomi ax^2, $2bxy$, cy^2 (a, b, c ne zavise ni od x ni od y) jesu *sastavni* ***aditivni*** *dijelovi* kvadratne forme $ax^2 + 2bxy + cy^2$.

Zgodno je ovaj izraz pisati i ovako:

$$x\,a\,x + x\,b\,y + x\,b\,y + y\,c\,y;$$

tu se bolje vidi *nizanje pojedinih dijelova.*

Ako se služimo indeksima, pa ako *varijable*, odnosno *neodređenice* označimo sa x_1, x_2, tada bi kvadratna forma bila

$$x_1 a_{11} x_1 + x_1 a_{12} x_2$$
$$+ x_2 a_{21} x_1 + x_2 a_{22} x_2 .$$

Tu je pravilnost građenja očigledna i odmah se prenosi na slučaj da imamo 3, 4, ... veličina x_1, x_2, ... Tako npr. za 5 veličina z_1, z_2, z_3, z_4, z_5 kvadratna forma — nezavisna je z — s koeficijentima imena b glasila bi ovako:

$$\begin{aligned} & z_1 b_{11} z_1 + z_1 b_{12} z_2 + z_1 b_{13} z_3 + z_1 b_{14} z_4 + z_1 b_{15} z_5 + \\ + & z_2 b_{21} z_1 + z_2 b_{22} z_2 + z_2 b_{23} z_3 + z_2 b_{24} z_4 + z_2 b_{25} z_5 + \\ + & \cdots\cdots\cdots\cdots\cdots + \\ + & \cdots\cdots\cdots\cdots\cdots + \\ + & z_5 b_{51} z_1 + \cdots\cdots\cdots + z_5 b_{55} z_5 \end{aligned}$$

ili simbolički $\sum_{i,k=1}^{5} z_i b_{ik} z_k$, tj., na sve moguće načine sparuje se z_i, z_k i formira produkt $z_i b_{ik} z_k$ i onda sve *zbroji*.

⟶ **1.3.** Opća definicija. Kvadratna forma zadanih n nezavisnih varijabli ili veličina x_1, x_2, ..., x_n je suma monoma oblika $a_{ik} x_i x_k$, pri čemu i, k prolaze nezavisno skupom $[1\, n\}$ od n indeksa 1, 2, ..., n; pri tom koeficijenti a_{ik} *ne zavise od x-ova* (inače, naravno, *a-ovi mogu zavisiti od raznih drugih veličina*!) Kvadratnu formu možemo kraće pisati u obliku $\sum_{i,k=1}^{n} a_{ik} x_i x_k$ ili naprosto $\Sigma a_{ik} x_i x_k$, znajući pri tom da za i, k treba stavljati sve vrijednosti iz množine zadanih indeksa pa onda sumirati.

1.3.1. Tako npr. kvadrat svake linearne forme je kvadratna forma a.

Suma od konačno mnogo kvadrata linearnih formi istih veličina je kvadratna forma. Zanimljivo je da vrijedi obrat: *svaka kvadratna forma može se prikazati kao algebarska suma kvadratâ linearnih formi* (isp. § 2).

1.4. Zadana kvadratna matrica kao zapis koeficijenata kvadratne forme. Pođimo od zadane kvadratne matrice (tablice), npr.

$$\begin{matrix} 2, & -3, & 4 \\ -7, & 1, & 5 \\ 3, & 2, & 7. \end{matrix}$$

Odatle možemo formirati kvadratnu formu triju veličina x_1, x_2, x_3 po ovoj shemi:

$\dot{+}$	x_1	x_2	x_3
x_1	2	−3	4
x_2	−7	1	5
x_3	3	2	7

$$
\begin{aligned}
&= x_1(\ \ 2x_1 - 3x_2 + 4x_3) + \\
&+ x_2(-7x_1 + \ \ x_2 + 5x_3) + \\
&+ x_3(\ \ 3x_1 + 2x_2 + 7x_3).
\end{aligned} \tag{1}
$$

Tu smo množili x_i sa a_{ik} i rezultat sa x_k; naravno, mogli smo i ovako $a_{ik}\,x_i\,x_k$ (opiši riječima!) ili $x_i\,a_{ik}\,x_k$ ili $x_i\,x_k\,a_{ik}$. Tako se nalaze *članovi (termi) forme* i onda se oni svi zbroje. Konačni rezultat u gornjem primjeru je izraz

$$2x_1x_1 - 10x_1x_2 + 7x_1x_3 + x_2x_2 + 7x_2x_3 + 7x_3x_3$$

(veličine x nismo izmnožili da se vidi kako smo terme uređivali po veličini dvocifrenih brojeva 11, 12, 13, 22, 23, 33 predstavljenih indeksima u brojevnoj bazi 4).

Istu kvadratnu formu možemo *simetrično* napisati ovako:

	x_1	x_2	x_3
x_1	2	−5	7/2
x_2	−5	1	7/2
x_3	7/2	7/2	7.

Tu *simetričnu* matricu zvat ćemo *matricom kvadratne forme.*

Ako gledamo na matrice

$$x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix},\ x^T = [x_1, x_2, x_3],$$

i gornju matricu

$$a = \begin{bmatrix} 2 & -3 & 4 \\ -7 & 1 & 5 \\ 3 & 2 & 7 \end{bmatrix},$$

onda stvarno vidimo da smo do rezultata mogli doći i ovako:

p r v i k o r a k: naći

$$a\vec{x} = \begin{bmatrix} 2 & -3 & 4 \\ -7 & 1 & 5 \\ 3 & 2 & 7 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 2x_1 - 3x_2 + 4x_3 \\ -7x_1 + 1x_2 + 5x_3 \\ 3x_1 + 2x_2 + 7x_3 \end{bmatrix};$$

d r u g i k o r a k: naći $\vec{x}^T \cdot (a\vec{x})$:

$$[x_1,\ x_2,\ x_3] \cdot \begin{bmatrix} 2x_1 - 3x_2 + 4x_3 \\ -7x_1 + \ \ x_2 + 5x_3 \\ 3x_1 + 2x_2 + 7x_3 \end{bmatrix} = [x_1(\ \ ) + x_2(\ \ ) + x_3(\ \ )]$$

$$= x_1(2x_1 - 3x_2 + 4x_3) + x_2(-7x_1 + x_2 + 5x_3) + x_3(3x_1 + 2x_2 + 7x_3)$$

$$= \ldots$$

Zaključak je opći pa ga zapisujemo kao:

1.5. Teorem. *Ako je a kvadratna matrica reda n, tada je za svaki niz x od n veličina* $x_1, x_2, \ldots, x_n$, ***koje zamišljamo ispisane kao stupac***

$$x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix},$$

matrični produkt

$$x^T a\, x \tag{2}$$

određena kvadratna forma (kvadratni oblik) veličina $x_1, x_2, \ldots, x_n$, *ukoliko matrica a ne zavisi od tih veličina* $x_1, x_2, \ldots, x_n$.

Drugim riječima, *kvadratna forma* $x^T a\, x$ *je* ***skalarni produkt*** vektora $a\vec{x}$ i vektora $\vec{x}$. **Dakle je** $a\,x \circ x = x^T a\, x = \sum_{i,j=1}^{n} a_{ij}\, x_i\, x_j$.

Ako je niz x ispisan kao ***redak*** $x = [x_1, x_2, \ldots, x_n]$, tada umjesto produkta (2) imamo produkt $x\, a\, x^T$.

Zato treba uvijek naznačiti kako je matrično zapisan niz zadanih veličina $x_1, x_2, \ldots, x_n$.

Primjedba. Znajmo da $\vec{x}a$ ima smisla jedino onda ako je $\vec{x}$ ispisano *kao redak*. Zato ako je $\vec{x}$ *stupac*, treba preći na redak $\vec{x^T}$ i s njim početi tvoreći *matrični produkt* $x^T a\, x$. *Treba svaki put tu činjenicu imati na umu.*

Mi ćemo, već prema prilikama, x zapisivati kao redak ili kao stupac.

Obrnuto, ako je zadan sređen izraz kvadratne forme veličina $x_1, x_2, \ldots,$ može se taj izraz prikazati u obliku (2) uzimajući polovinu koeficijenata od $x_i\, x_k$ za a_{ik}. Npr.

$$x^2 - xy + y^2 = [x, y] \cdot \begin{bmatrix} 1 & -1/2 \\ -1/2 & 1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix}.$$

1.6. Simetrična matrica koja se na taj način dobije zove se *simetrična matrica* ili *naprosto matrica zadane kvadratne forme*. Determinanta forme je, po definiciji, *determinanta pripadne simetrične matrice forme.*

1.7. Odnos između linearnih i kvadratnih formi. Pogledajmo izraz (1). On je stvarno suma produkata. On je skalarni produkt. On je skalarni produkt zadanog niza veličina x_1, x_2, x_3 i *tri linearne forme tih veličina.*

Smisao matričnog prikazivanja $x^T a\, x$ *također je takav da pokaže da je kvadratna forma veličinâ* $x_1, x_2, \ldots$ *upravo skalarni produkt niza tih n veličina i još niza od n linearnih formi istih veličina.*

Tu je vezu korisno imati na umu!

1.7.1. Produkt dviju linearnih formi kao kvadratna forma. Produkt *dviju linearnih* formi *istih veličina* sasvim je određena *kvadratna* forma. Međutim, tako se ne može dobiti *najopćenitija* kvadratna forma! Tako npr.

$$(2x+3y)(5x-9y)=10x^2-3xy+27y^2.$$

Je li svaka kvadratna forma od *dvije* veličine x_1, x_2 produkt od dvije linearne forme? *Jest*! I to je jednostavna vježba za dokaz! Naime, npr.

$$cx^2+dxy+ey^2=y^2(cz^2+dz+e),\ \text{gdje je}\ z=\frac{x}{y}.$$

No, trinom u z je rastavljiv u linearne faktore $c(z-z_0)(z-z_1)$, dakle je zadana forma

$$f=cy^2\left(\frac{x}{y}-z_0\right)(z-z_1)=c(x-z_0y)(x-z_1y).$$

A slučaj da imamo kvadratnu formu od tri veličine x_0, x_1, x_2? Recimo $x_0x_1+x_1x_2+x_2x_0$? Je li to produkt od dvije linearne forme? Isto pitanje za

$$x_0^2+x_1^2+x_2^2+x_0x_1+x_0x_2+x_1x_2.$$

1.8. Formalna i funkcionalna jednakost (nejednakost) formi.

D e f i n i c i j a. Dvije kvadratne forme *istih* varijabli (veličina) *jednake su* ako su im *pripadne simetrične matrice jednake*; inače su forme različite.

Funkcionalna jednakost formi znači da obje forme imaju *iste vrijednosti u istim tačkama* i da su definisane u *istim oblastima*. Kao što smo već isticali u nekoliko navrata, te dvije definicije nisu ekvivalentne u općem slučaju (jesu, ako veličine x_1, x_2, ... prolaze recimo Q, R, $R(i)$ i sl.; no x_1, x_2, ... mogu biti i fiksne veličine, npr. $\sqrt{2}$, π, -5 i promatrati njihove kvadratne forme, recimo s cijelim koeficijentima). To je važna stvar; zato i spominjemo da x_1, x_2, ... mogu biti ne samo *varijable (promjenljivice)* nego i *indeterminate (neodređenice)*, obuhvatajući time i slučaj da su to stvarno *determinate* (određene veličine), no radeći s njima kao da su *indeterminate*, da procedura oko izjednačivanja bude jednostavnija.

Ako negdje govorimo o *varijablama*, čitalac će prosuditi da li stvar vrijedi i za *neodređenice;* i *obratno*. Važno je da imamo na umu oba slučaja.

1.9. Kososimetrična matrica i pripadna forma. Neka je zadana *kososimetrična matrica* (svojstvo $a^T=-a$), npr.

$$\begin{bmatrix}0 & -5\\ 5 & 0\end{bmatrix};$$

pripadna kvadratna forma za x_0, x_1 je

$$0x_0x_0+x_0\cdot -5x_1+x_1\,5x_0+0x_1x_1=0.$$

Prema tome, *kososimetrična matrica rađa nula-formu:* svi koeficijenti u sređenom obliku forme jesu 0. To izlazi i prema gornjem, jer je

$$\frac{a_{ik}+a_{ki}}{2}=0.$$

1.10. Opća matrica. Za svaku matricu a imamo njeno simetrično jezgro $\frac{a+a^T}{2}=a_s$ i njeno kososimetrično jezgro $a_k=\frac{a-a^T}{2}$; suma im je $=a$. To se u formiranju pripadnih kvadratnih formi odrazuje ovako:

$$\vec{x}^T a \vec{x}=\vec{x}^T\left(\frac{a+a^T}{2}+\frac{a-a^T}{2}\right)\vec{x}=$$

$$=\text{(zakon distribucije matričnog množenja)}=$$

$$=\vec{x}^T\frac{a+a^T}{2}\vec{x}+\vec{x}^T\frac{a-a^T}{2}\vec{x}=\vec{x}^T\frac{a+a^T}{2}\vec{x}+0 \qquad \text{(po 1.8)}.$$

Dakle vidimo i formalno da se *u generiranju kvadratnih formi iz matricâ možemo ograničiti na simetrične matrice.*

1.11. Uloga matrica kod kvadratnih formi. *Uloga matrice ovdje je bitna, jer matrica potpuno određuje formu. Zato se terminologija matrica prenosi na kvadratne forme.* Npr. *forma je regularna, jedinična, dijagonalna, itd.*, već prema tome da li je takva matrica forme. Govori se o *inverznoj, adjungiranoj, o simboličkom kvadratu zadane forme* $\vec{x}\,a\,\vec{x}^T$, misleći pri tom na forme

$$\vec{x}^T a^{-1}\vec{x}, \quad \vec{x}^T a^{\Gamma}\vec{x}, \quad \vec{x}^T a^2\vec{x} \quad \text{itd.}$$

Govori se o *sličnim*, odnosno *ekvivalentnim* kvadratnim formama, već prema tome da li su matrice tih formi međusobno slične, odnosno ekvivalentne. Drugim riječima, kvadratna forma $x^T b\,x$ *slična* je (ekvivalentna) s kvadratnom formom $x^T a\,x$ ako postoji regularna matrica f, za koju je $b=f^{-1}af$ (odnosno ako postoje regularne matrice f, g, za koje je $b=fag$).

1.12. Adjungirana forma kao determinanta. Zanimljivo je npr. da se *adjungirana forma* $\sum a^{\Gamma}_{ik}x_i x_k$ zadane forme $\sum a_{ik}x_i x_k$ može napisati u obliku determinante, i to ovako:

$$(1)\qquad \sum (a^{\Gamma})_{ik}x_i x_k=-\begin{vmatrix} 0 & x_1 & x_2 & \dots \\ x_1 & & & \\ x_2 & & & \\ \vdots & a_{ij} & & \end{vmatrix}\begin{matrix}\\ \\ \\ \longleftarrow i\\ \\ \uparrow\\ j\end{matrix}.$$

(gl. poglavlje 16, § 6.10 i § 6.12).

Naime razvijajući napisanu determinantu po prvom retku i prvom stupcu dobijemo upravo (1) (v. 11 § 8.8).

1.13. Zadaci. 1. Odredi matricu ovih kvadratnih formi:

1) $3x^2+6xy-y^2$; 2) x^2-y^2; 3) ax^2+y^2-bxy; 4) $(3x-2y)^2$;

5) $(3x-5y)(4x-3y)$; 6) $(mx+ny)(px+qy)$; 7) $(5x-2y)x+$

$+(3x+y)(x-5y)$; 8) $2x^2-3y^2+7xy-z^2$; 9) $x_3^2+x_0x_1+x_2x_3$.

2. Koja je od ovih funkcija kvadratna forma i kolika je determinanta te kvadratne forme:

1) $2x^2+y^2$; 2($(x+1)(x-y)$; 3) $(10x-5y)(4x-3y)+5xy-$

$-(2x-y)(x+5y)$; 4) u^2+v^2+2xy; 5) $(u+v)^2-(u-v)^2$;

6) $x^2+3y^2-(x-y)(x+y)-4y^2$; 7) $u_4^2-5u_2u_1+u_1^2$;

8) $(x_0+2x_1+3x_2)(3x_0-x_1+5x_2)$?

3. Napiši sve prethodne kvadratne forme u obliku *skalarnog produkta*.

4. Nađi adjungirane forme prethodnih kvadratnih formi.

5. Nađi inverzne forme formi iz zadatka 1.

6. Nađi simbolički kvadrat formi iz zad. 2.

7. Odredi nekoliko matrica a za koje je $[x, y]\, a\begin{bmatrix} x \\ y \end{bmatrix}$ jednako $3x^2-$

$-6xy+y^2$; odredi vrijednost pripadnih determinanata.

Postoji li za svaki broj b i takva matrica a da bude

$$\det a=b \text{ (npr. } b=1,\ 3,\ 0,\ -1,\ \ldots)?$$

8. Odredi nekoliko kvadratnih formi veličina $2^{1/2}$, $3^{1/2}$ s koeficijentima u skupu: a) cijelih; b) racionalnih; c) kompleksnih brojeva.

9. Nađi nekoliko parova linearnih formi veličina:

1) x, y; 2) x, y, z; 3) 1, 1/2, 1/3; 4) x, 5, $2^{1/2}$; nađi produkt tih formi i napiši matricu. Odredi rang te matrice.

10. Dva osnovna slučaja kvadratnih formi: 1) kvadrat dužine vektora odnosno skalarni kvadrat vektora je kvadratna forma komponenata toga vektora; 2) kinetička energija T mehaničkog sistema od n stepena slobode u polju s potencijalom u kojem funkcija sile ne zavisi od vremena jest kvadratna forma od tzv. Lagrangeovih koordinata $q_1, q_2, \ldots, q_n$.

11. Ako je $Q=Q(x_1, \ldots, x_n)$ kvadratna forma veličinâ $x_1, x_2, \ldots, x_n$, onda je

$$\sum_{\nu=1}^{n} \frac{\partial Q}{\partial x_\nu}=2Q \text{ (Euler).}$$

2. OSNOVNI PROBLEM KVADRATNIH FORMI: UKLANJANJE MJEŠOVITIH ČLANOVA I SVOĐENJE NA DIJAGONALNI OBLIK

2.0. U matematici i primjenama kvadratne su forme, uz linearne, najbrojnije. Primjene su zaista velike. Mnogo toga nalazi svoj izražaj u kvadratnim formama i njihovim spojevima s linearnim i drugim *formama*. Izučavanje naravi fenomena zapisanog u kvadratnoj formi pristupačnije je ako u formi *nema mješovitih* članova odnosno ako se kvadratna forma prikaže kao suma kvadrata linearnih formi. Npr. odmah znamo za karakter formi $3x^2+8y^2$, $3x^2-8y^2$, ali je teže nešto reći, naprečac, o formi $2x^2-5xy+y^2$. Nakon kraće transformacije moći ćemo i u posljednjem slučaju stvar riješiti; npr.

$$x^2-5xy+2y^2=(x^2-5xy)+2y^2=\left(x-\frac{5}{2}y\right)^2-\frac{25}{4}y^2+2y^2=$$

$$=\left(x-\frac{5}{2}y\right)^2-\frac{17}{4}y^2.$$

Tu je već karakter poznatiji jer je to

$$=x'^2-\frac{17}{4}y^2, \quad \text{stavljajući} \quad x'=x-\frac{5}{2}y.$$

2.1. Problem je opći: Zadanu kvadratnu formu nastoj prikazati kao algebarsku sumu kvadrata linearnih formi odnosno: *uvođenjem novih veličina umjesto starih pomoću* ***linearnih formi*** *prevedi zadanu kvadratnu formu na dijagonalan oblik* (tj. takav oblik da pripadna matrica bude dijagonalna — znači: mješoviti članovi u formi otpadaju).

To je tzv. *problem dijagonalizacije* ili *osni problem kvadratnih matrica*[1].

Tako je npr. forma $2x^2-y^2$ dijagonalna; forma $2x^2+y^2+3xy$ nije dijagonalna. No, ova se forma lako prevede u dijagonalnu formu, jer je očigledno

$$2x^2+y^2+3xy=2\left(x+\frac{3}{4}y\right)^2-\frac{1}{8}y^2.$$

Stavi li se $x+\frac{3}{4}y=x'$, dobiva se *dijagonalna kvadratna forma*

$$2x'^2-0{,}125y^2 \quad \text{u veličinama} \quad x',\ y.$$

Isto tako forma $5xy$ nije dijagonalna; no supstitucijom

$$x=x'+y',\ y=x'-y'$$

prelazi ona u $5x'^2-5y'^2$, a to je dijagonalni oblik.

Slično se, prema Lagrangeu [Lagránž], *svaka kvadratna forma svodi na dijagonalni oblik*.

---

[1] Naime, iz dijagonalnog oblika vidi se, u geometriji, narav geometrijskog predmeta što je povezan s promatranom formom, a pogotovu njegove osi.

2.2. Lagrangeov postupak svođenja dijagonalizacije kvadratnih formi[1]. Neka je, naime, $Q(x_1, x_2, \ldots, x_n)=\sum_{i,j}^{n} a_{ij}\, x_i\, x_j$ zadana kvadratna forma; naravno, $a_{ik}=a_{ki}$. Razlikujemo *dva slučaja* koji se međusobno isključuju.

2.2.1. P r v i s l u č a j. Bar jedna vrijednost matrice a na dijagonali je $\neq 0$, npr. $a_{11}\neq 0$. Tada je

$$Q=a_{11}\, x_1^2+2\sum_{j=2}^{n} a_{1j}\, x_1\, x_j+\sum_{i,j=2}^{n} a_{ij}\, x_i\, x_j=$$

$$=a_{11}\left(x_1^2+\sum_{j=2}^{n}\frac{2a_{1j}}{a_{11}}\, x_1\, x_j\right)+\sum_{i,j=2}^{n} a_{ij}\, x_i\, x_j=$$

$$=a_{11}\left(x_1+\sum_{j=2}^{n}\frac{a_{1j}}{a_{11}}\, x_j\right)^2-a_{11}\left(\sum_{j=2}^{n}\frac{a_{1j}}{a_{11}}\, x_j\right)^2+\sum_{i,j=2}^{n} a_{ij}\, x_i\, x_j.$$

A ovo je već forma (oblik) u kojoj varijabla x_1 dolazi samo u prvoj zagradi; druga dva dijela gornjeg izraza čine kvadratnu formu Q_1, ali bez varijable x_1. Stavimo li

$$x_1+\sum_{j=2}^{n}\frac{a_{1j}}{a_{11}}\, x_j=x_1',\ x_2=x_2',\ \ldots,\ x_n=x_n', \tag{1}$$

tada je *polazna* kvadratna forma pojednostavnjena i *postala*

$$a_{11}\, x_1'^2+Q_1(x_2',\ x_3',\ \ldots,\ x_n').$$

2.2.2. D r u g i s l u č a j. $a_{ii}=0$ za $i=1, 2, \ldots, n$. Izaberi jednu nedijagonalnu vrijednost $a_{ij}\neq 0$, $i\neq j$ (naravno da ona postoji — inače bi matrica a bila nula-matrica, stvar bez interesa!).

Tada ćemo umjesto *x-ova* uvesti veličine x' obrascima

$$\begin{aligned} x_i&=2^{-1/2}\, x_i'-2^{-1/2}\, x_j' \\ x_j&=2^{-1/2}\, x_i'+2^{-1/2}\, x_j' \end{aligned} \tag{2}$$

te $x_\nu=x_\nu'$ za ostale indekse ν. Koeficijenti u (2) su uzeti tako da rezultat bude što jednostavniji (isporedi formulu (4)).

Polazna forma sadrži član $2\, a_{ij}\, x_i\, x_j$, koji sada postaje $a_{ij}\, x_i'^2-a_{ij}\, x_j'^2$; novi oblik forme sadrži bar jedan *»čist član«*, pa se nalazimo *u prethodnom slučaju* i onaj opisani postupak redukcije može se sada primijeniti npr. za koeficijent od $x_i'^2$. U svakom slučaju polazna kvadratna forma postaje sumom jednog čistog kvadratnog člana i kvadratne forme od najviše $n-1$ varijabli. *Ponavljajući proces* određen broj puta, dolazi se do dijagonalne forme.

---

[1] Lagrange, Recherches sur la méthode de maximis et minimis 1759.

2.2.3. Također se direktno lako provjeri da za slučaj $a_{ij} \neq 0$ za neke $i \neq j$ vrijedi ova redukcija:

$$Q(x_1, x_2, \ldots, x_n) = \frac{1}{2a_{ij}} \sum_{\nu=1}^{n} [(a_{i\nu} + a_{j\nu}) x_\nu]^2 - \frac{1}{2a_{ij}} [\sum (a_{i\nu} - a_{j\nu}) x_\nu]^2 + Q_{ij};$$

Q_{ij} ne zavisi od x_i, x_j.

2.3. Pri *svakom* uvođenju novih varijabli na opisan način radi se o *linearnim* supstitucijama s *regularnom* matricom. Tako npr. matrica supstitucije (1) glasi (izražavajući stare koordinate novima):

$$(3) \qquad \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \end{bmatrix} = \begin{bmatrix} 1, & -\frac{a_{12}}{a_{11}}, & -\frac{a_{13}}{a_{11}}, & \ldots, & -\frac{a_{1n}}{a_{11}} \\ & 1 & & & \\ & & 1 & 0 & \\ 0 & & & \cdot & \\ & & & & \cdot \end{bmatrix} \begin{bmatrix} x_1' \\ x_2' \\ \cdot \\ \cdot \\ \cdot \end{bmatrix};$$

determinanta je očigledno $= 1$.

Slično se vidi da je matrica supstitucije (2) regularna. Recimo da se u (2) radi o x_1, x_2; tada čitava supstitucija glasi:

$$(4) \qquad \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \end{bmatrix} = \begin{bmatrix} 2^{-1/2} & -2^{-1/2} & 0 & 0 & \cdot & \cdot & \cdot \\ 2^{-1/2} & 2^{-1/2} & 0 & 0 & \cdot & \cdot & \cdot \\ 0 & 0 & 1 & & & & \\ & & & 1 & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix} \begin{bmatrix} x_1' \\ x_2' \\ \cdot \\ \cdot \\ \cdot \end{bmatrix}.$$

U oba slučaja je $\vec{x} = c\vec{x'}$ pa je determinanta matrice c jednaka 1.

2.4. Nizanjem takvih uvođenja sve novih veličina umjesto prethodnih, dobiva se najzad poslednji vektor $\vec{y}$ odnosno poslednji niz varijabli, nazovimo ih y_1, y_2, ..., pa se vidi da vrijedi ovo:

$$\vec{x} = c\vec{x'}$$

$$\vec{x'} = c'\vec{x''}$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

$$\vec{x^{(k)}} = c^{(k)}\vec{y};$$

tada je

$$x = (c\, c'\, c''\, \ldots\, c^{(k)})\, y = by; \quad \text{pri tom je } c\, c'\, c''\, \ldots\, c^{(k)} = b;$$

dakle

$$b^T = c^{(k)T}\, c^{(k-1)T}\, \ldots\, c^T;$$

nadalje je

$$\det b = \det c \, \det c' \, \ldots = 1 \cdot 1 \cdot \ldots = 1.$$

Najzad, vrijednosti svake matrice dobivaju se *elementarno* iz koeficijenata kvadratne forme. Na taj smo način dokazali

—→ **2.5. Teorem o redukciji.** *Svaka kvadratna forma može se svesti na dijagonalan oblik linearnom promjenom varijabli: matrica kojom se polazne varijable izražavaju novim varijablama ima determinantu* $=1$, *a elementi joj se dobiju elementarno iz koordinata polazne matrice kvadratne forme.* Rang ishodne kvadratne forme jednak je rangu *dobivene dijagonalne forme i dakle je jednak broju neiščezavajućih članova dobivene dijagonalne forme.*

2.6. Problem dijagonalizacije u svjetlu matrica. Problem je ovaj: zadana je kvadratna forma u veličinama $x_1, x_2, \ldots$; neka je a matrica forme; tada forma glasi

$$(1) \qquad \vec{x}^T a \vec{x}, \text{ gdje je } \vec{x}^T = [x_1, x_2, \ldots, x_n],\ \vec{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \end{bmatrix}.$$

Uvodimo nove veličine $x_1', x_2', \ldots$ supstitucijom

$$(2) \qquad \vec{x} = c\vec{x}', \quad \text{tj.} \quad x_k = c_{k1}x_1' + c_{k2}x_2' + \cdots + c_{kn}x_n'.$$

Kako glasi novi oblik forme (1)? Radimo!

$$(3) \qquad \vec{x}^T = (c\vec{x}')^T = (\text{transponat produkta}) = \vec{x}'^T c^T.$$

Time iz (1) izlazi:

$$(\vec{x}'^T c^T)\, a\, (c\vec{x}') = (\text{asocijacija!}) = \vec{x}'^T (c^T a c)\vec{x}',$$

Dakle: *supstitucijom* (2) *prelazi forma* (1) *u oblik*

$$(4) \qquad \vec{x}'^T (c^T a c)\vec{x}'.$$

To je formalno sličan oblik kao (1):

$$\text{umjesto} \quad x \to \vec{x}'$$

$$\text{umjesto} \quad a \to c^T a c.$$

To je opet kvadratna forma; matrica joj je $c^T a c$; determinanta dobivene forme glasi

$$\det(c^T a c) = (\text{pogl. 11 § 9.9.1}) = \det c^T \det a \det c = (\text{radi } \det c^T = \det c;$$

$$\text{pogl. 11 § 5.1)} = (\det c)^2 \det a. \text{ Dobili smo}$$

2.7. Teorem. *Kvadratna forma* $\vec{x}^T a \vec{x}$ *prelazi linearnom supstitucijom* $\vec{x} = c\vec{x}'$ *u kvadratnu formu novih veličina* x_i'; *nova forma glasi* $\vec{x}^T (c^T a c)\vec{x}$: *matrica nove forme je* $c^T a c$; *determinanta nove forme je* $(\det c)^2 \det a$.

Izlaz (4) sličan je ulazu (1), samo što je *nova matrica* nešto *zamršenije formalno građena*! Premda njen *izračunat* oblik može biti već — čak *dijagonalan*. Uostalom, Lagrangeov postupak nam i kazuje da postoji jedna *regularna* matrica c za koju supstitucija (2) dovodi do oblika (4) koji je dijagonalan! Doduše, to c nije nužno već ona matrica koja se pojavila pri prvom koraku ukroćivanja jedne veličine! To je *c rezultat niza operacija* oko pojednostavnjivanja forme.

Pri prvom smo koraku vidjeli da je c rezultat množenja *regularnih* matrica (ako se već c nije čak odmah pojavilo pri prvom koraku). Znači da postoji obratna matrica c^{-1}. I sada dolazi glas geometrije: *prijelaz od matrice a na matricu* $c^T a c$, *odnosno od forme* (1) na formu (4) treba učiniti (*promjenom koordinatnog sistema*) tako da bude $c^T = c^{-1}$ tj. „*ortogonalnom*" matricom c.

2.8. Jacobijeva dijagonalizacija. U praksi se češće pojavljuju kvadratne forme

$$Q = \sum_{i,j=1}^{n} a_{ij} x_i x_j \tag{1}$$

koje imaju svojstvo da je prvih $r\,(=r(a))$ glavnih podmatrica regularno:

$$d_\rho = \det a_{12\ldots\rho}^{12\ldots\rho} = \begin{vmatrix} a_{11} & \cdots & a_{1\rho} \\ \cdots & \cdots & \cdots \\ a_{\rho 1} & \cdots & a_{\rho\rho} \end{vmatrix} \neq 0 \quad (\rho = 1, 2, \ldots, r). \tag{2}$$

Za takve forme (1) vrijedi

Teorem (Jacobi, 1875).[1] *Iz* (2) *izlazi*

$$\sum_{i,j=1}^{n} a_{ij} x_i x_j = \frac{X_1^2}{d_1} + \frac{X_2^2}{d_1 d_2} + \cdots + \frac{X_r^2}{d_{r-1} d_r} \tag{3}$$

pri čemu je

$$X_1 = \frac{1}{2}\frac{\partial Q}{\partial x_1} = a_{11} x_1 + a_{12} x_2 + \cdots + a_{1n} x_n$$

$$X_\rho = \begin{vmatrix} a_{11} & \ldots & a_{1\rho-1} & \frac{1}{2}\frac{\partial Q}{\partial x_1} \\ \cdots & \cdots & \cdots & \cdots \\ a_{\rho 1} & \ldots & a_{\rho\rho-1} & \frac{1}{2}\frac{\partial Q}{\partial x_\rho} \end{vmatrix}, \quad (\rho = 2, \ldots, r);$$

nove veličine X_ρ *zavise homogeno-linearno od* $x_\rho, x_{\rho+1}, \ldots, x_n$, *a uopće ne zavise od* $x_1, x_2, \ldots, x_{\rho-1}$.

---

[1] Jacobi, Journal für Mathematik 53 (1857), 265; također Gesammelte Werke (Djela) 3, 583.

Također se može pisati

$$\sum_{i,j=1}^{n} a_{ij}\, x_i\, x_j = \lambda_1\, y_1{}^2 + \cdots + \lambda_r\, y_r{}^2, \tag{4}$$

$$\lambda_\rho = \frac{d_{\rho-1}}{d_\rho}\ (\rho = 1,\ 2,\ \ldots,\ r;\ d_0 = 1), \tag{5}$$

$$y_\rho = \lambda_\rho\, x_\rho + h_{\rho\,\rho+1}\, x_{\rho+1} + \cdots + h_{\rho\, n}\, x_n,$$

$$h_{\rho j} = \frac{\det a_{1\,2\cdots\rho-1\,j}^{1\,2\cdots\rho-1\,\rho}}{d_{\rho-1}}\ (j = \rho+1,\ \ldots,\ n;\ \rho = 1,\ 2,\ \ldots,\ r).^{1)}$$

2.9. Zadaci o svođenju kvadratnih oblika.

1. Slijedeće kvadratne forme svedi na takve oblike u kojima neće biti mješovitih članova; transformacije neka budu linearne i realne:

1) $x^2+4xy+y^2$; 2) $x^2+3xy-y^2$; 3) $x^2-3xy+y^2$;

4) $-x^2+3xy+y^2$; 5) $x^2-3xy-y^2$; 6) $-x^2+3xy-y^2$;

7) $-x^2-3xy-y^2$; 8) $x^2-2xy-3y^2+5xz+2z^2$; 9) $xy+yz+xz$;

10) $2xy+3yz+4xz$; 11) $-xy+yz+xz$; 12) $5xz-yz+6xy+3x^2$.

2. Napiši formu $x^T a x$ i svedi je na dijagonalni oblik, ako a označuje matricu: I, J, K, α_1, α_2, α_3, α_4, β_1, β_2, β_3, β_4, (pogl. 10 § 4.7.10).

3. Odredi matricu kvadratnih oblika iz zadatka 1; napiši te oblike u obliku matričnog produkta.

4. Isto pitanje ako a označuje ove matrice: svedi forme na dijagon. oblik:

1) $\begin{bmatrix} 2 & -1 & 2 \\ 5 & -3 & 3 \\ -1 & 0 & -2 \end{bmatrix}$; 2) $\begin{bmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{bmatrix}$; 3) $\begin{bmatrix} 4 & -5 & 2 \\ 5 & -7 & 3 \\ 6 & -9 & 4 \end{bmatrix}$;

4) $\begin{bmatrix} 1 & -3 & 3 \\ -2 & -6 & 13 \\ -1 & -4 & 8 \end{bmatrix}$; 5) $\begin{bmatrix} 1 & -3 & 4 \\ 4 & -7 & 8 \\ 6 & -7 & 7 \end{bmatrix}$; 6) $\begin{bmatrix} 7 & -12 & 6 \\ 10 & -19 & 10 \\ 12 & -24 & 13 \end{bmatrix}$;

7) $\begin{bmatrix} 4 & -5 & 7 \\ 1 & -4 & 9 \\ -4 & 0 & 5 \end{bmatrix}$; 8) $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$; 9) $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$;

10) $\begin{bmatrix} 3 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 3 & 0 & 5 & -3 \\ 4 & -1 & 3 & -1 \end{bmatrix}$; 11) $\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$.

---

[1] Isp. Ф. Р. Гантмахер [1], str. 245., odnosno str. 273.

5. 1) Jacobijev (Jakobi, 1804—1851) postupak dijagonalizacije provjeri bar za slučaj $r=2$ i $n=2, 3, 4, \ldots$

2) U vezi s uslovima 2.8, (3) dokaži ovo: ako je (n, n)-matrica a regularna, tada se njeni stupci (redići) mogu međusobno tako permutirati da u dobivenoj matrici a' sve početne glavne podmatrice budu regularne;

3) stupci i redići matrice a dužine n mogu se tako transponirati da u nastaloj matrici a' prvih $r(:=r(a))$ *početnih glavnih podmatrica bude regularno*; ako je $r<a$, tada je općenito potrebno transponirati i retke i stupce.

3. ZAKON USTRAJNOSTI (INERCIJE) ZA KVADRATNE FORME

3.1. Zakon inercije. Vidjeli smo da za svaku kvadratnu realnu formu

$$\vec{x}^T a \vec{x} \tag{1}$$

postoji bar jedna ***realna*** nesingularna transformacija b:

$$\vec{x}=b\vec{y}, \tag{2}$$

tako da forma

$$\vec{y}^T (b^T a\, b)\vec{y} \tag{3}$$

poprimi *normalni, kanonski ili dijagonalni oblik*, recimo

$$c_1 y_1^2 + c_2 y_2^2 + \cdots + c_r y_r^2. \tag{4}$$

Takvih transformacija (2) ima neizmjerno mnogo. No, ipak se u (3), odnosno (4) dobije uvijek *isti broj*, r, *kvadratnih članova*; $r=$ rang od a; Sylvester je dokazao da vrijedi

—→ 3.2. Teorem inercije[1]. *Na koji se god način kvadratna realna forma prevela pomoću regularne linearne supstitucije na dijagonalan oblik, uvijek se dobije jedan te isti broj, p, pozitivnih nezavisnih članova i jedan te isti broj $q=r-p$ negativnih nezavisnih članova.*

Dokaz. Stvarno, neka je također

$$x=\beta\eta \tag{5}$$

jedna nesingularna realna transformacija, tako da bude

$$\vec{\eta}'\beta' a\beta\vec{\eta}=\gamma_1\eta_1^2+\gamma_2\eta_2^2+\cdots+\gamma_r\eta_r^2. \tag{6}$$

---

[1] Sylvester 1852. i 1853; i ime je dao Sylvester (Philos. Magazine 1852, Philos. Transactions 1859). Inače su taj zakon poznavali i prije toga vremena: Gauss, Riemann, Jacobi.

Stavimo li još

$$y_i = |c_i^{-1/2}| y_i',$$

prevest će se forma (4) u oblik u kojem su koeficijenti $+1$ ili -1; isto vrijedi i za formu (6). Provodeći eventualno drukčiju numeraciju varijabli (ukinimo akcente i sl.), *možemo uzeti* da pozitivni članovi u (4) i (6) polaze prije negativnih, recimo da je (3), odnosno (4) oblika

$$y_1^2 + y_2^2 + \cdots + y_p^2 - y_{p-1}^2 - y_{p+2}^2 - \cdots - y_r^2 \tag{7}$$

(naravno, može biti $p = r$).

Isto tako neka forma (6) glasi

$$\eta_1^2 + \eta_2^2 + \cdots + \eta_p^2 - \eta_{\pi+1}^2 - \cdots - \eta_r^2, \tag{8}$$

tako da je, dakle, (7) = (8), tj.

$$y_1^2 + \cdots + y_p^2 + \eta^2_{\pi+1} + \cdots + \eta_r^2 = y^2_{p+1} + \cdots + y_r^2 + \eta_1^2 + \cdots + \eta_\pi^2. \tag{9}$$

Tvrdimo da je $p = \pi$; kad bi naime bilo $p < \pi$, tada bi se moglo učiniti da bude $(9)_1 = 0$ a $(9)_2 \neq 0$ što je nemoguće. Stavimo naime

$$\begin{aligned} y_i &= 0 \quad (i = 1, 2, \ldots, p) \\ \eta_k &= 0 \quad (k = \pi + 1, \ldots, r). \end{aligned} \tag{10}$$

No, matrica b u (2) kao i matrica β u (5) su regularne i kvadratne, pa iz (2) i (5) izlazi

$$\vec{y} = b^{-1}\vec{x} \quad \text{tj.} \quad y_\nu = (b^{-1})_{\nu\cdot} \circ \vec{x}$$

$$\eta = \beta^{-1}\vec{x} \quad \text{tj.} \quad \eta_\nu = (\beta^{-1})_{\nu\cdot} \circ \vec{x} \quad \text{za } \nu = 1, 2, \ldots, n.$$

Zato jednakost (9) glasi i ovako:

$$\sum_{i=1}^{n} \left[(b^{-1})_{i\cdot} \circ \vec{x}\right]^2 + \sum_{k=\pi+1}^{n} \left[(\beta^{-1})_{k\cdot} \circ \vec{x}\right]^2 = \sum_{j=p+1}^{n} \left[(b^{-1})_{j\cdot} \circ \vec{x}\right]^2 + \sum_{e=1}^{n} \left[(\beta^{-1})_{e\cdot} \circ \vec{x}\right]^2. \tag{9'}$$

Jednadžbe (10) postaju

$$\begin{aligned} (b^{-1})_{i\cdot} \circ \vec{x} &= 0 \quad (i = 1, 2, \ldots, p) \\ (\beta^{-1})_{k\cdot} \circ \vec{x} &= 0 \quad (k = \pi + 1, \ldots, r). \end{aligned} \tag{11}$$

U (11) imamo $r_0 (:= p + r - \pi)$ homogenih linearnih jednadžbi za $\vec{x} = [x_1, x_2, \ldots, x_n]^T$; no zbog pretpostavke $p < \pi$ bilo bi $r_0 < r$; zato iz tih r_0 jednadžbi (10) odnosno (11) ne izlazi da nužno vrijedi i preostalih $r - r_0$ jednadžbi $y_{p+1} = 0, \ldots, y_r = 0$ jer su linearne jednadžbe $y_{r'} = (b^{-1})_{r'} \circ \vec{x} = 0$ (ima ih r) linearno nezavisne i ne mogu se linearno izraziti pomoću r_0 linearnih jednadžbi, zbog, $r_0 < r$. Dakle zaista ima neko $\vec{x}$ za koje vrijedi (10) odnosno

(11) i ujedno $y_k \neq 0$ tj. $(b^{-1})_{l.} \circ \vec{x} \neq 0$ za bar jedno $l \in \{p+1, \ldots, r\}$; to prema (9) znači da bi za takvo $\vec{x}$ bilo $(9)_1 = 0$ i $(9)_2 \neq 0$, što je apsurd jer (9) mora vrijediti za svaki vektor $\vec{x}$. Slično se dokazuje da ne može biti $p > \pi$.

3.3. Signatura matrice, odnosno forme. Definicija. *Razlika* $p - q$ između broja p pozitivnih i broja q negativnih članova dijagonalnog oblika kvadratne forme zove se *signatura forme*, odnosno *matrice te forme* (prema Frobeniusu, 1895). Označuje se sa σ. Prema tome, signatura može biti i pozitivan broj i negativan broj i nula.

Naravno

$$p + q = r \text{ (rang)}$$

$$p - q = \sigma, \text{ dakle je } p = \tfrac{1}{2}(r + \sigma), \quad q = \tfrac{1}{2}(r - \sigma).$$

Jedinična forma $x_1^2 + x_2^2 + x_3^2$ ima signaturu $\sigma = 3 - 0 = 3$; negativna jedinična forma $-x_1^2 - x_2^2 - x_3^2$ ima signaturu $\sigma = 0 - 3 = -3$.

Signatura forme $x_1^2 - x_2^2 - x_3^2$ je $\sigma = 1 - 2 = -1$.

Naravno, signatura zadane kvadratne forme ne može se odmah uvijek očitati iz same forme!

⟶ **3.4.** Teorem. *Ako dvije kvadratne forme Q_1, Q_2 imaju isti rang r i istu signaturu σ, može se svaka od njih prevesti u drugu nekom realnom nesingularnom linearnom transformacijom.* Postoji regularna transformacija t_i varijabli kojom Q_i prelazi u

$$y_1^2 + y_2^2 + \cdots + y_p^2 - y_{p+1}^2 - \cdots - y_r^2, \tag{12}$$

gdje je

$$p = \frac{r + \sigma}{2}.$$

To znači da obratna transformacija t_i^{-1} prevodi formu (12) u formu Q_i $(i = 1, 2)$. A to znači da transformacija $t = t_2^{-1} t_1$ prevodi formu Q_1, preko (12), odmah u formu Q_2, dok obratna transformacija $t_1^{-1} t_2$ prevodi Q_2 u Q_1. No, obje su te transformacije t, t^{-1} realne i regularne jer su proizvod takvih dviju transformacija.

Q. E. D.

3.5. ***Kada je kvadratna forma produkt linearnih formi?***

Teorem. *Kvadratna forma se može prikazati kao produkt dvojke linearnih formi istih varijabli onda i samo onda ako je rang forme ≤ 2.*

Nužnost. Ako je kvadratna forma $\vec{x}^T a \vec{x}$ jednaka $\vec{b} \circ \vec{x} \cdot \vec{c} \circ \vec{x}$, onda je matrica $a = \text{stupac} \cdot \text{redak} = \vec{b} \cdot c^T = [b_i c_j]$ pa joj je rang ≤ 2 (isp. pogl. 11, § 9.6).

Dovoljnost. Ako je rang kvadratne forme ≤ 2, postoji jednakost

$$\vec{x}^T a \vec{x} = \lambda_1 y_1^2 + \lambda_2 y^2, \quad \text{gdje su } \lambda_1, \lambda_2 \text{ realni brojevi,}$$

a y_1, y_2 su linearne homogene funkcije veličinâ $x_1, x_2, \ldots, x_n$. No,

$$\lambda_1 y_1^2 - \lambda_2 y_2^2 = (\lambda_1^{1/2} y_1 - \lambda_2^{1/2} y_2)(\lambda_1^{1/2} y_1 + \lambda_2^{1/2} y_2);$$

kako su obje ove zagrade linearne forme u odnosu na $x_1, x_2, \ldots, x_n$ cilj je postignut (naravno, u općem slučaju koeficijenti traženih linearnih formi nisu realni).

4. DEFINITNE KVADRATNE FORME

4.1. Gaussova transformacija forme $x^T a x$. To je prijelaz na formu

$$x^T a^T a x, \tag{1}$$

koja je, kao što se vidi, simetrična:

$$(a^T a)^T = a^T a^{TT} = a^T a.$$

No,

$$x^T a^T a x = (a x)^T (a x), \tag{2}$$

tj. *Gaussova forma što pripada zadanoj kvadratnoj formi jest* ***norma*** vektora $a x$ pa kao suma kvadrata ne može postati negativna: ona je uvijek ≥ 0.

4.2. Definicija definitnosti. Realna kvadratna forma je *pozitivno* (*negativno*) *definitna* ako je uvijek ≥ 0 (≤ 0), a poništava se jedino kad su sve varijable $= 0$.

4.3. Definicija. Forma je pozitivno (negativno) *semidefinitna* ako je uvijek ≥ 0 (≤ 0), no može se poništavati i za koji vektor $\neq \vec{0}$.

Tako vidimo da je forma (2) definitna, i to ≥ 0; samo se još radi o tome da li može (2) biti $= 0$ također za $\vec{x} \neq \vec{0}$, tj. da li može biti $a\vec{x} = \vec{0}$ i za $\vec{x} \neq \vec{0}$. No, iz matrične jednakosti $a\vec{x} = \vec{0}$ izlazi da je vektor $\vec{x} \neq \vec{0}$ onda i samo onda kad je matrica a singularna. Na taj način imamo ovaj važni

—→ 4.4. Osnovni teorem. ***Gaussova transformacija svake realne kvadratne forme uvijek je ≥ 0; ona je definitno pozitivna ili semidefinitno pozitivna, već prema tome da li je polazna kvadratna forma regularna ili singularna, odnosno da li su vektori matrice te forme linearno nezavisni ili linearno zavisni.***

4.5. Teorem. Zadanih s vektora $x_1, x_2, \ldots, x_s$ je linearno zavisno onda i samo onda ako je pripadna Gramova determinanta, tj. determinanta

$$\Gamma(\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_n) = \det [x_i^T x_j] = \begin{vmatrix} x_1^T x_1 & x_1^T x_2 & \cdots & x_1^T x_s \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & x_s^T x_s \end{vmatrix}$$

jednaka 0. Inače, ta je determinanta $= \det a^T a$ pri $a = [\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_s]$ pa je prema poučku 4.4 ona ≥ 0.

4.6. Definitne kvadratne forme od dvije veličine. Promatrajmo formu

(3) $$p x^2 + q x y + r y^2.$$

Matrica je $\begin{bmatrix} p & \frac{q}{2} \\ \frac{q}{2} & r \end{bmatrix}$, determinanta je

$$D = pr - q^2/4 = 1/4\ (4pr - q^2).$$

Ako je forma $px^2 + qxy + ry^2$ *uvijek* >0, *tada je*

$$p>0, \quad r>0, \quad D>0: \qquad \textit{i obrnuto.}$$

Naime, ne može biti $p<0$, jer bi tada (3) glasilo

(4) $$p\left(x + \frac{q}{2p} y\right)^2 + \frac{4pr - q^2}{4p} y^2$$

pa bi za $y=0$ izraz (4), a time i (3) bili <0; iz istog razloga ne može biti $r<0$. No, iz (4) se vidi da ne smije biti $D<0$, jer bi inače drugi član u (4) bio <0, a time i čitav izraz npr. onda ako je prvi član u (4) $=0$. To je tako ako je $p>0$; isto vrijedi za $r>0$. Ostaje slučaj kad je $p=r=0$. Tada se forma svodi na qxy; očigledno, ona može biti i >0 i <0, već prema izboru brojeva x i y. Uostalom, ne može biti $p=0$; tada bi izraz (3) glasio

$$r\left(y + \frac{q}{2r} x\right)^2 - \frac{q^2}{4r} x^2,$$

a to se može učiniti i <0.

Obratno: ako je $p>0$, i $D>0$, tada je (4) >0, tj. (3) >0, $r>0$. Na taj smo način dokazali za slučaj kvadratnih formi od dvije veličine jedan teorem koji vrijedi i za forme od 3, 4, ... veličina i glasi ovako:

4.7. Teorem (kriterij o pozitivno definitnim kvadratnim formama; Sylvester) *Kvadratna forma* $x^T a x$, *gdje je* $a^T = a$, *s realnim koeficijentima, onda je i samo onda pozitivno definitna forma ako je determinanta matrice i determinanta svake početne glavne podmatrice* >0 (isp. pogl. 10, § 2.9).

Na osnovu tog teorema lako je *formirati* pozitivno definitne forme i *prepoznati* takve forme.

Tako npr. forma s matricom

$$a = \begin{bmatrix} 3 & 1 & 4 \\ 1 & 4 & 2 \\ 0 & 2 & 5 \end{bmatrix}$$

je pozitivno definitna jer je $\det a = 60 - 5 - 12 = 43 > 0$, a glavne su joj početne podmatrice:

[3] $\begin{bmatrix} 3 & 1 \\ 1 & 4 \end{bmatrix}$ i a; determinante su im >0.

4.7.1. *Uslov teoreme je nuždan.*

Provedimo dokaz induktivno: stvar je istinita ako je Dom $a=(1, 1), (2, 2)$; pretpostavimo da je teorem istinit za svaku kvadratnu formu kojoj matrica ima manje od n redaka; dokažimo da onda iskaz u teoremu vrijedi i za Dom $a=(n, n)$. No,

$$\sum_1^n a_{ij}\,x_i\,x_j = a_{11}\,x_1{}^2 + 2x_1 \sum_2^n a_{1z}\,x_z + \sum_2^n a_{ij}\,x_i\,x_j. \tag{1}$$

Za svaki izbor vrijednosti za $x_2, x_3, \ldots, x_n$ koje nisu sve $=0$ izraz (1) mora biti >0 za svako $x_1 \neq 0$; to znači da mora biti

$$a_{11}>0 \text{ (slično } a_{ii}>0); \tag{2}$$

zato diskriminanta funkcije (1) kao funkcije od x_1 mora biti <0 tj.

$$\left(2\sum_2^n a_{1j}\,x_j\right)^2 - 4\,a_{11}\sum_2^n a_{ij}\,x_i\,x_j<0 \text{ pri } (x_2, \ldots, x_n)\neq(0, \ldots, 0).$$

Dijeleći tu nejednadžbu sa -4 i pišući

$$\left(\sum_2 a_{1j}\,x_j\right)^2 = \sum_2^n a_{1i}\,a_{1j}\,x_i\,x_j \quad \text{postaje ona}$$

$$\sum_{i,\,j=2}^{n} (a_{11}\,a_{ij} - a_{1i}\,a_{1j})\,x_i\,x_j>0 \text{ pri } x_\nu\neq 0 \ (\nu=2, 3, \ldots, n). \tag{3}$$

No, lijeva strana u (3) je kvadratna forma od $x_2, \ldots, x_n$ pa (3) kazuje da je ona pozitivno definitna forma; prema indukcionoj hipotezi vrijede za matricu c s komponentama

$$c_{ij} = [a_{11}\,a_{ij} - a_{1i}\,a_{1j}]_{i,\,j=2,\ldots,n} \quad \text{ove relacije:} \tag{4}$$

$$\det I_e c>0 \ (e=1, 2, \ldots, n-1); \tag{5}$$

$I_e c$ znači početnu glavnu podmatricu od a dužine e.

S druge strane, s determinantama oblika $(4)_1$ sreli smo se pri *Gauss-Chio-ovu postupku* u poglavlju 11, § 11.4; tamošnja formula (2) primijenjena na matricu $I_e a$ za $e=1, 2, 3, \ldots, n$ daje

$$\det I_e a = a_{11}{}^{-e+2} \det I_{e-1} c \quad (e=2, 3, \ldots, n).$$

Na osnovu ovih jednakosti daju indukcione nejednakosti (5) tražene nejednakosti $\det I_e a>0$ $(e=2, \ldots, n)$; imajući u vidu (1), znači to da iz pozitivne definitnosti izlazi

$$\det I_\nu a>0 \qquad (\nu=1, 2, \ldots, n). \tag{6}$$

4.7.2. *Uslov teorema* 4.7. *je dovoljan*: ako vrijedi (6), onda je kvadratna forma strogo pozitivna. Naime, uz uslove (6) može se primijeniti Jacobijev postupak dijagonalizacije (isp. § 2.6; formule (3), (4) za $r=n$), iz kojih se odmah vidi da je ishodna forma suma od n pozitivnih izraza.

4.8. Nejednakost Bunjakovski-Švarcova. *Za koja god dva konačna niza **realnih** brojeva po n članova*:

$$x = x_1,\ x_2,\ \ldots,\ x_n$$

$$y = y_1,\ y_2,\ \ldots,\ y_n$$

vrijedi

$$(x \circ y)^2 \leq (x \circ x)^2 \cdot (y \circ y)^2, \quad \text{tj.} \quad (x\,y^T)^2 \leq x\,x^T \cdot y\,y^T.$$

Naime, promatrajmo proizvoljnu *linearnu formu* tih nizova:

$$p\,x + q\,y = p\,x_1 + q\,y_1 + p\,x_2 + q\,y_2 + \cdots$$

Tada za *skalarni kvadrat* tih nizova odmah vidimo da vrijedi (množenje matrica!)

$$(p\,x + q\,y)(p\,x + q\,y)^T = (p\,x + q\,y)\,(p\,x^T + q\,y^T) =$$

$$= p^2\,x\,x^T + q\,p\,y\,x^T + p\,q\,x\,y^T + q^2\,y\,y^T \ \text{(jer je } y\,x^T = x\,y^T\text{)}$$

$$= p^2\,x\,x^T + 2\,p\,q \cdot x\,y^T + q^2\,y\,y^T.$$

To je kvadratna forma za veličine p, q; forma je ≥ 0 jer je ona *skalarni kvadrat* niza $p\,x + q\,y$. Dakle, diskriminanta mora biti ≥ 0:

$$x\,x^T \cdot y\,y^T - (x\,y^T)^2 \geq 0, \qquad \text{a to se baš i tvrdi.}$$

5. ZAHTJEV PRAKSE I TEORIJE: DIJAGONALIZACIJU KVADRATNE FORME TREBA PROVESTI ORTOGONALNOM SUPSTITUCIJOM (OSNI PROBLEM)

5.1. U raznim oblastima (astronomija, mehanika, geometrija, fizika, ...) postavlja se problem da se nađe *realna ortogonalna* — naglašujemo *ortogonalna*— transformacija ω (tj. $\omega^T = \omega^{-1}$) *kojom će kvadratna forma preći u dijagonalni oblik*. Treba, dakle, odrediti *ortogonalnu* realnu matricu ω za koju je

$$\vec{x'}^T\,\omega^T\,a\,\omega\,\vec{x'}$$

dijagonalna matrica, dakle

$$x'^T\,\omega^T\,a\,\omega\,x' = \lambda_1\,x'_1{}^2 + \lambda_2\,x'_2{}^2 + \cdots$$

Kasnije ćemo vidjeti da time što je ω ortogonalna i realna matrica, redukcija na pripadni dijagonalni oblik kvadratne matrice *znači naprosto zgodno izabrati koordinatnu bazu vektorâ* (isp. pogl. 27). I u toj koordinatnoj bazi forma postaje dijagonalnom.

5.2. Karakteristična jednadžba. No, ortogonalnom supstitucijom

$$\vec{x} = \omega\,\vec{x'} \tag{0}$$

prelazi i jedinična kvadratna forma

$$\vec{x}^T \vec{x} = x_1^2 + x_2^2 + \cdots \quad \text{u jediničnu} \quad x'^T x' = x'_1{}^2 + x'_2{}^2 + \cdots$$

To znači da supstitucijom (0) *kvadratna forma*

$$\lambda \vec{x}^T \vec{x} - \vec{x}^T a \vec{x} = \vec{x}^T (\lambda I - a) \vec{x} \tag{1}$$

prelazi u formu

$$\lambda(x'_1{}^2 + x'_2{}^2 + \cdots) - \lambda_1 x'_1{}^2 - \lambda_2 x'_2{}^2 - \cdots = (\lambda - \lambda_1) x'_1{}^2 + (\lambda - \lambda_2) x'_2{}^2 + \cdots; \tag{2}$$

to vrijedi za svaki skalar λ, dakle i za $\lambda = \lambda_1, \lambda_2, \ldots$

No, to znači da za $\lambda = \lambda_i$ dobivena forma (2) ima manje od n veličina $x_1', x_2', \ldots, x_n'$; kako je transformacija ω regularna, znači da polazna forma (1) mora biti singularna, tj. mora biti

$$\det(\lambda_i - a) = 0, \text{ tj. } \det \begin{bmatrix} \lambda - a_{11} & -a_{12} \cdots -a_{1n} \\ \cdots\cdots\cdots\cdots\cdots \\ -a_{n1} & \lambda - a_{nn} \end{bmatrix} = 0. \tag{3}$$

Na taj način dolazimo do tzv. *karakteristične jednadžbe matrice* a tj. do jednadžbe (3), kojoj koeficijenti tražene dijagonalne forme treba da zadovoljavaju.

5.3. Rješavanje problema glavnih osi kvadratne forme.

5.3.1. Zadana je kvadratna forma $x^T a x$ sa simetričnom matricom a i pripadnom karakterističnom jednadžbom (3). Treba jednadžbu (3) riješiti, tj. naći niz od n brojeva

$$\lambda_1, \lambda_2, \ldots, \lambda_n \tag{4}$$

za koje je

$$\det(\lambda - a) = (\lambda - \lambda_1)(\lambda - \lambda_2) \ldots (\lambda - \lambda_n).$$

5.3.2. Za svako to rješenje λ_i, matrica $\lambda_i - a$ je *singularna* (v. (4)), pa zato postoji bar jedan *jedinični vektor* l_i za koji je

$$(\lambda_i - a) l_i = 0. \tag{5}$$

5.3.3. Ako je moguće formirati na taj način n jediničnih vektora međusobno okomitih, dobivamo time njihovu matricu

$$l = [l_1, l_2, \ldots, l_n]. \tag{6}$$

5.3.4. I ta matrica l je tražena *ortogonalna supstitucija*. Uistinu, prema (5) imamo $\lambda_i l_i = a l_i$ tj.

$$a l_i = \lambda_i l_i \quad (i = 1, 2, \ldots, n), \tag{7}$$

$$[a l_1, a l_2, \ldots, a l_n] = [l_1 \lambda_1, l_2 \lambda_2, \ldots, l_n \lambda_n]. \tag{8}$$

No, lijeva strana (8) je produkt $a\,l$ matrice a i matrice (6). Desna strana u (8) je produkt od l i dijagonalne matrice

$$\begin{bmatrix} \lambda_1 & & 0 \\ & \lambda_2 & \\ & & \ddots \\ 0 & & \end{bmatrix};$$

na taj način jednadžba (8) daje

$$(9) \qquad a\,l = l \begin{bmatrix} \lambda_1 & & 0 \\ & \lambda_2 & \\ & & \ddots \\ 0 & & \end{bmatrix}, \quad \text{gdje je } l \text{ matrica (6).}$$

Odatle predmnoženjem sa l^{-1}:

$$(10) \qquad l^{-1}\,a\,l = \begin{bmatrix} \lambda_1 & & 0 \\ & \lambda_2 & \\ & & \ddots \\ 0 & & \end{bmatrix}.$$

No, matrica l sastavljena je od međusobno okomitih stupaca (tako smo odabrali l_i); to znači da je $l_i^T\,l_k = 0$ za $i \neq k$; kako je $l_i^T\,l_i = 1$, znači to da je $l\,l^T =$ jedinična matrica tj.

$$(11) \qquad l^T = l^{-1}.$$

5.3.5. Dakle je l ortogonalna matrica i cilj je postignut! Dovoljno je sada uvesti nov vektor x', stavljajući $x = l\,x'$ pa da polazna kvadratna forma $x^T\,a\,x$ postane dijagonalnom; naime imamo

$$x^T\,a\,x = (l\,x')^T\,a\,(l\,x') = x'^T\,l^T\,a\,l\,x' = x'^T\,(l^{-1}\,a\,l)\,x' =$$

$$= x'^T \begin{bmatrix} \lambda_1 & & \\ & \lambda_2 & \\ & & \ddots \end{bmatrix} x' = \lambda_1\,x'_1{}^2 + \lambda_2\,x'_2{}^2 + \cdots$$

Dijagonalizacija pomoću ***ortogonalne*** supstitucije l je postignuta.

5.3.6. Sve je to u redu, ali smo mi u 5.3.3. počeli rečenicu sa „Ako je moguće . . .“ I tu se otvara široka oblast istraživanja! Kada će zbilja biti moguće odrediti gornju matricu l? Sigurno npr. onda ako su brojevi λ_i iz (4) međusobno različiti. Naime, onda automatski iz (5) izlazi da je $l_i \perp l_k$ za $i \neq k$ (isp. 27, § 4.1. (3)). Poslije ćemo dokazati da je uslov $a^T = a$ dovoljan da osigura gornju matricu l (isp. 27, § 4.2). Ali taj je uslov upravo adekvatna mjera za postojanje spomenute ***realne*** ortogonalne matrice l; ako l postoji, tada je $a^T = a$ (isp. 27, § 11).

5.3.7. Vrlo je zanimljivo (pogl. 26. § 12) da *brojevi* λ_i *zadovoljavaju neka* ***ekstremna*** *svojstva.* Zbog ekstremnog svojstva brojeva λ_i može se nastojati pomoću fizičkih, geometrijskih i mehaničkih svojstava brojeve λ_i i »*vlastite vektore*« l_i *odrediti* i time na praktičan način *riješiti osni problem kvadratnih formi.* Specijalno se na taj način dokazuje da su brojevi λ_i realni (a ne imaginarni i sl.).

5.4. Zadaci o dijagonalizaciji kvadratnih oblika.

1. Odredi signaturu σ i brojeve p, q ovih kvadratnih forama:

   1) x^2+y^2, x^2-y^2, $-x^2-y^2$; 2) $x^2+y^2+z^2$, $x^2+y^2-z^2$, $x^2-y^2-z^2$, $-x^2-y^2-z^2$.

2. Isto pitanje za forme iz zad. 1. i zad. 2. iz § 29.

3. Napiši dijagonalni oblik forme za koju je:

   1) $p=2$, $q=3$; 2) $p=2$, $\sigma=1$; 3) $\sigma=3$, $q=2$; 4) $p=q=2$; 5) $p=5$, $q=0$; 6) $p=0$, $q=5$.

4. Koja je od formi iz zad. 3 pozitivno-definitna, a koja pozitivno-semi-definitna?

5. Isto pitanje za kvadratne forme s matricom I, J, K (pogl. 10, § 4.7.9), α_1, α_2, α_3, α_4, β_1, β_2, β_3, β_4, (pogl. 10, § 4.7.10).

6. Da li su ove dvije forme međusobno ekvivalentne ili nisu:

   1) x^2+3y^2, $2x^2+y^2$; 2) x^2+y^2, x^2-y^2, 3) $-x^2+y^2$, x^2-y^2; 4) x^2-xy, x^2+y^2; 5) x^2-xy, x^2-y^2; 6) x^2+xy, x^2+y^2; 7) x^2+xy, $-x^2+y^2$; 8) $x^2+3xy-y^2$, $-x^2-5xy+4y^2$; 9) $6x^2-5xy-6y^2$, $35x^2-18xy-10y^2$; 10) $f=x^2+4y^2+4xy-2xz$, $g=x^2+2y^2-z^2+4xy-2xz-4yz$; 11) f, $h=-4x^2-y^2-z^2-4xz+4xz+18yz$; 12) g, h iz 11) i 12).

7. Dokaži: 1) Da bi kvadratna forma $x^T a x$ bila pozitivno definitna nužno je i dovoljno da svi njeni uglovni glavni minori budu >0: 2) Kvadratna forma je negativno definitna onda i samo onda ako niz njenih kutnih glavnih minora ima predznake -1, 1, -1, 1, . . . , 3) Ako kvadratna forma $x^T a x$ koja je uvijek ≥ 0 postaje 0 za bar jedan vektor $\vec{x} \neq \vec{0}$, tada je nužno $\det a = 0$.

8. Šta je nužno i dovoljno pa da kvadratne forme f, $-f$ budu ekvivalentne?

9. Nađi ortogonalnu linearnu transformaciju koja slijedeću kvadratnu formu prevodi u kanonski oblik:

1) $6x_1^2+5x_2^2+7x_3^2-4x_1x_2+4x_1x_3$;

2) $11x_1^2+5x_2^2+2x_3^2+16x_1x_2+4x_1x_3-20x_2x_3$;

3) $x_1^2+x_2^2+5x_3^2-6x_1x_2-2x_1x_3+2x_2x_3$;

4) $x_1^2+x_2^2+x_3^2+4x_1x_2+4x_1x_3+4x_2x_3$;

5) $17x_1^2+14x_2^2+14x_3^2-4x_1x_2-4x_1x_3-8x_2x_3$;

6) $x_1^2-5x_2^2+x_3^2+4x_1x_2+2x_1x_3+4x_2x_3$;

7) $8x_1^2-7x_2^2+8x_3^2+8x_1x_2-2x_1x_3+8x_2x_3$;

8) $2x_1x_2-6x_1x_3-6x_2x_4+2x_3x_4$;

9) $5x_1^2+5x_2^2+5x_3^2+5x_4^2-10x_1x_2+2x_1x_3+6x_1x_4+6x_2x_3+$
$+2x_2x_4-10x_3x_4$;

10) $3x_1^2+8x_1x_2-3x_2^2+4x_3^2-4x_3x_4+x_4^2$;

11) $x_1^2+2x_1x_2+x_2^2+2x_3^2-4x_3x_4-2x_4^2$;

12) $9x_1^2+5x_2^2+5x_3^2+8x_4^2+8x_2x_3-4x_2x_4+4x_3x_4$;

13) $4x_1^2-4x_1x_2+x_2^2+5x_3^2-4x_4^2+12x_4x_5+x_5^2$;

14) $4x_1^2-4x_2^2-8x_2x_3+2x_3^2-5x_4^2+6x_4x_5+3x_5^2$;

15) $3x_1^2+8x_1x_2-3x_2^2+4x_3^2-6x_3x_4-4x_4^2+4x_5^2+4x_5x_6+x_6^2$.

10. Odredi vrijednosti λ za koje ova forma postaje pozitivno definitna:

1) $x^2+3\lambda y^2$; 2) $x^2+2\lambda xy+y^2$; 3) $x^2+\lambda xy-y^2$;

4) $x^2+y^2+z^2+\lambda xy+xz+yz$.

11. *Kompozicija kvadratnih forama* $A=x^Tax$, $B=x^Tax$ zove se forma $(A, B)=\sum_{i,j=1}^{n} a_{ij}b_{ij}x_ix_j$; dokaži ovo: 1) Ako su forme A, B definitno pozitivne, tad je i (A, B) definitno pozitivna; 2) Ako su A, B neodrečne, onda je i forma (A, B) neodrečna.

12. Za kojagod dva niza kompleksnih brojeva po n članova:

$$a_1, a_2, \ldots, a_n$$
$$b_1, b_2, \ldots, b_n$$

vrijedi $(\Sigma|a_k|^2)(\Sigma|b_k|^2)\geq|\Sigma a_kb_k|^2$; znak jednakosti stoji onda i samo onda ako je jedan niz proporcionalan s drugim nizom.

6. BILINEARNE FORME

6.1. Primjer. Pogledajmo izraze

$$2x_1-3x_2+4x_3, \tag{1}$$

$$4y_1+5y_2-7y_3. \tag{2}$$

Prvi je od tih izraza linearna forma od x_1, x_2, x_3, a drugi je linearna forma od y_1, y_2, y_3. Nađimo produkt izraza (1), (2):

$$\begin{aligned}(2x_1-3x_2+4x_3)(4y_1+5y_2-7y_3)= \\ =8x_1y_1+10x_1y_2-14x_1y_3-12x_2y_1-15x_2y_2+21x_2y_3+ \\ +16x_3y_1+20x_3y_2-28x_3y_3.\end{aligned} \tag{3}$$

Računanje je jednostavno u mislima, no za oko nije pregledno. A što da izraz (1) ima mnogo više članova, (2) isto tako?!

Gledajmo stvar sada više plastično. Izraz (1) možemo pisati i kao matrični produkt

$$[x_1\ x_2\ x_3]\begin{bmatrix}2\\-3\\4\end{bmatrix}\quad\text{ili kao}\quad[2,\ -3,\ 4]\begin{bmatrix}x_1\\x_2\\x_3\end{bmatrix}.$$

Isto tako

$$4y_1+5y_2-7y_3=[4,\ 5,\ -7]\begin{bmatrix}y_1\\y_2\\y_3\end{bmatrix}=[y_1\ y_2\ y_3]\begin{bmatrix}4\\5\\-7\end{bmatrix}.$$

Nađimo produkt (3):

$$[x_1\ \ x_2\ \ x_3]\begin{bmatrix}2\\-3\\4\end{bmatrix}\cdot[4,\ 5,\ -7]\begin{bmatrix}y_1\\y_2\\y_3\end{bmatrix}= \tag{4}$$

$$=[x_1\ \ x_2\ \ x_3]\begin{bmatrix}8&10&-14\\-12&-15&21\\16&20&-28\end{bmatrix}\begin{bmatrix}y_1\\y_2\\y_3\end{bmatrix}.$$

U rezultatu se odmah *slikovito vide svi koeficijenti*. Odatle se odmah očitava koeficijent od $x\cdot y$. Možemo to shematski predstaviti ovako:

$\dot{+}$	y_1	y_2	y_3
x_1	8	10	−14
x_2	−12	−15	21
x_3	16	20	−28

Rezultat (3) je *bilinearna* (dvaput linearna) *forma veličina* x_1, x_2, x_3 i veličina y_1, y_2, y_3, jer je (3) linearan spoj produkata po jedne veličine iz jednog niza i po jedne veličine iz drugog niza.

Recimo ono 20 je a_{32}; znači, to je koeficijent od $x_3 y_2$; isto tako $21 = a_{23}$ (drugi redak matrice i treći stupac matrice); odgovarajući član glasi $21\, x_2 y_3$.

Naravno, produkt (3) se zapisuje i u obliku $\sum_{i,k=1}^{n} a_{ik} x_i y_k$, gdje je a_{ik} produkt koeficijenta od x_i u (1) i koeficijenta od y_k u (2).

Slično u općem slučaju.

6.2. Definicija dvaput linearnih formi. *Ako imamo dva* ***istobrojna*** *niza*

$$x_1, x_2, \ldots, x_n \tag{5}$$

$$y_1, y_2, \ldots, y_n, \tag{5'}$$

pa ako *svaki* član x_i prvog niza pomnožimo *svakim* članom y_j drugog niza i dobiveni produkt $x_i y_j$ još pomnožimo nekim izrazom koji ne zavisi od veličina (5), a može biti 0 ili $\neq 0$ i sve te produkte saberemo, dobit ćemo izraz koji se zove *bilinearna ili dvaput linearna forma veličina* (5) i veličina (5'). Ako koeficijent od produkta $x_i y_j$ označimo sa a_{ij}, onda znači da imamo član

$$a_{ij} x_i y_j. \tag{6}$$

Takvih članova ima $n \cdot n$ (neki mogu i otpasti: koeficijent je 0), a zbroj im označujemo kraće sa

$$\sum_{i,j=1}^{n} a_{ij} x_i x_j. \tag{7}$$

Važno je da koeficijenti ne zavise od x_1, x_2, ... ni od y_1, y_2 ...

6.2.1. Evo primjerâ bilinearnih forama veličina $x_1, x_2, \ldots, x_n, y_1, \ldots, y_n$ odnosno vektorâ $\vec{x}, \vec{y}$;

$$x_1 y_1, \quad x_2 y_2, \quad x_i y_i, \quad x_i y_j, \quad \lambda x_i y_j, \quad \lambda_{ij} x_i y_j,$$

$$x_1 y_1 + x_2 y_2, \quad \sum_{i=1}^{n} x_i y_i, \quad \sum_{i=1}^{n} a_i x_i y_i, \quad \sum_{i,j=1}^{n} a_{ij} x_i y_j.$$

Tu se počinje posebnim oblicima a završava općim oblikom (7); naravno, λ, λ_{ij}, a_i, a_{ij} ne zavise od x_ν, y_ν.

6.2.2. *Tipični primjeri bilinearnih formi.* Skalarni produkt vektora $\vec{x}$ i vektora $\vec{y}$, odnosno vektora $\vec{x}$ i vektora $a\vec{y}$ (a je matrica) je bilinearna forma komponenata vektora $\vec{x}$ i vektora $\vec{y}$.

Produkt linearne forme komponenata vektora $\vec{x}$ i linearne forme komponenata sličnog vektora $\vec{y}$ kao i suma takvih produkata je bilinearna forma veličina x_i, y_k; to je i najopćenitiji oblik bilinearne forme.

6.3. U izrazu (7) pojavljuje se matrica a; zove se *matrica* ili *rodilja forme* (7). Možemo stvar ovako prikazati

$$\begin{array}{c|ccccc} \cdot & & & \downarrow & & \\ + & y_1 & y_2 & \cdots & y_j & \cdots \\ \hline x_1 & & & & \cdot & \\ x_2 & & & & \cdot & \\ \vdots & & & & \cdot & \\ \rightarrow x_i & \cdot & \cdot & \cdot & a_{ij} & \\ x & & & & & \end{array} \quad y$$

Tu se vidi da je a_{ij} koeficijent produkta $x_i y_j$.

6.4. No, zbrajanje u (7) možemo izvršiti i tako da zbrajamo po recima kako i pišemo. Tako npr. po prvoj liniji $\perp x$ imamo (tu je $i=1$) sumu

$$a_{11} x_1 y_1 + a_{12} x_1 y_2 + \cdots + a_{1n} x_1 y_n =$$

$$= x_1 a_{11} y_1 + a_{12} y_2 \quad + \cdots + a_{1n} y_n) = x_1 a_{1.} y;$$

tu $a_{1.} y$ predstavlja produkt od prvog retka matrice a i od y (y je stupac). Isto tako koeficijent od x_2 je $a_{2.} y$ itd.

Na taj je način čitava suma (7) oblika

$$x_1 a_{1.} y + x_2 a_{2.} y + \cdots + x_n a_{n.} y.$$

No, to je opet produkt

(8)
$$[x_1 \quad x_2 \ldots x_n] \begin{bmatrix} a_{1.} y \\ a_{2.} y \\ \vdots \\ a_{n.} y \end{bmatrix}.$$

A taj je stupac upravo $a y$.

Imamo, dakle, da je (8) jednako $x^T a y$. Zapišimo to kao

—→ 6.5. ***Teorem o prikazivanju bilinearnih formi kao skalarni, odnosno matrični produkt.*** Zadana je kvadratna matrica a s oblasti (n, n) i dva niza po n veličina:

$$\text{niz } x = (x_1, x_2, \ldots, x_n)$$

$$\text{niz } y = (y_1, y_2, \ldots, y_n).$$

Pripadni izraz

(9)
$$\sum_{i,k=1}^{n} x_i a_{ik} y_k$$

označit ćemo sa $a(x, y)$, da se vidi da on zavisi od a, x i y. Izraz (9) može se predočiti na ova četiri načina kao *matrični produkt* (ne dirajući u matricu a):

$$(10)\qquad \begin{array}{ll} x\cdot a\cdot y & x\cdot a\cdot y^T \\ x^T\cdot a\cdot y & x^T\cdot a\cdot y^T. \end{array}$$

U prva dva slučaja nužno je $x=[x_1, x_2, \ldots, x_n]$, tj. zadani niz zapisujemo kao redić; u druga dva slučaja nužno je x^T redić, tj. x je stupac

$$\begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ x_n \end{bmatrix}.$$

Što se tiče slova y u (10), ono što je poslije njegova znaka množenja $\cdot$ mora biti stupac. Množidbeni prikazi (10) formalno su različiti, no kad se umjesto slova uvedu koordinate, onda su sva četiri prikaza (10) *jednaka* u tom smislu da lijevi faktor od a svuda predstavlja istu stvar; desni također.

Specijalno, ako su $\vec{x}$, $\vec{y}$ vektori-stupci, tada *bilinearna forma* $a(x, y)$ *je isto što i skalarni produkt vektorâ* $\vec{x}$, $a\vec{y}$, pa je $a(x, y)=x^T a y=\sum_{i,j} a_{ij} x_i y_j$.

6.5.1. Primjer.

$\dot{+}$	q	r	s	
m	2	-3	5	=
n	4	9	11	
p	-35	45	91	

$$=2mq-3mr+5ms+4nq+9nr+11ns-35pq+45pr+91ps=$$

=(pazi na znak $\dot{+}$ u vanjskom uglu; on znači: množi pa zbrajaj!).

$$[m,\ n,\ p]\begin{bmatrix} 2 & -3 & 5 \\ 4 & 9 & 11 \\ -35 & 45 & 91 \end{bmatrix}\begin{bmatrix} q \\ r \\ s \end{bmatrix}=[m,\ n,\ p]\begin{bmatrix} & & \\ & & \\ & & \end{bmatrix}[q,\ r,\ s]^T=$$

$$=\begin{bmatrix} m \\ n \\ p \end{bmatrix}^T\begin{bmatrix} & & \\ & & \\ & & \end{bmatrix}\begin{bmatrix} q \\ r \\ s \end{bmatrix}=\begin{bmatrix} m \\ n \\ p \end{bmatrix} a[q,\ r,\ s]^T=\begin{bmatrix} m \\ n \\ p \end{bmatrix}^T a[q,\ r,\ s]^T.$$

6.5.2. Primjer.

$\dot{+}$	y_1	y_2	y_3	y_4	y_5
x_1	2	-3	4	7	9
x_2	12	18	20	-3	4

.

Ta forma nije kvadratna. Inače je shemom predstavljen ovaj izraz:

$$(10)\qquad x_1(\,2y_1-\,3y_2+\,4y_3+7y_4+9y_5)+$$
$$+x_2(12y_1+18y_2+20y_3-3y_4+4y_5).$$

To je linearna forma u odnosu na dvije veličine x_1, x_2 kao i u odnosu na veličine y_1, y_2, ..., y_5. Ali, treba dobro zapaziti da izraz (10) *nije linearna forma* u odnosu na *sve veličine* x_1, x_2, y_1, ..., y_5 uzete zajedno.

6.5.3. Mogu se izučavati i bilinearne forme

$$\sum_{i,j} x_i\, a_{ij}\, y_j$$

pri čemu je $i=1,\ 2,\ \ldots,\ m$; $j=1,\ 2,\ \ldots,\ n$, te $m \neq n$.

6.6. Nastajanje dvaput, triput ... linearnih formi. Iz prethodnog primjera vidimo ovo: *pođemo li od linearne forme veličina* $x_1, x_2, \ldots, x_n$ *pa koeficijente zamijenimo linearnim formama drugih n veličina* $y_1, y_2, \ldots, y_n$ *koje su nezavisne od* $x_1, x_2, \ldots, x_n$, *tada će dobiveni izraz biti* ***dvaput linearna forma*** (naime, i s obzirom na $x_1, \ldots, x_n$ kao i s obzirom na $y_1, y_2, \ldots, y_n$).

6.7. Proces možemo nastaviti: umjesto *novih koeficijenata* uvesti *linearne forme trećeg istobrojnog skupa veličina* $z_1, z_2, \ldots, z_n$. Rezultat? Slično kao maloprije: ako su novouvedeni koeficijenti kao i *z-ovi* nezavisni od *x-ova* i *y-onâ*, dobiveni će izraz biti linearna forma i prema *x*-ovima i prema *y*-onima i prema *z*-ovima (ali ne zajedno prema npr. *x* i *y* ili prema *x* i *z*).

Tako je npr. svaka determinanta linearna forma i prema elementima svakog svog stupca (retka). Dakle je determinanta *n-puta linearna forma*, naime prema *n* elemenata u *svakom* od *n* stupaca (redaka) determinante.

6.8. Problematika bilinearnih formi. Problematika koju smo obrađivali kod *kvadratnih* formi obrađuje se i za bilinearne forme, i to na posve sličan način.

Tako se npr. svaka bilinearna forma može svesti regularnim transformacijama na dijagonalni oblik: ako je forma simetrična, tj. $a^T = a$, tada se ta redukcija na dijagonalni oblik može provesti *ortogonalnom supstitucijom.*

6.9. Uvođenje novih varijabli. Ako umjesto stupca x, $x^T=[x_1, x_2, \ldots, x_n]$ i stupca y, $y^T=[y_1, \ldots, y_n]$ uvedemo istobrojni stupac x', $x'^T=[x'_1, \ldots, x'_n]$ i istobrojan stupac y', $y'^T=[y'_1, \ldots, y'_n]$ pomoću supstitucija $x=b\,x'$, $y=c\,y'$, tada od forme $a(x,\ y)=x^T a\,y$ dobivamo $(bx')^T a\,(cy')=x'^T(b^T a\,c)\,y'$, tj. izlazi *opet dvaput linearna forma*; matrica joj je $b^T a\,c$. To znači da matrice b, c možemo tako odabrati pa da nova matrica $b^T a\,c$ bude što jednostavnija. Specijalno je zanimljivo promatrati slučaj kad su matrice b, c recipročne jedna prema drugoj.

6.10. Slučaj determinanata. Kako determinanta matrice zavisi od dvije ukrštene linije matrice? Recimo da se radi o matrici a, o prvom retku $a_{1.}$ i prvom stupcu $a_{.1}$. Razvijmo determinantu po prvom retku i prvom stupcu; imamo (v. 11, § 8.8):

$$(1)\qquad \det a = a_{11}\, f\, a_{11} - \sum_{i,\,k=2}^{n} a_{i1}\, a_{1k}\,(-1)^{i+k} \det (a \setminus a_{1k} \setminus a_{i1});$$

tj. *determinanta je bilinearna forma svojih vrijednosti iz prvog retka i prvog stupca* (naravno da to vrijedi i za svaki redak i svaki stupac) (isporedi pogl. 16, § 1.12).

6.11. Adjungirane bilinearne forme. Definicija. *Adjungirana forma* zadane dvaput linearne forme jest ona kojoj je matrica adjungirana matrica matrice zadane forme (pogl. 12, § 4.2).

Na osnovu gornjeg obrasca (1) vidimo da vrijedi

6.12. Teorem. *Adjungirana forma zadane forme* $a(x, y)$ *glasi* $a^{\Gamma}(x, y)$ *i jednaka je determinanti*

$$(2) \qquad -\begin{vmatrix} 0 & x_1 & x_2 & x_n \\ y_1 & & & \\ y_2 & a & & \\ \vdots & & & \\ y_n & & & \end{vmatrix} = -\sum f a_{ki}\, x_i\, y_k = a^{\Gamma}(x, y);$$

a^{Γ} *naznačuje adjunktu matrice* a.

Adjungirana forma nastaje obrubljivanjem matrice zadane forme gore sa $x_1, x_2, \ldots, x_n$, *lijevo sa* $y_1, y_2, \ldots, y_n$ (*ne obrnuto!*) *i množenjem pripadne determinante sa* -1 (*u lijevi gornji ugao dolazi* 0).

6.13. Primjer. Naći adjungiranu bilinearnu formu forme

$$3x_1y_1 + 5x_1y_2 + 6x_2y_1 + 7x_2y_2.$$

Matrica zadane forme je

$$t = \begin{bmatrix} 3 & 5 \\ 6 & 7 \end{bmatrix};$$

obrubljivanje:

$$\begin{vmatrix} 0 & x_1 & x_2 \\ y_1 & 3 & 5 \\ y_2 & 6 & 7 \end{vmatrix}$$

i množenje sa -1:

$$-\begin{vmatrix} 0 & x_1 & x_2 \\ y_1 & 3 & 5 \\ y_2 & 6 & 7 \end{vmatrix} = 7x_1y_1 - 5x_1y_2 - 6x_2y_1 + 3x_2y_2.$$

Matrica je $\begin{bmatrix} -7 & 5 \\ -6 & -3 \end{bmatrix}$, pa adjungirana forma adjungirane forme glasi

$$-\begin{vmatrix} 0 & x_1 & x_2 \\ y_1 & -7 & 5 \\ y_2 & 6 & -3 \end{vmatrix} = 3x_1y_1 + 5x_1y_2 - 6x_2y_1 - 7x_2y_2.$$

Dakle: u našem primjeru adjungirana forma adjungirane forme jest polazna forma. Slučajnost ili pravilnost? Pokušaj promatrati opći slučaj kad je matrica kvadratna i reda 2, odnosno 3 (isp. pogl. 11, § 14.19).

6.14. Bilinearne forme i kvadratne forme. Ako imamo dva identična niza x varijabli (izrazâ) $x_1, \ldots, x_n$ tada za pripadnu skalarnu sumu

$$\sum_{i,k=1}^{n} x_i\, a_{ik}\, x_k$$

smamo matrične prikaze $x\,a\,x^T$ i $x^T\,a\,x$, već prema tome da li je x redić ili *f*tupac. Dobivamo kvadratnu formu zadanih veličina. Prema tome, *kvadratne orme su specijalan slučaj dvaput linearnih formi.* Ako je $a(x, y)$ bilinearna forma, onda je $a(x, x)$ kvadratna forma (često se označuje sa $Q(x, x)$ zbog početnog slova Q — quadratus) (isp. 16, § 8).

6.15. Funkcionalne jednadžbe za bilinearne forme $a(x, y)$. Vidi se da je

$$a(\lambda\vec{x}+\mu\vec{x},\ \vec{y}) = \lambda\, a(\vec{x},\ \vec{y}) + \mu\, a(\vec{x},\ \vec{y}) \tag{1}$$

za svaki par skalarâ λ, μ i vektora $\vec{x}$, $\vec{y}$ te

$$a(\vec{x},\ \lambda\vec{y}+\mu\vec{y'}) = a(\vec{x},\ \vec{y})\,\lambda + a(\vec{x},\ \vec{y'})\,\mu \tag{2}$$

za skalare λ, μ i vektore $\vec{y}$, $\vec{y'}$.

Dakle je forma $a(x, y)$ zaista linearno-homogena i prema prvom svojem vektor-argumentu $\vec{x}$ i prema drugom svojem vektor-argumentu $\vec{y}$. Također se vidi da je

$$a(x,\ y) = a^T(y,\ x). \tag{3}$$

Tako npr. ako se radi o matričnom prikazu $x^T\,a\,y$ za $a(x, y)$, tada je $(x^T\,a\,y)^T = y^T\,a^T\,x$; no to je baš forma $a^T(y, x)$.

6.16. Zadaci. 1. Jesu li ovi izrazi forme stupnja 2:

$$2xy-3xz+4yz, \quad 8ut-t^2, \quad ab+cd+ef?$$

2. Isto pitanje za

$$x-y, \quad x+y^2, \quad 2x^2+3xy-y^2, \quad x^2+xy^2-y^3.$$

3. Prikaži kao matrični odnosno skalarni produkt ove izraze:

$$2x-5y+4z, \quad x^2-2xy+y^2, \quad x_0^2+x_1^2+x_2^2+x_3^2,$$

$$2x_1y_2-3x_2y_1+4x_1y_1+5x_1y_2.$$

4. Nađi

$$[x_1,\ x_2,\ x_3]\begin{bmatrix} 2 & 3 & 4 \\ 0 & 1 & 2 \\ -3 & 0 & 5 \end{bmatrix}\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}.$$

5.

$\dot{+}$	y_1	y_2	y_3	
x_1	5	7	6	$=?$
x_2	8	5	8	
x_3	6	7	5	

Isto pitanje za permutiran položaj vanjskog stupca i vanjskog retka.

6.

$\dot{+}$	3	2	4
5	3	2	4
1	9	1	$5=?$
-2	3	-2	6

7. U što prelazi bilinearna forma iz zadatka 5. kad se stavi:

1)
$$x=\begin{bmatrix} 2 & 3 & 4 \\ 5 & -2 & 6 \\ 3 & 8 & 2 \end{bmatrix}x';$$

2)
$$y=\begin{bmatrix} 1 & 0 & 5 \\ 4 & 2 & 1 \\ 5 & 0 & 3 \end{bmatrix}y';$$

3) oboje?

8. Svedi bilinearnu formu $2x_1y_1-3x_1y_2+6x_2y_1-5x_2y_2$ na dijagonalan oblik.

9. Nađi adjungiranu formu forme iz zadatka 5, odnosno 8.

10. Napiši jednu formu koja je adjungirana sa samom sobom.

11. Nađi inverznu formu $a^{-1}(x,\ y)$ za formu iz zadatka 4.

7. HERMITSKE FORME

7.0. Priprava. Često imamo posla s nizovima — konačnim ili beskonačnim — kojima su vrijednosti *kompleksni brojevi*. Kad bismo za takve nizove definirali unutrašnji ili skalarni produkt na način kako se to obično radi, dobili bismo nezgodne izraze, kao npr. da bi *unutrašnji kvadrat niza* mogao biti i <0. Tako npr. za niz $3i,\ 5i,\ 4i$ skalarni „kvadrat" bio bi $(3i)^2+(5i)^2+(4i)^2=$ $=-50$. Da se tome izbjegne, *definira se hermitski produkt dvaju nizova* (vektora i sl.) kompleksnih brojeva (pogl. 10, § 7.4), a onda izgrađuje čitava teorija analogna onoj za skalarno *obično* množenje. Zato ćemo se ovdje moći služiti pojedinim pojmovima, a da ih i ne definiramo posebno.

7.1. Hermitsko množenje nizova (vektora). Hermitski produkt dvaju *kompleksnih brojeva* z, z' definira se kao $z\overline{z'}$[1] i označuje sa $\mathrm{H}(z, z')$, $z\,\mathrm{H}\,z'$ ili (z, z'), tj. $z\,\mathrm{H}\,z' = z\overline{z'}$, npr.

$$(2+5i)\,\mathrm{H}\,(4-2i) = (2+5i)(4+2i) = -2+24i.$$

7.1.1. Definicija. (pogl. 10, § 7.4). *Hermitski produkt dvaju istobrojnih vektora* x, y definira se kao matrični produkt $y^* x$; pri tom je $y^* = \overline{y^T}$; označuje se također i pomoću zagrade, i to ovako $\mathrm{H}(x, y)$ ili (x, y) ili $x\,\mathrm{H}\,y$. Dakle

$$\mathrm{H}(x, y) = x\,\mathrm{H}\,y = (x, y) = y^* x.$$

Specijalno,

$$(x, x) = x^* x.$$

7.2. Lako se provjerava da za brojeve vrijede ova pravila:

$$z\,\mathrm{H}\,z' = \overline{z'\,\mathrm{H}\,z}$$

$$(cz)\,\mathrm{H}\,z' = c(z\,\mathrm{H}\,z')$$

$$(cz)\,\mathrm{H}\,z' = z\,\mathrm{H}(\bar{c}z').$$

Primjer. Nađi (u, v) ako je $u = \begin{bmatrix} 3-2i \\ 4i \end{bmatrix}$, $v = \begin{bmatrix} 4+5i \\ 3+i \end{bmatrix}$. Bit će

$$(u, v) = (3-2i)(4-5i) + 4i(3-i) = 6-11i:$$

ili matrično:

$$u^* = [3+2i,\ -4i] \qquad v^* = [4-5i,\ 3-i].$$

$$(u, v) = v^* \cdot u = [4-5i,\ 3-2i] \begin{bmatrix} 3-2i \\ 4i \end{bmatrix} =$$

$$= [(4-5i)(3-2i) + (3-i)\,4i] = [6-11i]^{2)} = 6-11i.$$

Analogno

$$(v, u) = (4+5i)(3+2i) + (3+i)(-4i) = 6+11i.$$

Dakle je

$$(u, v) = \overline{(v, u)}.$$

Hermitsko množenje *brojeva* prenosi se i na skalarno-hermitsko množenje *nizova* na odgovarajući način.

7.3. Definicija. **Hermitski produkt niza** $(x_1, x_2, \ldots)$ i niza $(y_1, y_2, \ldots)$ jest izraz $x_1\overline{y_1} + x_2\overline{y_2} + \cdots$; označuje se sa

$$(x_1, x_2, \ldots)\,\mathrm{H}\,(y_1, y_2, \ldots).$$

---

[1] Dobro je izraz $z\overline{z'}$ usporediti s izrazom $z-z'$ (znak — se nalazi *iznad* z' umjesto *iznad* z).

[2] Znajmo da je za svaki skalar s po definiciji $[s] = s$.

Dakle

$$(x_1,\ x_2,\ \ldots)\,\mathrm{H}\,(y_1,\ y_2,\ \ldots) = x_1\,\overline{y}_1 + x_2\,\overline{y_2} + \cdots$$

Analogno

$$\begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \end{bmatrix} \mathrm{H} \begin{bmatrix} y_1 \\ y_2 \\ \cdot \\ \cdot \end{bmatrix} = [y_1,\ y_2,\ \ldots]^{\star} \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \end{bmatrix} = y^{\star}\,x = x^{T}\,\vec{y}.$$

Tako se *hermitsko množenje izražava matričnim množenjem*. Prema tome, matrični je oblik različit već prema tome da li se radi o redićima ili stupcima.

7.4. K o n v e n c i j a. Bez obzira na to o kakvu se obliku radi, kod hermitskog produkta dvaju izraza sprezanje se izvodi na ***drugom*** izrazu, tj. na y, ako se radi o $x\,\mathrm{H}\,y$. To je važno da se izbjegne nesporazum!

7.4.1. Umjesto $x\,\mathrm{H}\,y$ specijalno fizičari pišu $(x,\ y)$, pogotovu ako su x, y vektori.

7.5. Na osnovu definicije lako se dokazuju ove činjenice:

7.5.1. Spregnuta komutativnost:

$$(x,\ y) = \overline{(y,\ x)},$$

tj.

$$x\,\mathrm{H}\,y = \overline{y\,\mathrm{H}\,x}.$$

7.5.2. $$(c_1\,x_1 + c_2\,x_2)\,\mathrm{H}\,y = c_1\,(x_1\,\mathrm{H}\,y) + c_2\,(x_2\,\mathrm{H}\,y)$$

za proizvoljne skalare c_1, c_2 i vektore x_1, x_2, y; ili ovako:

$$(c_1\,x_1 + c_2\,x_2,\ y) = c_1\,(x_1,\ y) + c_2\,(x_2,\ y).$$

Odnosno matrično:

$$y^{\star}\,(c_1\,x_1 + c_2\,x_2) = c_1\,(y^{\star}\,x_1) + c_2\,(y^{\star}\,x_2).$$

7.5.3. T e o r e m. $(c_1\,y_1 + c_2\,y_2)^{\star}\,x = c_1^{\star}\,(y_1\,x) + c_2^{\star}\,(y_2\,x)$; c_1, c_2 su skalari, x_1, x_2, y su vektori. Ili ovako:

$$x\,\mathrm{H}\,(c_1\,y_1 + c_2\,y_2) = \vec{c}_1\,(x\,\mathrm{H}\,y_1) + \vec{c}_2\,(x\,\mathrm{H}\,y_2),$$

odnosno

$$(x,\ c_1\,y_1 + c_2\,y_2) = \vec{c}_1\,(x,\ y_1) + \vec{c}_2\,(x,\ y_2).$$

Gornji obrasci izlaze neposredno iz definicije 7.3.

Tako je npr. prvi obrazac neposredna posljedica pravila da je sprezanje $z \to \overline{z}$ distributivna operacija prema zbrajanju i prema množenju kompleksnih brojeva. Zato npr. spregnut broj od produkta $\overline{(3+2i)}\,(4-2i)$ jest produkt $(3+2i)\,\overline{(4-2i)}$; a spregnut izraz sume $m+n$ jest $\overline{m}+\overline{n}$.

Primijetimo da za kompleksni broj a znak $a^{\star}$ predstavlja broj koji je sa a konjugiran (spregnut), tj. $a^{\star} = \overline{a}$.

7.6. Hermitski produkt vektora za zadanu vektorsku bazu. Posebno, ako je izabrana vektorska baza $e=(e_1\, e_2 \ldots e_n)$ pa ako je

$$x=\sum_{i=1}^{n} x_i\, e_i,\ y=\sum_{i=1}^{n} y_i\, e_i,$$

tada kao posljedicu gornje definicije i gornjih obrazaca imamo:

$$(x,\, y)=(\Sigma\, y_i\, e_i)^{\star}\,(\Sigma\, x_i\, e_i)=\sum_i (y_i\, e_i)^{\star}\,\Sigma\, x_i\, e_i=$$

$$\Sigma\, e_i^{\star}\, y_i^{\star}\,\Sigma\, x_k\, e_k=\Sigma\,(e_i^{\star}\, y_i^{\star}\, x_k\, e_k)=\Sigma\,(e_i^{\star}\, e_k)\, y_i^{\star}\, x_k,$$

tj.

$$(x,\, y)=y^{\star}\, x=\Sigma\,(e_i^{\star}\, e_k)\, y_i^{\star}\, x_k=\Sigma\, y_i^{\star}\,(e_i^{\star}\, e_k)\, x_k.$$

Dakle vrijedi ovaj

⟶ **7.6.1.** Teorem. *Hermitski produkt dvaju vektora-stupaca jest bilinearna forma konjugiranih komponenata drugog vektora i komponenata prvog vektora. Matrica a forme definirana je ovako: $a_{ik}=e_i^{\star}\, e_k$. U specijalnom slučaju, kad je baza ortonormirana, tj. kad je $e_i^{\star}\, e_k=\delta_k^i=\begin{matrix}1 & za\ i=k\\ 0 & i\neq k\end{matrix}$, hermitski produkt vektorâ jest jedinična bilinearna forma.*

7.7. Hermitske kvadratne i hermitske bilinearne forme. Ti se pojmovi definiraju slično kao obične kvadratne i bilinearne forme — samo što umjesto skalarnog produkta i množenja dolazi hermitski produkt i hermitsko množenje.

7.7.1. Definicija hermitski građene kvadratne forme. Neka je zadana kvadratna matrica a s vrijednostima koje su kompleksne, i niz od $(\mathrm{st}\, a=)\, n$ *veličina* $x_1,\ x_2,\ \ldots,\ x_n$ (varijable ili kakve nepoznate veličine); tada se pod *hermitski građenom kvadratnom formom s matricom a* razumjeva hermitski produkt vektora ax i vektora x tj. izraz

$$(1)\qquad (a\vec{x},\ \vec{x})=x^{\star}\, a\, x=\sum_{i,\,j} a_{ij}\,\overline{x_i}\, x_j=\sum_{i,\,j=1}^{n}\overline{x_i}\, a_{ij}\, x_j.$$

7.7.2. Definicija hermitskih i kosohermitskih kvadratnih formi. To su one forme kojima je matrica hermitska, odnosno kosohermitska.

Ako se ne kaže obrnuto, tada se podrazumijeva da je forma građena na hermitski način.

Prema tome, hermitska (kosohermitska) forma je izraz oblika

$$(a\vec{x},\ \vec{x})=\Sigma\, a_{ij}\,\overline{x_i}\, x_j \quad \text{uz uslov} \quad a^{\star}=a \quad (\text{odnosno} \quad a^{\star}=-a).$$

Hermitske (tj. hermitski simetrične), odnosno kosohermitske kvadratne forme logički su pandan simetričnim (kososimetričnim) kvadratnim formama u realnom području.

7.7.3. Primjeri.

$$(2+4i)(x_1^2-y_1^2)+(5-3i)(x_1+y_1 i)(x_2-y_2 i)+(8-2i)(x_2^2-y_2^2)$$

je jedna hermitski građena kvadratna forma s obzirom na dvije veličine

$$x_1 + iy_1,\ x_2 + iy_2.$$

7.7.4. Primjer matrice

$$m = \begin{bmatrix} 2+4i & 5-3i \\ 4-7i & 8-2i \end{bmatrix}$$ i veličinâ $z_1 = x_1 + iy_1,\ z_2 = x_2 + ix_2$.

Pripadna kvadratna forma građena na hermitski način glasi.

(1)
$$z_1 m_{11} \bar{z}_1 + z_1 m_{12} \bar{z}_2 + z_2 m_{21} \bar{z}_1 + z_2 m_{22} \bar{z}_2 = \cdots =$$
$$= (2+4i)(x_1^2 + y_1^2) + (9-10i) x_1 x_2 + (-4+i) x_1 y_2 +$$
$$+ (4-i) x_2 y_1 + (9-10i) y_1 y_2 + (8-2i)(x_2^2 + y_2^2).$$

Rastavimo matricu m na njen hermitsko simetrični dio h (tj. $h^\star = h$), kosohermitski dio k (tj. $k^\star = -k$):

$$m^\star = \begin{bmatrix} 2-4i & 4+7i \\ 5+3i & 8+2i \end{bmatrix},$$

$$h = \frac{1}{2}(m + m^\star) = \begin{bmatrix} 2 & \frac{9}{2}+2i \\ \frac{9}{2}-2i & 8 \end{bmatrix},$$

$$k = \frac{1}{2}(m - m^\star) = \begin{bmatrix} 4i & \frac{1}{2}-5i \\ -\frac{1}{2}-5i & -2i \end{bmatrix}.$$

Time se i forma (1) rastavlja u formu s matricom h i preostatak s matricom k. Nađimo ovaj posljednji dio:

$$\bar{z}_1 k_{11} z_1 + \bar{z}_1 k_{12} z_2 + \bar{z}_2 k_{21} z_1 + \bar{z}_2 k_{22} z_2 =$$
$$= (\text{zbog } k^\star_{21} = -k_{12} \text{ te zbog } z_1 \bar{z}_2 = \overline{\bar{z}_2 z_1}) =$$
$$= (x_1^2 + y_1^2)\, 4i + (x_2^2 + y_2^2) \cdot -2i + (\bar{z}_1 k_{12} z_2 - \overline{\bar{z}_1 k_{12} z_2}).$$

Ta zagrada kao razlika spregnutih brojeva iznosi dvostruk imaginarni dio prvog broja. To se lako nađe. Na taj način vidimo da je *vrijednost kosohermitske forme uvijek čisto imaginarna*. Zaključak je, naime, isti i u općem slučaju.

Pogledajmo kako je s vrijednosti forme ako je matrica h hermitska: $h^\star = h$.

Izračunajmo ovo:

$$\bar{z}_i h_{ik} z_k + \bar{z}_k h_{ki} z_i = \bar{z}_i h_{ik} z_k + \overline{z_k h_{ik}} z_i = \bar{z}_i h_{ik} z_k + \overline{\bar{z}_i h_{ik} z_k};$$

ovo je, dakle, realno za svako i, k. A baš od takvih se dijelova sastoji čitava forma. Zapišimo taj rezultat:

⟶ Teorem. *Ako je kvadratna matrica a hermitski simetrična, tj.* $a^* = a$, *onda je vrijednost pripadne hermitske kvadratne forme realna tj.*

$$\sum \bar{x}_i a_{ik} x_k \tag{1}$$

je realan broj za svaki izbor kompleksnih brojeva $x_1, \ldots, x_n$.

Ako je $a^* = -a$, *tada je vrijednost odgovarajuće forme* (1) *čisto imaginarna.*

7.8.2. Teoremi o dijagonalizaciji, inerciji, ... prenose se bez daljega na hermitske forme; pri tom umjesto kvadratnih članova x_i^2 kod običnih forama treba razmatrati produkt $x_i \bar{x}_i$ kod hermitskih forama. Važno je da i kod hermitskih formi na dijagonali dijagonalnog oblika dolaze samo ***realni*** koeficijenti (pogl. 26, § 10).

7.9. Hermitski građene bilinearne forme. Ako imamo dva istobrojna niza

$$x = (x_1, x_2, \ldots, x_n)$$

$$y = (y_1, y_2, \ldots, y_n)$$

i matricu a reda n, tada se pod *hermitski građenom pripadnom bilinearnom formom* razumijeva skalarni produkt

$$(ay, x) \equiv (ay)\,\mathrm{H}\,x = \sum a_{ik} \bar{x}_i y_k = \sum \bar{x}_i a_{ik} y_k \tag{2}$$

(pazi na raspored indeksa i na potez!).

$$(ay, x) = \bar{x}\, a\, y^T; \tag{3}$$

to znači da su x i y stupci, tj. specijalno svaka kvadratna hermitska forma zadanih veličina jest bilinearna forma istih veličina. Bilinearna forma je hermitska (kosohermitska), ako joj je takva matrica.

7.10. Uvođenje novih veličina (varijabli). Ako imamo bilinearnu formu (3) provedimo supstitucije prikazane matrično obrascima

$$x = bx', \quad y = cy'; \tag{4}$$

iz (4) izlazi da su x i y stupci!).

Uvrštenjem ovih izraza u definicioni izraz (2), odnosno $(3)_2$ lako se uvjerimo da dobivamo opet bilinearnu formu s obzirom na x' i y', odnosno s obzirom na $x_1', x_2', \ldots, x_n'$ i $y_1', \ldots, y_n'$.

Radeći matrično (i recimo sa stupcima), tada imamo ovo:

$$(ay,\ x) = (\text{prema (3), jer promatramo slučaj redaka}) =$$

$$= x^{\star}\, ay = (bx')^{\star}\, a\,(c\,y') = (\text{to je matrično množenje}) = x'^{\star}\, b^{\star}\, a\, c\, y',$$

tj.

$$(ay)\,\mathrm{H}\,x = x'^{\star}\,(b^{\star}\, a\, c)\, y'.$$

7.11. Kongruentnost. Matrica nove forme glasi $b^{\star}\, a\, c$. U specijalnom slučaju, ako je $b = c$, nova matrica glasi $b^{\star}\, a\, b$ (kaže se da je nova matrica *hermitski kongruentna sa starom*).

7.12. Jedinična bilinearna hermitska forma. Vrlo je zanimljiv i važan slučaj kad imamo *jediničnu bilinearnu formu* $\sum_i \overline{x_i}\, y_i = y\,\mathrm{H}\,x$. Nova matrica, po supstituciji (4), glasi

$$b^{\star}\, ac = b^{\star}\, c;$$

zahtjev da to bude jedinična matrica, tj. da bude

$$b^{\star}\, c = 1,$$

dovodi do *kontragredijentne veze matrica b i c*. I jedino ako su transformacione matrice međusobno *kontragredijentne*, prevest će one jediničnu bilinearnu formu opet u jediničnu bilinearnu formu.

7.13. *Kvadratne i bilinearne forme s beskonačno mnogo varijabla.* Oblika su

$$\sum_{i,j} a_{ij}\, x_i\, x_j \quad \text{odnosno} \quad \sum_{i,j} a_{ij}\, x_i\, y_j,$$

pri čemu indeksi i, j prolaze skupom svih prirodnih pa i skupom svih cijelih brojeva. Tu vrstu formi uveo je Hilbert početkom ovog stoljeća[1]. Teorija kvadratnih i bilinearnih formi s beskonačno mnogo varijabla razvila se u vanredno opsežnu i važnu matematičku granu; odraz te teorije je i pojam Hilbertova prostora koji na prirodan način poopćuje pojam Euklidova odnosno Descartesova prostora od n dimenzija.

7.14. Zadaci o hermitskim formama.

1. Nađi hermitski produkt ovih nizova a i b:

   1) $a = 2-3i,\ 3+i,\ b = 4,\ 5i$; 2) $a = 2+3i,\ 3-4i,\ i$
   $b = 1-i,\ 3+4i,\ 2i$;

   3) $5-2i,\ 4i,\ 6-2i$
   $5-2i,\ 6-2i,\ 4i$;

   4) $5-2i,\ 4i,\ 6-2i$
   $4i,\ 5-2i,\ 6-2i$.

2. Zadan je tročlan niz $2-i,\ 3+4i,\ -5+2i$; promatraj permutacije toga niza i tablicu hermitskog množenja među tim nizovima.

---

[1] Riječ je o 6 naučnih radova koje je veliki njemački matematičar David Hilbert (23. 01. 1862—1943) objavio u Göttinger Nachrichten u vremenu od 1904—1910. Isp. David Hilbert, Gesammelte Abhandlungen III 1935.

3. Nađi hermitski građenu kvadratnu formu kojoj je matrica:

$$1)\begin{bmatrix}1 & i\\ i & 1\end{bmatrix},\quad 2)\begin{bmatrix}i & 1\\ 1 & i\end{bmatrix},\quad 3)\begin{bmatrix}2+3i, & 3-i\\ 1 & i\end{bmatrix},\quad 4)\begin{bmatrix}3-i & 5\\ -5 & 4i\end{bmatrix},$$

$$5)\begin{bmatrix}2-3i & 5+i\\ 4+5i & 7-2i\end{bmatrix},\quad 6)\begin{bmatrix}5 & 2+i\\ 2-i & 6\end{bmatrix},\quad 7)\begin{bmatrix}4 & 3+4i\\ 3-4i & 0\end{bmatrix},$$

$$8)\begin{bmatrix}0 & 3+4i\\ -3+4i & 0\end{bmatrix},\quad 9)\begin{bmatrix}0 & -2-i\\ 2-i & 0\end{bmatrix}.$$

Nađi hermitski i kosohermitski dio te forme te obje hermitske komponente te forme (isp. zadatak 7).

4. Nađi hermitski građenu bilinearnu formu kojoj je matrica ona iz zad. 3.

5. Svedi na dijagonalni oblik forme iz zad. 3.

6. Svedi na dijagonalni oblik forme iz zad. 4.

7. *Hermitske komponente kvadratne matrice a* zovu se *hermitske* matrice a_1, a_2 za koje je $a=a_1+ia_2$. Analogno se govori o hermitskim komponentama kvadratne, odnosno bilinearne forme. Dokaži:

$$1)\ a_1=\frac{1}{2}(a^\star+a),\quad a_2=\frac{1}{2i}(a^\star-a);\quad 2)\ a\,a^\star=a^\star a \Leftrightarrow a_1\,a_2=a_2\,a_1$$

tj. kvadratna matrica je normalna onda i samo onda ako njene hermitske komponente komutiraju.

8. VEZA IZMEĐU KVADRATNIH I BILINEARNIH FORAMA

8.1. Ako bilinearnu formu

$$(1)\qquad \sum_{i,k=1}^{n} x_i\,a_{ik}\,y_k$$

označimo simbolički sa $a(x,y)$, onda znamo da se funkcionalni izraz $a(x,\ y)$ može nadomjestiti *matričnim* množenjima (§ 6.5).

U drugu ruku, jasno je da je kvadratna forma $a(x,\ y)$ specijalan slučaj bilinearne forme (to je onaj posebni slučaj kad je $x=y$).

8.2. Polarna forma. Dokažimo sad obratno kako je *uz svaku kvadratnu formu*

$$(2)\qquad Q(x,\ x)=\sum x_i\,a_{ik}\,x_k$$

na prirodan način vezana bilinearna forma $Q(x,\ y)$ *s istom matricom* Q; ova se bilinearna forma zove *polarna forma* u odnosu na promatranu kvadratnu formu[1])

[1]) Naziv je u vezi s činjenicom da polara tačke $x_0:y_0:z_0$ u odnosu na konični presjek

$$[x,\ y,\ z]\ a\begin{bmatrix}x\\ y\\ z\end{bmatrix}=0 \text{ glasi } [x_0,\ y_0,\ z_0]\ a\begin{bmatrix}x\\ y\\ z\end{bmatrix}=0$$

(razmatraju se homogene koordinate; isp. R. Cesarec [1], str. 356, B. N. Rašajski [1]. str. 128).

Nađimo *što kvadratna forma radi s linearnim spojem*

$$rx+sy \tag{3}$$

proizvoljnih vektora x, y (r, s su skalari).

8.3. Radimo matrično i odlučimo se, recimo, na ovakav zapis:

$$Q(x,\ x)=x^T Q\, x \qquad \text{(tj. } x \text{ je stupac).} \tag{4}$$

$$Q(rx+sy,\ rx+sy)=(rx+sy)^T\cdot Q\cdot(rx+sy)=$$
$$=(\text{to su sve matrice!})=(x^T r+y^T s)(r\,Q\,x+Qsy)=$$
$$=x^T r\,Q\,rx+x^T r\,Q\,sy+y^T s\,Q\,r\,x+y^T s\,Q\,sy=$$
$$=r^2 x^T Q\,x+rs\,(y^T Q\,x+x^T Qy)+s^2 y^T Q\,y=$$
$$=r^2 Q(x,\ x)+rs\,Q(x,\ y)+rs\,Q(y,\ x)+s^2 Q(y,\ y).$$

No, matrica Q je simetrična; zato je $Q(y,\ x)=Q(x,\ y)$, pa gornji rezultat postaje

8.4. Teorem. Za svaku kvadratnu formu $Q(x,\ x)$ vrijedi

$$Q(rx+sy)=r^2 Q(x,\ x)+2rs\,Q(x,\ y)+s^2 Q(y,\ y)$$

(r, s su skalari, x, y su vektori).

Specijalno:

$$Q(rx,\ rx)=r^2 Q(x,\ x) \qquad (s=0);\quad (r=1=s):$$
$$Q(x+y,\ x+y)=Q(x,\ x)+2Q(x,\ y)+Q(y,\ y).$$

Eto, tako vidimo kako se dvaput linearna forma $Q(x,\ y)$ prikazuje pomoću kvadratnih formi:

$$2Q(x,\ y)=Q(x+y,\ x+y)-Q(x,\ x)-Q(y,\ y). \tag{5}$$

8.5. Slučaj hermitske forme. Na sasvim sličan način, polazeći od hermitske forme

$$\sum \overline{x_i}\, h_{ik}\, x_k=x^*\, hx,\ h^*=h$$

imamo po redu:

$$(rx+sy)^*\cdot h\cdot(rx+sy)=(x^*\, r^*+y^*\, s^*)(hrx+hys)=$$
$$=rr^*\, x^*\, hx+sr^*\, x^*\, hy+rs^*\, y^*\, hx+ss^*\, y^*\, hy.$$

Specijalno, za $r=s=1$ imamo tako obrazac:

$$(x+y)^*\, h\,(x+y)=x^*\, hx+x^*\, hy+y^*\, hx+y^*\, hy, \tag{6}$$

kojim se povezuje hermitska dvaput linearna forma $x^*\, hy$ s kvadratnim formama. No, $y^*\, hx=\overline{x^*\, h^*\, y}=(\text{radi } h^*=h)=\overline{x^*\, hy}$, pa je

$$x^*\, hy+y^*\, hx=x^*\, hy+\overline{x^*\, hy}-2\,Re\,(x^*\, hy).$$

Na taj način relacija (6) postaje

$$Re\, x^* hy = \frac{1}{2}[(x+y)^* h(x+y) - x^* hx - y^* hy] \equiv F(x, y).$$

Odatle se može dobiti

$$x^* hy = F(x, y) + iF(ix, y),$$

jer za svaki kompleksni broj z imamo $z = \mathrm{Re}\, z + i\,\mathrm{Re}(-iz)$.

Za jediničnu matricu $h = 1$ znači to da je

$$x^* y = \frac{1}{2}[(x+y)^* (x+y) - x^* x - y^* y] +$$

$$+ \frac{i}{2}[(ix+y)^* (ix+y) - (ix)^* (ix) - y^* y].$$

Time je skalarni produkt $x^* y$ izražen pomoću normi:

$$2\, x^* y = N(x+y) - Nx - Ny + iN(ix+y) - iN(ix) - iNy.$$

U realnom području bit će

$$x^T y = \frac{1}{2}(x+y)^T (x+y) - x^T x - y^T y,$$

$$2\, x^T y = N(x+y) - Nx - Ny.$$

9. DODATNI ZADACI O KVADRATNIM I BILINEARNIM FORMAMA

1. Slijedeću kvadratnu formu svedi na normalni oblik; odredi pripadne linearne transformacije te rang i signaturu forme:

   1) $xy + yz + zx$; 2) $x^2 + 2xy + 2y^2 + 4yz + 5z^2$;

   3) $x^2 + xz + yt - t^2$; 4) $x^2 + 2y^2 - xy + xz + z^2$;

   5) $x^2 + xy + zt$; 6) $x^2 + xy + yz - z^2$.

2. Zadana je kvadratna forma $x_1^2 + x_2^2 + \cdots + x_n^2 + (x_1 + x_2 + \cdots + x_n)^2$;
   1) nađi matricu i signaturu te forme;
   2) svedi je na kanonski oblik. Specijaliziraj je za $n = 2$ i $n = 3$.

3. Slijedeću bilinearnu formu svedi na kanonski oblik i odredi pripadne linearne transformacije varijabli:

   1) $x_2 y_1 + 2 x_1 y_2$; 2) $2 x_1 y_2 - 3 x_2 y_1 + x_1 y_3$; 3) $x_1 y_1 + 3 x_1 y_3 -$
   $- x_2 y_1 + x_2 y_3$; 4) $5 x_1 y_1 + 2 x_1 y_2 - 3 x_1 y_3 + 5 x_2 y_1 - 4 x_2 y_3$;

   5) $3 x_1 y_2 - 5 x_1 y_3 + 4 x_2 y_1 - 5 x_3 y_4$.

4. Isto pitanje za ove dvaput linearne forme:

1) $f_1 = x_1 y_1 + 3 x_1 y_2$; 2) $f_2 = f_1 - 2 x_1 y_3$; 3) $f_3 = f_2 + 5 x_1 y_4$;

4) $f_4 = f_3 - x_2 y_1$; 5) $f_5 = f_4 + 3 x_2 y_3$; 6) $f_6 = f_5 - 8 x_2 y_2$;

7) $f_7 = f_6 + x_3 y_1$; 8) $f_8 = f_7 - 6 x_3 y_4$; 9) $f_9 = f_8 + x_4 y_1$;

10) $f_{10} = f_9 + 5 x_4 y_2$; 11) $f_{11} = f_{10} = 4 x_4 y_3$.

5. Napiši matrice bilinearnih formi iz zad. 4.

6. Kako glase polarne forme kvadratnih formi u zad. 1?

7. Kako glasi kvadratna forma kojoj je polarna forma zadana u zad. 3?

8. *O polarnoj formi* 1) Polarna forma $ax \circ y$ kvadratne forme

$$Q = ax \circ x \text{ glasi } \frac{1}{2} y_1 \frac{\partial Q}{\partial x_1} + \frac{1}{2} y_2 \frac{\partial Q}{\partial x_2} + \cdots + \frac{1}{2} y_n \frac{\partial Q}{\partial x_n};$$

dokaži (isp. § 3.2); 2) svaka simetrična bilinearna forma je polarni oblik jedne kvadratne forme; 3) varijable u kvadratnoj formi i u pripadnoj polarnoj formi podvrgni nekoj transformaciji koja je linearno-homogena; polarni oblik nove kvadratne forme podudara se s odnosnim transformatom stare polarne forme (zato se polarni oblik zove kovarijanta kvadratne forme).

9. Matrici a ranga $r(:=r(a)) \neq 0$ pridruži matricu $a(r)$ determinanata *svih* (r, r)-podmatrica od a; dokaži da je $r(a(r)) = 1$. Pri tom naravno, ako su x, y dvije (r, r)-podmatrice od a za koje je $D_1 x = D_1 y$ (odnosno $D_1 x \neq D_1 y$), tada $\det x$ i $\det y$ će biti (neće biti) u istom retku matrice $a(r)$; slično za stupce.

10. Na osnovu činjenice 9. dokaži da svaka simetrična matrica a sadržava bar jednu regularnu ***glavnu*** (r, r)-podmatricu; primjeni to na kvadratne forme.

11. Provedi razmatranja u § 8.3—§ 8.5 uz pretpostavku da su vektori x, y zapisani kao redići.

Literatura: Vidjeti na koncu poglavljâ: 8, 10, 11, 12, 13, 14, 15.

POGLAVLJE 17.

TEORIJA GRUPA

0. UVODNA RAZMATRANJA

0.0. U teoriji grupa učimo se najraznovrsnijim transformacijama, povezivanjima, računanjima. Pri tom je bitno ovo pitanje: *ako pođemo od stanovitih podataka iz neke množine M, pita se da li se i pripadni rezultat nalazi u istoj množini.* Možemo kraće govoriti o »*unosu*« ili podacima i »*iznosu*« ili rezultatima ili proizvodima i pitati se da li je proizvod u istom području odakle su i podaci.

To je tzv. *grupoidno* pitanje. Kao tipičan primjer da iznos ili proizvod leži u području unosa spomenimo ove primjere:

1. Skup N svih prirodnih brojeva i zbrajanje u njemu; „iznos" ili „proizvod" (suma dvaju prirodnih brojeva) leži u N.

2. Sve rotacije ravnine α oko zadanog središta O iz α obrazuju skup $(\alpha; O)$: dvije rotacije r, s izvršene uzastopno oko O mogu se nadomjestiti jednom rotacijom t ravnine α oko O; simbolički: r pa s daje t; dakle $sr = t$.

3. Kao primjer razmatranja kad odgovor nije vidljiv naprečac možemo promatrati opet ravninu α i skup $[\alpha]$ svih njenih rotacija (dakle se ne radi samo o rotacijama oko jednog te istog središta). Je li sada iznos u $[\alpha]$, odnosno je li proizvod od dvije uzastopne rotacije ravnine α opet jedna rotacija te ravnine? Jest, ali dokaz nije očigledan! Pri tom i translaciju ravnine shvatamo kao rotaciju.

4. Isto vrijedi za skup A (odnosno A_n) svih brojeva koji zadovoljavaju bar jednu normiranu jednadžbu (zadanog stupnja n) oblika $a_0 + a_1 x + a_2 x^2 + \cdots + x^n = 0$ s *cjelobrojnim* koeficijentima. A (odnosno A_n) se zove skup *cijelih algebarskih* brojeva (stupnja n). Pokušaj slučaj $n = 1$ i 2!

5. Kao primjer kad je odgovor *uslovan* spomenimo par $(N, -)$ množine N svih prirodnih brojeva te *oduzimanje* u N: ako je $x \in N$ i $y \in N$, onda „iznos" ili „proizvod" $x - y$ može ali ne mora biti u N.

6. Kao tipičan i za mnoge zagonetan slučaj da rezultat leži izvan oblasti podataka spomenimo *skup S negativnih brojeva i množenje*: za $x \in S$, $y \in S$ proizvod [umnožak] xy nikad nije u S.

Pri svim tim i mnogim drugim situacijama *radi se o nekoj množini M i poslu da za* ***svaku uređenu dvojku*** *x, y iz M, kao unose, nađemo pripadni iznos ili proizvod i da se pitamo da li taj iznos leži ili ne leži u M.* Ako *da,* onda se govori o nekoj *zatvorenosti unutar M* u odnosu na promatrani posao ili operaciju: *tehnički se govori o grupoidu,* kao što ćemo to sada utanačiti.

Ali prije toga evo jedan zanimljiv primjer na kojem se vide glavne ideje-vodilje u teoriji grupa.

0.1. Vodeći primjer o „računanju". Možemo li u zadanoj ravnini R^2 „računati"? Pokušajmo npr. ovako. Odaberimo u ravnini proizvoljnu tačku O; nadalje, za svaki nađeni par tačaka A, B neka $A+B$ bude tačka koja je simetrična slika od O prema središtu $\frac{A+B}{2}$ odreska AB (posebno, $A+A$ će značiti simetričnu sliku od O u odnosu na A kao središte simetrije).

0.1.1. Je li proizvod $A+B$ operacije + uvijek određen time što znamo oba podatka A, B? Jest! I k tome je u R^2. Npr. $A+A$ je takva tačka da je A sredina odreska s krajevima O i $A+A$: treba, dakle, segment OA produžiti preko A upravo za $\overline{OA}$. Kraj je $A+A$.

0.1.2. Koliko je npr. $O+A$? „Računajmo"! Središte odreska OA je određeno, a ogledalna slika od O prema njemu je A; dakle, $O+A=A$; isto tako $A+O=A$; specijalno je $O+O=O$.

0.1.3. Što znači da je $A+B=O$? Znači da je „iznos" O; no „iznos" O je simetrična slika od O; znači da je središte simetrije $A+B$ moralo biti u O; a to znači da je O središte odreska AB. Rezultat je ovaj: relacija $A+B=O$ u *našoj »algebri«,* tj. *u ovom primjeru,* znači da su tačke A, B položene simetrično prema istaknutoj tački O (nazovimo to O *»nulom«*). Zato je A određeno iz B, a B iz A, i to simetrijom na O.

Da to istaknemo, možemo umjesto

$$A+B=O \qquad \text{pisati}$$

$$A=O-B \qquad \text{ili naprosto}$$

$$A=-B.$$

Prema tome, znak — pred oznakom B tačke znači ovdje *simetričnu sliku od B prema O.* Koliko je $--B$? Naravno B, jer slika $---B$ slike $-B$ od B je opet B (crtaj!!).

Uopće, umjesto

$$a+b=c$$

pišemo

$$a=c-b.$$

Provjeri da je $$c-b=c+(-b).$$

Provjeri da je $$-(a+b)=(-a)+(-b)$$

$$-(a-b)=(-a)+b.$$

Također je $$a+b=b+a.$$

0.1.4. Najzad se na osnovu zaključaka elementarne geometrije „vidi“ da je

$$(a+b)+c=a+(b+c).$$

0.1.5. Na taj način vidimo da formalno za *zbrajanje i oduzimanje* u ravnini R^2 vrijede naša svakodnevna pravila; ulogu »*nule*« ima ona istaknuta tačka O (opravdanije je element O iz M zvati *neutrum*, jer je O zaista istaknuta u čitavu sklopu „računanja“).

0.1.6. Tako vidimo da zaista, na taj način, *možemo računati u svakoj ravnini*. Pa čak u istoj ravnini možemo računati na bezbroj načina — računanje zavisi od izabrane „nule“ (mi ćemo je ipak radije zvati „neutrum“ ili neutralni član). No, ipak su sva ta zbrajanja i oduzimanja *slična*, »*izomorfna*« među sobom.

0.1.7. Ako u tom računanju podatke uzimamo uvijek i jedino s nekog pravca ili pravulje p kroz O, i rezultati će biti na p; *zato je zbrajanje i oduzimanje na p upravo vjerna slika zbrajanja i oduzimanja realnih brojeva.*

0.1.8. Pa kao što se prve dvije računske operacije „izomorfno“ ogledaju na računanju na pravulji p, tako je gornje računanje u ravnini „izomorfni“ nosilac pravilnosti ili prava ogledalna slika računanja u skupu — kompleksnih brojeva (za prve dvije operacije $+$, $-$ dovoljno je sa 1 označiti *proizvoljnu tačku* iz $R^2 \setminus \{O\}$, a sa i (»*imaginarna jedinica*«) proizvoljnu *tačku* iz ravnine izvan pravulje 01; kad prelazimo na *operacije množenja i dijeljenja*, onda će „imaginarna jedinica“ ležati na pravulji $\perp 01$ i na kružnici $k(0; 1)$.

0.1.9. Mogli smo isto tako računati i u prostoru. Na posve isti način. I računanje u prostoru je nosilac jedne pravilnosti računanja s jednom vrstom „brojeva“, koji se zovu vektori.

0.1.10. Ukratko, vidjesmo kako se pojam i riječ „računati“ može i treba shvatiti u širem značenju — u značenju određenih pridruživanja. Tako npr. baš za naprijed navedeno računanje u M (M je pravulja ili ravnina ili prostor) — nazovimo to računanje *zbrajanjem u M* — vrijede iskazi:

1. *Za svaki uređeni par x, y iz M znamo za pripadni proizvod* (*rezultat*) $x+y$, *i on je u M.*

2. $(x+y)+z=x+(y+z)$.

3. *U M postoji neutrum* (označimo ga sa O) *za koji je*

$$O+a=a+O=a \quad \textit{za svako } a \textit{ iz } M.$$

4. *Svakom a iz M pripada $-a$ iz M sa svojstvom*

$$a+(-a)=(-a)+a=\textit{neutrum}.$$

Kraće se kaže: *množina M je grupa u odnosu na operaciju $+$.*

0.1.11. No, *najbitniji korak* u čivavoj toj stvari bio je odrediti $x+y$ za *svako* x, $y \in M$, tj. osigurati da proizvod operacije ne ide izvan M: osigurati da M bude »*grupoid*« . Zato poslije u § 1 i počinjemo s grupoidima.

0.1.12. Na taj je način i računanje na pravulji p zaseban okvir, mada kao cjelina ulazi i u računanje u ravnini, a ovo opet ulazi u računanje u prostoru: p je *djelitelj* (*podgrupa*) kratnika (nadgrupe) M, koji je, sa svoje strane, podgrupa šire grupe.

0.1.13. Posebno, istaknimo *ovu fundamentalnu ideju.*

Pogledajmo gornju operaciju $+$ u ravnini M s istaknutom tačkom O (O je *početak*, *origo* na latinskom, praizvor). Promatrajmo i proizvoljnu *pravulju* p kroz O. Neka je M određen inače proizvoljan član u M, i pridružimo podatku M kao iznos »*pripadni razred*«

$$p+M, \tag{1}$$

tj. skup sastavljen od svih parcijalnih rezultata $p'+M$, pri čemu p' prolazi skupom p. Kako izgleda razred, odnosno novi položaj $p+M$ od p? Ako je $M\in p$, tada je

$$p+M=p; \text{ ako } M \text{ non}\in p \text{ (tj. ako } M \text{ nije u } p),$$

tada je $p+M$ paralela sa p; uopće, $p+M$ nastaje iz p

translacijom za vektor $\overrightarrow{OM}$.

0.1.14. Kad M prolazi kroz M, tada razred $p+M$ svaki put označuje pravulju $\|p$ (može biti i $=p$). Dva se razreda ili podudaraju ili su disjunktni (mimoležni) skupovi.

0.1.15. Time se čitavo M *raspada u posve određenu množinu* »*razreda*« $p+M$; tu množinu razreda možemo funkcionalno označiti sa

$$M/p \tag{2}$$

i zvati »*kvocijentom od M i p*«. Specijalno je $p\in M/p$; ako je i $q\in M/p$, onda znajmo da je $q\|p$ i $q\subset M$.

A sada dolazi *kulminacija razmatranja.*

U novoj množini (2) razredâ možemo s novim članovima (-paralelama sa p) *također računati* — čak smo u neku ruku i ponukani *računati* i *izjaviti da za* (paralelne) *elemente* r, s *iz* (2) znači $r+s$ množinu svih parcijalnih rezultata $r'+s'$ (oznaka je očigledna).

0.1.16. A „elementarnim“ geometrijskim rasuđivanjima vidimo da je novi rezultat $r+s$ opet iz (2) — jedna paralela sa p i oblika je $p+(R+S)$, ako je $r=p+R$, $s=p+S$ za neko $R\in M$ i neko $S\in M$.

0.1.17. *Što je neutrum u tom računanju na višem stupnju? Čitavo p! Bivši čitavi zatvoreni okvir,* „grupa“, sad je u *novoj zajednici* (2) *neutrum.* Naime, svaka paralela $r\|p$ pomaknuta za $\overrightarrow{Op'}$ dolazi opet na samu sebe. Dakle je

$$p+x=x \text{ za svako } x\in M/p.$$

I sva formalna računanja prenose se sada na računanje s „paralelama“ ili razredima, kako nazivamo elemente iz M/p.

0.1.18. Umjesto da „računamo“ s tim tako glomaznim komadima kao što su „razredi — elementi“ u M/p, možemo iz svakog tog razreda *izabrati po jedan jedini element* da služi kao *predstavnik čitava »svojeg« razreda* i s tim predstavnicima raditi.

0.1.19. Izbor predstavnika svakog razreda može biti zbilja proizvoljan, no najjednostavnije je da izabrano predstavništvo bude što prikladnije za rad; u našem primjeru, svi predstavnici mogu se uzeti s pravulje p' kroz O, tako da je sada p' kao kolektiv, *predstavništvo svih rasreda* (2), tj. svih pravulja $\| p$. Sada za svaki „razred“ r vidimo da je $r = p + r \cap p'$ gdje je $r \cap p'$ skup sastavljen od tačke u kojoj se sijeku r, p'.

0.1.20. Računanje u skupu M/p razredâ odraz je — *homomorfni odraz — računanja u p*, odnosno u M. Naime, ako za svako $x \in M$ označimo sa $p(x)$ onaj razred kojem pripada x, tada je $p(x+y) = px + py$. A ta *aditivna jednakost* iskazuje međusobnu ogledalnost računanja u M i računanja u M/p.

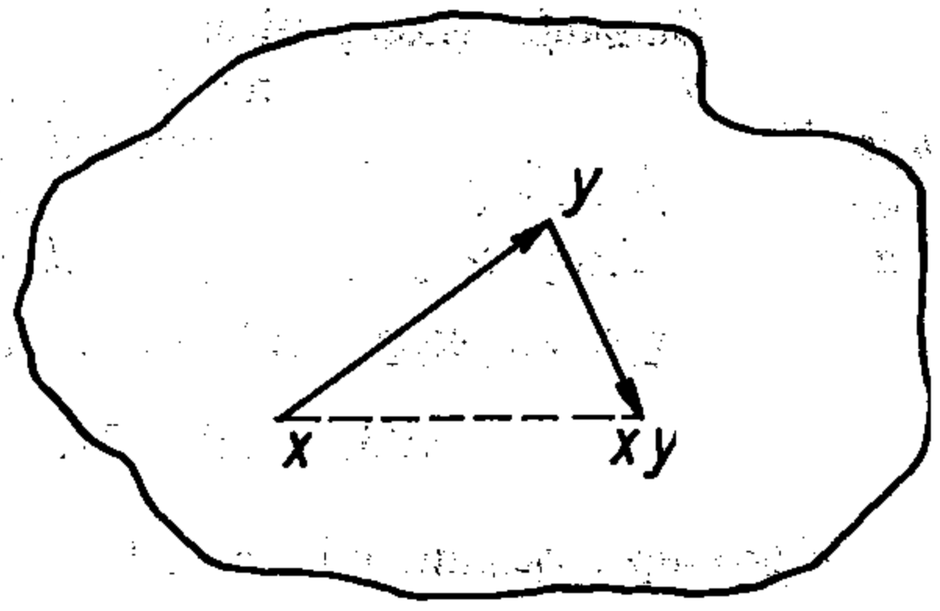
0.1.21. Zanimljivo je pogledati da za svake različite dvije pravulje p, q kroz O vrijedi $p + q =$ ravnina.

0.1.22. Duboko je ovo svojstvo: *ako je K množina svih konveksnih skupova u ravnini, tada je* $(K, +)$ *grupoid.*[1]

1. POJAM GRUPOIDA ILI MONOIDA

⟶ **1.1. Definicija.** ***Neka je M bilo kakva neprazna množina; ako nekim postupkom f svakom uređenom paru*** (x, y) ***elemenata iz M pridružimo određen element iz M, tada kažemo da je M određen grupoid ili monoid u odnosu na postupak f ili također da je množina M zatvorena u odnosu na pridruživanje (operaciju) f; ono što paru*** (x, y) ***pridružujemo označujemo sa*** $f(x, y)$ ***ili*** xfy ***ili često*** $x + y$ ***ili još češće*** $x \cdot y$ ***te*** xy***. Sam grupoid može se označiti kao uređen par*** $(M; f)$***, odnosno*** $(M; +)$***;*** $(M; \cdot)$***. Dopusti li se da*** $f(x, y)$ ***može imati i više vrijednosti*** $\in M$***, tada se govori o nejednoznačnom grupoidu*** $(M; f)$ ***(isp. § 1.6).***

1.1.1. Shematsko predočenje grupoida. Grupoid se može shematski prikazati kao proizvoljna množina M sa *strukturom orijentiranog trokuta*: ***strelici*** (stranici) ***od x do y kao podatku automatski se pridružuje treći vrh xy kao proizvod,*** rezultat. Pri tom *»trovrh«* x, y, xy može i da degenerira u dvovrh, pa čak i u jednu tačku x.



Sl. 17.1.1.

Uvođenjem grupoida u matematiku (Galois)[2] učinjen je jedan od *najrevolucionarnijih koraka* u matema-

[1]) Množina M je *konveksna* ako ima svojstvo da sadrži *svaki pravocrtni odrezak* kojem krajevi leže u M. Svaku tačku smatramo konveksnim skupom.

[2]) Vidi Galoisovu sliku u pogl. 5, § 10.

tici; matematička razmatranja su time vanredno proširena prema onima koja su dotada rađena u matematici. Primjene su vrlo umnožene!

1.2. Primjeri. Ako je N skup prirodnih brojeva, tada su $(N;\ +)$, $(N;\ \cdot)$, (N; *potenciranje*) tri grupoida: proizvod je u sva tri slučaja sadržan u N. To pogotovu vrijedi za $(R;\ +)$, $(R;\ -)$, $(R;\ \cdot)$ gdje je R skup svih realnih brojeva naprotiv, $(R;\ :)$ *nije grupoid*, jer npr. uređenom paru $(3, 0)$ ne pripada određen kvocijent $3:0$ u R. Skup $R\setminus\{0\}$ je grupoid u odnosu na dijeljenje, ali nije više u odnosu na zbrajanje, jer su npr. brojevi $3, -3$ u $R\setminus\{0\}$, ali im suma nije unutra.

Ako R^{I3} označuje skup svih tročlanih nizova kojima su članovi iz R, tada je R^{I3} određen grupoid u odnosu i na zbrajanje, i na oduzimanje, i na množenje nizova.

1.3. Projiciranje. Ako za svaki uređen par $x,\ y\in M$ stavimo $xp_1\,y=x$, tada je $(M;\ p_1)$ određen grupoid; također je grupoid i $(M;\ p_2)$, pri čemu p_2 ima ulogu da paru (x, y) pridruži drugi član y_2 tj. $xp_2\,y=y$. Može se reći da je pridruživanje $(x,\ y)\to x$ upravo *prva projekcija* od $(x,\ y)$; isto tako pridruživanje $(x,\ y)\to y$ zove se *drugo projiciranje* uređene dvojke $(x,\ y)$.

1.4. Primjer. $I5=\{0, 1, 2, 3, 4\}$ je grupoid u odnosu na „zbrajanje i množenje modulo 5“; te su operacije definirane ovako:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

odnosno

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$-_5$	0	1	2	3	4
0	0	4	3	2	1
1	1	0	4	3	2
2	2	1	0	4	3
3	3	2	1	0	4
4	4	3	2	1	0

To znači: $x+_5y$ kazuje razliku između obične sume $x+y$ i najvećeg kratnika broja 5 koji je $\leq x+y$. Slično je za $x._5y$. Rezultat $b-_5a$ definira se pomoću jednakosti: $(b-_5a)+_5a=b$.

1.5. Slaganje (komponiranje) permutacija. Za skup S neka $S!$ označuje skup svih permutacija množine S. To znači da za svako $p\in S!$ imamo *tolikovanje* (obostrano jednoznačno pridruživanje) $x\leftrightarrow px$ za svako $x\in S$. Neka za $p,\ q\in S!$ znak $q\cdot p$ *kazuje rezultat izvođenja obiju permutacija* p, q *i to najprije* p, *a onda* q. Skup $S!$ *je grupoid u odnosu na slaganje njegovih članova.*

Tako npr. za skup $1(3)=\{1,\ 2,\ 3\}$ imamo ove permutacije:

$$123,\quad 132,\quad 213,\quad 231,\quad 312,\quad 321.$$

Tako npr. permutacija $p=312$ ukazuje na ovo pridruživanje:

$$1\to 3,\quad 2\to 1,\quad 3\to 2 \quad \text{tj.} \quad p1=3,\quad p2=1,\quad p3=2 \qquad \text{ili kraće:}$$

$$\begin{matrix}1 & 2 & 3\\ 3 & 1 & 2\end{matrix};$$

slično za permutaciju $q=2\,1\,3$ imamo pridruživanje

$$1\to 2,\quad 2\to 1,\quad 3\to 3 \quad \text{tj.} \quad q1=2,\quad q2=1,\quad q3=3.$$

Evo tablice slaganja u $\{1, 2, 3\}$!

$p \downarrow \; q\to$	1 2 3	1 3 2	2 1 3	2 3 1	3 1 2	3 2 1
1 2 3	1 2 3	1 3 2	2 1 3	2 3 1	3 1 2	3 2 1
1 3 2	1 3 2	1 2 3	3 1 2	3 2 1	2 1 3	2 3 1
2 1 3	2 1 3	2 3 1	1 2 3	1 3 2	3 2 1	3 1 2
2 3 1	2 3 1	2 1 3	3 2 1	3 1 2	1 2 3	1 3 2
3 1 2	3 1 2	3 2 1	1 3 2	1 2 3	2 3 1	2 1 3
3 2 1	3 2 1	3 1 2	2 3 1	2 1 3	1 3 2	1 2 3

1.6. Ako svakom paru tačaka prostora A, B pridijelimo jednu tačku $A\,f\,B$ iz prostora (npr. središte simetrije skupa $\{A, B\}$, neku tačku iz ravnine simetrije skupa $\{A, B\}$), dobije se grupoid (R_3, f); Ako $A\,\mathrm{m}\,B$ označuje *svaku* tačku zatvorenog odreska $[A\,B]$, dobije se *nejednoznačan grupoid* (R_3, m).

1.6.1. Ako je S proizvoljan skup, a O neki njegov element, tada možemo staviti $x\,f\,y=O$; time je skup S postao grupoid (vrlo jednostavan grupoid!).

1.7. Regularni elementi grupoida. Neka je $(M; +)$ proizvoljan grupoid — označujemo ga aditivno; analogna razmatranja, naravno, vrijede pišući umjesto $+$ znak $\cdot$ ili f i sl.

Neka je $a\in M$; tada su potpuno određeni: *preslikavanje* (»*translacija ulijevo*«) $M\to a+M$ množine M u samu sebe i množina $a+M$ svih $a+M$.

To se preslikavanje zove *lijeva translacija za a*; skup $a+M$ zove se *lijevi a—položaj od M*. Ako je to preslikavanje *regularno u M*, tj. ako za $x\neq y$ i $x\in M$, $y\in M$ izlazi $a+x\neq a+y$, tada se a zove *lijevo regularan element grupoida* $(M; +)$. Za lijevo regularan element a jednakost $a+x=a+y$ ima za posljedicu jednakost $x=y$ (*mogućnost ispuštanja istih*, odnosno *jednakih* početnih *članova u jednakosti*).

Ako je *svaki* element grupoida *lijevo regularan*, kaže se da je grupoid *lijevo regularan*, i također da je *operacija + lijevo regularna*.

Analogno se definira *desna regularnost*.

Ako se govori o regularnosti, onda će se podrazumevati *obostrana regularnost*; pri operaciji treba izričito reći da je obostrano regularna ili da dopušta obostrano *dokidanje*.

Primjer. U skupu svih cijelih ili kompleksnih brojeva pri operaciji množenja broj 0 je *jedini neregularni član*; pri operacijama $\cup$ sa skupovima prazni skup je jedini regularni član.

Zbrajanje je obostrano regularna operacija u skupu brojeva (međutim, i zbrajanje ipak nije regularna operacija u tom smislu da je ona *tolikovanje*; npr. uređen par $(3, 4)\neq(2, 5)$ a ipak je $3+4=2+5$).

1.8. Položaji pojedine množine u grupoidu. Vidjeli smo u uvodnom razmatranju da je prostor (ravnina, pravulja) određen grupoid. Ako je određeno tijelo u prostoru, npr. kugla, tada za svaku tačku a u prostoru imamo $T+a$, kao skup svih tačaka $T\cdot+a$; može se reći da $T+a$ nastaje iz T pomakom za a (ili pomakom za vektor $\vec{a}$). Zato se $T+a$ može zvati jedan *položaj od T u grupoidu*, i to položaj što je određen prijelazom $T\cdot\to T\cdot+a$.

Može se govoriti o skupu svih položaja $T+G\cdot$ unutar zadanog grupoida G. Grupoidna struktura osigurava da će $T+G\cdot$ biti u G.

Za svaki podskup $X\subset G$ aditivno pisanog grupoida $(G, +)$ možemo govoriti o (lijevim i desnim) položajima

$$(*) \qquad G\cdot+X, \quad X+G\cdot$$

množine X; ti isti skupovi (*) zovu se *razredi grupoida* u odnosu na X i to *lijevi* razredi $G\cdot+X$ i *desni* razredi $X+G\cdot$.

U mnogome će struktura grupoida zavisiti od toga kako izgledaju i gdje se nalaze položaji raznih dijelova grupoida.

Izrazit je slučaj, npr., da svaka tačka a grupoida može da zauzme mjesto svake tačke b grupoida, tj. da za $a\in G$ $b\in G$ vrijedi $a+x=b$ za bar jedno $x\in G$. Vidjet ćemo da je to jedno od bitnih svojstava posebnih grupoida — grupâ!

Tako npr. za prostor kao grupoid i ravninu α svi položaji ravnine α jesu paralelne ravnine sa α (α uključeno).

⟶ **1.9.** Teorem. *Ako je grupoid regularan, tada svaki njegov podskup u svakom položaju ima jednako mnogo elemenata; specijalno, svaki je dvočlani podskup u svakom svojem položaju dvočlan; i obrnuto.*

Naime, neka je $S\subset G$ i $a\in G$, $b\in G$; tada imamo pripadne položaje (pišimo multiplikativno!) aS i bS; $aS\cdot\leftrightarrow bS\cdot$ je tolikovanje između tačaka tih položaja; naime, ako su x, y u S i $x\neq y$, tada je $ax\neq ay$ i $bx\neq by$, jer su a, b regularni. Obrat prve polovine teorema je očigledan, jer smo regularnost grupoida i definirali svojstvom da mu svaki dvočlani dio ostane dvočlan u svakom svom položaju, tj. da iz $x\neq y$ izlazi $ax\neq ay$ i $xa\neq ya$.

1.10. Pojam djelitelja ili podgrupoida zadanog grupoida. U grupoidu $(R, \cdot)$ svih realnih brojeva imamo raznih užih grupoida, kao npr: $(\{0, 1\}, \cdot)$, $(\{-1, -1\}, \cdot)$, $(R[0, \infty), \cdot)$, $(R(0, \infty), \cdot)$ itd. Naprotiv, slučaj $(R(-\infty, 0), \cdot)$ je izrazit slučaj koji nije grupoid.

Definicija. Neka je $(G, \cdot)$ grupoid, neka je $F\subset G$; ako je i $(F, \cdot)$ grupoid u odnosu na ***istu operaciju*** $\cdot$, tada se kaže da je $(F, \cdot)$ *podgrupoid* (*ili djelitelj*) *grupoida* $(G, \cdot)$ ili da je G *nadgrupoid* (*kratnik*) od F.

Pisat ćemo tada

$$(F, \cdot)\subset(G, \cdot) \quad \text{odnosno} \quad (G, \cdot)\supset(F, \cdot).$$

Kaže se također da je podgrupoid *uronjen* ili *smješten u nadgrupoid*.

Skup svih podgrupoida grupoida $(G, \cdot)$ označivat ćemo sa pG (prema tome $pG \subset PG$; PG označuje množinu svih djelova od G). Skup pG smatrat ćemo uređenim relacijom $\supset$.

Posebno je $G \in pG$, tj. svaki grupoid je svoj vlastiti podgrupoid i nadgrupoid.

⟶ Važna napomena. *Zadane veze unutar zadanog grupoida iste su bez obzira u kakvu se on većem grupoidu smjestio.*

Nije *dovoljno* da bude $F \subset G$, pa da zaključimo da je $(F, \cdot)$ podgrupoid od $(G, \cdot)$. Relacija $F \subset G$ je nužna za to; no još treba biti ispunjeno $FF \subset F$ tj. $x \cdot y \in F$ za svako $x, y \in F$ pa da se govori o podgrupoidu $(F, \cdot)$ grupoida $(G, \cdot)$.

1.11. O raznim položajima zadanog grupoida. Za svaki grupoid $(F, \cdot) \subset (G, \cdot)$ i svako $a \in G$ određen je *položaj* aF množine F kao skup svih aF; slično za položaj Fa svih $F \cdot a$.

Tako npr. za podgrupoid $(\{-1, 1\}, \cdot)$ u skupu D cijelih brojeva za svako $a \in D$ imamo $a\{-1, 1\} = \{-a, a\}$; ovi su »*parovi*« disjunktni i svaki se sastoji od dva različna broja — izuzetan je slučaj 0 jer je $0\{-1, 1\} = \{-0, 0\} = \{0\}$. Zanimljivo je da od svih tih položaja podgrupoida $\{-1, 1\}$ jedino on sam i krajnji slučaj $(\{0\}, \cdot)$ jesu grupoidi; ni u jednom drugom položaju nije $(a\{-1, 1\}, \cdot)$ grupoid!

1.12. Komutativni grupoidi. Definicija. Grupoid $(G, \cdot)$ je *komutativan* ako mu je njegova operacija komutativna (simetrična), tj. ako je $x \cdot y = y \cdot x$ (funkcionalno: $f(x, y) = f(y, x)$) za svako $x \in G$ i svako $y \in G$.

Npr. zbrajanje (oduzimanje) je (nije) komutativno; grupoid $(D, +)$ je komutativan; naprotiv, grupoid $(D, -)$ nije komutativan.

1.13. Rađanje grupoida. Primjer. Zadani su brojevi -3 i 7. Oni ne čine aditivan grupoid, jer sume $(-3)+(-3) = -6$, $-3+7 = 4$, $7+7 = 14$ nisu u polaznom skupu; ovi prvi rezultati zajedno s polaznim podacima daju opsežniju strukturu

$$(\{-3, 7; -6, 4, 14\}; +), \tag{1}$$

koja obuhvata polaznu strukturu $(\{-3, 7\}; +)$. Međutim ni struktura (1) nije još grupoid; zato, priklapajući njene proizvode u (1), struktura se proširuje i ide sve bliže ka najmanjem grupoidu, koji rađa polazna struktura $(\{-3, 7\}, +)$. Zanimljivo je da je rezultat grupoid $(D, +)$ *svih* cijelih racionalnih brojeva.

Tako npr. u grupoidu $(R, \cdot)$ svih realnih brojeva svaki broj $x \geq 0$ rađa (generira) *najmanji mogući grupoid koji ga sadrži* tj. skup $x^N = \{x, x^2, x^3, \ldots\}$.

1.14. Zadaci. 1. Je li skup $I10 = \{0\ 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ grupoid u odnosu na: 1) zbrajanje; 2) oduzimanje; 3) množenje, 4) potenciranje? Sastavi odgovarajuće tablice. Vrijedi li zaključak za skup $In = \{0, 1, \ldots, n-1\}$, gdje je n prirodni broj? Promatraj specijalno skup $I1 = \{0\}$.

2. Isto pitanje za: 1) skup N svih prirodnih brojeva; 2) skup $I\omega = \{0, 1, 2, \ldots, m, m+1 \ldots\}$; 3) skup D; 4) skup Q svih racionalnih brojeva; 5) skup R svih realnih brojeva; 6) skup $Q + Q\,2^{1/2}$ svih bro-

jeva oblika $x+y\,2^{1/2}$, gdje je $x, y \in Q$; 7) skup $R+R\,2^{1/2}$; 8) $R+R\,5^{1/3}$. Odredi regularne elemente.

3. Napiši tablicu slaganja za permutacije brojeva 0, 1 odnosno množine $I\,4$. Dobije li se grupoid? (Isp. tablicu § 1.5).

4. Promatraj izraze 0, x, $-x$; obrazuju li oni grupoid u odnosu na zbrajanje?

5. Promatraj funkcije x, $1-x$, x^{-1}, $(x-1)\,x^{-1}$, $x\,(x-1)^{-1}$, $(1-x)^{-1}$ i njihov skup S; je li S grupoid u odnosu na slaganje funkcija, tj. u odnosu na operaciju $\circ$, ako $g \circ f$ znači: umjesto x u $g(x)$ piši f. Npr. $(1-x) \circ (1-x)^{-1} = (1-(1-x)^{-1}) = x\,(x-1)^{-1}$. Napravi radnu tablicu. Je li koji element neregularan?

6. Je li skup svih radijus-vektora grupoid u odnosu na zbrajanje, odnosno oduzimanje? Što je s regularnošću?

7. Promatraj kakvu množinu M, npr. $M=\{3, 4, 5\}$ i skup PM svih dijelova iz M (prazni skup $\varnothing$ i M uključivo). Je li PM grupoid u odnosu na: 1) uniju; 2) presjek; 3) odstranjivanje skupova? Što je s regularnošću?

8. Je li množina svih: a) neprekidnih; b) izvodljivih; c) integraljivih funkcija grupoid u odnosu na $+$, $-$, $\cdot$, i slaganje?

9. Za par prirodnih brojeva a, b neka $a\,\mathrm{W}\,b$ (odnosno $a\,\mathrm{M}\,b$) označuje najmanji (najveći) zajednički višekratnik (divizor) brojeva a i b. Je li (N, W), odnosno (N, M) određen grupoid? Ima li regularnih elemenata? Odredi $18\,\mathrm{W}\,24$, $18\,\mathrm{M}\,24$ te $18\,f\,(24\,f\,32)$ i $(18\,f\,24)\,f\,32$ za $f=\mathrm{W}$ i $f=\mathrm{M}$.

10. Odredi najmanji aditivni grupoid u kojem leži:
1) broj 2; 2) broj 1/2; 3) vektor v; 4) brojevi 3, 1/2; 5) 4, $5^{1/2}$; 6) 3, $+4$; 7) -3, -4; 8) -3, 4; 8) 3, -4; 10) 1, -1.

11. Isto pitanje za multiplikativne grupoide.

12. Ako je grupoid $(G, +)$ asocijativan, tj. ako vrijedi $(x+y)+z = x+(y+z)$, onda za svako $a \in G$ podgrupoid što ga rađa element a glasi

$$(a,\ a+a,\ a+a+a,\ a+a+a+a,\ \ldots,\ +).$$

Kako izgleda analogni minimalni grupoid što ga rađa a ako $(G, +)$ nije asocijativan grupoid; primjer u $(D; -)$ ili $Q \setminus \{0\}; :)$ i $a=2$.

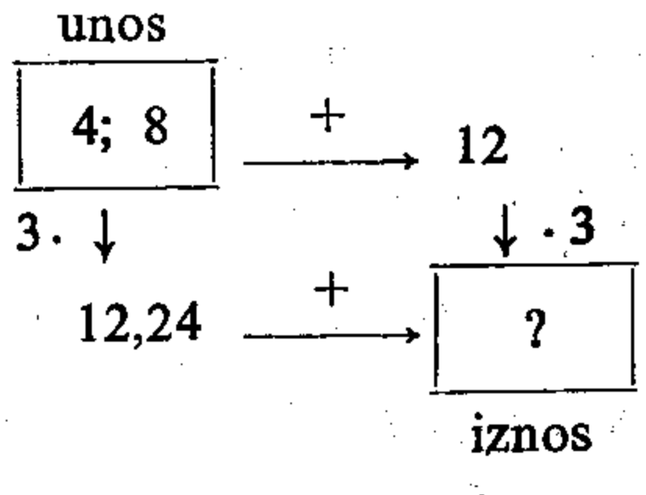
13. Polazeći od broja 1, izgradi najmanji skup koji je zatvoren u odnosu na: 1) $+$; 2) $-$; 3);. 4) $:$; 5) $+$ i $-$; 6) $+$, $\cdot$; 7) $+$, $:$; 8) $+$, $-$, $\cdot$; 9) $+$, $-$, $:$ (dijeljenje sa 0 isključujemo); 10) $+$, $-$, $\cdot$, $:$.

14. Isto pitanje polazeći od broja 1) 3; 2) i; 3) $5^{1/2}$; 4) π; 5) $5^{1/3}$.

15. Isto pitanje polazeći od brojeva 1) 2, 5; 2) 1, $2^{1/2}$; 3) $2^{1/2}$, $3^{1/2}$, $2^{1/3}$.

16. 1) Čine li sve simetrije ravnine R_2 grupoid u odnosu na slaganje? 2) A sve centralne simetrije? 3) Aksijalne simetrije?

2.0. Iz elementarne matematike znamo da je $3(4+8)=3\cdot 4+3\cdot 8$; shematski:



Sličan zakon (1) $a(b+c)=ab+ac$ vrijedi za bilo kakve brojeve a, b, c. Kaže se da je operacija množenja *distributivna* (*razdjelna*) prema operaciji *zbrajanja*; to vrijedi u području brojeva, vektora, funkcija, matrica itd.

2.1. Iz elementarne geometrije znamo da je

$$\text{proj}\ (A\cup B)=\text{proj}\ A\cup\text{proj}\ B; \tag{2}$$

riječima: *projiciranje skupova je distributivna operacija prema operaciji udruživanja skupova.*

2.2. Primjer. Promatrajmo krug K i množinu $PK=G$ svih njegovih dijelova; tada je $(G, \cup)$ određen grupoid; neka je a zadana pravulja ili ravnina; za svaku tačku $T\in K$ neka proj T znači projekciju od T na a; za svaki skup $X\subset K$ definira se projekcija množine X kao množina projekcija svih njenih tačaka. Neka je $G'=\text{proj}\ PK=$skup svih proj G.

Tada imamo grupoid $(G', \cup)$; svaki član iz G' je oblika proj X za bar jedno $X\in G$; nadalje, što je bitno, prema relaciji (2): rezultat „računanja" $A\cup B$ u polaznom grupoidu prelazi u rezultat računanja s odgovarajućim slikama u *novom grupoidu* $(G', \cup)$. Kaže se da je *dobiveni grupoid homomorfan s ishodnim grupoidom* i da je projiciranje *homomorfija* ili *homomorfna transformacija* od $(PK, \cup)$ na $(\text{proj}\ PK, \cup)$.

2.3. Na taj način vidimo kako na prvi pogled tako različite operacije, kao što su množenje i zbrajanje, odnosno projiciranje i ujedinjavanje (sabiranje), imaju međusobno slična vladanja.

Zato je jasno da će naredna definicija morati da igra fundamentalnu ulogu kad obuhvata s *jedinstvenog gledišta* tako *razne* stvari.

⟶ **2.4. Osnovne definicije. — 2.4.0. Osnovna definicija. Homomorfizam kao preslikavanje.** Zadan je uređen par grupoida $(G, \cdot)$, $(G', .')$. *Svako jednoznačno preslikavanje h kojem je oblast G i protuoblast G' zove se homomorfija ili homomorfizam od grupoida $(G, \cdot)$ na grupoid $(G', .')$, ako rezultat slaganja u prvom grupoidu prelazi u rezultat slaganja odgovarajućih elemenata u drugom grupoidu: $h(x\cdot y)=hx\,.'\,hy$* za svaki uređeni par $x, y\in G$; to se može reći i ovako: *h je distributivno ili razdjelno prema operaciji u grupoidu.* Piše se $(G, \cdot)\sim(G', .')$. i čita $(G', .')$ je homomorfno s $(G, \cdot)$. Oprez! Ne mora biti! $(G, \cdot)$ homomorfno s $(G', .')$[1].

[1]) Mnemotehnički: dijete je slično roditelju (a ne: roditelj je sličan djetetu).

U posebnom slučaju, ako je $G' \subset G$, zove se homomorfizam od G na G' također *endomorfizam.*

Također se kaže da je *h deformacija* grupoida $(G, \cdot)$.

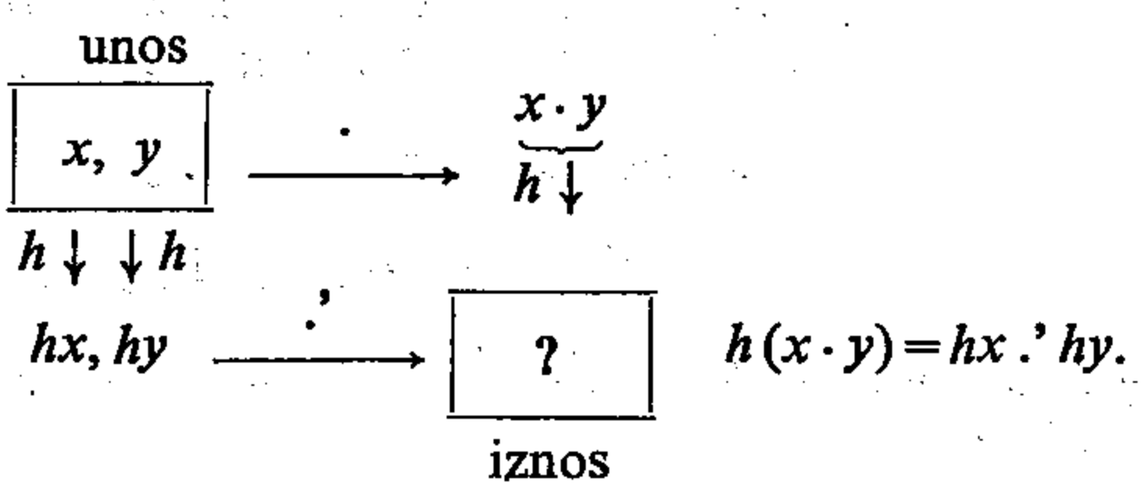
2.4.1. Homomorfizam grupoida. Kaže se da je grupoid $(G', .')$ *homomorfan* s grupoidom $(G, \cdot)$ ili da je $(G', .')$ homomorf grupoida $(G, \cdot)$ i piše

$$(G, \cdot) \sim (G', .'),$$

ako postoji bar jedna homomorfija h od $(G, \cdot)$ *na* $(G', .')$.

Dakle je specijalno $hG = G'$.

Shematski



Shematski: u uokvireni pravokutnik u kojem se nalazi znak pitanja treba da stigne isti iznos: odozgo i slijeva!

2.4.2. Autohomomorfizam. Svaki homomorfizam h grupoida $(G, \cdot)$ *sa samim sobom* zove se *autohomomorfizam grupoida.* Dakle je $hG = G$ (a ne samo $hG \subset G$ kao kod endomorfizma).

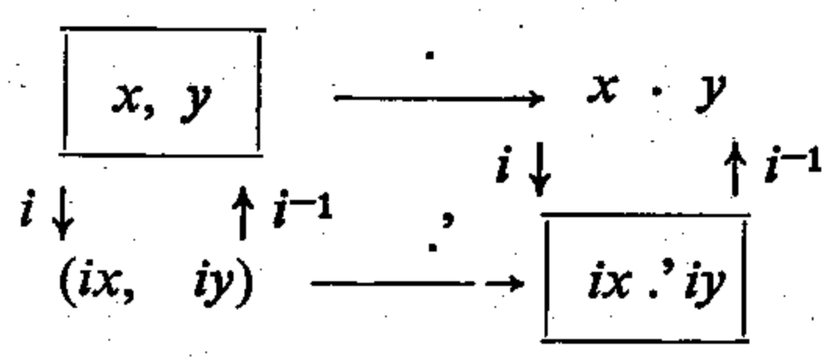
⟶ **2.4.3. Izomorfizam.** Svaki *homomorfizam* koji je *obostrano jednoznačan* zove se *izomorfizam.* Relacija izomorfizma označuje se sa $\simeq$. Prema tome, *eksplicitna definicija izomorfizma glasi ovako:*

Grupoid $(G', .')$ *izomorfan* (*sličan*) *je s grupoidom* $(G, \cdot)$ *i piše* $(G, \cdot) \simeq G \cdot')$, *ako postoji bar jedno tolikovanje, i, kojem je G oblast, a G' protuoblast, tako da za svaku uređenu dvojku* (x, y) *elemenata* $x, y \in G$ *vrijedi*

$$i(x \cdot y) = ix .' iy.$$

Specijalno, za svako $x' \in G'$ postoji jedno jedino $x \in G$ za koje je $ix = x'$; nadalje je $iG = G'$.

Shematski prikaz izomorfizma:



Tu imamo kontrolu na dva mjesta: i gore desno, a ne samo dolje desno, kao kod homomorfizma; nadalje je omogućen jednoznačan povratak iz protuoblasti (drugi redak) u oblast (prvi redak) preslikavanja *i.*

2.4.4. Autoizomorfizam ili automorfizam grupoida je svaki izomorfizam toga grupoida na sama sebe.

2.4.5. Izotopija. Neka su $(G, \cdot)$, $(G', \circ)$ grupoidi; postoji li uređena trojka f, g, h tolikovanja od G na čitavo G' sa svojstvom

$$a \cdot b = f^{-1}(ga \circ hb) \quad (a, b \in G), \tag{1}$$

tada se kaže da je $(G, \cdot)$ *izotopno* sa $(G', \circ)$; trojka (f, g, h) zove se izotopija od $(G, \cdot)$ na $(G', \circ)$. Naravno, ako je $G = G'$, ne mora biti $a \cdot b = a \circ b$.

Dokaži: ako je $f = g = h$, onda se izotopija svodi na izomorfiju.

2.5. Primjer. Za krug K i njegovu projekciju K_a na pravulju a imamo grupoide

$$(PK; \cup), \ (PK_a; \cup); \tag{3}$$

drugi je homomorfan, ali ne može biti izomorfan s prvim (projiciranje je takav homomorfizam); ako K_a označuje projekciju kruga na ravninu a, tada je opet drugi grupoid u (3) homomorfan s prvim — čak je izomorfan u svakom slučaju, osim kad je $K \perp a$. Na taj način vidimo kako izomorfizam i homomorfizam mogu biti u vezi s unutrašnjim svojstvima skupova: postojanje izomorfizma između grupoida (3) ukazuje na jednakost dimenzija od K i a.

2.6. Primjer. Grupoid $(2D, +)$ parnih cijelih racionalnih brojeva izomorfan je s grupoidom $(D, +)$; preslikavanje $D \cdot \longleftrightarrow 2D \cdot$ je izomorfno baš zato jer je $2(m+n) = 2m + 2n$.

Promatrajmo ove multiplikativne grupoide:

$$(D, \cdot), \quad (4D, \cdot) \quad (\{0, 1\}, \cdot). \tag{4}$$

Treći je homomorfan sa svakim od njih.

Preslikavanje $2D \cdot \to 0$, $2D \cdot + 1 \to 1$ pokazuje da je treći homomorfan s prvim (produkt dvaju neparnih brojeva je neparan onda i samo onda ako su oba broja neparna).

Pridruživanje $0 \to 0$

$$4D \cdot \neq 0 \to 1, \quad \text{tj.} \quad x \in 4D \to |\operatorname{sgn} x|$$

pokazuje da je treći grupoid homomorfan s drugim. Identično preslikavanje pokazuje automorfizam svakog grupoida sa samim sobom.

Zanimljivo je da drugi grupid $(4D, \cdot)$ nije homomorfan s $(D, \cdot)$. U obratnom slučaju postojao bi bar jedan homomorfizam h od $(D, \cdot)$ na $(4D, \cdot)$.

No, tada bi iz $m = 1 \cdot m$ izlazilo

$$h(m) = h(1 \cdot m) = (\text{distr. od } h \text{ prema } \cdot) = h(1) \cdot h(m), \text{ tj.}$$

$$h(m) = h(1) \cdot h(m) \text{ za svako } m \in D. \tag{5}$$

No ne smije biti $h(m) = 0$ za svako m jer bi inače protuoblast homomorfizma h bila jednočlani skup $\{0\}$, protivno definiciji homomorfizma od D na $4D$. S druge strane, za $h(m) \neq 0$ izlazilo bi iz (5) $1 = h(1)$, što je apsurd, jer $h(1)$ mora biti $4D$ pa ne može biti $= 1$. A na prvi pogled čovjek bi prije

rekao da je skup $(4)_1$ sličniji skupu $(4)_2$ nego skupu $(4)_3$. To je i istina za *aditivne* pripadne strukture!

2.7. *Relacija homomorfizma je povratna i prelazna*:

$$(G, \cdot)\sim(G, \cdot).$$

Ako je

$$G\sim H,\ H\sim K, \quad \text{tada je} \quad G\sim K.$$

Prvu stvar ostvaruje identičko pridruživanje, a drugu stvar ostvaruje preslikavanje složeno od homomorfizma prvog grupoida na drugi i homomorfizma od drugog na treći.

Formule

$$5(3x+3y)=5(3(x+y))=(5\cdot 3)(x+y)$$

pokazuju kako se može ostvariti homomorfizam od $(D, +)$ na $15D, +)$ pomoću homomorfizama

$$(D, +)\overset{\cdot 3}{\to}(3D, +), \quad (3D, +)\overset{\cdot 5}{\to}(15D, +).$$

2.8. *Relacija izomorfizama je i povratna i prelazna i simetrična* (obrtna). Ovo posljednje ostvareno je inverzijom promatranog izomorfizma.

2.8′. *Relacija izotopije među grupoidima je relacija ekvivalencije.* To se lako dokazuje!

2.9. Teorem. *Izomorfizmom se ne narušava svojstvo regularnosti*: svaki grupoid koji je izomorfan sa zadanim regularnim grupoidom i sam je regularan. Drugim riječima ako je $(G, \cdot)$ regularan grupoid i $(G, \cdot)\simeq(H, \cdot)$, tada je i $(H, \cdot)$ regularan grupoid.

Pa neka je i izomorfizam od prvog na drugi grupoid. Dokažimo da je $(H, \cdot)$ regularan. No, svaki član od H je oblika iG, jer je protuoblast $=H$. Pa neka je $ia\in H$, ix, $iy\in H$; tada se radi o tome da se dokaže da

$$ix\neq iy \Rightarrow ia\cdot ix\neq ia\cdot iy,\ ix\,ia\neq iy\,ia.$$

Dokažimo npr. prvu relaciju

$ix\neq iy \Rightarrow$ (č. uključuje ili ima za posljedicu) $x\neq y$ (naime, inače bi bilo $x=y$, pa dakle i $ix=iy$ jer je i jednoznačna funkcija) (a je regularno!) $\Rightarrow ax\neq ay \Rightarrow$ (i jednolisno!) $\Rightarrow$ $i(a\cdot x)\neq i(a\cdot y) \Rightarrow$ (i je distributivno prema $\cdot$) $\Rightarrow ia\cdot ix\neq ia\cdot iy$.

Dakle, zaista $ix\neq iy \Rightarrow ia\,ix\neq ia\cdot iy$. Na isti se način dokazuje i $ix\cdot ia\neq \neq iy\,ia$. A to znači da je za svako $a\in G$ element ia regularan u $(H, \cdot)$, tj. ovaj je grupoid regularan.

2.10. Homomorfizam i svojstvo komutativnosti. *Svaki homomorf komutativnog grupoida i sam je komutativan*, tj.

$$x+y=y+x \Rightarrow hx+hy=hy+hx.$$

(Pišući za vježbu grupoide aditivno.)

Idemo po redu:

$hx+hy=(h$ je distributivno prema $+)=h(x+y)=$(zbog $x+y=y+x$ i zbog jednoznačnosti od $h)=h(y+x)=$(homomorfija!)$=hy+hx$.

Dakle, zaista $hx+hy=hy+hx$.

2.11. Homomorfizam i asocijativnost. *Ako u grupoidu vrijedi zakon asocijacije, tada taj zakon vrijedi i u njegovu homomorfu; štaviše : iz*

$$(a+b)+c=a+(b+c) \text{ izlazi } (ha+hb)+hc=ha+(hb+hc).$$

Računajmo!

$$(ha+hb)+hc=\text{(homomorfija, tj. „izlučivanje faktora“)}=$$
$$h(a+b)+hc=\text{(isti razlog)}=h((a+b)+c)=h(a+(b+c))=$$
$$\text{(hom.!)}=ha+h(b+c)=\text{(hom.!)}=ha+(hb+hc).$$

2.12. *Ako je* $(G, \cdot)$ *proizvoljan grupoid, a* h *proizvoljan homomorfizam u njemu, tada svaki grupoid* $(F; \cdot)\subset(G; \cdot)$ *prelazi opet u podgrupoid.*

Ukratko, vidimo da homomorfizmom grupoida mnoga svojstva ostaju sačuvana. To pogotovu vrijedi za izomorfizam. Uopće, sve što se o jednom grupoidu može reći, prenosi se na *svaki izomorfni* grupoid.

2.13. Evo jedan važan primjer. Aditivni grupoid $(R, +)$ realnih brojeva *izomorfan* je množidbenom grupoidu $(R(0, \infty); \cdot)$ pozitivnih brojeva; preslikavanje $x\to 10^x$ je izomorfizam između tih grupoida.

Vidimo da tim izomorfizmom operacija $+$ prvog grupoida prelazi u odgovarajuću grupoidnu operaciju $\cdot$ drugog grupoida.

3. ASOCIJATIVNO SVOJSTVO BINARNIH OPERACIJA. POJAM SEMIGRUPE

3.1. Definicija. Operacija f je u množini M *asocijativna* ako vrijedi $(xfy)fz=xf(yfz)$ za *svaku uređenu trojku* (x, y, z) članova $x, y, z\in M$. Grupoid (G, f) je *asocijativan* ako mu je operacija f asocijativna u G.

3.2. Polugrupa. *Svaki grupoid* $(G; f)$ *za koji je operacija* f *asocijativna zove se polugrupa ili asocijativni grupoid ili semigrupa.*

Prema tome, svaka polugrupa je određen grupoid; obrat ne mora vrijediti. Tako je npr. skup D cijelih brojeva grupoid prema oduzimanju, ali nije polugrupa, jer ne vrijedi formula $a-(b-c)=(a-b)-c$.

Asocijativno svojstvo je vanredno važno. Smisao mu je taj da se bazična grupoidova operacija, koja je funkcija s **dvije** varijable, proširi i na 3, 4 varijable zgodnim svođenjem na dvije varijable. Tako npr. da među brojevima ne vrijedi asocijativnost za zbrajanje, moralo bi se razlikovati $(3+4)+2$ od $3+(4+2)$, kao što je to npr. slučaj za operator $-$, $:$, x^y, itd., npr. 3^{4^2} nije definirano jednoznačno, osim ako se dogovorimo da je $3^{4^2}=3^{(4^2)}$, a ne da je $3^{4^2}=(3^4)^2$. Isto tako $3/4/2$ obično znači $(3/4)\,2$ a ne $3/(4/2)$. Prije smo već

vidjeli da je homomorfna slika svake polugrupe opet polugrupa (v. pogl. 17, § 2.11).

Vrlo je dalekosežna stvar da za *slaganje* (*komponiranje*) *funkcija vrijedi zakon združivanja ili asocijacije.* Sve permutacije svake množine čine semigrupu ili polugrupu u odnosu na slaganje. Recimo, ako za svaki par tačaka A, B u ravnini, $A \circ B$ znači središte prečke AB, tada je ravnina grupoid, ali nije polugrupa. Isto tako (R, s) nije polugrupa gdje je $asb = 1/2\,(a+b)$.

3.3. Zadaci. Promatraj zadatke iz § 2. i ispitaj da li za njih vrijedi zakon asocijacije.

4. POJAM NEUTRALNOG ELEMENTA GRUPOIDA

Neka je $(G, \cdot)$ grupoid; tada za svako $a \in G$ imamo funkciju $\dot{G} \to a\dot{G}$. Koliko ima takvih funkcija za zadani grupoid? Nalazi li se među njima najjednostavnija, tj. identitet? Drugim riječima, da li za neko $a \in G$ vrijedi $ag = g$ za svako $g \in G$?

Svako takvo a iz G zove se *lijevi neutralni element*, lijevi *neutral* zadanog grupoida $(G, \cdot)$. Slično se definira *desni neutralni element* ili desni neutral.

Važni slučajevi grupoidâ imaju takav *neutral* ili *jedinicu* (u pisanju $\cdot$) ili *nulu* (u pisanju $+$) n; za nju je $gn = ng = g$ za svako $g \in G$.

Tako npr. grupoidi $(D, +)$, $(R, +)$, $(R \setminus \{0\}; \cdot)$, $(R(0, \infty), \cdot)$, $(D/3D, +)$ imaju neutrale i to: 0, 0, 1, 1, odnosno $3D$. Grupoid $(D, -)$ ima *desnu* nulu, ali nema *lijeve.*

4.1. Adjunkcija neutrala. Ako u grupoidu $(G, \cdot)$ nema neutrala može se on dovesti izvana: dovoljno je promatrati bilo koji element e koji je različit od svih članova G, pa promatrati množinu $G' = G \cup \{e\}$ i proglasiti *e obostranim neutralom* u G' *ne dirajući u stare veze unutar polaznog grupoida* $(G, \cdot)$. Bit će, dakle, $ex = xe = x$ za svako $x \in G'$. Polazni grupoid je podgrupoid u $(G', \cdot)$, koji ima e kao jedini neutralni element.

⟶ **4.2.** *Pri svakoj homomorfiji grupoida s neutralom prelazi neutral u neutral.*

Dokaz. Neka je, naime, 1 neutral u $(G, \cdot)$, dakle je $1 \cdot x = x \cdot 1 = x$ za svako $x \in G$. No, odavde dobivamo $h(1 \cdot x) = h(x \cdot 1) = hx$, odakle zbog svojstva homomorfnosti $h1 \cdot hx = hx \cdot h1 = hx$. A to baš znači da je $h(1)$ neutral u novom grupoidu $(G', \cdot)$, gdje je $G' = hG$.

4.3. Dokaži: Svaki grupoid može imati najviše jedan neutral.

5. SIMETRIJA PREMA NEUTRALU: INVERZIJA UNUTAR GRUPOIDA

U $(D, +)$ neutral je 0, pa se čitav preostatak cijepa u parove $\{-1, 1\}$, $\{-2, 2\}, \ldots$ položene simetrično prema neutralu. Isto je tako u polugrupi $(R(0, \infty); \cdot)$; tu je neutral 1, a pridruženi parovi su $\{x, x^{-1}\}$, za svako $x \neq 0$. Pri tom se $-a$ definira kao rješenje jednadžbe $a + x = 0$; isto tako a^{-1} je rješenje jednadžbe $ax = 1$.

Za permutaciju 1 3 2 pripadna antipermutacija $^{-}1\ 3\ 2$ je 1 3 2 jer je $1\ 3\ 2 \cdot 1\ 3\ 2 = 1\ 2\ 3 =$ neutral. Za zadanu rotaciju r pripadna antirotacija ^{-}r je rotacija oko istog središta i za isti kut, ali u protivnom smislu.

Ako svakom $a \in G$ grupoida $(G, \cdot)$, s neutralom 1 pripada jedno a_d^{-1} odnosno a_l^{-1}, za koje je $aa_d^{-1} = 1$, odnosno $a_l^{-1}a = 1$, kaže se da *grupoid dopušta desnu odnosno lijevu inverziju ili desnu odnosno lijevu simetriju prema neutralnom elementu* 1.

Svakidašnji nas primjeri navode da grupoidima koji dopuštaju simetriju prema neutralu poklonimo pažnju.

Sad možemo skupiti navedene uslove i definirati pojam grupe.

6. DEFINICIJA GRUPE

⟶ *Grupa je svaka semigrupa u kojoj postoji najmanje jedan neutralni element i najmanje jedna suprotna vrijednost svakog elementa grupoida.* Drugim riječima, grupa je svaki uređen par $(M, +)$ neprazne množine M i preslikavanja $+$ s ovim svojstvima:

$M_e(+)$ (*Aksiom egzistencije, grupoidnosti ili zatvorenosti*): *za svaki uređeni par* $x, y \in M$ *određen je element* $x+y$ *iz* M, *tj. iz* $x \in M$, $y \in M$ *izlazi* $x+y \in M$.

$M_a(+)$ **(Asocijativnost):** $(x+y)+z = x+(y+z)$ *za svaku uređenu trojku* (x, y, z) *elemenata* $x, y, z \in M$.

$M_n(+)$ **(Postojanje neutralnog elementa):** *postoji najmanje jedan član* $O \in M$ *sa svojstvom da je* $x+O = O+x = x$ *za svako* $x \in M$.

$M_i(+)$ **(Postojanje suprotnih elemenata):** *za svako* $x \in M$ *postoji u* M *najmanje jedan suprotni element (označimo ga* $-x$*) sa svojstvom da je*

$$x+(-x) = O = (-x)+x.$$

6.1. Primjedba. Ako umjesto znaka $a+b$ pišemo $a \cdot b$ ili naprosto ab, tada se umjesto 0 obično piše 1 ili e ili u, a umjesto $-x$ piše se ^{-}x ili x^{-1} i čita antiiks; tada se umjesto o »*aditivnoj*« grupi $(M; +)$ govori o *multiplikativnoj* grupi $(M; \cdot)$. Obično ćemo pretpostavljati da je grupa multiplikativno označena.

6.2. Komutativne ili Abelove[1] grupe. Grupa je *komutativna* (ili *Abelova*) ako je njena operacija simetrična ili komutativna, tj. $xy = yx$ za svako x, y G.

6.3. Modul. Svaka aditivna komutativna grupa zove se *modul*.

6.4. Zadaci (na ove zadatke treba se povratiti opet, poslije § 7).

1. Promatrajmo skup In za $n = 1, 2, 3, \ldots$ i struktutu $(In; +)$; za svaki prirodni n i redni broj ω ispitaj koji od četiri grupovna aksioma vrijede, a koji ne vrijede.

---

[1] N. H. Abel (1802—1829), norveški matematičar.

2. Isto pitanje za $(In; f)$, gdje f znači —, odnosno ., odnosno :.
3. Isto pitanje za $(5D, +)$ i $(5D, -)$.
4. Promatraj cifarski skup $\{0, 1, \ldots, 9\}$ s cifarskim zbrajanjem i množenjem (radi se kao s brojevima, ali se u rezultatu uzme samo cifra jedinica). Je li taj skup: a) grupoid: b) grupa u odnosu na tako definirano zbrajanje, odnosno množenje? Dokaži da je $(\{1, 3, 7, 9\}; \cdot)$ grupa za cifarsko množenje.
5. Je li skup funkcijâ x, $1-x$, x^{-1}, $x(x-1)^{-1}$, $x^{-1}(x-1)$, $(1-x)^{-1}$ grupa u odnosu na slaganje funkcija? (v. § 1.14.5).
6. Da li sve translacije u: 1) prostoru; 2) ravnini; 3) pravulji obrazuju aditivnu grupu?
7. Da li sve rotacije ravnine sa zadanim središtem rotiranja obrazuju grupu?
8. Dokaži da rješenja jednadžbe $x^2-1=0$ čine multiplikativnu grupu. Isto pitanje za jednadžbu $x^n-1=0$, gdje je n bilo koji: 1) prirodni broj; 2) cijeli broj; 3) broj 3/7; 4) racionalan broj; 5) $\sqrt{3}$; 6) realni broj; 7) kompleksni broj.
9. Dokaži da brojevi $\cos 3^{\cdot} \cdot \frac{2\pi}{3} + i \sin 3^{\cdot} \cdot \frac{2\pi}{3}$ za $3^{\cdot} = 0, 1, 2$ čine multiplikativnu grupu.
10. Može li se u prethodnom zadatku znak 3 zamijeniti sa znakom 4, 2, 1, 6, n, gdje je $n \in N$?
11. Promatraj skup svih realnih funkcija u zadanom skupu R; obrazuju li one aditivnu grupu?
12. Može li se u prethodnom zadatku R zamijeniti svakim nepraznim skupom S? Npr. $S = I2$? $S = I10$? $S = \{a, b, c\}$? $S = I2 \times I3$?
13. Dokaži da sve matrice stupnja (3, 3) i s vrijednostiima u R čine aditivnu grupu.
14. Može li se tu umjesto (3, 3) pisati: 1) (3, 5); 2) (10, 10); (r, s) gdje je $r, s \in N$?
15. Dokaži da sve matrice zadanog stupnja (r, s) i s vrijednostima u zadanoj aditivnoj grupi obrazuju aditivnu grupu.
16. Sve regularne realne matrice stupnja: 1) (2, 2); 2) (5, 5); 3) (s, s) obrazuju multiplikativnu grupu. Dokaz!
17. Promatraj skup svih skalarnih matrica zadanog stupnja. Obrazuju li one: 1) aditivnu grupu; 2) multiplikativnu grupu?
18. Promatraj jediničnu matricu 1_3 stupnja (3×3) i sve matrice koje iz nje nastaju permutacijom stupaca. Obrazuju li one grupe s obzirom na: 1) zbrajanje; 2) množenje?
19. Neka je S zadan neprazan skup; neka je $a \cdot b = a$ za svako $(a, b) \in S^{I2}$; koji aksiomi za grupe vrijede, a koji ne vrijede, u strukturi $(S; \cdot)$?

20. Promatraj skup $5D$ (odnosno 5^D) sastavljen od svih brojeva oblika $5x$ (odnosno 5^x), gdje je $x \in D$. Dokaži da je taj skup grupa u odnosu na zbrajanje (odnosno množenje). Jesu li te dvije grupe izomorfne?
21. Promatraj skup $D_0[x]$ svih x-polinomâ $a(x)$ s koeficijentima iz D i sa svojstvom da je najveća zajednička mjera svih koeficijenata $= 1$; skup $(D_0[x], \cdot)$ je grupoid; ako je $a(x) \in D_0[x]$ umnožak elemenata iz $D(x)$, onda je $a(x)$ umnožak i nekih članova iz $D_0[x]$ (Gauss; 7 § 74).

7. PRIMJERI GRUPA

7.1. Skup svih cijelih racionalnih brojeva je grupa, i to komutativna grupa u odnosu na zbrajanje; neutralni element joj je 0.

Ako za zadano a označimo sa aD skup svih ax, pri čemu x prolazi kroz D, tada je $(aD, +)$ određena *komutativna grupa*; tako npr. za $a = 2$ imamo grupu $(2D, +)$, gdje je $2D = \{\ldots -4, -2, 0, 2, 4, 6, \ldots\}$.

Sva su četiri aksioma grupe ispunjena: 1) suma dvaju parnih brojeva opet je paran broj; 2) asocijativnost je na snazi; 3) 0 je paran broj; 4) za svaki parni broj $2n$ i suprotni broj $-2n$ je paran.

7.2. Isto tako imamo aditivne grupe:

$$(3D, +),\ (4D, +),\ (100D, +),\ (\tfrac{2}{3}D, +),\ (3\tfrac{1}{2}D, +),\ (\pi D, +),$$
$$((x^2+1)D, +),\ (\cos x\, D, +)\ ((3, 4, 8)D; +)\ \text{itd.}$$

U vezi s posljednjim primjerom treba se sjetiti da je (3, 4, 8) tročlan niz i da produkt $(3, 4, 8) \cdot x$ znači niz $(3x, 4x, 8x)$ za svako $x \in D$. Sjetimo se također kako se računa s nizovima: suma (produkt) dva niza je niz sumâ (produkata) odgovarajućih članova u tim nizovima.

Prema tome, $(3, 4, 8)D$ označuje skup svih ovih nizova:

$$\ldots,\ (-2\cdot 3, -2\cdot 4, -2\cdot 8),\ (-1\cdot 3, -1\cdot 4, -1\cdot 8),\ (0\cdot 3, 0\cdot 4, 0\cdot 8),$$
$$(1\cdot 3, 1\cdot 4, 1\cdot 8),\ (2\cdot 3, 2\cdot 4, 2\cdot 8),\ (3\cdot 3, 3\cdot 4, 3\cdot 8), \ldots$$

Dokažimo da je taj skup aditivna grupa.

Aksiom grupoidnosti ili egzistencije: ako je $x \in D$, $y \in D$ onda je

$$(3, 4, 8)x + (3, 4, 8)y = (3, 4, 8)(x+y),$$

tj. iznos $(3, 4, 8) \cdot (x+y)$ je opet u skupu $(3, 4, 8)D$.

Stvarno, $(3, 4, 8)x$ znači niz $(3x, 4x, 8x)$. Isto tako $(3, 4, 8)y$ znači niz $(3y, 4y, 8y)$. Dakle je $(3, 4, 8)x + (3, 4, 8)y = (3x, 4x, 8x) + (3y, 4y, 8y) =$ (definicija sume nizova!) $= (3x+3y,\ 4x+4y,\ 8x+8y) = (3(x+y),\ 4(x+y),\ 8(x+y)) = (3, 4, 8)(x+y)$.

Aksiom asocijativnosti je na snazi. To je očigledno:

$$((3, 4, 8)x + (3, 4, 8)y) + (3, 4, 8)z = (3, 4, 8)x + ((3, 4, 8)y + (3, 4, 8)z).$$

Aksiom o neutralu vrijedi: konstanta

$(3, 4, 8) \cdot 0$, tj. $(0, 0, 0)$, neutralan je element.

Aksiom o inverziji: suprotno od

$$(3, 4, 8)x \text{ je } (3, 4, 8)\cdot(-x), \text{ tj. } (-3x, -4x, -8x).$$

7.3. Skup $(D; \cdot)$ je semigrupa s neutralnim elementom 1, ali nije grupa, jer npr. suprotno od 2 nije u D, a 0^{-1} uopće nije definirano.

Ni skup $(Q, \cdot)$ svih racionalnih brojeva nije grupa, zato jer je $0 \in Q$, ali nije $0^{-1} \in Q$. No, skup $Q \setminus \{0\}$ brojeva $\neq 0$ je određena multiplikakivna grupa.

7.4. Grupe permutacija. Grupe S_n i A_n. Skup $S!$ svih permutacija množine S je određena grupa u odnosu na slaganje permutacija. Za poseban slučaj množine $S = I3$ treba dobro pogledati tablicu slaganja iz § 1.3.

Posebno, ako je S konačan skup i ima n elemenata, označuje se grupa $S!$ sa S_n. I sve *parne* permutacije iz S_n obrazuju grupu, a zove se *alternirajuća grupa*, i označuje se sa A_n.

7.5. Partitivni skup PS i operacija $\cup_2$. Za svaki skup S neka PS označuje množinu svih podskupova od S; specijalno, prazni skup $\varnothing$, i sam skup S su elementi u PS; nadalje, definirajmo *»uniju modulo* 2« ili *simetričnu diferenciju skupova* A, B ovako:

$$A \cup_2 B = (A \setminus B) \cup (B \setminus A).$$

$$\text{Npr. } \{3, 4, 5\} \cup_2 \{3, 8, 9\} = \{4, 5, 8, 9\}$$

(ispušta se ono što je i u A i u B).

Tako npr. za skup $S = I3$ imamo:

$$PI3 = \{\varnothing, \{0\}, \{1\}, \{2\}, \{01\}, \{02\}, \{12\}, \{012\}\}.$$

Evo pripadne tablice za operator $\cup_2$ u $PI3$:

$\cup_2$	$\varnothing$	{0}	{1}	{2}	{01}	{02}	{12}	{012}
$\varnothing$	$\varnothing$	{0}	{1}	{2}	{01}	{02}	{12}	{012}
{0}	{0}	$\varnothing$	{01}	{02}	{1}	{2}	{012}	{12}
{1}	{1}	{1}	$\varnothing$	{12}	{0}	{012}	{2}	{02}
{2}	{2}	{02}	{12}	$\varnothing$	{012}	{0}	{1}	{01}
{01}	{01}	{1}	{0}	{012}	$\varnothing$	{12}	{02}	{2}
{02}	{02}	{2}	{012}	{0}	{12}	$\varnothing$	{01}	{1}
{12}	{012}	{012}	{2}	{1}	{02}	{01}	$\varnothing$	{0}
{012}	{12}	{12}	{02}	{01}	{2}	{1}	{0}	$\varnothing$

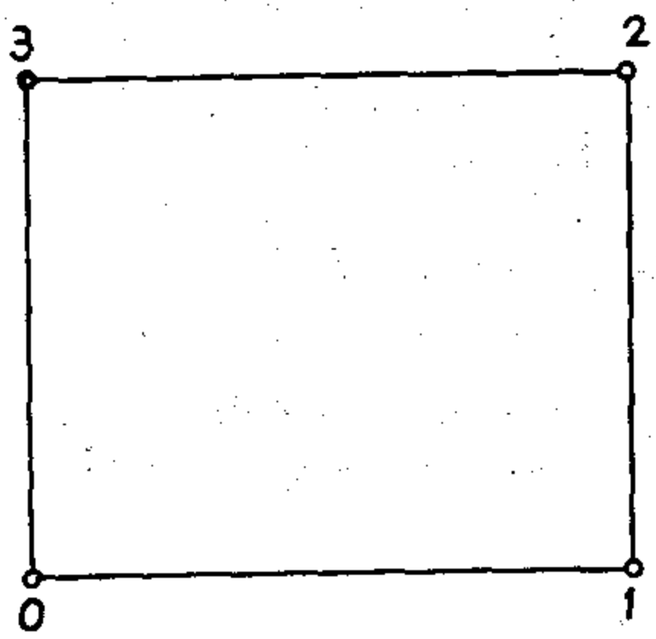
Iz te se tablice odmah vidi da je $PI3$ određena grupa u odnosu na $\cup_2$ i da vrijedi opći

Teorem. *Za svaki skup S imamo grupu* $(PS; \cup_2)$.

7.5.1. Primjedba. Često se umjesto $\cup_2$ piše $\dot{-}$ pa se govori o grupi $(PS; \dot{-})$.

7.6. Grupa što pripada kvadratu. Grupa kvadrata sastoji se od svih kretanja u prostoru koja taj kvadrat prevode u sama sebe; *operacija s obzirom na koju se govori o grupi jest slaganje* (*kompozicija*). Označimo kvadrat sa p_4

(pravilni *poligon* sa četiri stranice); neka njegova grupa bude Gp_4. Očigledno da su članovi te grupe rotacije i simetrije kvadrata. Označimo vrhove kvadrata sa 0, 1, 2, 3, kao na slici. Tad imamo najprije tri rotacije oko središta S: rotacije su za $2\pi/4$, $2\cdot\frac{2\pi}{4}$, $3\cdot\frac{2\pi}{4}$. Pri rotaciji za $2\pi/4$ prelazi kvadrat 0123 u 1230 pa imamo cikličku permutaciju $(0\,1\,2\,3)=1230$ (pogl. 3, § 8.8.2), tj. 0 dolazi u 1, 1 u 2, 2 dolazi u 3, a 3 u 0; pri drugoj rotaciji novi je položaj 2301, tj. 0 dolazi u 2, 1 u 3, 2 u 0, a 3 u 1. Treća rotacija daje položaj ili permutaciju 3012.



Sl. 7.5.

Zatim dolaze simetrije. Ako os simetrije raspolavlja stranicu 0 1, tada je novi položaj kvadrata 1032; slično za os 1 2; položaj je (0 3) (1 2); simetrija oko dijagonale 0 2 daje (0) (2) (1 2); isto take imamo (0 2) (1) (3) za simetriju oko dijagonale 1 3.

Ukratko, imamo ova preslikavanja u vezi s kvadratom 0 1 2 3;

$f_0 = 0\ 1\ 2\ 3$ identičko preslikavanje 0 1 2 3

$f_1 = (0\ 1\ 2\ 3) = 1\ 2\ 3\ 0$ rotacija za $2\pi/4$

$f_2 = (1\ 2\ 3\ 0) = 2\ 3\ 0\ 1$ rotacja za $2\cdot\ \pi/4$

$f_3 = (2301) = 3\ 0\ 1\ 2$ rotacija za $3\cdot 2\pi/4$

$f_4 = (01)\ (23) = 1\ 0\ 3\ 2$

$f_5 = (03)\ (12) = 3\ 2\ 1\ 0$

$f_6 = (02)\ (13) = 0\ 3\ 2\ 1$

$f_7 = (02)\ (13) = 2\ 1\ 0\ 3.$

Svega 8 preslikavanja, odnosno osam permutacija množine $I4 = \{0, 1, 2, 3\}$. Neutralni element je identička permutacija f_0. Tablica antipreslikavanja je očigledna: $^{-}f_0 = f_0$, $^{-}f_1 =$ rotacija za $\pi/4$ u obrnutom smislu, dakle

$$^{-}f_1 = {}^{-}(0321) = {}^{-}1230 = 3012$$

$$^{-}f_2 = {}^{-}2301 = 2103$$

$$^{-}f_3 = {}^{-}3012 = 1230.$$

Za sva ostala preslikavanja f vrijedi $^{-}f = f$.

Za vježbu je dobro sastaviti tablicu slaganjâ svih tih rotacija. Tako npr. izvedemo li f_2 pa f_6, izlazi $f_6 f_2 = (02)(13)\cdot(1230) = 2103 = f_7$.

7.7 Dijedarske grupe. To su grupe što pripadaju pravilnim n-kutima. Ako je p_n pravilan n-kut, tada se pripadna grupa Gp_n ili D_n (dijedarska grupa Gp_n) sastoji najprije od rotacije r za $2\pi/n$ oko pravulje $\perp p_n$ kroz središte poligona p_n

te potencija $r^2, r^3, \ldots, r^{n-1}, r^n = e$; k tome dolazi n rotacija za $\pi/2$ oko svake od n osi simetrije lika p_n koje leže u ravnini p_n; drugih članova Gp_n nema, tj. Gp_n ima $2n$ članova: $kGp_n = 2n = kD_n$.

7.8. Cikličke grupe C_n. Neka je n prirodni broj >2; promatrajmo pravilni n— kut i grupu C_n svih rotacija ravnine koje taj n— kut provode u sama sebe. Sa C_1 označujemo grupu od jednog člana. Sa C_2 označujemo dvočlanu grupu (isp. § 7.4).

Ako vrhove n— kuta označujemo sa 0, 1, 2, 3, ..., $n-1$, tada rotacijama za $0, 2\pi/n, 2\cdot 2\pi/n, \ldots, (n-1)\,2\pi/n$ odgovaraju ove „cikličke“ permutacije ili „cikličke“ supstitucije:

$$
\begin{array}{lllll}
p_0 & 0, & 1, & 2, \ldots, & n-1 \\
p_1 & 1 & 2 & 3 \ldots & n-1\ 0 \\
p_2 & 2 & 3 & 4 \ldots & n-1\ 0\ 1 \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
p_{n-1}, & n-1, & n-2, \ldots, & 3,\ 2,\ 1,\ 0. &
\end{array}
$$

Radna tablica izgleda ovako:

	p_0	p_1	$\cdots$	p_{n-1}
p_0	p_0	p_1	$\cdots$	p_{n-1}
p_1	p_1	p_2	$\cdots$	p_0
.				
.				
.				
p_{n-1}	p_{n-1}	p_0	$\cdots$	p_{n-2}

To su primjeri cikličkih grupa. Opća definicija glasi ovako:

7.8.1. Definicija. Kaže se da je zadana grupa $(G, \cdot)$ *ciklička*, ako postoji najmanje jedan član $a \in G$ sa svojstvom da proizvede čitavu grupu G u tom smislu da je $a^D = G$; pri tom a^D znači skup svih a^x (x prolazi skupom D cijelih brojeva); stavlja se $a^0 = \text{jed.}$, $a^1 = a$, $a^{n+1} = aa^n$, $a^{-n} = (a^{-1})^n$ za *svaki* prirodni broj n.

7.8.2. Radimo li u aditivnoj grupi $(G; +)$, ona je ciklička ako za neko $a \in G$ vrijedi $aD = G = Da$; pri tom definiramo: $0a = a0 = \text{neutral}$, $1a = a1 = a$, $(n+1)a = a(n+1) = na + 1a$, $-na = -(na) = a(-n)$ za svaki prirodni broj n. Npr. grupa $(D; +)$ je ciklička; grupa $(Q; +)$ nije ciklička.

7.9. Poredak ili red perioda člana g grupe $(G; \cdot)$ je glavni broj množine a^D; označuje se sa $\pi(g)$.

7.10. Periodične grupe. Grupe bez torzije. Kaže se da je grupa *periodična* (odnosno bez *torzije* ili *kovrčanja*) ako joj svaki element (koji je $\neq$ neutral) ima konačan (beskonačan) poredak. Tako npr. skup kompleksnih brojeva je aditivna

grupa bez torzije; naprotiv, u odnosu na množenje skup kompleksnih brojeva $\neq 0$ nije ni periodična grupa ni bez torzije ili kovrčanja, jer npr. skup $(-1)^D$ ima tri člana, a skup $\sqrt{2}^D$ ima beskonačno mnogo članova.

7.11. Grupa kocke. Ona se sastoji od svih kretanja u prostoru kojima se kocka prevodi u samu sebe. Označimo je sa G_K ili GK. Jasno je da se GK sastoji od rotacija. *Operacija s obzirom na koju se govori o grupi G_K jest slaganje* (*kompozicija*) *rotacijâ iz G_K.*

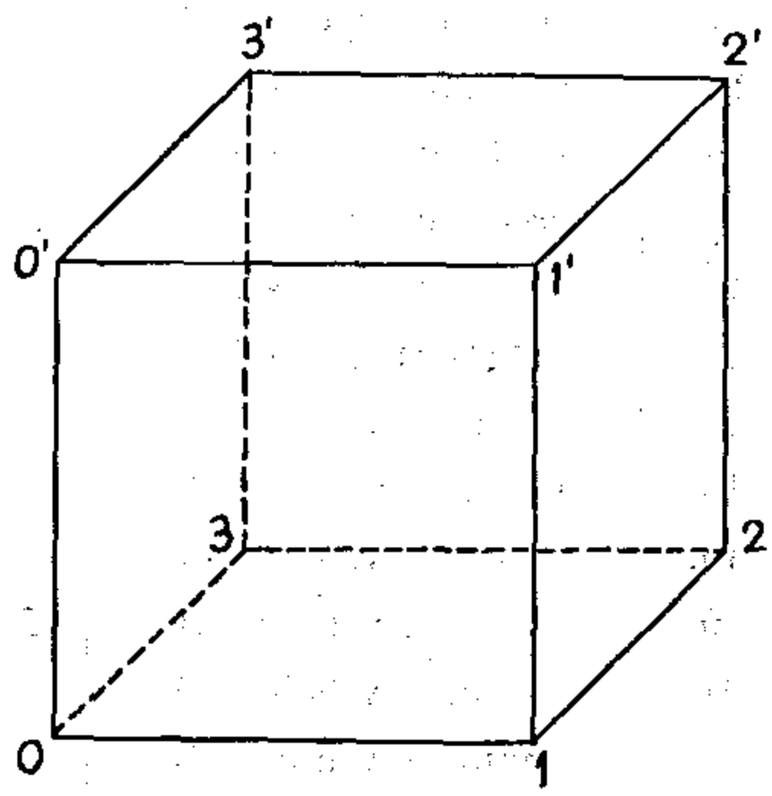
Nabrojimo *sve* elemente grupe GK.

1. U prvom redu, za *svaku os kocke* vezana je ciklička grupa reda 4, a sastavljena je od rotacijâ oko te osi za 0, $2\pi/4$, $2\cdot\frac{2\pi}{4}$, i $3\cdot\frac{2\pi}{4}$.

Kako kocka ima tri osi i kako je identička transformacija zajednički element, unija ili zbir od te tri cikličke grupe daje $1+3\cdot 3$. tj. 10 rotacija.

2. Nadalje dolaze rotacije oko osi koje su osi simetrije za dvojku suprotnih bridova: tu se radi o 6 cikličkih grupa reda 2. One pridonose 6 novih rotacija.

Tako npr. osi što spaja središte brida 01 i središte brida $2'\,3'$ odgovara ciklička grupa sastavljena od identičke rotacije i rotacije za π; zanimljivo je pogledati u što prelaze vrhovi 0, 1 2, 3, $0'$, $1'\,2'$, $3'$ pri toj rotaciji. Očigledno je $0\to 1$, $1\to 0$, $2'\to 3'$, $3'\to 2'$. Manje je očigledno da od preostala četiri vrha svaki prelazi u dijametralno suprotni, tj. $2\Leftrightarrow 0'$, $3\Leftrightarrow 1'$ To ujedno znači da je okomica na dvije dijagonale kocke u njihovu sjecištu ujedno os simetrije ona dva brida kocke koji s tim dijagonalama nemaju nikoje tačke zajedno.



Sl. 17.7.1.1.

3. Najzad dolaze rotacije oko dijagonale kocke. *Oko svake dijagonale možemo kocku rotirati za* 0, $2\pi/3$, $2\cdot 2\pi/3$ i *prevesti kocku u sama sebe*. Tu se dakle, radi o 4 cikličke grupe reda 3; oduzevši identičku rotaciju, pridonose one zajedno $4\cdot 2=8$ novih elemenata grupi kocke.

U svemu, grupa kocke ima $1+3\cdot 3+6\cdot 1+4\cdot 2=24$ člana, tj. $kG_K=24$.

4. Svakoj rotaciji $r\in GK$ odgovara potpuno određena permutacija pr niza vrhova $0\ 1\ 2\ 3\ 0'\ 1'\ 2'\ 3'$. Skup $p[K]$ svih tih permutacija vidi se iz tabele na str. 590. Tako npr. rotaciji r oko osi bridova $0\ 1$ i $2'\ 3'$ odgovaraju ciklusi $(0\ 1)$, $(2'\ 3')$, $(0'\ 2)$, $(3\ 1')$ i njihov proizvod $(0\ 1)\ (2'\ 3')\ (0'\ 2)\ (3\ 1')=$
$=\begin{pmatrix}0\,1\,2\,3\,0'1'\,2'\,3'\\1\,0\,0'\,1'2\,3\,3'\,2'\end{pmatrix}$, tj. permutacija $100'\ 1'\ 233'\ 2'$; ta permutacija nosi broj 11.

Može se napraviti tablica slaganja gornjih permutacija (rotacija) 1 — 24.

Također se vidi da vrijedi

$$p(rs)=(pr)s \quad \text{za svaki par} \quad r,\ s\in GK.$$

Lista svih rotacija kojima kocka 0 1 2 3 0′ 1′ 2′ 3′ prelazi u samu sebe

Redni broj	Os rotacije	Veličina rotacije	Rotacija kao permutacija vrhova	Rotacija kao produkt ciklusa (jednočlani ciklusi su ispušteni)
1.	Početni položaj		0 1 2 3 0′ 1′ 2′ 3′	
2.	odozdo prema gore	$2\pi/4$	1 2 3 0 1′ 2′ 3′ 0′	(0 1 2 3) (0′ 1′ 2′ 3′)
3.		$2\cdot 2\pi/4$	2 3 0 1 2′ 3′ 0′ 1′	(0 2) (1 3) (0′ 2′) (1′ 3′)
4.		$3\cdot 2\pi/4$	3 0 1 2 3′ 0′ 1′ 2′	(0 3 2 1) (0′ 3′ 2′ 1′)
5.	lijevo prema desno	$2\pi/4$	3 2 2′ 3′ 0 1 1′ 0′	(0 3 3′ 0′) (1 2 2′ 1)
6.		$2\cdot 2\pi/4$	3′ 2′ 1′ 0′ 3 2 1 0	(0 3′) (1 2′) (2 1′) (3 0′)
7.		$3\cdot 2\pi/4$	0′ 1′ 1 0 3′ 2′ 2 3	(0 0′ 3′ 3) (1 1′ 2′ 2)
8.	sprijeda prema straga	$2\pi/4$	0′ 0 3 3′ 1′ 1 2 2′	(0 0′ 1′ 1) (2 3 3′ 2′)
9.		$2\cdot 2\pi/4$	1′ 0′ 3′ 2′ 1 0 3 2	(0 1′) (1 0′) (2 3′) (3 2′)
10.		$3\cdot 2\pi/4$	1 1′ 2′ 2 0 0′ 3′ 3	(0 1 1′ 0′) (2 2′ 3′ 3)
11.	srednjica $01 \to 3'\ 2'$	π	1 0 0′ 1′ 2 3 3′ 2′	(0 1) (2 0′) (3 1′) (2′ 3′)
12.	srednjica $12 \to 0'\ 3'$	π	2′ 2 1 1′ 3′ 3 0 0′	(0 2′) (1 2) (3 1′) (0′ 3′)
13.	srednjica $23 \to 0'\ 1'$	π	2′ 3′ 3 2 1′ 0′ 0 1	(0 2′) (1 3′) (2 3) (0′ 1′)
14.	srednjica $30 \to 2'\ 1'$	π	3 3′ 0′ 0 2 2′ 1′ 1	(0 3) (1 3′) (2 0′) (1′ 2′)
15.	srednjica $00' \to 22'$	π	0′ 3′ 2′ 1′ 0 3 2 1	(0 0′) (1 3′) (2 2′) (3 1′)
16.	srednjica $11' \to 33'$	π	2′ 1′ 0′ 3′ 2 1 0 3	(1 0 2′) (1 1′) (2 0′) (3 3′)
17.	spojnica vrhova 0,2′	$2\pi/3$	0 3 3′ 0′ 1 2 2′ 1′	(1 3 0′) (2 3′ 1′)
18.	spojnica vrhova 0,2′	$2\cdot 2\pi/3$	0 0′ 1′ 1 3 3′ 2′ 2	(3 0′ 1) (3′ 1′ 2)
19.	spojnica vrhova 3,1′	$2\pi/3$	2 2′ 3′ 3 1 1′ 0′ 0	(0 2 3′) (1 2′ 0′)
20.	spojnica vrhova 3,1′	$2\cdot 2\pi/3$	3′ 0′ 0 3 2′ 1′ 1 2	(0 3′ 2′) (0′ 2′ 1)
21.	spojnica vrhova 2,0′	$2\pi/3$	1′ 2′ 2 1 0′ 3′ 3 0	(0 1′ 3′) (1 2′ 3)
22.	spojnica vrhova 2,0′	$2\cdot 2\pi/3$	3′ 3 2 2′ 0′ 0 1 1′	(0 3′ 1′) (1 3 2′)
23.	spojnica vrhova 1,3′	$2\pi/3$	1′ 1 0 0′ 2′ 2 3 3′	(0 1′ 2) (3 0′ 2′)
24.	spojnica vrhova 1,3′	$2\cdot 2\pi/3$	2 1 1′ 2′ 3 0 0′ 3′	(0 2 1′) (3 2′ 0′)

Tako npr. $2 \cdot 6 = 15$ tj. izvedemo li rotaciju br. 6 pa rotaciju br. 2, izlazi

$$1\ 2\ 3\ 0\ 1'\ 2'\ 3' \cdot 0\ 3'\ 2'\ 1'\ 0'\ 3\ 2\ 1 = 0'\ 3'\ 2'\ 1'\ 0\ 3\ 2\ 1.$$

7.12. Grupe drugih pravilnih tijela. Na posve isti način definira se grupa što pripada kakvu drugom skupu S iz prostora; ta se grupa sastoji od svih kretanja koja skup S prevode u sama sebe.

Tako sada znamo što je grupa tetraedra, a što grupa oktraedra, pa grupa ikozaedra, grupa piramide, valjka itd. Za opći skup S pripadna je grupa sastavljena jedino od identičke transformacije.

7.13. Četvorna grupa V_4 ili V. To je grupa rotacija koje tri međusobno okomite pravulje koje prolaze istom tačkom prevode *svaku u samu sebe.*

V se sastoji od e i triju rotacija za π oko svake od tih zadanih pravuljâ x, y, z. Ako sa X, Y, Z označimo rotaciju za π oko pravulje x, odnosno y odnosno z, onda se vidi da X ima oblik $(x, -y, -z)$, čime hoćemo naznačiti da X prevodi y i z u same sebe, ali mijenja smjer na x i na z. Isto tako $Y\ldots(-x, y, -z)$, $Z=(-x, -y, z)$, pa se vidi da je $XY=Z$ i da vrijedi ova tablica

	X	Y	Z
X	e	Z	Y
Y	Z	e	X
Z	Y	Y	e

7.14. Grupa što pripada zadanom izrazu s više neodređenica. Promatrajmo npr. izraz $x_1 x_2 + x_3$; on zavisi od tri neodređenice x_1, x_2, x_3, pa je očigledno da permutiranjem neodređenica x_1, x_2 izraz prelazi u sama sebe; jedine permutacije indeksa 1, 2, 3 koje izraz prevode u sama sebe jesu: jedinična permutacija i permutacija 2 1 3; one obrazuju grupu za izraz $x_1 x_2 + x_3$.

Općenito, ako je $f(x_1 \ldots x_n)$ *izraz ili funkcija od n neodređenicâ*, tada se *grupa te funkcije* sastoji od svih permutacija tih neodređenih koje taj izraz $f(x_1, \ldots, x_n)$ prevode formalno u sama sebe. Tu grupu možemo označiti sa Gf. Tako npr. ako je f simetrična (alternirajuća) funkcija od n varijabli, tada je $Gf = S_n$ = simetrična grupa od n varijabli (odnosno $Gf = A_n$ = alternirajuća grupa).

7.15. Zadaci. 1. Objasni grupu Gp_6 pravilnog 6-kuta; obuhvaća li ona koju grupu trokuta? Je li Gp_6 unija (zbir) cikličkih grupa?

2. Je li svaka grupa unija cikličkih grupa?

3. Koliko elemenata ima grupa: 1) tetraedra; 2) oktaedra; 3) ikozaedra?

4. Navedi nekoliko funkcija oblika $\frac{a\dot{R}+b}{c\dot{R}+d}$ za koje su a, b, c, d cijeli brojevi i $ad-bc=1$. Dokaži da *sve* takve funkcije čine grupu. Dobije li se grupa i onda ako uz uslov $ad-bc=1$ pretpostavimo da su koeficijenti a, b, c, d: 1) realni; 2) racionalni; 3) kompleksni brojevi?

4′. 1) Dokaži da je skup $Q[0, 1)$ svih $x \in Q$ za koje je $0 \leq x < 1$ grupa prema operaciji $\circ$, za koju je $a \circ b = a + b - E(a+b)$; pri tom Ex označuje najveći cijeli broj $\leq x$.
2) Može li se tu Q zamijeniti sa R?

5. Promatraj simetričnu grupu $S_3 = I(3)!$ i njenu radnu tablicu i grupu $S_3!$ svih permutacija množine S_3. Jesu li redići i stupci te tablice elementi grupe $S_3!$? Vrijedi li sličan odgovor za svako S_n, $n \in N$?

6. Pogledaj kocku 0 1 2 3 0′ 1′ 2′ 3′ i tetraedre 0 1′ 2 3′, 1 2′ 3 0′ „upisane u kocku“. Jesu li grupe tih tetraedara sadržane u grupi oktaedra? Nađi presjek i uniju tih dviju grupa tetraedara.

Navedi sve elemente grupe oktaedra koje permutiraju ta dva tetraedra.

7. Promatraj grupu $(6\,D, +)$; za koje je elemente $x \in D$ skup $6\,D + x$ grupa? Isto pitanje za $6\,Q$, $6\,R$, $6\,R(i)$.

8. Promatraj multiplikativnu grupu 6^D i skup $6^D \cdot x$ za svaki realni broj $x \neq 0$; za koje x je taj skup multiplikativna grupa?

9. Odredi grupu što pripada pravokutniku.

10. Odredi sve translacije prema kojima je invarijantna funkcija (odnosno krivulja): 1) $y = \cos x$; 2) $y = \sin x$; 3) $y = \operatorname{tg} x$; 4) $y = 3\,x$; 5) $y = 3\,x + 2$; 6) $y = x^2$; 7) $y = x^3$.
Obrazuju li sve te translacije grupu?

11. Odredi: 1) kretanja; 2) kretanja i simetrije, prema kojima je krivulja iz gornjeg zadatka invarijantna. Dobije li se time grupa?

12. Pogledaj mrežu kongruentnih kvadrata ravnine; neka je stranica tih kvadrata $s = 2,\ 5,\ 3 \cdot 4$; kako glase sve translacije prema kojima je ta mreža invarijantna, tj. koje uniju svih nacrtanih pravuljâ prevode u samu sebe. Odredi grupu što pripada toj mreži.

13. Isto pitanje za mrežu kongruentnih pravokutnika sa stranicama 2 i 3, odnosno a i b.

14. Isto pitanje za mrežu pravilnih konkruentnih 3-kuta, odnosno 6-kuta.

15. Neka je M bilo kakva beskonačna množina (npr. $M = N$); promatraj skup $M!$ svih permutacija te množine kao i skup M_0' svih permutacija p množine M sa svojstvom da se p podudara s identičkom permutacijom ili se od nje razlikuje tek na konačnom skupu; dokaži da je i $M!$ i M_0' grupa u odnosu na slaganje. Je li koja od njih bez torzije?

16. Obradite opet čitav § 6.3.

8. NEKOLIKO ELEMENTARNIH TEOREMA O GRUPAMA. CIKLIČKE GRUPE

8.0. Imajmo na umu da je teorija grupa zapravo opća teorija zbrajanja ili množenja, i to ne samo ako radimo s brojevima nego i s vrlo raznovrsnim predmetima. Zato je naravno da ćemo sada naići i na osnovne teoreme aritmetike i zapravo dokazati kako oni izlaze iz onih iskaza (e), (a), (n), (i) (o egzistenciji, asocijativnosti, neutralnosti, inverziji).

Specijalno skrećemo pažnju na elementarne obrasce o inverziji:

$$-(a+b) = -b-a, \text{ odnosno } (ab)^{-1} = b^{-1}\,a^{-1}.$$

Tek u komutativnim grupama može se preći na polazni redoslijed i pisati

$$-(a+b) = -a-b.$$

Naročitu pažnju skrećemo na *elementarno pitanje o predznacima.* Vrlo je korisno sva razmatranja u ovom paragrafu razmatrati i aditivno pisano (sa znakom $+$ umjesto znaka $\cdot$ u našim izlaganjima), odnosno uopće sa znakom f ili sl. Ukazujemo posebno na teoreme 8.1.3 i 8.2.1.

8.1. O simetričnom preslikavanju $x \to x^{-1}$ u grupi. *Pridruživanje $x \mapsto x^{-1}$ možemo shvatiti kao jednu vrstu simetrije u grupi jer je $(x^{-1})^{-1} \to x$. To se pogotovu ogleda u aditivnoj grupi : $x \to -x$, dakle $-(-x) = x$.*

8.1.1. Teorem. *Operacija u grupi dopušta obrat: ako je $a, b \in G$, tada iz $ax = b$ proizlazi $x = a^{-1}b$; isto tako iz $ya = b$ proizlazi $y = ba^{-1}$. U općem slučaju nije $a^{-1}b = ba^{-1}$.*

Stvarno imamo ovaj postupak:

$$\begin{aligned} a^{-1}\,|. \quad & ax = b \\ & a^{-1}(ax) = a^{-1}b \qquad \text{(asoc.)} \\ & (a^{-1}a)\,x = a^{-1}b \qquad \text{(zbog } a^{-1}a = 1\text{)} \\ & 1\,x = a^{-1}b \qquad \text{(zbog } 1\,x = x\text{)} \\ & x = a^{-1}b. \end{aligned}$$

Isto se tako dokazuje da iz $ya = b$ izlazi $y = ba^{-1}$.

Ako je grupa komutativna, onda je, naravno, $ba^{-1} = a^{-1}b$, pa je obrat grupovne operacije jednoznačan; ako grupa nije komutativna, tada postoje dvije obrnute operacije od binarne operacije $(x, y) \to x \cdot y$ (sjeti se npr. obrata potenciranja!).

⟶ **8.1.2.** Teorem. **Obrat produkta:** $(ab)^{-1} = b^{-1}a^{-1}$.

Nađimo $(ab)^{-1}$. Po definiciji imamo:

$$(ab)(ab)^{-1} = 1.$$

Odatle, množeći *sprijeda* sa a^{-1} i primjenjujući zakon asocijacije, imamo:

$$\begin{aligned} & a^{-1}(ab)(ab)^{-1} = a^{-1} \cdot 1 \\ & (a^{-1}a)\,b\,(ab)^{-1} = a^{-1} \quad \text{(jer je } a^{-1} \cdot 1 = a^{-1}\text{)} \\ & 1 \cdot b\,(ab)^{-1} = a^{-1} \\ & b\,(ab)^{-1} = a^{-1}. \end{aligned}$$

Množeći sprijeda sa b^{-1}, dobiva se analogno traženi obrazac da je

$$(ab)^{-1} = b^{-1}a^{-1},$$

odnosno aditivno

$$-(a+b) = -b-a,$$

pri čemu, naravno, $-b-a$ znači $-b+(-a)$. Analogno imamo

$$(abc)^{-1} = ([ab]\,c)^{-1} = c^{-1}[ab]^{-1} = c^{-1}b^{-1}a^{-1} \text{ itd.}$$

8.1.3. Teorem. **Obrat (invers)** produkta je produkt *obratâ* (*inversâ*), ali u obratnom redoslijedu.

Drugim riječima, *inverzija je distributivna, ali u obratnom redoslijedu*:

$$(a_1 \quad a_2 \quad \cdots \quad a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}, \quad \text{odnosno}$$

$$-(a_1 + a_2 + \cdots + a_n) \quad = -a_n - a_{n-1} - \cdots - a_2 - a_1.$$

Specijalno,

$$(xy)^{-1} = y^{-1} x^{-1}, \quad \text{odnosno} \quad -(x+y) = (-y) + (-x).$$

Dokaz se provodi prelazom od k faktora na jedan faktor više.

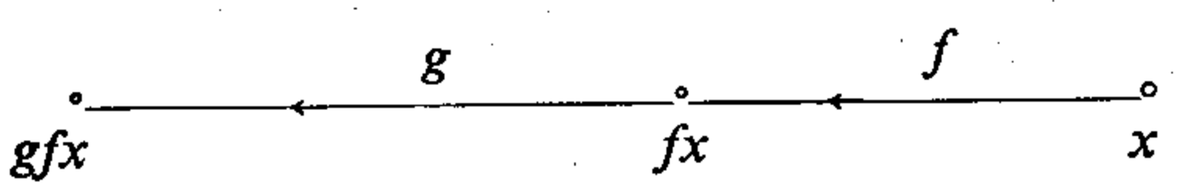
8.1.4. Korolar. *U komutativnim grupama inverzija je distributivna prema operaciji grupe.*

Zato vidimo npr. da je $-(2+3)$ ispravnije sa stanovišta teorije grupa pisati najprije u obliku $-3+(-2)$, odnosno $-3-2$, a tek poslije zbog komutacije preći na oblik $-2-3$.

8.1.5. *Isto tako, za slaganje funkcijâ vrijedi obrazac*:

$$\bar{}(gf) = \bar{}f \bar{}g,$$

što je očigledno, jer pri slaganju gf imamo najprije stazu f, pa g, a pri obratnom hodu imamo najprije stazu $\bar{}g$, pa onda $\bar{}f$.



Provjerimo stvar na primjeru permutacija

$$f = 4\ 2\ 1\ 3\ 1\ 5 \qquad g = 3\ 5\ 2\ 4\ 1.$$

Imamo: $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix}$, tj. $\bar{}f = \begin{pmatrix} 4 & 5 & 3 & 1 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix} = 4\ 2\ 3\ 1\ 5.$

Isto tako $\bar{}g = 5\ 3\ 1\ 4\ 2$. Dakle $\bar{}f\bar{}g = 4\ 2\ 3\ 1\ 5 \cdot 5\ 3\ 1\ 4\ 2 = 5\ 3\ 4\ 1\ 2$

$$gf = 3\ 5\ 2\ 4\ 1 \cdot 4\ 2\ 3\ 1\ 5 = 4\ 5\ 2\ 3\ 1$$

$\bar{}(gf) = 5\ 3\ 4\ 1\ 2$. Dakle je zaista $\bar{}(gf) = \bar{}f\bar{}g$.

8.2. Definicija potencije ili stepena u grupi. Za svako $a \in G$ definiramo

$$a^1 = a, \quad a^0 = e, \quad a^{n+1} = a a^n \quad \text{te} \quad a^{-n} = (a^{-1})^n \quad \text{za svako} \quad n \in N$$

(N je skup prirodnih brojeva).

⟶ **8.2.1.** Teorem. *Za potenciranje vrijede uobičajena pravila*:

(1) $$a^m \cdot a^n = a^{m+n}$$

(2) $$(a^m)^n = a^{n \cdot m},$$

pri čemu su m, n cijeli brojevi.

Dokažimo najprije prvu formulu. Ona je očigledna ako su m, n istog znaka ili jedan od njih $=0$; zato možemo pretpostaviti da su m, n različitog predznaka, recimo $m>0$, $n<0$, npr. $m=2$, $n=-3$.

Tada je $a^2 \cdot a^{-3} = aa\,a^{-1}\,a^{-1}\,a^{-1} = a^{-1} = a^{2-3}$.

Ako je $m+n=0$, tada je $a^m \cdot a^n = (\underbrace{a \cdot a \cdot \ldots a}_{m})(\underbrace{a^{-1}\,a^{-1}\,a^{-1}}_{m}) =$

$$= \underbrace{aa \ldots a}_{m-1}\ \underbrace{(aa^{-1})}_{e}\ (\underbrace{a^{-1} \ldots a^{-1}}_{m-1}) = a^{m-1}\,e \cdot a^{-(m-1)} = a^{m-1} \cdot a^{-(m-1)}.$$

Na sličan način ovo je dalje =

$$= a^{m-2} \cdot a^{-(m-2)} = \ldots = a^2 \cdot a^{-2} = a^1 \cdot a^{-1} = a^0 = a^{m-m} = a^{m+n}.$$

Svakako je $m = (m+n)-n$, pri čemu je zbog $n<0$ broj $-n$ pozitivan; na taj način m je suma pozitivnih brojeva $m+n$ i $-n$, pa je prema prethodnom slučaju $a^m = a^{m+n} \cdot a^{-n}$, odakle, množeći straga sa a^n, izlazi $a^m \cdot a^n = a^{m+n}\,a^{-n} \cdot a^n$, odakle zbog $a^{-n} \cdot a^n = 1$ izlazi tražena relacija.

Druga je relacija očigledna ako je $n \geq 0$. Obradimo zato slučaj $n<0$; tada je po definiciji $(a^m)^n = ((a^m)^{-1})^{-n}$.

No, $a^m\,a^{-m} = e$, tj. $(a^m)^{-1} = a^{-m}$, pa zato gornja jednakost postaje

$(a^m)^n = (a^{-m})^{-n}$. No sada je $-m>0$, pa je zato

$$(a^{-m})^{-n} = a^{(-m)(-n)} = a^{m \cdot n}.$$

Na taj način vidimo zaista da i drugi obrazac u teoremu vrijedi.

8.2.2. Teorem. *Neka je D skup cijelih brojeva; za svako $a \in G$ neka a^D znači antioblast preslikavanja $x \to a^x$ $(x \in D)$, tj. skup svih a^x. Skup a^D je komutativna grupa. Specijalno,* $1^D = \{1\}$.

8.2.3. Primjedba. Gledajući obrasce (1), (2), treba imati na umu da je a bilo koji element grupe zapisane multiplikativno; da je grupa zapisana aditivno, obrasci (1) i (2) glasili bi

$$ma + na = (m+n)\,a,\quad n(ma) = (n \cdot m)\,a,$$

pri čemu definiramo

$$0\,a = 0,\quad 1\,a = a,\quad (n+1)\,a = na + a,\quad -na = n(-a).$$

Množina a^D označavala bi se sa aD, odnosno Da, a sastoji se od svih ax, gdje je $x \in D$.

Da je oznaka grupovne operacije f (umjesto $+$, odnosno $\cdot$), tada bismo imali analogne obrasce, no njihov zapis bio bi zamršeniji, pogotovu ako funkciju

$$(x,\ y) \xrightarrow{f} xfy \qquad \text{pišemo} \qquad f(x, y).$$

8.2.4. Ukratko, *u svakoj grupi* $(G, \cdot)$ imamo definirane *potencije s cijelim eksponentima* i bazom u G, tj. za svaki cijeli broj $c \in D$ imamo određenu funkciju u G: $x \to x^c$ s vrijednostima u G; ali imamo i definiranu funkciju u D: $x \to c^x$ za svako $c \in G$ s vrijednostima u G.

Kad bismo htjeli definirati i $c^{1/2}$ za svako $c \in G$, naišli bismo na teškoće, jer u općem slučaju $c^{1/2}$ kao rješenje jednadžbe $x^2 = c$ nije definirano. Tako npr. za permutacije množine $I3$ nije definirano $0\ 2\ 1^{1/2}$, jer kvadrat nijedne permutacije množine $\{0, 1, 2\}$ ne daje permutaciju 0 2 1, kao što se možemo lako osvjedočiti. To se još lakše vidi kod grupe rotacija recimo trokuta ili kvadrata.

8.3. Homotetija ili translacija u grupi. — 8.3.0. Ako npr. u grupi $(D, +)$ svakom cijelom broju $x \in D$ dodamo broj 2, dobivamo preslikavanje $x \to x+2$; ono je određena *permutacija* množine D, tj. ono je obostrano jednoznačno, a oblast i protuoblast se podudaraju sa D. Ako uzmemo multiplikativnu grupu npr. pozitivnih realnih brojeva, zaključak je isti: preslikavanje $x \to 2x$ je određena permutacija. Za grupu $S!$ *svih* permutacija proizvoljne množine S vrijedi *sličan iskaz: za svako* $a \in S!$ *preslikavanje* $x \to ax$ *kojim svakoj permutaciji* $x \in S$, *pridružujemo ax jest određena permutacija množine* $S!$ *svih permutacija skupa* S. Naslućujemo da vrijedi:

8.3.1. Teorem. *Ako je* $(G, \cdot)$ *grupa. tada za svako* $a \in G$ *preslikavanje*

$$p_a;\ x \in G:\ x \to ax$$

jest permutacija (*automorfizam*) *množine G. Svaka je grupa regularna.*

Dokaz. Najprije, preslikavanje je obostrano jednoznačno, jer ako je $x \neq y$, tada su i pripadne vrijednosti ax, ay nejednake; kad bi, naime, bilo $ax = ay$, bilo bi također $a^{-1}(ax) = a^{-1}(ay)$, dakle i $(a^{-1}a)x = (a^{-1}a)y$, dakle i $x = y$, protivno pretpostavci da je $x \neq y$. Nadalje je protuoblast preslikavanja $= G$, specijalno svako $b \in G$ nastupa kao vrijednost preslikavanja p_a. Naime, zahtjevu $ax = b$ zadovoljeno je za $x = a^{-1}b$. To znači da je zaista $p_a(a^{-1}b) = b$,

tj. $$^{-}\mathrm{Dom}\, p_a = G.$$

8.3.3. Posljedica. *U grupi G sa bar dva elementa preslikavanje* $x \to ax$ (x prolazi kroz G, a je određen element u G) *ne može biti konstantno.*

To nije u protuslovlju s konstantnim preslikavanjem $x \to 0x$ u skupu R realnih brojeva, zato što R *nije grupa* u odnosu na množenje. Naime, nije $0^{-1} \in R$, zato nije ispunjen uslov teorema, odnosno posljedice 2.

8.4. Potpuno uređene grupe. Zanimljivo je sparivanje $\{x, x^{-1}\}$ unutar grupe, jer takva dva para ili se podudaraju ili su bez zajedničkog člana.

Kod realnih brojeva radi se o *jednom pozitivnom* i *jednom negativnom* broju (osim za $\{0, -0\}$); no kako da u općem slučaju kod grupe $(G, +)$ kažemo koji je član u $\{x, -x\}$ pozitivan, a koji negativan? Specijalno, može li se iz svakog dvočlanog para $\{x, -x\}$ izabrati po jedan element, tako da skup P svih tih izabranih elemenata bude *grupoid*, tj. da iz $x, y \in P$ izlazi $x+y \in P$? Tada bi se moglo reći da je svako $P^{\cdot}$ „pozitivno“, a svako $-P^{\cdot}$ „negativno“ (naravno, neutral 0 nije ni „pozitivno“ ni „negativno“).

Za svaku grupu $(G, +)$ koja se može pocijepati u tri *disjunktna dijela* $\{0\}$, P, $-P$, sa svojstvom da $(P, +)$ bude grupoid kaže se da je *potpuno uređena*. Moglo bi se pisati $P^{\cdot} > 0$, $-P^{\cdot} < 0$ te $x > y$ za $x - y > 0$ i dokazati

specijalno da iz $x>y>z$ izlazi $x>z$. Naime, $x>y$ znači $x-y\in P$; isto tako $y>z$. znači $y-z\in P$; kako je P grupoid, to je $(x-y)+(y-z)\in P$, tj. $x-z>0$, tj. $x>z$.

8.5. Realizacija svake grupe pomoću permutacija. — 8.5.1. Ako u grupi $(R, +)$ izvršimo najprije translaciju p_2 za 2, pa translaciju p_3 za 3, rezultat je isti kao da smo *odmah izvršili* translaciju p_5 za 5, tj. $p_3 p_2 = p_5$. Slično vrijedi za svaku grupu:

8.5.2. Teorem. (Cayley[1]). *Neka je $a, b\in G$; tada su preslikavanja*

$$p_a \cdots \quad x \to ax \qquad p_b \cdots \quad x \to bx \qquad p_{ab} \cdots \quad x \to (ab)\,x$$

određene permutacije skupa G za koje vrijedi

$$p_{ab} = p_a p_b. \tag{1}$$

Da se tu radi o permutacijama množine G, dokazano je u 8.3.1. Dokažimo i (1).

Naime, $p_{ab}\,x = (\text{po definiciji}) = (ab)\,x = a\,(bx) = ay$, gdje je $y = bx$; no, $ay = p_a\,y$; dakle je $p_{ab}\,x = p_a\,(p_b\,x) = (\text{definicija složenih funkcija}) = (p_a p_b)\,x$ tj. $p_{ab}\,x = (p_a p_b)\,x$ za svako $x\in G$; to znači upravo da vrijedi tražena relacija (1).

Na taj način vidimo kako svakoj grupi $(G, \cdot)$ odgovara neka grupa permutacija; *operacija $\cdot$ u $(G, \cdot)$ je bilo kakva; operacija među permutacijama* ***posve je određena*** — naime slaganje permutacija. U tome je interes gornjeg rezultata. Kaže se da se *svaka grupa može predstaviti ili ostvariti* (*realizirati*) *pomoću permutacija.*

8.6. Jednostavnija definicija grupe. — 8.6.1. *Desni neutral. Desni inverz.* Grupu smo definirali kao polugrupu u kojoj postoji *jedan jedini neutralni* element te u kojoj je svakom članu a pridružen *jedan jedini* inverzni član a^{-1} iz polugrupe za koji je $a^{-1}a = aa^{-1} = \text{neutral}$.

Taj se zahtjev može prividno oslabiti tražeći da u polugrupi postoji *bar jedan desni neutral* ili *desna jedinica* 1_d sa svojstvom

$$g\,1_d = g \quad (g\in G) \tag{1}$$

i da svakom $a\in G$ pripada određen *bar jedan desni inverz* a_d^{-1} za koji je

$$aa_d^{-1} = 1_d \quad (a\in G). \tag{2}$$

Naravno, analogno se definira *lijeva jedinica* 1_l i *lijevi inverz* a_l^{-1} i to pomoću $1_l g = g$ $(g\in G)$ odnosno $a_l^{-1}a = 1_l$.

Naravno, ako grupoid ima jedinicu, 1, onda je $1 = 1_l$, $1 = 1_d$ tj. $1_l = 1_d = 1$; ako još postoji i inverz a^{-1} od a, onda je $a_l^{-1} = a^{-1} = a_d^{-1}$.

To prividno oslabljenje uslova neutralnosti i inverzije u polugrupama ne daje ništa novo — opet smo u grupi:

---

[1] A. Cayley [Kejli] (1821—1895), engleski matematičar.

⟶ **8.6.2.** Teorem. *Ako asocijativan grupoid* $(G, \cdot)$ *ima najmanje jednu desnu jedinicu i ako sadržava najmanje jedan desni inverz svakog svojeg elementa, onda je* $(G, \cdot)$ *i grupa, pa je desna jedinica ujedno i lijeva jedinica i to jedna jedina, a desni inverz od svakog člana* $g \in G$ *je jednoznačno određen i ujedno je i lijevi inverz.*

Nazovimo takvo $(G, \cdot)$ „grupom" i dokažimo da je „grupa" = grupa.

(*i*) Lema. *Za svaki element a »grupe« imamo ne samo* $aa_d^{-1} = (1_d) = (= e)$ *nego također* $a_d^{-1} a = 1_d$. *Dakle je* $aa_d^{-1} = a_d^{-1} a = 1_d$ *te* $(a_d^{-1})_d^{-1} = a$.

Stvarno, promatrajmo $(a_d^{-1} a) a_d^{-1}$; ovo je po zakonu asocijacije $= a_d^{-1} (a a_d^{-1}) =$ (po aksiomu inverzije) $= a_d^{-1} \cdot 1_d =$ (po aksiomu o desnom neutralu) $= a_d^{-1}$, tj.

$$(a_d^{-1} a) a_d^{-1} = a_d^{-1}.$$

Množeći tu jednakost zdesna sa $(a_d^{-1})_d^{-1}$, izlazi primjenjujući zakon asocijacije na dobivenu lijevu stranu:

$$(a_d^{-1} a) (a_d^{-1} (a_d^{-1})_d^{-1}) = a_d^{-1} (a_d^{-1})_d^{-1},$$

odnosno po aksiomu G_n $(\cdot)$ (zamisli $x_d^{-1} = x$);

$$(a_d^{-1} a) 1_d = 1_d \text{ i dalje po aksiomu } G_n(\cdot):$$

$$a_d^{-1} a = 1_d.$$

Time je prva tražena jednakost dokazana; ostale su njena neposredna posljedica. Specijalno, po definiciji, relacija $a_d^{-1} a = 1_d$ upravo se ispisuje i na način $a = (a_d^{-1})_d^{-1}$.

(*ii*) Lema. *U svakoj »grupi« ima jedan jedini desno-neutralni element; on je ujedno i lijevo-neutralni element.* Drugim riječima, za svaku „grupu" $(G, \cdot)$,

relacije $$1_d \in G, \quad 1_d' \in G, \quad a 1_d = a$$
$$a 1_d' = a$$

imaju za posljedicu $1_d = 1_d'$ te $1_d a = a 1_d = a$.

Naime, $1_d = aa_d^{-1}$, dakle $1_d a = (aa_d^{-1}) a =$ (asoc.) $= a (a_d^{-1} a) =$ (lema (*i*)) $= a \cdot 1_d =$ (po aksiomu G_n) $= a$, tj. $1_d a = a$: *desno neutralni element* 1_d *je i lijevo-neutralan.* Dokažimo da u „grupi" ne mogu postojati dva različita desno-neutralna elementa 1_d, $1_d'$. Stvarno, promatrajmo $1_d \cdot 1_d'$; ovo je $= 1_d$, jer je $1_d'$ desna jedinica; ujedno je $1_d \cdot 1_d' = 1_d'$, jer je 1_d prema dokazanom svojstvu također lijeva jedinica.

Dakle je $1_d = 1_d \cdot 1_d' = 1_d'$ tj. $1_d = 1_d'$.

8.7. Dijeljenje u grupoidu. Neka je $(G, \cdot)$ grupoid i $g, g' \in G$. Ako iz $gx = g'$ izlazi $x \in G$, kaže se da grupoid dopušta prednje ili lijevo dijeljenje; to dijeljenje ne mora biti jednoznačno. Ako grupoid dopušta i lijevo i desno dijeljenje, onda se govori *o grupoidu s dijeljenjem*; specijalno se ističu *grupoidi s jednoznačnim dijeljenjem*; kod njih je i lijevo i desno dijeljenje izvedivo *jednoznačno.*

8.8. Kvazigrupa. Definicija. Svaki grupoid u kojem je jednoznačno izvedivo i lijevo dijeljenje i desno dijeljenje zove se *kvazigrupa*. Drugim riječima, $(G, \cdot)$ je kvazigrupa onda i samo onda ako iz g, $g' \in G$ i $gx = g'$ izlazi da je x jednoznačno određen član u G isto tako kao što je y jednoznačno određeno iz $yg = g'$.

Npr. grupoid $(\{1, 2, 3\}, \cdot)$ s tablicom

	1	2	3
1	1	3	2
2	2	1	3
3	3	2	1

je kvazigrupa bez neutrala.

8.9. Pseudogrupa ili **petlja** ili **omča** (engl. **loop** č. **lup)** je naziv za svaku kvazigrupu u kojoj se pojavljuje i neutral.

Prema tome, pseudogrupa je vrlo blizu grupi jer

svaka asocijativna pseudogrupa ≡ *grupa.*

8.10. Oslabljena asocijativnost grupoida $(G, \cdot)$. **1.** Umjesto stroge asocijativnosti

$$(ab)\,c = a\,(bc) \quad (a,\ b,\ c \in G)$$

može se govoriti o *oslabljenoj ili blagoj asocijativnosti grupoida* $(G, \cdot)$ u smislu da za neka preslikavanja $f_1, f_2, \ldots, f_6$ od G u G vrijedi

$$(ab)\,c = f_1\,a\,(f_2\,b\,f_3\,c)$$

$$a\,(bc) = (f_4\,a\,f_5\,b)\,f_6\,c^{1)}.$$

Ako se ta preslikavanja f_i podudaraju s identičkom permutacijom I: $x \to x$ množine G, prelazi blaga asocijativnost u strogu. Tako npr. grupoid $(R \setminus \{0\}; :)$ nije strogo ali jest blago asocijativan, jer je

$$(a : b) : c = a : (b : c^{-1}); \text{ tu je } f_1 = f_4 = I,\ f_2 = f_5 = I,\ f_3\,x = x^{-1},\ f_6\,x = x^{-1}.$$

8.10.2. U vezi s asocijativnosti nameće se i ovo pitanje: Zadani grupoid $(G, \cdot)$ može biti takav da za neke transformacije f, g s vrijednostima u G bude

$$(ab)\,c = f(a\,(bc)) \text{ odnosno } a\,(bc) = g\,((ab)\,c).$$

Druga varijanta je ova: Ispitati da li postoje transformacije α, β za koje je

$$\alpha\,[(ab)\,c] = \beta\,[a\,(bc)] \quad (a,\ b,\ c \in G),$$

odnosno odrediti skup svih takvih parova α, β; pretpostavljamo da protuoblasti funkcija α, β leže u G.

---

[1]) Isp. Vladimir Devidé, *Uber eine Klasse von Gruppoiden — O jednoj klasi grupoida*, Glasnik mat. fiz. astr., Zagreb, 10 (1955), 265 — 286; također Bogdan Zelenko, *Schwach assoziative Gruppoide — Slabo asocijativni grupoidi* Glasnik mat. fiz. astr., Zagreb 16 (1961), 3 — 73.

8.11. Oslabljena komutativnost. Umjesto stroge komutativnosti $ab = ba$ može se promatrati *oslabljena komutativnost* kojeg od ovih oblika:

(1) $$ab = k_1 b \cdot k_2 a.$$

(2) $$k_3 (ab) = k_4 (ba)$$

(3) $$k_5 a \cdot b = k_6 b \cdot a$$

(4) $$ab = k_7 b \cdot a = b \cdot k_8 a.$$

(5) $$k_9 (ab) = k_{10} b \cdot k_{11} a$$

(6) $$k_{12} a \cdot k_{13} b = k_{14} b \cdot k_{15} a;$$

pri tom k_i znači neko preslikavanje od G u G. Svaka od prethodnih jednadžbi može se rješavati za svaki dani grupoid $(G, \cdot)$; tada se traže funkcije k_i u dotičnoj jednadžbi. Npr. u grupoidu $(R, -)$ koji nije komutativan zadovoljeni su uslovi komutativnosti:

(1) $[k_1 x = k_2 x = -x]$, (2) $[k_3 x = x, \ k_4 x = -x]$, (3) $[k_5 x = -x = k_6 x]$ itd

8.12. Zadaci u vezi s aksiomima grupe.

1. Promatraj grupu: 1) $(D, +)$; 2) S_3; 3) kocke; nađi za svaki element njegov inverzni.
2. Gledaj radnu tablicu u gornjim grupama, pa nađi na dva načina protu-element od svakog elementa.
3. Promatraj cikličke grupe C_3, C_4, C_5, C_6, C_7. Koliko svaka od njih sadrži elemenata x sa svojstvom da se x^D podudara sa samom grupom?
4. Neka je $(G, \cdot)$ proizvoljna grupa od n članova ($n \in N$); dokaži da je $a^n = 1$ za svako $a \in G$ **(Frematov teorem o grupama).**
5. Promatraj $(\{1, 2, 3\}, \cdot)$ s radnom tablicom

·	1	2	3
1	3	2	1
2	2	1	3
3	1	3	2

koji su od uslova ispunjeni: 1) grupoidnost; 2) regularnost; 3) mogućnost dijeljenja: 4) stroga ili blaga komutativnost?

6. 1) Jesu li u § 8.11 navedeni svi tipovi zakona komutativnosti?
   2) Da li svaki od zakona asocijativnosti iz § 8.10 zadovoljava uslovu $(GG)(G) = G(GG)$?
7. Navedi nekoliko kvazigrupa oblika $(\{0, 1, 2\}, \cdot)$.
8. Isto pitanje za pseudogrupe.
9. 1) Svaka regularna konačna polugrupa je grupa; 2) postoji beskonačna regularna polugrupa koja nije grupa, npr. $(D, \cdot)$; 3) postoji li kvazigrupa od dva elementa koja nije grupa? 4) Svaki grupoid može imati najviše jedan jedinični element. 5) Svaka polugrupa s lijevim i desnim dijeljenjem je grupa.

10. Ako elementi a, b polugrupe [grupe] komutiraju, onda komutiraju i a^m, b^n za sve prirodne [cijele] brojeve.

11. 1) Ako je $\{a, b, 1\}$ tročlan skup grupe $(G, \cdot)$, za koje je $a^3 = b^2 = (ab)^2 = 1$, dokaži da se G sastoji od ovih 6 elemenata $a^m b^n$ ($m \in 1\ (3)$, $n \in 1\ (2)$; ispiši tablicu;

    2) Vrijedi li sličan zaključak za pseudogrupu?

12. Dokazati da skup svih matrica

$$\begin{bmatrix} a & -b^* \\ b & a^* \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

čini multiplikativnu grupu; pri tom su a, b:
1) racionalni brojevi; 2) realni brojevi; 3) kompleksni brojevi.

13. Skup svih regularnih (n, n)-matrica čine multiplikativnu grupu; vrijednosti matrice su bilo racionalne bilo realne bilo kompleksne.

14. Je li $(R_>; \circ)$ grupa? Pri tom je $R_>$ skup svih pozitivnih brojeva; nadalje $a \circ b = a^{\log b}$.

15. Je li $(R; |a-b|)$: 1) grupoid, 2) kvazigrupa, 3) grupa?

9. PODGRUPE

9.0. Pojedina grupa može imati raznih dijelova koji su i sami već grupa s obzirom na promatranu operaciju u G. Tako npr. grupa $(D, +)$ cijelih brojeva sadrži ove podgrupe: $(2D, +)$, $(3D, +)$, ..., $(nD, +)$ za svaki prirodni broj n; pri tom nD znači skup svih nx kod $x \in D$. To znači da je nD antidomen funkcije $x \to nx$ kod $x \in D$. Čak je i $(0D, +)$, tj. $(\{0\}, +)$ podgrupa u $\subset$ $(D, +)$. I grupoid može sadržavati razne grupe.

9.1. Definicija. Ako je $(G, \cdot)$ grupoid, grupa, ako je, nadalje, $X \in G$, te ako je $(X, \cdot)$ *grupa* (*ista operacija*), tada se kaže da je $(X, \cdot)$ *podgrupa, djelitelj, ili subgrupa od* $(G, \cdot)$, a za $(G, \cdot)$ se kaže da je nadgrupoid, odnosno *nadgrupa grupe* $(X, \cdot)$.

Kao osobito interesantno ukazujemo da je za svako $a \in G$ skup a^D *podgrupa grupe* $(G, \cdot)$ (isp. teorem 8.2.2).

9.1.1. Važna primjedba. Kad se govori o *podgrupi* (X, f) grupe (G, f), onda to znači dvoje: prvo, da je $X \subset G$, i drugo, da je za svako $x, y \in X$ rezultat xfy isti s obzirom na operaciju u grupi (X, f) kao i u grupi (G, f). Tako npr. interval $I3 = \{0, 1, 2\}$ s obzirom na zbrajanje modulo 3 čini određenu grupu $(I3; +)$; no ta grupa *nije podgrupa u* $(D; +)$, jer je npr. $1 + 2 = 0$ u prvoj grupi, a u drugoj grupi je $1 + 2 = 3$.

Zato je bolje operaciju zbrajanja modulo 3 označiti sa $+_3$, a ne sa $+$.

9.2. Ako je $(X, \cdot)$ podgrupa, onda je jasno da je (1) $XX \subset X$, kao i (2) $X^{-1} \subset X$; pri tom, naravno, XX znači skup svih xy kod $x \in X$, $y \in X$; isto tako X^{-1} znači skup svih x^{-1} kod $x \in X$. Naime, ako je $(X, \cdot)$ grupa, onda je $xy \in X$ po aksiomu X_1, po aksiomu X_4 svakako je $x^{-1} \in X$ ako je $x \in X$.

Međutim, relacije (1), (2) su i dovoljne pa da $(X; \cdot)$ bude grupa, jer prva relacija (1) upravo znači da vrijedi aksiom X_1; asocijativnost je ispunjena jer je ona na snazi čak i u skupu G; relacija (2) kazuje da vrijedi aksiom X_4; još ostaje aksiom X_3. No, ako je $x \in X$, tada je prema (2) također $x^{-1} \in X$, a prema (1) je i $xx^{-1} \in X$, tj. $1 \in X$. A to je upravo jedinica i u grupi $(X; \cdot)$.

Tako smo dokazali:

9.2.1. Teorem. Neka je $(G, \cdot)$ grupa, ako je $(X, \cdot)$ jedna podgrupa, onda je $XX \subset X$, $X^{-1} \subset X$; i obrnuto: ako neki dio X od G zadovoljava te dvije relacije, $(X, \cdot)$ je podgrupa od $(G, \cdot)$.

9.3. Teorem. *Zajednički dio bilo koje množine podgrupa grupe* $(G, \cdot)$ *opet je određena podgrupa; sve one imaju neutralni element same grupe* $(G, \cdot)$ *kao svoj vlastiti neutralni element.*

Tako npr. u grupi kvadrata imamo ove podgrupe:

1. Grupa sastavljena od neutralnog elementa $n = 0123$;
2. Grupa sastavljena od četiri rotacije kvadrata oko središta kvadrata za $\pi/2$, 2. $\pi/2$, 3. $\pi/2$, 4. $\pi/2$.
3. Skup sastavljen od n-te rotacije kvadrata za π.
4. Svaki skup koji je sastavljen od identičkog preslikavanja te simetrije prema jednoj osi simetrije kvadrata; tih osi ima četiri.

Na taj način imamo $1+1+4+1+1=8$ podgrupa (sama grupa kvadrata uračunata je također kao podgrupa, i to kao „neprava“ podgrupa). Prema tome, grupa kvadrata ima osam podgrupa (primijetimo da sama grupa ima osam članova pa, dakle, 2^8-1 nepraznih dijelova; to je velik broj, a samo osam tih dijelova, svaki za sebe, jest određena grupa s obzirom na slaganje).

9.4. Teorem. *Neka su* A, B *podgrupe grupe* $(G, \cdot)$; *ako je*

$$AB = BA, \quad \text{tada je} \quad (AB, \cdot) \text{ grupa.}$$

Dokažimo da je $(AB, \cdot)$ grupoid:

$$ab,\ a'b' \in AB \Rightarrow (ab)(a'b') \in AB; \text{ pri tom } a, a' \in A;\ b, b \in B.$$

No,

$$(ab)(a'b') = a(ba')b' = (\text{radi } ba' = a'b_1 \text{ za neko } b_1 \in B) =$$

$$a(a'b_1)b' = (aa')(b_1 b') \in AB \quad \text{jer} \quad aa' \in A,\ b_1 b' \in B.$$

Ostali aksiomi za grupe dokazuju se neposredno.

9.5. Centar grupoida. Definicija. Centar ili središte grupoida $(G, \cdot)$ je skup ZG svih članova $x \in G$ za koje je

$$gx = xg \quad \text{za svako} \quad g \in G.$$

Teorem. *Centar asocijativna grupoida je ili prazan skup ili određen podgrupoid. Centar svake grupe je određena komutativna podgrupa.*

Dokažimo da iz $a, b \in ZG$ izlazi $ab \in ZG$ tj. $(ab)\,g = g\,(ab)$ za svako $g \in G$. No,

$$(ab)\,g = a\,(bg) = (\text{radi } b \in ZG) = a\,(gb) =$$

$$= (ag)\,b = (\text{radi } a \in ZG) = (ga)\,b = g\,(ab).$$

Nadalje,

$$a, b \in ZG \Rightarrow ab = ba \text{ (staviti } b = g).$$

Ako G ima jedinični element, onda ga ima i ZG.

Ako je $(G, \cdot)$ grupa, onda je i $(ZG, \cdot)$ grupa, specijalno iz $a \in ZG$ izlazi $a^{-1} \in G$. No, jednakost $ag = ga$ daje $(ag)^{-1} = (ga)^{-1}$ tj.

$$g^{-1} a^{-1} = a^{-1} g^{-1}; \tag{1}$$

kad g prolazi kroz G, prolazi i g^{-1} kroz čitavo G pa zato jednakost (1) kaže da a^{-1} komutira sa svakim $x \in G$; dakle je $a^{-1} \in ZG$.

Naravno, u općem slučaju centar grupe je $(\{1\}, \cdot)$ tj. grupa sastavljena od neutralnog člana.

9.6. Opći problem da se odrede *sve podgrupe zadane grupe* vrlo je težak. Tako npr. što se može reći za podgrupe u $(I\,(10^{10})!\,;)$ svih permutacija rednih brojeva $<10^{10}$? A što opet za podgrupe u $(S!, \cdot)$ za $S = N$, R, itd.? Ukazujemo na to da su sve podgrupe u $(D, +)$ oblika $(m\,D, +)$, gdje je $m \in D$ (isp. pogl. 6, § 12).

9.7. Zadaci o podgrupama.

1. Promatraj multiplikativnu grupu brojeva ± 1, $\pm i$; odredi podgrupe!
2. Ima li ciklička grupa C_3 koju pravu podgrupu?
   A grupa C_p (p prost broj)?
3. Odredi sve podgrupe cikličke grupe C_6.
4. Isto pitanje za cikličke grupe C_8, C_{16}, C_{20}.
5. Promatraj skup $I\,6$ i pripadnu grupu s obzirom na $+_6$, tj. s obzirom na zbrajanje po modulo 6; odredi pripadne podgrupe.
6. Je li struktura $(I\,6; \cdot_6)$ grupa? Sadrži li koju podgrupu? Čine li neparni brojevi, 1, 3, 5 grupu prema $\cdot_6$? Isto pitanje za skup $I\,8 = \{0, 1, \ldots, 7\}$ i operaciju $\cdot_8$ množenja modulo 8. Specijalno dokaži da je $(\{1, 3, 5, 7\}, \cdot_8)$ određena grupa.
7. Za svaki član a neke grupe G promatraj grupu a^D, odnosno $a\,D$; koliko ona ima članova ako je $G = C_3$, C_6, D, grupa kocke?
8. Odredi sve cikličke grupe u grupi kocke.
9. Promatraj cikličku grupu G: 1) C_3; 2) C_4; 3) C_5; 4) C_6. Koliko ima članova iz G tako da bude $a^D = G$?
10. Isto pitanje za množidbenu grupu $e^{D\,2\pi i/n}$ brojeva, gdje je n zadan prirodan broj.

11. Odredi sve podgrupe grupe kocke.

12. Odredi centar grupe: 1) $(D, +)$; 2) $(R +)$; 3) S_3; 4) grupe kocke.

13. U polugrupi s 1 čine obratljivi elementi podgrupu.

10. OSNOVNO RASTAVLJANJE GRUPE U VEZI S PODGRUPAMA. INDEKS PODGRUPE

10.0. Svakidašnje iskustvo da se aditivna grupa D cijelih brojeva cijepa na aditivnu podgrupu $2D$ svih parnih cijelih brojeva i skup $2D+1$ svih neparnih brojeva prenosi se na stanovit način za svaku grupu i za svaku njenu podgrupu, pogotovu ako se ima na umu da su „komadi“ $2D$, $2D+1$, na koje se grupe D cijepa, upravo vrijednosti skupovne funkcije

$$x \to 2D + x,$$

kojoj je oblast sam skup D; pri tom, naravno, $2D+x$ označuje skup $2D$ pomaknut za x, tj. $2D+x$ je skup koji je sastavljen od svih brojeva oblika $2\dot{D}+x$ (kao i obično, $\dot{D}$ označuje svaki element od D). Uistinu, vidi se da je za svako $x \in D$ skup $2D+x$ jednak $2D$, odnosno $2D+1$, već prema tome da li je x paran ili neparan broj. Drugim riječima, vidi se da je za cijele brojeve x, x' jednakost $2D+x=2D+x'$ ravnopravna s relacijama $x-x' \in 2D$.

⟶ **Osnovna primjedba.** Kao što npr. broj 2/3 ima beskonačno mnogo ravnopravnih oblika, npr. 2/3, $(2\cdot 2)/(3\cdot 2)$, $(2\cdot x)/(3\cdot x)$ za svaki broj $x \neq 0$, tako i skupovi $2D$ ili $2D+1$ imaju beskonačno mnogo oblika:

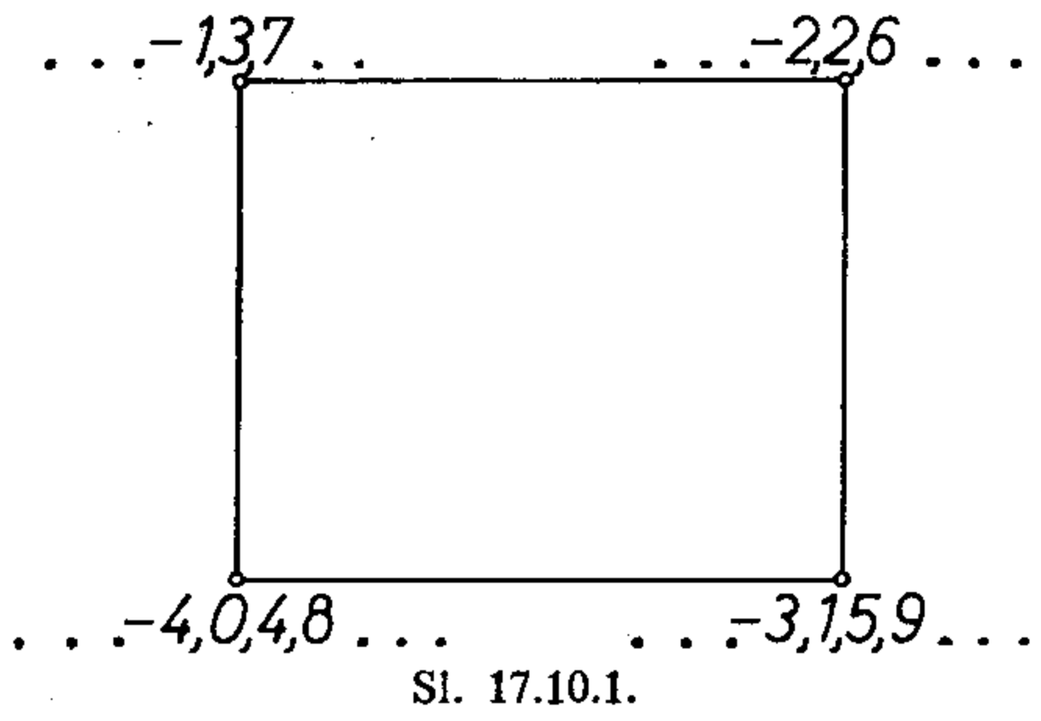
$$2D = 2D + 2D^{\cdot},\ 2D+1 = 2D+1+2D^{\cdot} \text{ za svako } D^{\cdot}.$$

Treba tu primjedbu shvatiti ovdje i u drugim analognim okolnostima. Time će se odstraniti pojedine pojmovne teškoće.

10.1. Sasvim sličnu stvar imamo kad promatramo grupu $(D, +)$ i njenu podgrupu $(4D, +)$ sastavljenu od svih 4-kratnika cijelih brojeva: skupovno preslikavanje $x \to 4D+x$ množine D ima samo četiri moguće različite vrijednosti, i to ove skupove:

$$4D,\quad 4D+1,\quad 4D+2,\quad 4D+3.$$

Tako se npr. skup $4D+4$ podudara sa $4D$; isto je tako $4D+12=4D$; uopće se vidi da je $4D+x=4D+x'$ onda i samo onda ako je $x-x' \in 4D$. Tako npr. $4D+17=4D+29$, a oboje je $=4D+1$.



Sl. 17.10.1.

Ujedno se vidi da četiri množine (1) iscrpljuju D, tj.

$$D = 4D \cup (4D+1) \cup (4D+2) \cup (4D+3)$$

i da nemaju zajedničkih članova. To se vrlo lijepo vidi na brojevnom pravilnom 4-kutu (tj. kvadratu).

Na vrhove kvadrata stavljamo po redu brojeve 0, 1, 2, 3, 4, 5, ... idući u pozitivnom smislu po obodu kvadrata; idući isto tako u suprotnom smjeru, stavljamo -1, -2, -3, ... Tako vidimo da u vrhove kvadrata dolaze upravo skupovi $4D$, $4D+1$, $4D+2$, $4D+3$. Četveročlani skup (1) potpuno je određen sa D i sa $4D$, pa se kraće označuje sa $D/4D$ (ili bolje sa $(D, +)/(4D, +)$, tj.

$$D/4D=\{4D+x;\ x\in D\}, \tag{2}$$

čitaj: $D/4D$ je skup svih $4D+x$ kad x prolazi kroz D.

Stvar se prenosi na opće grupe i podgrupe. O tom je bilo dosta govora u poglavlju 6, § 3.

10.2. Definicija i oznaka protuoblasti zadane funkcije. Ako je funkcija f definirana u skupu A, tada se njena protuoblast, simbolički fA, sastoji od svih vrijednosti $fA\cdot$ (kao obično, $A\cdot\in A$). Ako je f funkcija od *dvije varijable*: prva u skupu A, druga u skupu B, tada protuoblast funkcije f je skup $f(A, B)$ ili AfB, a sastavljen je od svih vrijednosti $f(A\cdot, B\cdot)$, odnosno $A\cdot fB\cdot$.

10.2.1. Tako je npr. $3D$ skup svih brojeva $3x$, pri čemu $x\in D$, tj. $3D=\{0, \pm 3, \pm 6, \pm 9, \ldots\}$. Isto tako npr. $5D+2$ je protuoblast funkcije $x\to 5x+2$ kojoj je oblast skup D cijelih brojeva.

Dalji primjer: $2D+3D$ je protuoblast funkcije $(x, y)\to 2x+3y$, pri čemu je $x\in D$ i $y\in D$.

Poimanje protuoblasti znatno skraćuje i pojednostavnjuje izlaganja.

Kao što nema ništa neobično kad govorimo o skupu od četiri kruga ili četiri grada i sl., tako se treba naučiti da imamo često posla i sa skupovima skupova; upravo smo naučili da se služimo skupom

$$\{4D,\quad 4D+1,\quad 4D+2,\quad 4D+3\},$$

koji je protuoblast skupovne funkcije $x\to 4D+x$ s domenom D. Prema (2), taj 4-član skup označujemo sa $D/4D$. Prema tome je npr. $4D\in D/4D$; naprotiv nije $3\in D/4D$, ali jest $4D+3\in D/4D$.

Na sličan način npr. $D/6D$ označuje protuoblast skupovne funkcije u D: $x\to 6D+x$, pa je $D/6D=\{6D,\ 6D+1,\ 6D+2,\ 6D+3,\ 6D+4,\ 6D+5\}$.

10.2.2. Uopće za svaki cijeli broj n imamo skup nD i podgrupu $(nD, +)$ grupe $(D, +)$, te skupovno preslikavanje $x\to nD+x$ za $x\in D$. Ako je specijalno, $n>1$, služimo li se pravilnim n-kutom pa brojeći 0, 1, 2, 3, ... i obilazeći po redu vrhove, stavljamo brojeve 0, 1, 2, ... u vrhove; isto tako brojeći u obrnutom pravcu 0, -1, -2, ... i obilazeći *n-kut* u obrnutom smislu, stavljajući te brojeve po redu na okvir, vidimo da u jedan vrh dolazi skup nD, u naredni vrh $nD+1$, a u posljednji vrh dolazi skup $nD+(n-1)$. Na taj način imamo n tih skupova koji su dva po dva bez zajedničkog člana, zajedno svi iscrpljuju D, a čine protuoblast preslikavanja $x\to nD+x$, pri čemu x prolazi kroz D. Svih tih n skupova ima jednako mnogo članova, jer je npr. za skupove $nD+5$, $nD+17$ veza

$$nd+5\longleftrightarrow nd+17\quad (d\in D)$$

određeno tolikovanje između skupova $nD+5$, $nD+17$.

10.2.3. Teorem. *Za grupu* $(D, +)$ *i njenu podgrupu* $(nD, +)$, *gdje je* n *cio broj, imamo pripadni skup* D/nD *s ova tri svojstva.*

1. nD *je jedan član u* D/nD; *ostali članovi su istobrojni sa* nD *i oblika su* $nD+x$ gdje je $x\in D$. Da bi bilo $nD+x=nD+y$, nužno je i dovoljno da bude $x-y\in nD$, tj. da diferencija $x-y$ bude djeljiva sa n.
2. Dva po dva člana u D/nD su bez zajedničkog elementa.
3. Unija svih članova iz D/nD je polazna grupa D[1].

To je sasvim jednostavna činjenica. No, treba je dobro razumjeti. Za vježbu neka se gornji teorem napiše pišući umjesto nD slovo X, a umjesto + znak · ili f. Teorem vrijedi općenito, kao što ćemo odmah dokazati.

⟶ **10.3. Osnovni teorem.** ***Neka je*** $(G, \cdot)$ ***proizvoljna grupa, a*** $(F, \cdot)$ ***njena podgrupa; tada je potpuno određeno skupovno preslikavanje***

(3) $$g \to Fg, \qquad \textit{kad } g \textit{ prolazi kroz grupu } G.$$

(a) ***Skup*** Fg ***je istobrojan sa*** F ***za svako*** $g\in G$.

(b) ***Vrijednosti te funkcije ili se podudaraju ili nemaju ni jedne tačke zajedno, no sve su te vrijednosti istobrojne.***

(c) $Fx=Fy \Leftrightarrow xy^{-1}\in F$ ***za svako*** $xy\in G$.

(d) ***Unija svih vrijednosti iznosi*** G.

(e) ***Kardinalni broj grupe*** G ***djeljiv je kardinalnim brojem podgrupe*** F. ***Isto tako imamo preslikavanje***

(4) $$g \to gF \quad za \quad g\in G;$$

svake dvije „vrijednosti“ ove funkcije su disjunktni skupovi.

Da bude $xF=yF$, ***nužno je i dovoljno da vrijedi*** $y^{-1}x\in F$. ***Skupovi*** gF (***odnosno*** Fg) ***zovu se lijevi*** (***desni***) ***položaji od*** F ***u*** G, ***odnosno lijevi*** (***desni***) ***razredi.***

10.4. Dokaz teorema sasvim je analogan slučaju aditivne grupe $(D, +)$ i njene podgrupe $(nD, +)$; promjena je u *multiplikativnom načinu* pisanja te u činjenici da grupa ne mora biti komutativna. Dokaz je trivijalan, ali vrlo instruktivan. Za jediničnu podgrupu $(\{1\}, \cdot)$ stvar je jasna; tada je, naime $1\cdot g=g$ za svako $g\in G$, pa je iskaz teorema trivijalan.

10.5. Provedimo dokaz, i to za preslikavanje (3). Dokaz za preslikavanje (4) posve je sličan.

Ad a. *Za svako* $g\in G$ *skup* Fg *je istobrojan sa* F. Stvarno, ako su f_1, f_2 dva različita elementa iz F, tada je $f_1x\neq f_2x$, jer bi iz $f_1x=f_2x$ proizlazilo (množeći straga sa x^{-1}) da je $(f_1x)x^{-1}=f_2x(x^{-1})$, tj. $f_1=f_2$, protivno pretpostavci da je $f_1\neq f_2$.

Ad b. *Ako za dva elementa* x, y *iz* G *skupovi* Fx, Fy *imaju bar jedan element* z *zajedno, tada je* $Fx=Fy$. Stvarno, $z\in Fx$ znači da je $z=fx$ za neko

---

[1]) Čak vrijedi i ovo: ako je $x, y\in D$, tada za pripadne $nD+x$, $nD+y$ vrijedi

$$(nD+x)+(nD+y)=nD+(x+y),$$

$f \in F$; isto tako $z \in Fy$ znači da je $z = hy$ za neko $h \in F$; dakle je $fx = z = hy$, tj. $fx = hy$. Odakle $x = (f^{-1}h)y$, tj. $x = ky$, gdje je $k \in F$, jer je $k = f^{-1}h$. Dakle je $Fx = F(ky) =$ (zbog asocijativnosti) $= (Fk)y = Fy$ (naime, $Fk = F$ zbog $k \in F$). Dakle je zaista $Fx = Fy$.

Ad c. Neka je $x, y \in G$ i $Fx = Fy$. Množeći ovu jednakost zdesna sa y^{-1}, izlazi $(Fx)y^{-1} = (Fy)y^{-1}$, odnosno zbog asocijativnosti

$$F(xy^{-1}) = F(yy^{-1}), \quad \text{tj.} \quad F(xy^{-1}) = F.$$

To znači da svako $f \in F$ vrijedi $fxy^{-1} \in F$, pa za $f = 1$ izlazi upravo tražena relacija $xy^{-1} \in F$.

Obrnuto, ako je $xy^{-1} \in F$ recimo $xy^{-1} = f \in F$, tada je $x = fy$, pa je

$$Fx = F(fy) = (Ff)y = Fy, \quad \text{tj.} \quad Fx = Fy.$$

Tim je i dio c) teorema pokazan.

Ad d. Stvar je jasna, jer za svako $g \in G$ vrijedi $g \in Fg$, jer je $1 \in G$ i $g = 1 \cdot g$. Dakle je G sadržano u uniji skupova Fg, kad g prolazi kroz G; kako je s druge strane svaki od tih skupova dio od G, izlazi da je $G = \bigcup Gg$, $(g \in G)$.

Ad e. Naime, G je unija disjunktnih skupova oblika Fg, od kojih svaki ima onoliko elemenata koliko ih ima F, tj. $k(Fg) = kF$. A to znači da je kardinalni broj kG grupe G produkt kardinalnog broja podgrupe F i kardinalnog broja množine svih skupova oblika Fg $(g \in G)$.

10.5.1. Primjedba o kraćem postupku komadanja grupe. Ako je $(F, \cdot)$ podgrupa od grupe $(G, \cdot)$, tada nije potrebno promatrati Fg za baš *svako* $g \in G$, pa da razbijemo G na komade oblika Fg. U jednostavnijim slučajevima može se raditi ovako: početi sa F, u preostatku $G \setminus F$ izabrati neki element g_1 pa promatrati skup Fg_1; u preostatku $G \setminus (Fg_0 \cup Fg_1)$, gdje je $g_0 = 1$, izabrati proizvoljan element g_2 i promatrati pripadni komad Fg_2 grupe G, itd.

10.5.2. Primjer. Promatrajmo skup $R^{\neq}$ svih realnih brojeva koji su $\neq 0$; tada je $(R^{\neq}, \cdot)$ određena grupa; pozitivni brojevi čine određenu podgrupu, označimo je sa $(R^{>}, \cdot)$ to znači da $R^{>}$ označuje skup svih realnih brojeva > 0. Grupovna operacija je množenje. Rastavimo $R^{\neq}$. Dolazi najprije sama podgrupa $R^{>}$; u preostatku $R^{\neq} \setminus R^{>}$ (= skup svih negativnih realnih brojeva) izaberimo jedan član, npr. -2; članu -2 odgovara skup $R^{>} \cdot -2$, a to je upravo skup svih negativnih realnih brojeva. Rastav je gotov: $R^{\neq} = R^{>} \cup R^{>} \cdot (-2)$. Naravno, umjesto -2 možemo tu promatrati bilo koji drugi realni negativni broj, kao npr. -1, $-0{,}5$; $-\pi$, $-3^1/_2$ itd.

10.6. Primjer. Promatrajmo „simetričnu grupu S_4“, tj. grupu $(I4)!$ svih permutacija množine $I4 = \{0, 1, 2, 3\}$. Tih permutacija ima $24 = 4!$.

Evo ih po alfabetskom redu:

$(0\,1)\cdot$	0123	0132	0213	0231	0312	0321
$(1\,2)\cdot$	1023	1032	1203	1230	1302	1320
$(2\,3)\cdot$	2013	2031	2103	2130	2301	2310
	3012	3021	3102	3120	3201	3210

Ako prvi red množimo sprijeda sa (0 1), tj. permutacijom 1 0 2 3, izlazi drugi redak; slično, množeći drugi redak sprijeda ciklusom (1 2), izlazi treći redak, a iz ovoga, množeći sprijeda ciklusom (2 3), izlazi posljednji redak.

10.6.1. No, prvi redak je očigledno jedna podgrupa, označimo je sa $0\{1, 2, 3\}! = F$, treći redak je (2 3) (1 2) $F = 0\,3\,1\,2 \cdot F$; posljednji se redak dobije množeći F sprijeda bilo kojim članom grupe, koji nije u prva tri retka, npr. najmanjim, 3 0 1 2. Uopće, množeći sprijeda prvi redak bilo kojim članom x tablice, dobije se skup članova retka u kojem je x. Zgodna vježba!

Prema tome je $I4! = 0\{1, 2, 3\}! \cup 1\,0\,2\,3 \cdot F \cup 2\,0\,1\,3 \cdot F \cup 3\,0\,1\,2 \cdot F$, gdje je $F = 0\{1, 2, 3\}!$ To je rastav grupe u „lijeve položaje" podgrupe.

10.6.2. Nađimo desne položaje iste podgrupe $F = 0\{1, 2, 3\}!$ Neutralan, početni položaj je sama podgrupa F. Izaberimo u preostatku, tj. izvan F jedan element, npr. 1023, i nađimo $F \cdot 1023$; izlazi $F \cdot 1\,0\,2\,3 = \{1\,0\,2\,3,\ 1\,0\,3\,2,\ 2\,0\,1\,3,\ 2\,0\,3\,1,\ 3\,0\,1\,2,\ 3\,0\,2\,1\}$. Vidi se da je $F \cdot 1\,0\,2\,3 \neq 1\,0\,2\,3\,F$. Izaberimo prvi element u preostatku $G \setminus (F \cup F \cdot 1023)$; to je 1023; pa je $F \cdot 1023 = \{1203,\ 1302,\ 2103,\ 2301,\ 3102,\ 3201\}$. Prvi član u preostatku je element 1302, pa se vidi da je $F \cdot 1302 = \{1302,\ 1203,\ 2301,\ 2103,\ 3201,\ 3102\}$.

Vidi se da su 0123, 1023, 1203, 1302 predstavnici *desnih* položaja podgrupe F i da je zadana grupa $S_4 = F \cdot 0123 \cup F \cdot 1023 \cup F \cdot 1203 \cup F \cdot 1302$.

10.6.3. *Skup lijevih položaja* podgrupe F *ne podudara se* sa skupom *desnih položaja iste te podgrupe* F u grupi $S_4 = \{I4\}!$

10.6.4. Četvorna grupa. Simetrična grupa $S_4 = I4!$ ima i drugih raznih podgrupa; zanimljiva je i jednostavna npr. grupa sastavljena od neutralnog elementa $e = 0123$ te permutacija (01) (23), (02) (13) i (03) (12). To je tzv. *četvorna grupa* V.[1)]

Nađimo sve desne i lijeve položaje četvorne grupe $V = \{0\,1\,2\,3,\ 1\,0\,3\,2,\ 2\,3\,0\,1,\ 3\,2\,1\,0\}$ u grupi $I4!$ izabirući u preostatku uvijek prvi član.

Izlazi ovo:

$$V = \{0\,1\,2\,3,\ 1\,0\,3\,2,\ 2\,3\,0\,1,\ 3\,2\,1\,0\}.$$

$$V \cdot 0\,1\,3\,2 = \{0\,1\,3\,2,\ 1\,0\,2\,3,\ 3\,2\,0\,1,\ 2\,3\,1\,0\} = 0\,1\,3\,2 \cdot V$$

$$V \cdot 0\,2\,1\,3 = \{0\,2\,1\,3,\ 2\,0\,3\,1,\ 1\,3\,0\,2,\ 3\,1\,2\,0\} = 0\,2\,1\,3 \cdot V$$

$$V \cdot 0\,2\,3\,1 = \{0\,2\,3\,1,\ 2\,0\,1\,3,\ 3\,1\,0\,2,\ 1\,3\,2\,0\} = 0\,2\,3\,1 \cdot V$$

$$V \cdot 0\,3\,1\,2 = \{0\,3\,1\,2,\ 3\,0\,2\,1,\ 1\,2\,0\,3,\ 2\,1\,3\,0\} = 0\,3\,1\,2 \cdot V$$

$$V \cdot 0\,3\,2\,1 = \{0\,3\,2\,1,\ 3\,0\,1\,2,\ 2\,1\,0\,3,\ 1\,2\,3\,0\} = 0\,3\,2\,1 \cdot V$$

Što vidimo? *Svaki desni položaj* Vx *četvorne grupe* V *ujedno je i pripadni lijevi položaj* xV, tj.

$$Vx = xV \quad \text{za svako} \quad x \in I4!$$

Kaže se da je V *normalna podgrupa u grupi* $I4!$

[1)] Njem: Vierergruppe, prema F. Kleinu [Klajn] (1849—1925), njem. matematičaru.

Ujedno vidimo kako je šest položaja grupe V u S_4 vezano za grupu S_3 svih permutacija brojeva 1, 2, 3; naime, ako x prolazi kroz S_3, tada je $0x$ određena permutacija brojeva 0, 1, 2, 3, pa je $V \cdot 0x$ određen položaj grupe V; unija svih tih šest položaja je upravo S_4.

10.7. Indeks. Lijeva i desna particija G s obzirom na podgrupu F. — **10.7.1.** Definicija. *Lijevi indeks* (*desni indeks*) *podgrupe F prema zadanoj grupi* $(G, \cdot)$ je broj *različitih* skupova gF (odnosno Fg) kad g prolazi grupom G.

Svi ti skupovi određuju tzv. *lijevu* (*odnosno desnu*) *particiju* ili podjelu zadane grupe G prema podgrupi F; ta se podjela označuje sa G/F (odnosno ${}_F\backslash^G$).

»*Modul*« *podjele* F dolazi svakako *ispod* crtâ $/$ odnosno $\backslash$; predmet dijeljenja ili parceliranja dolazi iznad crte; položaj crta određuje relativni položaj *argumenta* g u promatranom preslikavanju, odnosno parceliranju.

Oba su indeksa (lijevi i desni) jednaki. Ali particije ${}_F\backslash^G$ i ${}^G/_F$ jednake su samo kod tzv. *normalnih podgrupa* F.

Npr. indeks alternirajuće podgrupe A_3 u simetričnoj grupi S_3 je 2; indeks grupe tetraedra u grupi kocke je 2. Indeks podgrupe $(5D, +)$ u grupi $(D, +)$ je 5. Indeks grupe $(G, \cdot)$ u samoj sebi je 1.

⟶ **10.7.2.** Teorem. *Kardinalni broj G svake grupe jednak je produktu kardinalnog broja svake podgrupe i indeksa te podgrupe* (Lagrange).

Uistinu, znamo da je za svaku podgrupu F od G (v. 17 § 10.3)

$$G = \bigcup_{x \in G} xF$$

i da su skupovi xF ili identički ili disjunktni i svi su istobrojni; zato je kG produkt od kF i broja tih xF. No, broj skupova xF je upravo indeks od F u G.

10.7.3. Korolar. *Kardinalni broj svake grupe djeljiv je kardinalnim brojem svake podgrupe te grupe.*

10.8. Zadaci.

1. Promatraj neku grupu G i u njoj preslikavanje $x \to xG$, te preslikavanje $x \to Gx$. Jesu li ta dva preslikavanja:
   1) konstantna; 2) jednaka? Konkretiziraj!
2. U aditivnoj grupi $(D, +)$ promatraj podgrupu $(7D, \cdot)$ i preslikavanje $x \to 7D + x$. Navedi skup $D/7D$ svih vrijednosti tog preslikavanja.
3. Nađi D/X gdje je $X = 2D,\ 3D,\ 4D,\ 5D$.
4. Nađi $Q/2Q$ za aditivnu grupu $(Q, +)$ svih racionalnih brojeva. Koliko članova ima $Q/2Q$?
5. Promatraj grupu G kocke i jedan njen element a periode 4. Nađi a^D te G/a^D. Koliko članova ima posljednji skup?
6. Za skup R svih realnih brojeva promatraj $3R$ te $R/3R$. Je li taj skup konačan ili beskonačan? Navedi mu nekoliko članova.

7. Neka je $R(i)$ skup kompleksnih brojeva: 1) kako izgledaju članovi od $(R(i), +)/(R, +)$? 2) Je li ta kvocijentna grupa izomorfna sa grupom $(R, +)$?

8. Promatraj skup Qu svih matrica oblika

$$\begin{bmatrix} u & -v^* \\ v & u^* \end{bmatrix},$$

gdje su u, v kompleksni brojevi; 1) Je li Qu aditivna grupa? U potvrdnom slučaju, kako bi izgledali razredi podgrupe za koje su u, v realni brojevi? 2) Da li je

$$Qu \setminus \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$ multiplikativna grupa?

11. NORMALNE PODGRUPE ZADANE GRUPE. KVOCIJENT-GRUPA

11.0. Priprema. Znamo kako se svaka grupa $(G, \cdot)$ cijepa na svoju podgrupu $(F, \cdot)$ i desne položaje Fg te podgrupe i lijeve položaje gF te iste podgrupe F. Za komutativne grupe je, naravno, svaki desni položaj Fg ujedno i lijevi položaj gF. No, vidjeli smo u § 10.6.4. da može biti $gF = Fg$ za svako $g \in G$ (čak ako grupa G i nije komutativna). Kaže se da je u tom slučaju *podgrupa F normalna* ili *invarijantna*. Pripadno rastavljanje cijele grupe G dopušta da se grupna operacija vrši i među dijelovima i da su pri tom zadovoljeni neki jednostavni zahtjevi. Ti dijelovi služe kao elementi nove grupe — tzv. *faktorske* grupe ili *kvocijentne grupe G/F*.

⟶ **11.1. Definicije normalne podgrupe.** Kaže se da je podgrupa $(F, \cdot)$ grupe $(G, \cdot)$ *normalna ili invarijantna* ako vrijedi

(1) $gF = Fg$ za **svaki** član g cijele grupe G (Galois, 1830).

Naravno, sama grupa je svoja invarijantna podgrupa; također je jedinična podgrupa ($\{1\}$) normalna podgrupa grupe $(G, \cdot)$, jer je

$$g\{1\} = \{1\}g = \{g\} \quad \text{za svako } g \in G.$$

11.1.1. Proste grupe. Grupa je *prosta ili prim* ako osim sebe i jedinične podgrupe ne sadrži drugih invarijantnih podgrupa (isp. definiciju prostih brojeva 6 § 7.3).

11.1.2. Naravno, svaka grupa od p članova (p prost broj) je prosta.

11.1.3. Može se dokazati da je grupa rotacijâ Euklidova prostora E_3 prosta; ni unitarna grupa U_2 sa dvije varijable ni Lorentzova grupa nisu proste. Neka je $E = \{1(2), -1(2)\}$; tada je E normalna podgrupa od U_2; može se pokazati da je kvocijentna grupa U_2/E izomorfna sa grupom rotacija prostora R^3 (v. Smirnov III § 63 i § 64).

11.1.4. I A_n je prosta grupa za svako $n>4$ (Galois).

11.2. Teorem. *Da zadana podgrupa F grupe $(G, \cdot)$ bude invarijantna ili normalna, nužno je i dovoljno da za svako $x\in G$ bude*

$$F=xFx^{-1}. \tag{2}$$

Uslov je nuždan: (1) $\Rightarrow$ (2). To je jasno: dovoljno je jednakost (1) pomnožiti straga sa x^{-1}! Obratno, (2) $\Rightarrow$ (1): dovoljno je (2) pomnožiti zdesna sa x. — Zbog relacije (2) F se i zove *invarijantnom* podgrupom.

Svojstvom (2) često se služimo.

11.3. Prema definiciji invarijantne podgrupe F vrijedi $gF=Fg$ za svako $x\in G$. Prema tome, za normalnu podgrupu F skupovne se funkcije

$$g\to gF$$

$$g\to Fg$$

podudaraju, pa je prema osnovnom teoremu 10.3. potpuno određena množina

$$G/F$$

svih položaja gF, odnosno Fg normalne podgrupe F unutar grupe G: *dva se položaja ili podudaraju posve ili su disjunktni* (mimoležni), tj. ne podudaraju se ni u jednom članu.

11.4. Računanje s razredima. No, zanimljivo je vidjeti kompoziciju ili „produkt“ dvaju proizvoljnih položajâ

$$Fx,\ Fy.$$

Naime, $Fx\cdot Fy=$(asocijacija!)$=F(xF)y=$(uslov *normalnosti*!)$=$
$=F(Fx)y=$(asocijacija!)$=(FF)(xy)=F(xy)$ jer je $FF=F$.

Dakle je

$$Fx\cdot Fy=F(xy);$$

riječima: *produkt dvaju položaja koji su određeni svojim predstavnicima x, y je položaj što ga određuje produkt xy tih predstavnika.*

Dokazat ćemo da je *skup G/F svih položaja određena grupa*; to je tzv. *kvocijentna grupa* G i F.

Dokaz je vanredno jednostavan, a ujedno dalekosežan. Teškoća je jedino u tome što čovjek u početku teže poima da su članovi u G/F čitavi odlomci grupe G — među njima je podgrupa F od G, a ostali su razni pomaknuti položaji te podgrupe F.

11.4.1. Primjer. Uzmimo najprije jedan primjer, i to primjer aditivne grupe $(D, +)$ cijelih brojevu i njene podgrupe $(4D, +)$. Različiti položaji te podgrupe jesu

$$4D,\ 4D+1,\ 4D+2,\ 4D+3;$$

ostale oznake predočuju već zauzete položaje, jer je npr.

$$4D+4=4D,\ 4D+100=4D,\ 4D+723=4D+(4\cdot 180+3)=4D+3.$$

Inače za zbrajanje u skupu $D/4D$ položajâ vidi se da je npr.

$$(4D+2)+(4D+3)=4D+(2+3)=(4D+4)+1=4D+1.$$

Lako se uvjerimo da vrijedi ova radna tablica zbrajanja u skupu $D/4D$:

$+$	$4D$	$4D+1$	$4D+2$	$4D+3$
$4D$	$4D$	$4D+1$	$4D+2$	$4D+3$
$4D+1$	$4D+1$	$4D+2$	$4D+3$	$4D$
$4D+2$	$4D+2$	$4D+3$	$4D$	$4D+1$
$4D+3$	$4D+3$	$4D$	$4D+1$	$4D+2$

Tablica 1

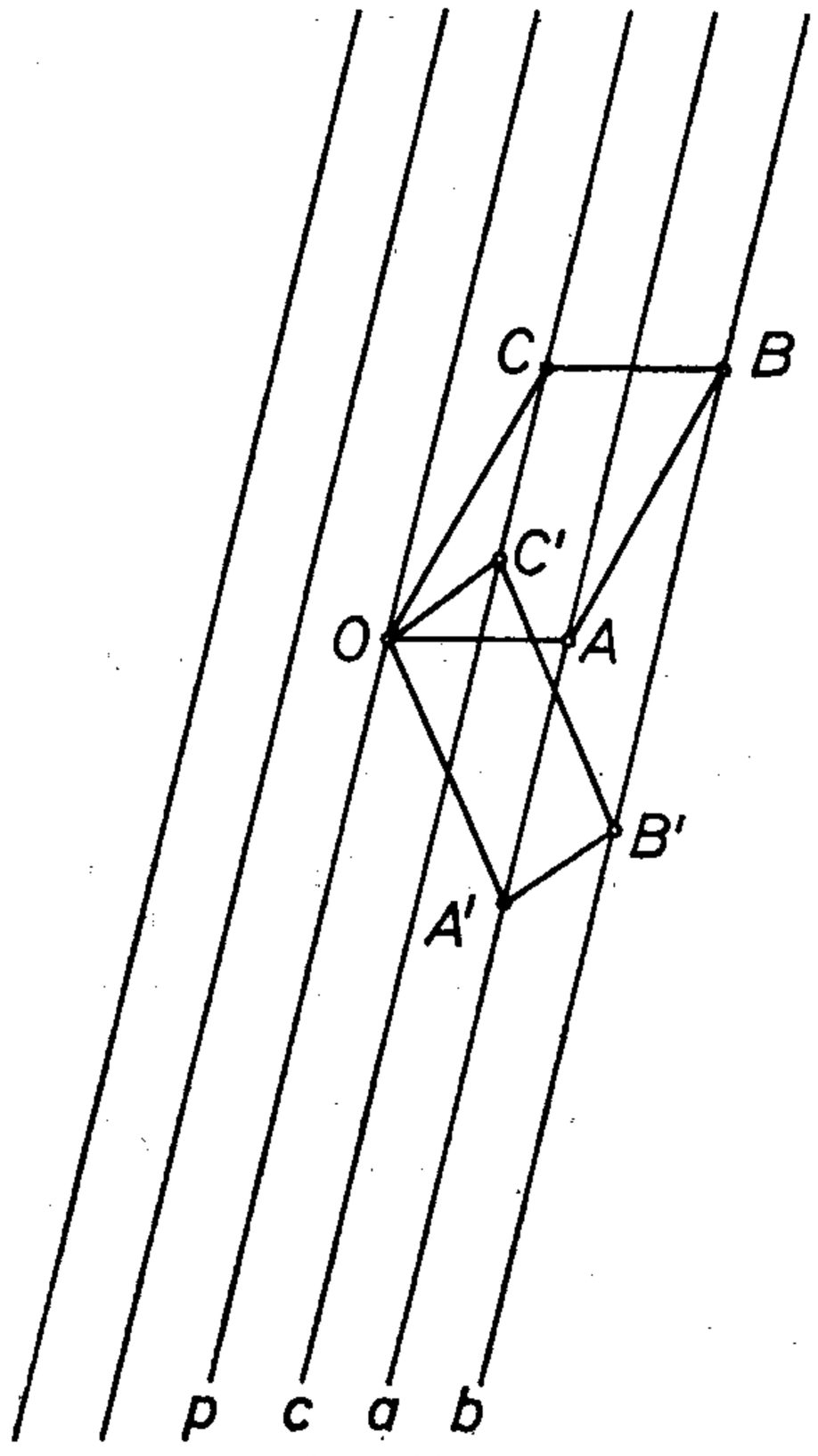
Iz tablice se očitava (kako?) ova tablica *suprotnih elemenata*:

x	$4D$	$4D+1$	$4D+2$	$4D+3$
$\bar{}x$	$4D$	$4D+3$	$4D+2$	$4D+1$

Također se vidi da je $x+4D=4D+x$ za svako $x\in D$ i da je $x+4D=y+4D$ onda i samo onda ako je $x-y\in 4D$, tj. ako je $x-y$ djeljivo sa 4.

11.4.2. Primjer (isp. 17. § 10.5.2). Za grupu $(R^{\neq}, \cdot)$ i njenu podgrupu $(R^{>}, \cdot)$ radna tablica u $R^{\neq}/R^{>}$ glasi ovako:

$\cdot$	$R>$	$R<$
$R>$	$R>$	$R<$
$R<$	$R<$	$R>$



Sl. 17.11.4.2.

11.4.3. Karakterističan primjer (pogl. 17, § 0.1). Neka je R_2 skup svih radijus-vektora u zadanoj ravnini E; neka je O početak tih vektora. Naravno, $(R_2, +)$ je grupa; neka je p proizvoljna pravulja u E, kroz O; tada radijus-vektori kojima kraj leži na p obrazuju određenu grupu $(rp, +)$. Promatramo li u ravnini E sve pravulje $\| p$, dobije se određeno rastavljanje ravnine u sve te pravulje; unija im je E. Ako je $a \| p \| b$ te $A\in a$, $B\in b$, tada drugi kraj sume $\overrightarrow{OA}+\overrightarrow{OB}$ leži na nekoj pravulji $c \| p$; c ne zavisi od izbora tačke A iz a i tačke b iz B, jer ako je $A'\in a$, $B'\in b$ i $\overrightarrow{A'O}+\overrightarrow{OB'}=\overrightarrow{OC'}$, tada je opet $C'\in c$. Naime pravulja c izlazi translacijom $\overrightarrow{OB}$ pravulje a; isto tako translacijom $\overrightarrow{OB}$ i translacijom $\overrightarrow{BB'}$ dobiva se translacija $\overrightarrow{OB'}$; no translacijom $\overrightarrow{BB'}$ prelazi c u sama sebe. Tako, dakle, $a+\overrightarrow{OB'}=c$ za svako $B'\in b$. Zato se može simbolički pisati $a+b=c$; na taj način *skup svih paralela postaje grupom*; neutralni element je polazna pravulja p.

Sam skup R_2 vektora rastavlja se u svoje komade rx, pri čemu je $x \| p$; rx označuje sve radijus-vektore koji se završavaju na pravulji x. Skup svih rx simbolički se označuje R_2/rp; naravno da tada znamo što je $(R_2/rp; +)$; naime $ra+rb$ definiramo kao skup svih vektora oblika $x+y$, gdje je $x \in ra$, $y \in rb$.

Prema tome, ako je $c \in R_2/rp$, tada je c sastavljeno od svih radijus-vektora $\overrightarrow{OX}$ kojima kraj X leži na nekoj određenoj paraleli sa p, tj. $c = ra$, gdje je $a \| p$ i $a \subset E$.

Analogan primjer imamo ako umjesto R_2 promatramo skup R_3 svih radijus-vektora prostora.

—→ 11.5. Teorem. ***Neka je $(G, \cdot)$ grupa, a $(I, \cdot)$ njena normalna ili invarijantna podgrupa; tada za položaj Ix podgrupe I unutar grupe G vrijedi pravilo računanja***

$$Ix \cdot Iy = I(xy) \text{ za svako } x, y \in G \tag{1}$$

pa je skup G/I svih položaja određena grupa s obzirom na to računanje:

$(G/I, \cdot)$ je grupa ili tačnije $((G, \cdot)/(I, \cdot), \cdot)$ je grupa (tu se vidi organska veza između računanja u polaznoj grupi $(G, \cdot)$ i u novoj grupi položaja, tj. u kvocijentnoj ili faktorskoj grupi G/I.

Dokaz teorema sastoji se u provjeravanju sva četiri grupovna aksioma.

1. *Aksiom grupovnosti vrijedi*: Iz X, $Y \in G/I$ izlazi $XY \in G/I$. Zaista, X, $Y \in G/I$ znači da postoji bar jedna dvojka elemenata x, $y \in G$ tako da je $X = Ix$, $Y = Iy$.

   Kako je $(G, \cdot)$ grupa, to iz x, $y \in G$ prema aksiomu G_e izlazi $xy \in G$. Kako je po obrascu (1) $XY = Ix\, Iy = I(xy)$, znači to da je $XY \in G/I$. Dakle vrijedi prvi aksiom, $(G/I, \cdot)$ *je grupoid.*

2. *Aksiom o asocijaciji za G/I vrijedi* $(XY)Z = X(YZ)$ jer uz očigledno značenje $z \in G$ vrijedi $(XY)Z = (Ix\, Iy)\, Iz =$ (obrazac (1)) $= I(xy)\, Iz =$ (obrazac (1)) $= I[(xy]\, z] =$ (asoc. u G) $= I[x\, (yz)] =$ (obrazac (1)) $= Ix\, I(yz) = X(Iy\, Iz) = X(YZ)$, tj. svojstvo asocijacije je na snazi i u G/I.

Treba uočiti da je $(XY)Z = X(YZ)$ jednakost među elementima množine G/I i ujedno jednakost u smislu skupova u skupu G. Ovo posljednje znači da smo promatrali X, Y, Z kao razrede u grupi G, pa onda gornja jednakost znači $(XY)Z \subset X(YZ)$ i $(XY)Z \supset X(YZ)$.

U cijelom dokazu teorema treba to imati na umu.

3. Element I je neutralan u $(G/I; \cdot)$ jer je $IX = I(Ix) = (I \cdot I)x = Ix = X$ za svako $X \in (G/I, \cdot)$.

4. Inverzno od Ix glasi Ix^{-1} jer je $Ix \cdot Ix^{-1} =$ (def) $= I(xx^{-1}) = I \cdot 1 = I$. Dakle je teorem 11.6. zaista istinit.

11.6. Na taj način za svaku grupu $(G, \cdot)$ i svaku normalnu subgrupu $(I, \cdot)$ te grupe imamo potpuno određenu podjelu grupe G na dijelove, koji sačinjavaju određen skup G/I, koji je i sam grupa vezana uz G i I; to je kvocijent-grupa ili faktor-grupa $(G/I, \cdot)$. S tim u vezi dokazali smo ovaj

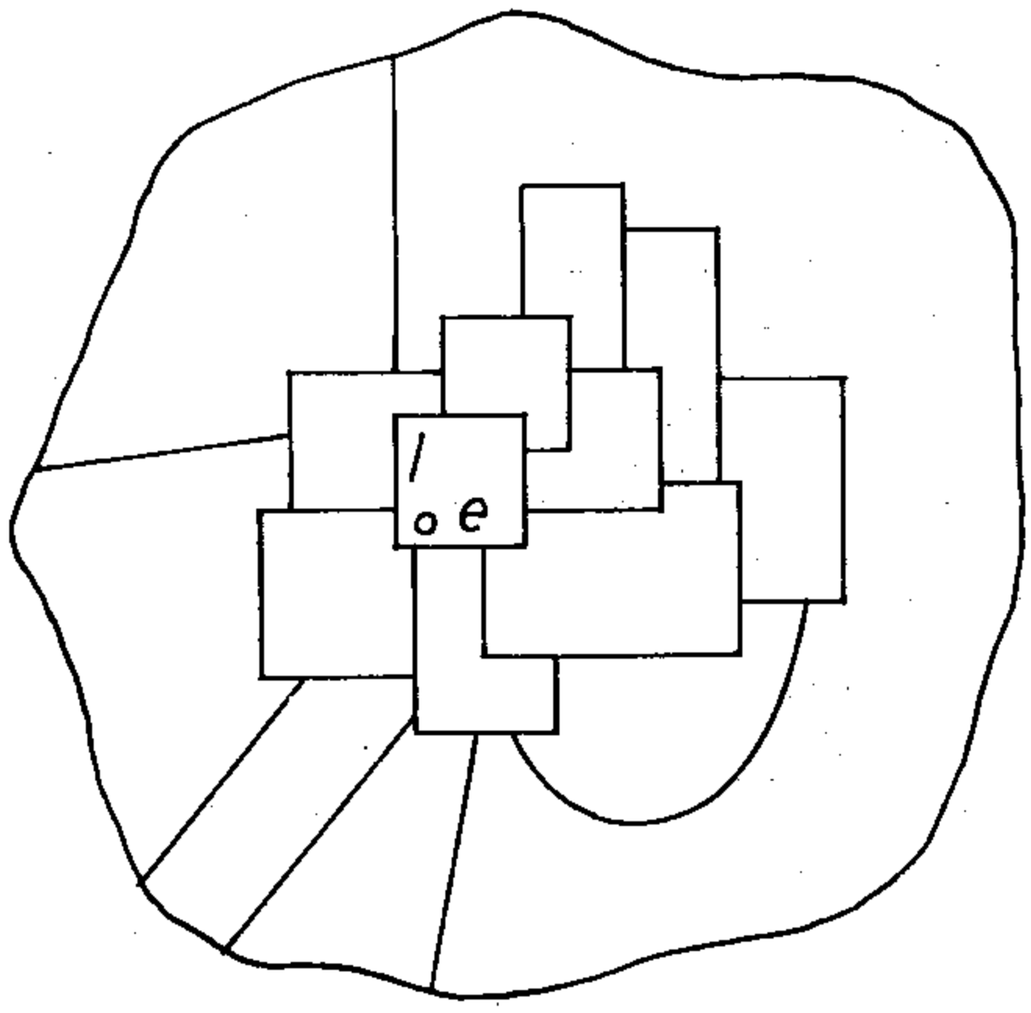
⟶ **11.6.1. Teorem.** ***Ako je*** $(G, \cdot)$ ***grupa, a*** $(I, \cdot)$ ***njena invarijantna podgrupa, tada je preslikavanje po incidenciji***

$$x \to Ix \quad (x \in G)$$

određena veza $x \to fx$ ***između grupe*** $(G, \cdot)$ ***i kvocijent-grupe*** $(G/I, \cdot)$ ***i pri tom vrijedi*** $f(xy) = fx \cdot fy$, ***tj. preslikavanje*** f ***je distributivno prema množenju, odnosno prema grupovnoj operaciji.***

Kaže se da je *f homomorfizam od grupe G prema grupi G/I* (isp. pogl. 17, § 2.4).

11.7. Veze između grupe G i kvocijentne grupe G/I neprestano iskrsavaju i vrlo su bliske. Naime, za svako $X \subset G/I$ potpuno je određen skup $\cup X$-unija svih članova iz X (treba uvijek imati na umu da su članovi iz G/I određeni podskupovi u G); specijalno je $\cup G/I = G$.



Sl. 17.11.7.

Također je očigledno ovo: ako je $(X, \cdot)$ podgrupa u (G/I), onda je $\cup X$ podgrupa u $(G, \cdot)$. Naime, ako je $a, b \in \cup X$, onda je $aI, bI \in X$ dakle $aI\,bI \in X$ (jer je X podgrupa), tj. $abI \in X$, dakle $ab \in \cup X$. Isto se tako vidi da je $a^{-1} \in \cup X$. Također se na sličan način zaključuje da vrijedi ovaj

⟶ **11.7.1. Teorem.** ***Neka je*** G ***grupa, a*** I ***njena invarijantna podgrupa; ako je tada*** X ***(invarijantna) podgrupa faktor-grupe*** G/I, ***onda je*** $\cup X = \bigcup_{x \in X} x$ ***(invarijantna) podgrupa grupe*** G.

Poslije ćemo dokazati da faktor-grupa $G/\cup x$ ima istu radnu tablicu kao faktor-grupa $(G/I)/X$ (isp. pogl. 17, § 16.10. — drugi teorem o izomorfizmu).

11.7.2. Teorem. *Neka je* $(G, \cdot)$ *grupa a I njena invarijantna podgrupa; ako je N bilo koja normalna podgrupa od G, tada je skup* $\overline{N}$ *svih članova u G/I koji presjecaju N normalna podgrupa u* $(G/I, \cdot)$.

Najprije je jasno da je $(\overline{N}, \cdot)$ podgrupa od $(G/I, \cdot)$; dokažimo još da je riječ o *invarijantnoj* ili *normalnoj* podgrupi, tj. da vrijedi

$$(1) \qquad (g\,I)\,\overline{N} = \overline{N}\,(g\,I) \quad \text{za svako} \quad g \in G.$$

Vrijedi $(1)_1 \subset (1)_2$, tj. $A \in (1)_1 \Rightarrow A \in (1)_2$. Naime, skup A je oblika $A = (g\,I)\,n_1\,I$ sa $n_1 \in N$; dakle je $A = (gn_1)\,I$. No, N je *normalna* podgrupa u G pa je za neko $n_2 \in N$ ispunjeno $gn_1 = n_2\,g$; dakle je $A = (n_2\,g)\,I = n_2\,(g\,I) \in (1)_2$. Analogno se dokazuje $(1)_2 \subset (1)_1$.

11.8. Teorem. *Neka je $(G, \cdot)$ bilo kakva grupa, a $(I, \cdot)$ bilo kakva njena invarijantna podgrupa; tada je*

$$(1) \qquad IS = SI \quad \textit{za svako} \quad S \subset G.$$

Za svaku podgrupu $(F, \cdot)$ od $(G, \cdot)$ imamo također podgrupu $(FI, \cdot)$ grupe $(G, \cdot)$.

Dokaz: Prema definiciji invarijantne podgrupe I vrijedi

$$g\,I = Ig \quad \textit{za svako} \quad g \in G;$$

zato tim prije za svako $s \in S$ vrijedi

$$(2) \qquad s\,I = Is \quad \text{jer je} \quad s \in G.$$

$$(3) \qquad \cup s\,I = \cup Is;$$

a ova jednakost (3) znači upravo da vrijedi (1).

Dokažimo da je FI podgrupa. Naravno, drugi i treći aksiom o grupama zadovoljeni su za $(FI, \cdot)$ Dokažimo da je zadovoljen i prvi aksiom; to se svodi na relaciju

$$(4) \qquad FI \cdot FI \subset FI.$$

No, $FI \cdot EI =$ (zbog invarijantnosti od I) $= IF \cdot FI =$ (asoc.) $= I\,(FF)\,I =$ (zbog $FF = F$) $= IFI = (IF)\,I = (FI)\,I = F\,(I \cdot I) = FI$, tj. relacija (4) vrijedi.

Četvrti aksiom o grupama svodi se na to da vrijedi

$$(5) \qquad (FI)^{-1} \subset FI.$$

No, $(FI)^{-1} = I^{-1}\,F^{-1} =$ (zbog $I^{-1} = I$, $F^{-1} = F$) $= IF =$ (stavi $S = F$ u (1)) $= FI$. Dakle vrijedi i (5).

⟶ **11.9.** Teorem (*Dedekindova modularna jednakost*). *Skup $n\,G$ svih normalnih podgrupa grupe $(G, \cdot)$ uređen relacijom inkluzije $\subset$ je mreža u smislu da iz $N, N_1 \in n\,G$ izlazi $\inf\{N, N_1\} \in n\,G$, $\sup\{N, N_1\} \in n\,G$; ujedno je*

$$(1) \qquad N \cap N_1 = \inf\{N, N_1\} \in n\,G,$$

$$(2) \qquad N \cdot N_1 = \sup\{N, N_1\} \in n\,G.$$

Vrijedi ova Dedekindova jednakost: ako je također

$$(*) \qquad N \subset N_1$$

onda je

$$N\cdot(A\cap N_1)=N\cdot A\cap N_1 \quad (A\in n\,G). \tag{3}$$

D o k a z. Relacije (1) su očigledne. Dokažimo (2). Najprije NN_1 je grupoid. Naime, neka je $x,\ x'\in N,\ y,\ y'\in N_1$, tj. $xy,\ x'y'\in NN_1$; tada je $(xy)(x'y')=$ $=x(yx'y')=$(zbog $yx'=x'y_1$ za neko $y_1\in N_1$; to izlazi iz pretpostavke $N_1\in n\,G)=x(x'y_1)y'=(xx')(y_1y_1')=x_2y_2$ gdje je $x_2=xx'\in N,\ y_2=y_1y_1'\in N_1$. Slično se provjere i ostala tri aksioma o grupama. No, NN_1 je i *normalna* podgrupa tj. iz $g\in G$ i $n\in NN_1$ izlazi $gn=n'g$ za neko $n'\in NN_1$. No, $n=xy_1$ za neko $x\in N,\ y_1\in N_1$ pa je $gn=g(xy_1)=(gx)y_1=(x'g)y_1$ (za neko $x'\in N$ jer je N normalno) $=x'(gy_1)=$(zbog $N_1\in n\,G)=x'(y_1'g)=(x'y_1')g=n'g$; pri tom je $y_1'\in N_1$ dakle zaista $n'=x'y_1'\in NN_1$. Time je dokazano (2).

Dokažimo i (3) tj. da vrijedi $(3)_1\subset(3)_2$ i $(3)_2\subset(3)_1$. Pa neka je $n\in(3)_1$ dakle $n=xy$, gdje je $x\in N,\ y\in A\cap N_1$; odatle i radi (*) izlazi $n\in N,\ y\in A,$ $y\in N_1$; dakle $n\in NA,\ n\in N_1$ tj. $n\in(3)_2$.

Dokažimo još dualnu inkluziju. Neka je sada $n\in(3)_2$, dakle $n=xy$ gdje je $x\in N,\ y\in A$ te $x\cdot y\in N_1$. Zbog (*) je $x,\ xy\in N_1$ odakle $y=(x^{-1}(xy)\in N_1$ tj. $y\in A\cap N_1$. Ta relacija zajedno sa $x\in N$ daje traženu relaciju $n=xy\in(3)_1$.

Q. E. D.

11.10. K o r o l a r. *Neka su $N,\ N_1$ normalne podgrupe od $(G,\cdot)$; ako je najmanje jedna od podgrupa $N,\ N_1$ maksimalna, tada je $(NN_1,\cdot)$ ili maksimalna normalna podgrupa ili je $NN_1=G$; ako su obje podgrupe $N,\ N_1$ maksimalne i $\neq$ tada je $NN_1=G$.* Pri tom vrijedi ova

11.11. *Definicija maksimalne* [*minimalne*] *normalne podgrupe.* Normalna podgrupa N grupe $(G,\cdot)$ zove se *maksimalnom* (odnosno *minimalnom*) ako za *svaku* eventualnu normalnu podgrupu $I\in n\,G$ sa svojstvom $N\subset I\subsetneq G$ (odnosno $N\supset I\supsetneq\{1\}$) izlazi $N=I$.

Naravno, ne mora svaka grupa sadržavati koju minimalnu, odnosno maksimalnu normalnu podgrupu. Tako npr. svaka podgrupa F od $(D,+)$ je normalna no nijedna nije *minimalna* u smislu gornje definicije; naime za svako $a\in F\setminus\{0\}$ imamo podgrupu $2a\cdot D$ koja je pravi dio od F pa zato F nije minimalno.

Isto tako $(Q,+)$ nema ni jedne *maksimalne* podgrupe F.

D o k a z. Kako ne može biti $F=\{0\}$, lako se vidi da je $F\cap D=D\cdot a$ za neki prirodan broj a. Uz F *maksimalno* nije ni $a\neq 1$ ni $a=1$. Ako $a\neq 1$, tada grupa $G=F\cdot 1/a$ striktno sadrži F, jer $G=F.\ 1/a\supset D\cdot a.\ 1/a=D$. Osim toga $G\neq Q$, jer bi inače bilo $1/a^2\in G$, tj. $1=a\cdot F\in D\cdot a$.

Ako je $a=1$, tada sigurno postoji $b\in D$ za koji $1/b\notin F$. Zbog toga grupa $G:=F+D\cdot 1/b$ strogo sadrži F. Osim toga $G\neq Q$, jer bi inače bilo

$$1/b^2=F+D\cdot 1/b,\ \text{tj.}\ 1/b=b\cdot F+D\in F.$$

U oba slučaja bilo bi $F\subsetneq G\subsetneq Q$.

Naprotiv, grupa $(D,+)$ *ima maksimalnih invarijantnih podgrupa*; one su oblika $(p\,D,+)$ za svaki prost broj p. Naime, neka je I invarijantna podgrupa od $(D,+)$ sa svojstvom

$$p\,D\subset I\subsetneq D. \tag{1}$$

Tada je $pD=I$. U obrnutom slučaju postojao bi broj $m\in I\setminus pD$; naravno m i p su međusobno prosti; zato postoje cijeli brojevi x, y za koje je $px+qy=1$ (6 § 10.6); no $px\in pD$ dakle $px\in I$; kako iz $q\in I$ izlazi i $qy\in I$ bilo bi px, $qy\in I$ dakle $px+qy\in I$ tj. $1\in I$, a time i $1\cdot D\subset I$, u protivnosti sa (1).

Na sličan se način dokazuju ove činjenice:

11.12. Teorem (*i*). *Ako je* $G\in\{D, Q, R, R(i)\}$, *tada* $(G, +)$ *nema minimalnih normalnih podgrupa; ako je* $G\neq D$, *nema* $(G, +)$ *ni maksimalnih, normalnih podgrupa;* $(D, +)$ *ima maksimalnih podgrupa i one su upravo grupe* $(pD, +)$ *gdje p znači prost broj.*

(*ii*) *Ako je* $(C_\infty, \cdot)$ *ciklička beskonačna grupa, tada ona nema minimalne invarijantne grupe, a maksimalne normalne podgrupe su grupe* $(g^{p\cdot D}, \cdot)$, *pri tom je p bilo koji prost broj, a g generatrisa grupe* C_∞ *tj.* $g^D=C_\infty$.

(*iii*) *Multiplikativna grupa kompleksnih brojeva* $\neq 0$ *nema nikoje maksimalne normalne podgrupe; skup minimalnih podgrupa se sastoji iz cikličkih grupa*

$$\left(e^{i\frac{2\pi}{p}D}, \cdot\right),\ p \text{ prost prirodan broj.}$$

$\longrightarrow$ **11.13. Teorem.** ***Neka je*** $N\in nG$. ***Ako je N maksimalna normalna podgrupa od*** $(G, \cdot)$, ***tada je pripadna kvocijentna grupa*** G/N ***prosta*** **(17, § 11.2); *i obrnuto: ako je*** $(G/N, \cdot)$ ***prosto, tada je N maksimalno.***

(*i*) Kad naime G/N ne bi bila prosta grupa, postojala bi neka normalna podgrupa I od G/N sa svojstvom $\{N\}\subsetneq I\subsetneq G/N$; odatle $N\subsetneq\bigcup I\subsetneq G$ pa bi $(\bigcup I, \cdot)$ bila invarijantna podgrupa smještena strogo između maksimalne podgrupe N i cijele grupe G — apsurd.

(*ii*) Ako je G/N prosto, tada je N maksimalno. Inače bi bilo neko normalno I sa svojstvom $N\subsetneq I\subsetneq G$; neka je $N_I=\{gN;\ g\in G;\ gN\subsetneq I\}$; tada bi N_I bila netrivijalna normalna podgrupa od $(G/N\ \cdot)$, protivno pretpostavci da je $(G/N\ \cdot)$ prosto.

11.14. Zadaci o normalnim podgrupama.

1. Promatraj simetričnu grupu S_3. Ima li ona koju pravu invarijantnu podgrupu?
2. Ako je x idempotentan član u G, tj. ako je $x^2=x$, tada je xI idempotentan u svakoj faktor-grupi G/I. Dokaz!
3. Dokaži da je grupa tetraedra invarijantna podgrupa grupe kocke. Koliko svaka od njih ima članova?
4. Ako je indeks podgrupe jednak 2, ta je podgrupa invarijantna. Dokaži!
5. Ako grupa G sadrži jednu jedinu podgrupu sa zadanim brojem elemenata, onda je ta podgrupa invarijantna. Dokaz!
6. Odredi sve invarijantne podgrupe u S_4.
7. Isto pitanje za grupu kocke, poligona, tetraedra, ...

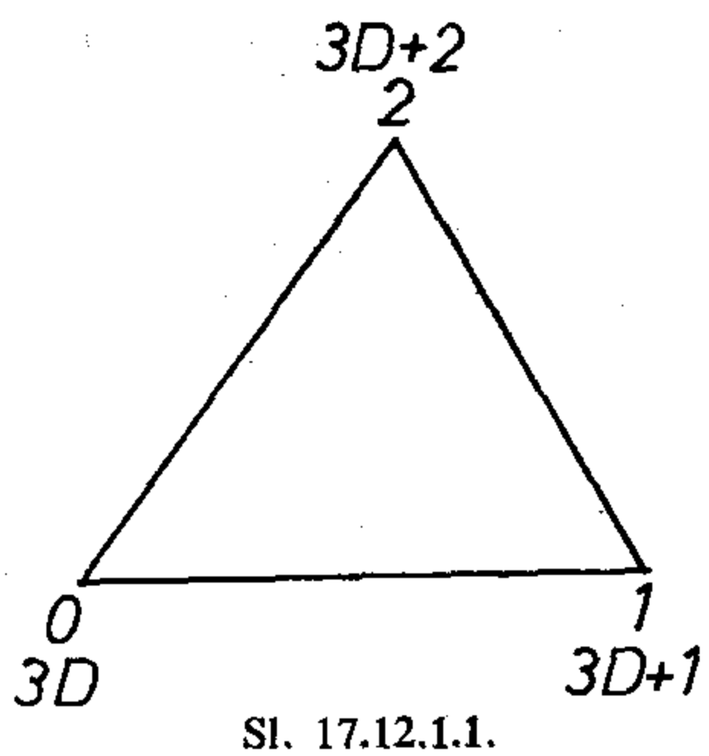
8. Dokaži da sva kretanja prostora R_3 čine grupu kojoj je grupa svih translacija jedna invarijantna podgrupa.

9. Čine li sve transformacije $x' = \cos\alpha \cdot x - \sin\alpha \cdot y + a$, $y' = \sin\alpha \cdot x + \cos\alpha \cdot y + b$ grupu a transformacije dobivene pri $\alpha = 0$ normalnu podgrupu? (α, a, b su proizvoljni realni brojevi).

12. IZOMORFIZAM I HOMOMORFIZAM IZMEĐU GRUPA

12.0. Priprema. Kao što se pojedini broj, npr. 2, pojavljuje u raznim situacijama, tako se i organizacija pojedine grupe ili kakve drupe strukture može pojavljivati raznoliko. Pri tom nećemo toliko gledati na elemente grupe kao takve koliko na *međusobne veze* u grupi.

12.1. Primjer. — **12.1.1.** Promatrajmo „cikličku grupu" C_3, tj. grupu rotacija kojom pravilan 3-kut prelazi u sama sebe; grupa je sastavljena od identične rotacije r_0 te rotacije r_1 za $2\pi/3$ i r_2 za $2 \cdot \frac{2\pi}{3}$ oko središta trokuta.



Sl. 17.12.1.1.

Očigledno, radna tablica u toj grupi glasi

·	r_0	r_1	r_2
r_0	r_0	r_1	r_2
r_1	r_1	r_2	r_0
r_2	r_2	r_0	r_1

Vidimo da je grupa sastavljena od rotacija.

12.1.2. Ako taj trokut shvatimo kao brojevni trokut, tada će i u njegove vrhove doći skupovi $3D$, $3D+1$, $3D+2$, pa će gornje rotacije trokuta definirati zbrajanje ovih skupova sa tablicom

+	$3D$	$3D+1$	$3D+2$
$3D$	$3D$	$3D+1$	$3D+2$
$3D+1$	$3D+1$	$3D+2$	$3D$
$3D+2$	$3D+2$	$3D$	$3D+1$

Tako imamo skupove $\{r_0, r_1, r_2\}$, $\{3D, 3D+1, 3D+2\}$ i pripadne grupe $(\{r_0, r_1, r_2\}, \cdot)$, $(\{3D, 3D+1, 3D+2\}, +)$.

Preslikavanje

$$r_0 \to 3\,D$$

$$r_1 \to 3\,D+1$$

$$r_2 \to 3\,D+2$$

$$\cdot \to +$$

je obostrano jednoznačno i prevodi prvu grupu na drugu tako da ujedno *rezultati* u prvoj grupi prelaze u *odgovarajuće rezultate* druge grupe; ono je izomorfija između prve i druge grupe (isp. pogl. 17, § 2.4).

12.1.3. Ako vrhove trokuta označimo sa 0, 1, 2, tada rotacijama r_0, r_1, r_2 odgovaraju cikličke permutacije 012, 120, 201 niza 0, 1, 2. Te tri permutacije čine grupu u odnosu na slaganje permutacija. Grupa rotacija i grupa permutacija su izomorfne, kao što se vidi iz tolikovanja:

$$r_0 \to 012, \qquad r_1 \to 120, \qquad r_2 \to 201.$$

Očigledno da je ta grupa permutacija izomorfna i sa zbrajanjem skupova $3\,D$, $3\,D+1$, $3\,D+2$, odnosno sa zbrajanjem $+_3$ cijelih brojeva modulo 3, pri čemu za cijele brojeve x, y suma $x+_3 y$ znači svaki član množine $(3\,D+x)+(3\,D+y)$; specijalno se $x+_3 y$ može jednoznačno odrediti da je k tome $x+_3 y \in I\,3$. U ovom slučaju imamo ovu tablicu:

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

i pripadnu grupu $(I\,3;\ +_3)$.

Na taj način vidimo da su ciklička grupa C_3, $(D/3\,D,\ +)$ i grupa $(D,\ +_3)$ modulo 3 međusobno *izomorfne*.

Naravno, to je opća činjenica: broj 3 *može se zamijeniti svakim prirodnim brojem* >1 (*pa i brojem* 1).

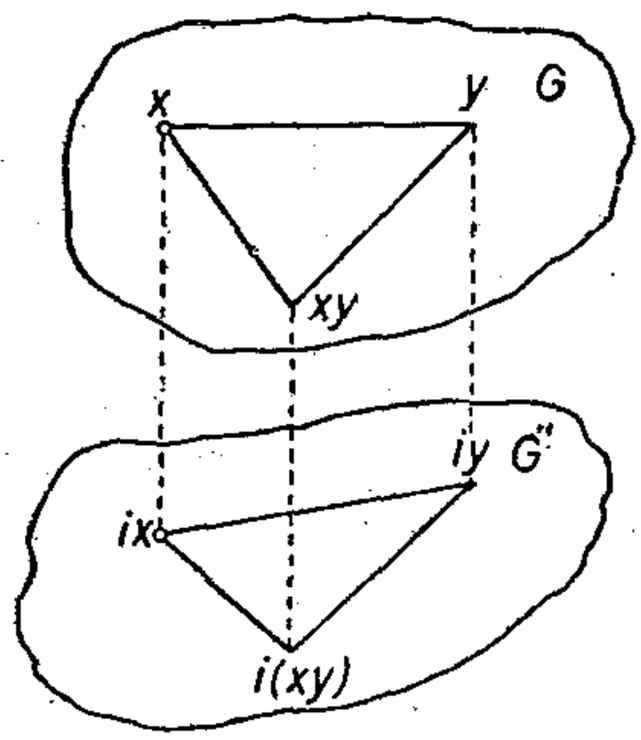
12.1.4. Vrlo poučan primjer. Svakidašnji primjer decimalnih brojeva: preslikavanje beskonačnog $(D,\ +)$ na konačno $(I\,10,\ +_{10})$. Pridružimo svakom cijelom broju b njegovu cifru jedinica b_0; npr. $75\,\underset{|\_|}{4} \to 4$, vidi se da se to preslikavanje h može opisati ovako:

$$10\,n \to 0, \quad 10\,n+1 \to 1, \quad 10\,n+2 \to 2, \ldots, \quad 10\,n+9 \to 9.$$

Time se dobiva određeno preslikavanje h od $(D,\ +)$ ka $(I\,10,\ +_{10})$ i vidi se da je $h(x+y) = hx +_{10} hy$.

Tako smo još bolje i za grupe osvijetlili pojmove o homomorfizmu i izomorfizmu uvedene u § 2.4. za grupoide. Definicija tih pojmova za grupe ista je kao za grupoide. Ponovimo ih i ovdje zbog njihove izuzetne važnosti.

12.2. Definicija izomorfizma i automorfizma grupa. *Grupa* $(G, \cdot)$ *je izomorfna sa grupom* $(G,' .')$ *simbolički* $(G, \cdot) \cong (G', .')$, *ako postoji obostrano jednoznačno preslikavanje i s oblasti G i protuoblasti G' tako da bude* $i(x \cdot y) = ix .' iy$ *za svako* $x, y \in G$, *tj. tako* da je to preslikavanje distributivno s obzirom na operaciju u grupi.



Sl. 17.12.2.

Kaže se da je i izomorfizam između $(G, \cdot)$ i $(G' .')$. Svaki izomorfizam grupe sa samom sobom zove se *automorfizam.*

Shematski, može se izomorfizam i između G, G' predstaviti ovako (vidi sl. 17.12.2):

12.3. Definicija homomorfizma. Grupa $(G', \cdot)$ je *homomorfna* s grupom $(G, \cdot)$, simbolički $(G, \cdot) \sim (G', .')$, ako postoji *jednoznačno* preslikavanje h množine G na množinu G' tako da bude $hG = G'$, te da produkt prelazi u produkt, tj. $h(xy) = hx .' hy$ za svaki par $x, y \in G$. Govori se i o *homomorfizmu* ili *deformaciji* h *od* G *na* G'.

Očigledno je izomorfizam ili izomorfija specijalan slučaj homomorfizma. Tako je npr. grupa translacija koje su paralelne sa zadanom pravuljom p izomorfna aditivnoj grupi $(R, +)$ realnih brojeva (operiranje s translacijama definira se kao uzastopno izvođenje translacija). Dovoljno je pravulju p shvatiti kao brojevnu pravulju; jedinični vektor na brojevnoj pravulju p; tada je dovoljno svakom $x \in R$ pridružiti translaciju za vektor $x \cdot \overrightarrow{OE}$ pa da se vidi da se radi o traženoj izomorfiji.

Grupa $(D, +)$ cijelih brojeva homomorfna je s kvocijentnom grupom $(D/2D, +)$ i pridruživanje $x \to 2D + x$ to pokazuje.

Rezultat 11.6.1. možemo sada izreći i kao

12.3.1. Teorem. *Ako je* $(G, \cdot)$ *grupa, a* $(I, \cdot)$ *invarijantna podgrupa, tada je kvocijentna grupa* $(G/I, \cdot)$ *homomorfna sa zadanom grupom* $(G, \cdot)$; *preslikavanje po incidenciji* $x \to \boldsymbol{x}$ *gdje je* $x \in \boldsymbol{x} \in G/I$, *jest homomorfizam između* $(G, \cdot)$ *i* $(G/I, \cdot)$.

12.4. Primjedbe. — 1.2.4.1. Možemo reći i ovako: *grupa* (G, f) *je izomorfna s grupom* (G', f') ako postoji tolikovanje i između skupova G, G' sa svojstvom da je $iG = G'$, te $i(xfy) = ixf'iy$ za svako $x, y \in G$.

Tako, u primjeru 12.1.2. smo vidjeli da je bilo $f = \cdot$, $f' = +$. No, obično ćemo ipak u obje grupe operacije označivati znakom množenja.

Jednostavno rečeno: *dvije grupe su izomorfne postoji li obostrano jednoznačno pridruživanje između njihovih elemenata koje poštuje grupno svojstvo,* tj. *rezultatu podataka u prvoj grupi odgovara rezultat odgovarajućih elemenata u drugoj grupi*: „trojki" x, y, xy odgovara *pridružena trojka* ix, iy, $i(xy)$ *u drugoj grupi.* Budući da je glavni zadatak teorije grupa proučavanje binarne ope-

racije definirane u skupu, to je nepotrebno, i s grupnog stanovišta nemoguće, razlikovati, *izomorfne grupe*. Zato je dovoljno izučiti *jednu grupu*, pa da *svako njeno grupovno svojstvo* automatski prenesemo na *svaku izomorfnu grupu*.

12.4.2. No, često je teško u klasi izomorfnih grupa naći pogodnu grupu za proučavanje grupne operacije; zato se uvodi pojam homomorfizma, kod koga se grupna operacija *djelomično* proučava.

12.4.3. Homomorfizmi i izomorfizmi se u primjenama često pojavljuju; npr. u teorijskoj fizici, gdje se grupa s obzirom na koju je neki fizikalni zakon invarijantan (recimo uvjet specijalne teorije relativnosti o ograničenosti brzine međudjelovanja) proučava pomoću izomorfne ili homomorfne grupe linearnih operatora.

12.4.4. Tako se prirodno nameće pitanje *reprezentacije grupa*. Grupa G' je uvijek homomorfna svom neutralnom elementu. No, nastoji se naći grupa G tako da je $G \sim G'$, a da G' bude dovoljno bogato, tako da ipak proučavamo ***dobar dio*** ili bar *željeni dio* grupne operacije iz G.

12.5. Nekoliko jednostavnih svojstava homomorfizma i izomorfizma. —

12.5.1. T e o r e m. *Svaki homomorfizam iz jedne grupe u drugu grupu prevodi neutralni (jedinični) element prve grupe u neutralni član druge grupe.*

Neka je h homomorfija od grupe $(G, \cdot)$ na grupu $(G', .')$; neka je 1 jedinica u prvoj, $1'$ jedinica u drugoj grupi. Nađimo $h\,1 = c$. No, $1 \cdot 1 = 1$, pa je zato $h(1 \cdot 1) = h\,1$ što zbog $h(1 \cdot 1) = h\,1\,.'\,h\,1$ postaje $h\,1\,.'\,h\,1 = h\,1$. No, $h\,1$ je određen element u grupi G'; njegov inverzni je $(h\,1)^{-1}$; pomnožimo li otraga njime prethodnu jednakost, izlazi

$$(h\,1\,.'\,h\,1)\,(h\,1)^{-1} = h\,1\,.'\,(h\,1)^{-1} \qquad \text{i dalje}$$

$$h\,1\,.'\,((h\,1\,.'\,(h\,1)^{-1}) = 1'$$

$$h\,1\,.'\,1' = 1', \text{ tj. } h\,1 = 1'.$$

12.5.2. *Pri homomorfnom preslikavanju sačuvan je princip suprotnosti: suprotni element prelazi u suprotni:*

$$h(x^{-1}) = (hx)^{-1}.$$

Dokaz se izvodi iz definicije suprotnosti; najprije je $xx^{-1} = 1$, odakle za homomorfiju h izlazi $hx\,.'\,(hx^{-1}) = h\,1$. No, prema prethodnom teoremu: $h\,1 = 1'$, pa je dakle $hx\,.'\,(hx^{-1}) = 1'$, a to upravo znači da je hx^{-1} suprotno od hx, tj.

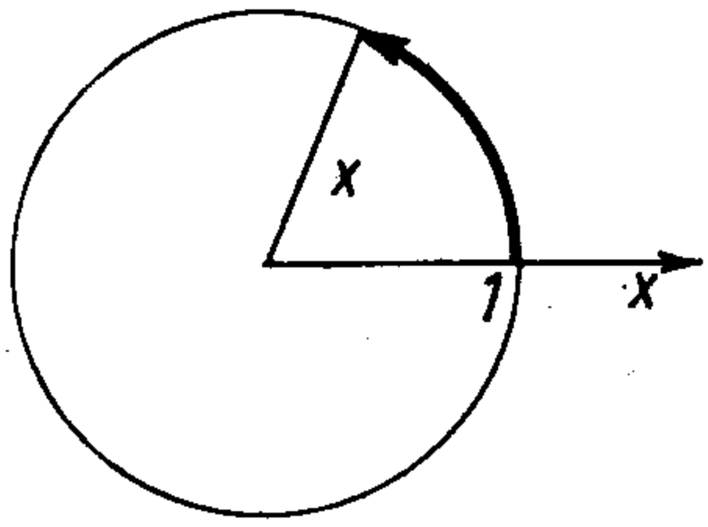
$$hx^{-1} = (hx)^{-1}.$$

Gornja dva svojstva homomorfije specijalan su slučaj ovog teorema:

—→ 12.5.3. T e o r e m. ***$h(x^n) = (hx)^n$ za svaki cijeli broj n i svaku homomorfiju h.***

Teorem je dokazan za $n = 0$, 1. Odatle se induktivno dokazuje za svaki prirodni broj n, kao i za $-n$; pri tom, naravno, definiramo $x^{-n} = (x^{-1})^n$.

12.5.4. Primjer. Promatrajmo grupu $(R, +)$ realnih brojeva te grupu c svih rotacija zadanog kruga oko njegovog središta. Pridružimo broju x rotaciju r_x za x u pozitivnom smislu. Tada je, naravno, $x+y \to r_{x+y} = r_y \cdot r_x = r_x r_y$. Dakle se radi o homomorfiji od $(R, +)$ na $(c, \cdot)$.



Sl. 12.5.4.

Pri tom $r_0 = r_{2\pi} = r_{k \cdot 2\pi}$ za svako cijelo k; r_0 je identičko preslikavanje kruga; r_0 je neutralni element.

Što čine brojevi x za koje je $r_x = r_0$? Njihov skup može se označiti sa $^{-}r_0$. Vidi se da $k \cdot 2\pi \in {}^{-}r_0$ i da je $D \cdot 2\pi = \{r_0\}$. To znači da se pri homomorfizmu $x \to r_x$ podgrupa $(D \cdot 2\pi, +)$ prevodi u $\{r_0\}$; r_0 je neutralni element.

Nadalje, razred $D \cdot 2\pi + x$ i samo on prelazi u $\{r_x\}$ za svako x; na taj način između rotacija r_x za $0 \leq x < 2\pi$ i skupova $2\pi D + x$ imamo tolikovanje. No, skupovi $2\pi D + x$, kad $x \in R$, jesu položaji podgrupe $(2\pi D, +)$ pa njihov skup $R/2\pi D$ daje kvocijentnu grupu $(R/2\pi D, +)$. Promatrano pridruživanje

$$2\pi D + x \to r_x \quad \text{za} \quad 0 \leq x < 2\pi$$

jest izomorfizam između kvocijentne grupe $(R/2\pi D, +)$ i grupe c rotacija.

Zaključak je općenit i vrijedi ovaj

⟶ **12.5.5. Teorem. (Homomorfija kao nosilac izomorfije).** ***Neka je h homomorfizam od grupe $(G, \cdot)$ na grupu $(G', .')$; dakle je $hG = G'$. Neka je g skup svih elemenata iz G za koje $hx = 1$; drugim riječima, $g = {}^{-}h\{1\} = h^{-1}\{1\}$; skup $g = {}^{-1}h\{1\}$ zove se jezgro homomorfizma. Tada je g normalna podgrupa grupe $(G, .')$. Pripadna kvocijentna grupa $(G/g, \cdot)$ izomorfna je s grupom $(G', .')$; pridruživanje***

$$gx \to hx \quad (x \in G) \tag{1}$$

je određen izomorfizam od $(G/g, \cdot)$ na $(G', .')$.

Dokaz. Najprije, $g = h^{-1}\{1\}$ *je normalna podgrupa* u $(G, \cdot)$. Skup g sadrži 1, jer je $h1 = 1.'$ (v. teorem 12.5.1). Nadalje, iz $a, b \in g$ izlazi $ab \in g$. Stvarno, $a, b \in g$ znači da je $ha = 1'$, $hb = 1'$, odakle množenjem: $ha .' hb = 1,'$ tj. $h(ab) = 1'$, jer je h homomorfija. Dakle je zaista $h(ab) = 1'$, tj. $a \cdot b \in g$. Najzad, iz $a \in g$ izlazi $a^{-1} \in g$. Naime, iz $aa^{-1} = 1$ izlazi $h(aa^{-1}) = h1$, tj. $ha .' ha^{-1} = 1'$, što zbog $ha = 1'$ daje $ha^{-1} = 1'$, tj. $a^{-1} \in g$. Dakle je g *podgrupa*. Dokažimo da je g *normalna* podgrupa, tj. da je $xg = gx$ za svako $x \in G$. No, jednakost $xg = gx$ je ekvivalentna sa $xgx^{-1} = g$. Drugim riječima, treba dokazati da iz $a \in g$ izlazi $xax^{-1} \in g$ za svako $x \in G$. No, $h(xax^{-1}) =$ (jer je h homomorfija) $= hx .' h\,a .' hx^{-1} = hx .' 1 .' (hx)^{-1}$, jer je $a \in g$ i $hx^{-1} = (hx)^{-1}$ (v. pogl. 17, § 12.5.2).

Najzad je $hx .' 1 .' (hx)^{-1} = hx .' (hx)^{-1} = 1'$, tj. $h(xax^{-1}) = 1'$, dakle $xax^{-1} \in g$. Time je dokazano da je $g = h^{-1}\{1\}$ invarijantna podgrupa u $(G, \cdot)$. Promatrajmo pripadnu kvocijentnu grupu $(G/g, \cdot)$. Za položaje gx, gy, gdje je $x, y \in G$, imamo

$$gx\,gy = g(xy), \tag{2}$$

jer je g invarijantna podgrupa. Iz (2) izlazi

$$h(gx\,gy) = h(g(xy)) = g \cdot h(xy) =$$

(prema (1)) $$h(xy) = hx.'\,hy.$$

Dakle, zaista je preslikavanjem (1) produktu $gx\,gy = g(xy)$ pridružen produkt $hx.'\,hy$, tj. preslikavanje je homomorfija. Još treba vidjeti da se radi o izomorfiji, tj. da iz $gx \neq gy$ izlazi $hx \neq hy$. Kad bi, naime, bilo $hx = hy$, izlazilo bi odatle množeći otraga sa $(hy)^{-1}$, da je $hx.'\,(hy)^{-1} = 1$ i, dalje, zbog svojstva funkcije h kao homomorfije:

$$hx.'\,hy^{-1} = 1' \;\Rightarrow\; h(xy^{-1}) = 1' \;\Rightarrow\; xy^{-1} \in g, \text{ tj. } xy^{-1} = a,$$

gdje je $a \in g$. Odatle

$$x = ay \;\Rightarrow\; gx = g(ay) = (ga)\,y = gy, \quad \text{tj.} \quad gx = gy,$$

protivno pretpostavci. Time je teorem 12.5.5. potpuno dokazan.

12.6. O invarijantnim podgrupama i homomorfiji. Vidjeli smo da svakom homomorfijom h od grupe $(G, \cdot)$ na grupu $(G', .')$ invarijantne podgrupe $\{1\}$ i G prelaze na odgovarajuće podgrupe u $(G', .')$. Dokazat ćemo da to vrijedi i općenitije.

12.6.1. Teorem. *Ako je h homomorfija grupe $(G, \cdot)$ na grupu $(G', .')$, tada je svakoj invarijantnoj podgrupi $I \subset G$ pridružena time invarijantna podgrupa $(h\,I, .')$ u $(G', .')$. Time se dobije svaka invarijantna podgrupa u $(G', .')$*; tačnije rečeno, ako je $(I', .')$ invarijantna podrupa u $(G', .')$ *onda je $({}^{-}h\,I', .')$ invarijantna podgrupa u $(G, \cdot)$.*

Kad I' prolazi skupom NG' svih normalnih podgrupa u $(G', .')$ prelazi $h^{-1}\,I'$ skupom NG svih normalnih podgupa grupe $(G, \cdot)$ koje sadrže ${}^{-}h\,1'$. Ako su I', I'' dvije različne invarijantne podgrupe u $(G', .')$, tada su ${}^{-}h\,I', \cdot {}^{-}hI''$ dvije različne invarijantne podgrupe u $(G, \cdot)$.

Dokaz. Stvarno, za svako x vrijedi $x\,Ix^{-1} = I$ (v. pogl. 17, § 11.2); odatle

$$hx.'hI.'hx^{-1} = h\,I, \quad \text{odnosno zbog} \quad hx^{-1} = (hx)^{-1}:$$

$$hx.'hI.'\,(hx)^{-1} = h\,I.$$

No, kad $x \in G$, onda $y = hx$ prolazi kroz čitavo G', jer je $h\,G = G'$. Drugim riječima, $y.'\,(h\,I).'\,y^{-1} = h\,I$ za svako $y \in G'$. To upravo znači da je $h\,I$ invarijantna podgrupa u $(G', .')$.

Obrnuto, dokažimo da se na taj način pojavljuje ***svaka*** invarijantna podgrupa I' u $(G', \cdot)$ kad I prolazi svim invarijantnim podgrupama u $(G, \cdot)$. Pa neka je $y\,I'.'\,y^{-1} = I'$ za svako $y \in G'$ tj. zbog $y = hx$, $y^{-1} = hx^{-1}$

(*) $$hx.'I'.'(hx^{-1}) = I' \quad \text{za svako} \quad x \in G.$$

Neka je I skup svih elemenata iz G koji se pomoću h prevode u I', tj. $I = {}^{-}hI'$. To znači da je $h\,I = I'$, pa relacija (*) postaje

$$hx.'h\,I.'hx^{-1} = h\,I.$$

Odatle zbog svojstva distributivnosti funkcije h prema množenju:

$$h(xIx^{-1}) = hI \quad \text{dakle} \quad xIx^{-1} \subset I,$$

a to znači da je I invarijantna podgrupa u $(G, \cdot)$ i da je $hI = I$.

Upravo smo dokazali da je $h^{-1}I'$ invarijantna podgrupa u $(G, \cdot)$ i da ona svakako obuhvata $h^{-1}\{1'\}$. Sa druge strane, neka je $I' \neq I''$; neka je npr. $y \in I' \setminus I''$; tada je ${}^{-}h\{y\}$ određen podskup od G; njega homomorfizam h prevodi u $\{y\} \subset I' \setminus I''$ i zato je ${}^{-}h\{y\} \cap {}^{-}hI'' = \varnothing$; kako je naravno ${}^{-}h\{y\} \subset {}^{-}hI'$, znači da je ${}^{-}hI' \neq {}^{-}hI''$.

12.7. O invarijantnim podgrupama u grupi i kvocijentnoj grupi. Ako je I invarijantna podgrupa od G, tada imamo faktor-grupu G/I i homomorfiju $x \to \overline{x} = Ix$ od G na G/I; ako za svako $X \subset G$ sa $\overline{X}$ označimo skup svih $\overline{x}$ pri čemu je $x \in X$, tada primjenom gornjeg teorema 11.6.1. izlazi

⟶ 12.7.1. Teorem. ***Za svaku invarijantnu podgupu I grupe G imamo $G \sim G/I$, tj. G/I je homomorfno sa G; homomorfijom $x \to \overline{x} = Ix$ prelazi svaka invarijantna podgrupa X iz G u invarijantnu podgrupu $\overline{X}$ u G/I; time se dobije svaka invarijantna podgrupa u G/I.***

Obrnuto, svakoj (invarijantnoj) podgrupi I' grupe G/I odgovara time određena (invarijantna) podgrupa ${}^{-}hI'$ grupe $(G, \cdot)$ koja obuhvata I; različnim (invarijantnim) podgrupama od G/I odgovaraju različite (invarijantne) podgrupe ${}^{-}hI'$, ${}^{-}hI''$ od $(G, \cdot)$.

12.8. Zadaci.

1. Promatraj grupu $(R, +)$ i aditivnu grupu R_n svih skalarnih matrica reda n i s realnim vrijednostima. Dokaži da su te dvije grupe izomorfne. Isto pitanje za odgovarajuće multiplikativne grupe u kojima se ne javljaju nule.

2. Promatraj cikličku grupu C_n od n elemenata; dokaži da je ona izomorfna s grupom $(D_n, +_n)$ „modulo n u skupu D cijelih brojeva", odnosno s cifarskom grupom $(In, +_n)$.

3. Dokaži da je grupa rotacija ravnine r oko zadane tačke 0 iz r kao središta rotacije izomorfna s aditivnom grupom R realnih brojeva modulo 2π.

4. Ciklička grupa C_3 ima tri elementa; postoji li kakva grupa od tri člana koja ne bi bila izomorfna s grupom C_3?
   Isto pitanje za C_p, gdje je p prost broj.

5. Dokaži da grupe C_4 i $(\{1, 3, 5, 7\}; \cdot_8)$ nisu izomorfne i da je svaka četveročlana grupa izomorfna s jednom od tih dviju grupa.

6. Dokaži da pridruživanje

$$a + bi \longleftrightarrow \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

predstavlja određenu izomorfiju između množine svih kompleksnih brojeva i množine svih matrica napisanog oblika (a, b su proizvoljni realni brojevi).

7. Dokaži da preslikavanje $a+bi \to a-bi$ predstavlja izomorfiju u aditivnoj (multiplikativnoj) grupi množine svih kompleksnih brojeva ($\neq 0$). Ima li još koji automorfizam pri kojem svaki realni broj miruje?

8. Koliko automorfizama ima ciklička grupa C_2, C_3, C_4, C_8?

9. Koliko automorfizama ima ciklička grupa
1) C_p; 2) $C_{pp'}$, gdje su p, p' dva različita *prosta* broja?

10. Broj raznih automorfizama grupe G jednak je broju izomorfizama između G i izomorfne grupe G'.

11. Promatraj grupu $(D, +)$ i u njoj preslikavanje $D \to I3$ po kongruenciji modulo 3. Radi li se tu o homomorfizmu? Zamijeni tu 3 sa n, gdje je $n \in N$.

12. Realnom broju x pridruži broj x' tako da bude $0 \leq x' < 2\pi$ te $x - x' \in 2\pi D$. Radi li se tu o homomorfnom preslikavanju h grupe $(R, +)$? Ako da, odredi pripadnu grupu $(hR, +)$ i skup svih članova iz R koji se preslikavaju u 0.

13. Isto pitanje kao u zadatku 12, zamjenjujući broj 2π brojem:
1) 1; 2) 5; 3) 60; 4) (3/2); 5) a, gdje je a bilo koji realni broj.

14. U multiplikativnoj grupi realnih brojeva $\neq 0$ promatraj preslikavanje:
1) $x \to |x|$; 2) $x \to -x$; 3) $x \to 2x$; 4) $x \to x^{-1}$; 5) $x \to x^2$;
6) $x \to x^{1/2}$; 7) $x \to x^{-1/2}$. U kojim se slučajevima radi o homomorfiji? Odredi pripadnu homomorfnu grupu.

15. Gledajte kocku $01230'1'2'3'$ na str. 589 kao i dijagonale $a = 02'$, $b = 13'$, $c = 20'$, $d = 31'$; svakoj rotaciji r_i ($i = 1, 2, \ldots, 24$) kocke u samu sebe odgovara određena permutacija p_i niza $a, b, c\ d$; dokaži da je preslikavanje $r_i \to p_i$ izomorfizam između grupe kocke i grupe S_4.

13. KAKO SE GRUPE POJAVLJUJU I KAKO SE PRAVE?

13.0. Grupa se može ostvariti iz pojedine situacije koja prirodno naginje ka grupi (npr. prelaz od grupoida $(N, +)$ na grupu $(D, +)$), nadalje se može automatski pojaviti (npr. skup svih obratljivih članova u kakvoj regularnoj polugrupi) ili se može izvesti iz zadanih grupa, itd.

Opišimo ovdje *tipičan način kako se iz grupoida* $(N, \cdot)$ *prirodnih brojeva izgrađuje proširenjem grupa* $(Q^>, \cdot)$ *pozitivnih racionalnih brojeva u kojoj je grupoid* $(N, \cdot)$ *smješten.*

Jedna je stvar jasna: ako zadani grupoid $(G, \cdot)$ *nije grupa*, onda će se u skup G zbilja morati dovoditi novih članova pa da se na *široj bazi izgradi zajednica* — grupa — *u kojoj će struktura polaznog grupoida ostati netaknuta.*[1)]

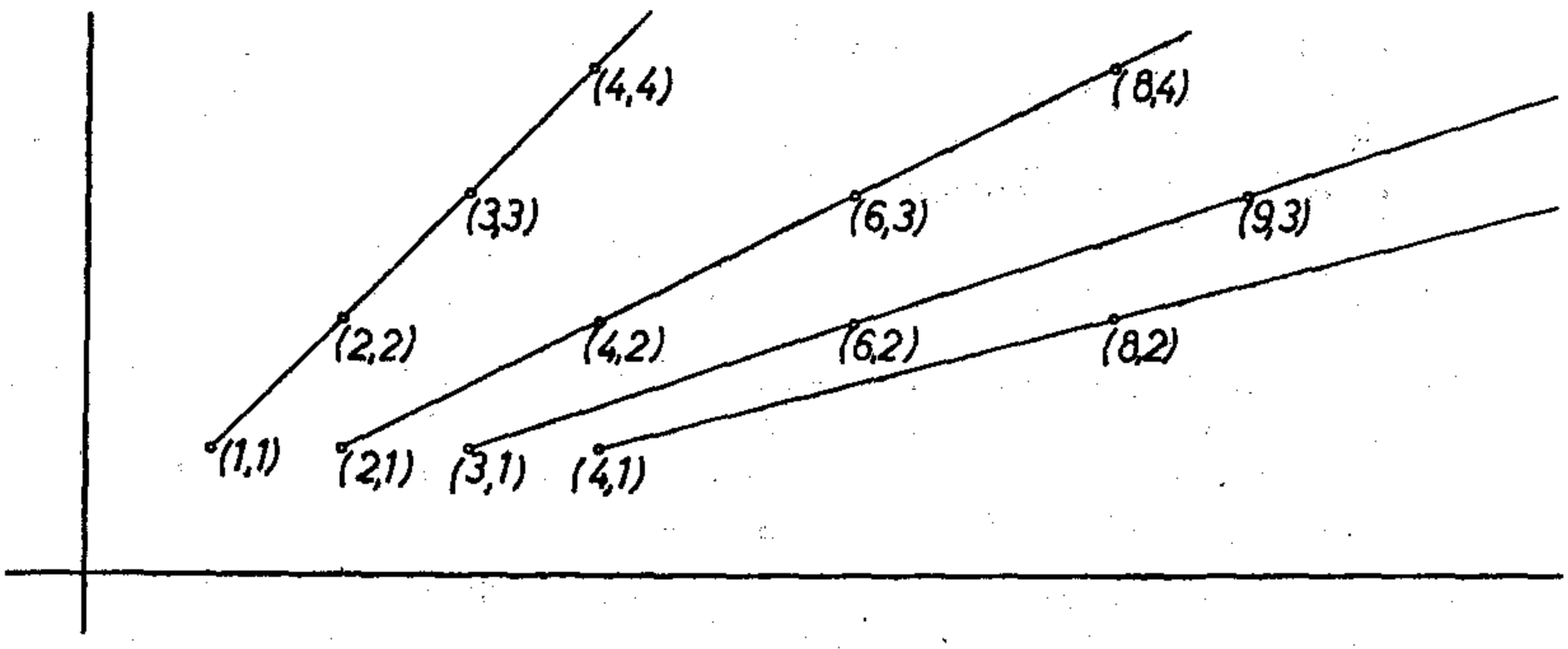
[1)] Drugo je pitanje ovo: imajući grupoid $(G, \cdot)$, izgraditi *grupu* kojoj je množina G materijalna baza-materijal. To je uvijek moguće, no organizacija (G, f) u toj grupi *mora rušiti bar neke veze u polaznom grupoidu*, tj. postoji najmanje jedan par $x, y \in G$ sa svojstvom $x \cdot y \neq xfy$.

13.1. O jednom obliku grupoida $(N, \cdot)$. U grupoidu $(N, \cdot)$ brojeva 1, 2, ... izgrađuje se čitav račun s kvocijentima m/n, za koje je n djelitelj od m, tj. $n|m$. Posebno se dokazuju ova dva pravila:

$$(1) \qquad m/n \equiv m'/n' \Leftrightarrow m \cdot n' \equiv m' \cdot n$$

$$(2) \qquad \frac{m}{n} \cdot \frac{m'}{n'} \equiv \frac{mm'}{nn'}.$$

Razmatrajmo stvar skupovno i slikovito i znajmo da je $m:n$ rezultat preslikavanja para (m, n). No, svi parovi (m, n) za koje je $n|m$ daju shematski ovakav skup N_∞:



Sl. 17.13.1.

Prema tome, N_∞ označuje skup svih pari (m, n) prirodnih brojeva za koje je m djeljivo sa n.

Računanje s gornjim kvocijentima u N odražava se kao računanje u skupu N_∞; npr. $(6:2)\cdot(16:4)\equiv 12$ znači u N_∞ ovo:

$$\text{element } (6, 2)\cdot \text{element } (16, 4)\equiv(6\cdot 16,\ 2\cdot 4).$$

I ta čudna mreža N_∞ uređenih parova (m, n) je *grupoid*: $(N_\infty, \cdot)$ je grupoid, pri čemu *definiramo* (isp. (1) i (2)):

$$(3) \qquad (m, n)\cdot(m', n')\equiv(m\cdot m',\ n\cdot n').$$

Grupoid $(N_\infty, \cdot)$ je homomorfan s polaznim grupoidom $(N, \cdot)$, preslikavanje $(m, n)\to m{:}\ n$ iz N_∞ u N je homomorfija.

Naravno, to preslikavanje nije izomorfija, jer vidimo da ono narušava individualnost. Različite tačke, npr. (3, 1), (6, 2), (9, 3), ... iz N_∞ prelaze u isti element množine N.

No, time se množina N_∞ *na prirodan način cijepa u razrede*; prvi razred: sve tačke na prvoj gornjoj kosoj liniji, pa one na idućoj itd.

Nazovimo tačke (m, n), (m', n') *ekvivalentnima* ako vrijedi (1), tj.

$$(m, n)\sim(m', n') \Leftrightarrow m\cdot n'\equiv n\cdot m'; \tag{4}$$

tada su razredi definirani kao *najopsežniji skupovi ekvivalentnih tačaka. Skup svih razreda* označuje se sa $N_\infty|\sim$, da se bolje uoči množina N_∞, koja se razdjeljuje, i relacija $\sim$, koja to cijepanje vrši. Radi kraćeg pisanja označimo ipak sa $N_\sim$ skup svih tih razreda. Tako npr.

$$\{(3, 1), (6, 2), (9, 3), (18, 6), \ldots, (n\cdot 3, n), \ldots\}\in N_\sim.$$

Računanje u skupu N_∞ odrazuje se u računanju s razredima; i vidi se npr. da je $\{(2, 1), (6, 2)\cdots, (2m, m)\cdots\}\cdot\{(7, 1), (7\cdot 2, 2), \ldots (7n, n)\cdots\}\equiv$ $\equiv$skup svih tačaka $(2m\cdot 7n, m\cdot n)$; izlazi razred $r(2\cdot 7)$, dakle $r(2)\cdot r(7)\equiv$ $\equiv r(2\cdot 7)$.

Pri tom označujemo sa $r(n)$ množinu $\{(n, 1), (2n, 2), (3n, 3), \ldots\}$.

Vidi se da je uvijek *produkt dvaju razreda opet razred*; to znači ovo: $(N_\sim, \cdot)$ je grupoid. Elementi toga grupoida su razredi. I vidi se da je taj grupoid izomorfan s polaznim grupoidom $(N, \cdot)$: dovoljno je svako $r(n)$ iz $N_\sim$ i n iz N spariti. Dobije se izomorfija: $n\leftrightarrow r(n)$. A sada dolazi pouka:

13.2. Izgradnja grupe svih pozitivnih racionalnih brojeva.

13.2.1. Radimo na posve isti način (ne u čudnom skupu N_∞ nego) u čitavu Descartesovu kvadratu

$$N\times N \tag{5}$$

svih parova (m, n) prirodnih brojeva (*bez ograničenja da je m djeljivo sa n*).

Računajmo po propisu (3): struktura

$$(N\times N, \cdot) \quad \text{je grupoid.} \tag{6}$$

Promatrajmo relaciju ekvivalentnosti (4) i u množini (5); promatrajmo pripadne razrede, i skup $(N\times N/\sim$ — označimo ga sa E — svih tih razreda.

13.2.2. Računanje (struktura) u grupoidu (6) ima za posljedicu određeno računanje u skupu svih razreda.

13.2.3. I dolazi iznenađenje: $(E, \cdot)$ *je grupa koja na prirodan način »proširuje« polazni grupoid* $(N, \cdot)$. Da je $(E, \cdot)$ grupoid, i to asocijativan i s neutralnim članom $\{(1, 1), (2, 2), \ldots\}\equiv r(1)$, dokazuje se na vlas isto kao i za $(N, \cdot)$. No, sad se pojavljuje i *simetrija*:

Razred $r(n)\equiv\{(n, 1), (n, 2, \ldots\}$ i razred $\{(1, n), (2, n), (3, n), \ldots\}$ jedan su drugom protivni, produkt im je neutral.

13.2.4. *Polazni grupoid* $(N, \cdot)$ *i novi grupoid* $(E, \cdot)$ *mogu se dovesti u vezu time da povežemo razred* $r(n)$ *i broj* $n\in N$. Čak je praktično taj *razred* označiti naprosto sa n, njegov a suprotni sa n^{-1}; kaže se i ovako: *za svako n iz polaznog grupoida reći ćemo da su elementi odgovarajućeg razreda njegova* ***predočivanja,*** *pa ih zato možemo identificirati sa n;* možemo sve elemente razreda protivnog od n identificirati i kazati da ti elementi predstavljaju jedno te isto matematičko biće koje ćemo označiti sa n^{-1} ili ^{-}n (anti n), da se vidi veza sa n (odnosno $n\cdot n^{-1}\equiv 1$).

13.2.5. Prelaz $(N, \cdot) \to \overline{(N, \cdot)}$. Na taj način, identifikacijom ekvivalentnih elemenata u $N \times N$ i identifikacijom svakog člana iz N sa članovima „njegova" razreda u $N \times N$, *dobije se određeni skup i određena struktura u njemu*; naznačimo to sa $\overline{(N; \cdot)}$; *to je grupa u kojoj je* $(N, \cdot)$ *podgrupoid.* Kaže se da je iz grupoida $(N, \cdot)$ nastalo $\overline{(N, \cdot)}$ procesom, pravljenjem svih *kvocijenata članova iz N.*

13.2.6. Inače, da nismo provodili gornje identifikacije svakog elementa iz $N \times N$ i svih članova odgovarajućeg razreda u $N_\sim$, ne bismo mogli reći da je $(N, \cdot)$ *podgrupoid od* $\overline{(N, \cdot)}$, nego da je *izomorfan* s jednim podgrupoidom od $\overline{(N, \cdot)}$. S teorijskog gledišta, ovo je stanovište ispravnije. Tada se vidi ovo:

13.2.7. Teorem. U svakoj *grupi X* u kojoj se nalazi *izomorfna slika grupoida* $(N, \cdot)$ nalazi se i izomorfna slika *čitave grupe* $\overline{(N, \cdot)}$.

Naime, ako za svako $n \in N$ označimo sa $i(n)$ element u X koji pri nekoj izomorfiji od $(N, \cdot)$ u podskupu od X odgovora članu n, onda (X je grupa!) mora također $(i(n))^{-1}$ biti u X; smjestimo li, dakle, n^{-1} od $\overline{(N; \cdot)}$ u $(i(n))^{-1}$ od X, dobije se smještaj u X za čitavo $\overline{(N; \cdot)}$.

13.3. Teoremi o proširenju. Na posve isti način, ponavljajući od riječi do riječi gornje razmatranje § 13.2, dokazuje se ovaj

⟶ 13.3.0. Teorem. ***Neka je*** $(G, \cdot)$ ***bilo kakav asocijativan komutativan regularan grupoid; tada se*** $(G, \cdot)$ ***može proširiti u komutativnu grupu, u kojoj je svaki element kvocijent članova iz G; svaka dva takva proširenja međusobno su izomorfna.***

Ili u aditivnoj formi: *neka je* $(G, +)$ *bilo kakav asocijativan komutativan regularan grupoid; tada se, ne gledajući na izomorfiju,* $(G, +)$ *može na jedan i samo jedan način proširiti na komutativnu grupu u kojoj će svaki član formalno biti diferencija uređenog para članova iz polaznog grupoida.*

⟶ 13.3.1. Korolar. ***Specijalno, može se grupoid*** $(N, \cdot)$, ***odnosno grupoid*** $(N, +)$ — ***ne obazirući se na razlike u pogledu izomorfnosti — na jedan jedini način proširiti na komutativnu grupu u kojoj je svaki član kvocijent (diferencija) članova iz N; [time se dobiva grupa*** $(Q, \cdot)$ ***(odnosno*** $(D, +)$***) svih pozitivnih racionalnih brojeva (cijelih racionalnih brojeva).***

13.3.2. Pođemo li od *grupoida* $(D_{\neq}, \cdot)$ cijelih racionalnih brojeva $\neq 0$, dolazimo na gornji način do grupe $\overline{(D_{\neq}, \cdot)} \equiv$ grupa $Q_{\neq}, \cdot)$ svih racionalnih brojeva $\neq 0$.

13.3.3. Ako proces iteriramo, tj. napravimo li slično $\overline{(Q_{\neq}, \cdot)}$ ovaj se rezultat podudara s upravo dostignutim.

Slično $\overline{\overline{(G, \cdot)}} \equiv \overline{(G, \cdot)}$ za svaki asocijativni komutativni regularni grupoid $(G, \cdot)$.

13.3.4. Primjedba. Inače je *zgodnije polazni grupoid* $(G, \cdot)$ *proširiti neutralom*, ako ga još nema. To je jednostavan posao, kao što smo vidjeli u pogl. 17, § 4.1; a lakše je provoditi identifikaciju u $G \times G$.

13.3.5. Koliko se god gornje proširenje grupoida $(N, \cdot)$ činilo zamršeno, ipak treba znati da je ono u stvari jednostavno i da vodi do cilja; vanredno je korisno paralelno promatrati proširenje od $(\{0, 1, 2, \ldots\}, +)$ i proširenje od $(N, \cdot)$; prvo je mnogo jednostavnije. Naime, u prvom slučaju, kao proširenje, dolazi samo „zrcalna slika" grupoida prema neutralu. Mnogo je zamršenija stvar pri zatvaranju $(N, \cdot) \to \overline{(N, \cdot)}$, jer zrcalna slika od N prema neutralu 1 daje samo skup $N^{-1} \equiv \{1^{-1}, 2^{-1}, 3^{-1} \ldots\}$, a proširenje $N \cup N^{-1}$ ni izdaleka *još nije grupa*: zadovoljava doduše, sva tri grupna aksioma osim prvog, ali ne zadovoljava *osnovni prvi aksiom*: biti grupoid!

—→ Gornji duboki prelaz $(G, \cdot) \to \overline{(G, \cdot)}$ znat će se procijeniti npr. kad se hoće ***nekomutativna** polugrupa proširiti na grupu*!

13.4. Generatori grupe. Slobodne grupe! Svaki element a grupe $(G, \cdot)$ proizvodi podgrupu a^D te grupe; a^D je ujedno *najmanja podgrupa* koja sadrži a. Može se desiti da se za koji svoj element a *ciiela grupa podudara sa* a^D; kaže se tada da je *grupa ciklična*. Takav je slučaj npr. s aditivnom grupom $(D, +)$ svih cijelih racionalnih brojeva. Grupa $(Q_{\neq}, \cdot)$ racionalnih brojeva koji su $\neq 0$ nije ciklična.

Analogno je za dva elementa a, b iz grupa; oni najprije generiraju svaki za sebe podgrupe a^D, b^D; svaka grupa koja treba da sadrži $\{a, b\}$ sadrži i a^D, b^D, kao i skupove $a^D \cdot b^D$, pa skupove dobivene iz ovih $b^D \cdot a^D$, množeći svaki od njih lijevo i desno sa a^D, b^D, itd., itd. Unija svih tih skupova daje grupu $[a, b]$, *koju generira zadani dvočlani skup* $\{a, b\}$, Slično za tročlani podskup $\{a, b, c\}$ imamo grupu $[a, b, c]$ *sastavljenu od svih članova što ih rađaju* a, b, c. Ujedno je $[a, b, c]$ ***najmanja*** grupa koja obuhvata i a i b i c. Naime, $[a, b, c]$ se nalazi u *svakoj grupi* u kojoj se pojavljuje struktura $(\{a, b, c\}, \cdot)$ kao podstruktura, tj. u kojoj će biti ne samo a, b, c nego i produkti tih elemenata.

Kaže se da su elementi a, b *generatori ili izvodnice grupe* $[a, b]$; oni su *slobodne izvodnice* (*generatori*), a grupa $[a\ b]$ zove se *slobodnom s dva generatora ako* a i b zadovoljavaju jedino trivijalne veze $a^0 \equiv b^0 \equiv 1$ i produkte takvih veza.

Slično se definiraju *slobodne grupe s* 3, 4, ... *slobodne izvodnice*. Tako npr. ako φ označuje rotaciju kugle za π oko zadane osi x, a ψ rotaciju te kugle za $2/3\,\pi$ oko neke druge osi y, onda je, naravno, $\varphi^2 = 1$, $\psi^3 = 1$, dakle

$$\varphi^2 = \psi^3. \tag{*}$$

No, može se dokazati da između φ i ψ nema nikakve druge veze osim veze (*) i relacijâ koje se odatle na očigledan način dobivaju (naime potenciranjem). Na tom svojstvu rotacija φ, ψ osniva se *famozno Hausdorffovo otkriće* (1914) *da se polovina kugline površine može rotacijom dovesti u prekrivanje s trećinom kugline površine.*

13.5. Zadaci o generiranju grupa.

1. Koju podgrupu u grupi $(D, +)$ generira skup:
   1) $\{4, 6\}$; 2) $\{3\}$; 3) $\{3, 4\}$; 4) $\{10, 25\}$; 5) $\{-10, 25\}$;
   6) $\{12, 28\}$; 7) $\{4, 14, 26\}$ 8) $\{a, b\}$?

2. Koju podgrupu u multiplikativnoj grupi kompleksnih brojeva generira skup: 1) $\{-1\}$; 2) $\{i\}$; 3) $\{e^{i\frac{2\pi}{3}}\}$; 4) $\{1+i\}$; 5) $\{i,\ 1+i\}$; 6) $\{3+4i,\ 3-4i\}$?

3. Promatraj grupoid $(I\,8;\ \cdot_8)$ prema množenju modulo 8; da li ovaj skup generira podgrupu:
1) $\{3\}$; 2) $\{3,\ 5\}$; 3) $\{2\}$; 4) $\{4\}$; 5) $\{5,\ 7\}$?

4. Da li su grupe $(\{-1,\ 1,\ i,\ -i\};\ \cdot)$; $(\{1,\ 3,\ 5,\ 8\};\ \cdot_8)$ izomorfne? Ima li koja 4-člana grupa koja nije izomorfna ni s jednom ni s drugom?

5. Jesu li grupe S_3, C_6 izomorfne? Ima li ikoja grupa od 6 elemenata koja nije izomorfna ni sa S_3 ni sa C_6?

6. *Kvaternionska grupa.* Sastavi tablicu množenja ovih 8 matrica:

$$a\equiv\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\quad b\equiv\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix},\quad c\equiv\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix},\quad d\equiv\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix},$$

$$e\equiv\begin{bmatrix}i & 0\\ 0 & -i\end{bmatrix},\quad f\equiv\begin{bmatrix}-i & 0\\ 0 & i\end{bmatrix},\quad g=\begin{bmatrix}0 & -i\\ -i & 0\end{bmatrix},\quad h=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix};$$

i dokaži da se dobije grupa. Dokaži da je ta grupa izomorfna s kvaternionskom grupom $Qu=(\{1,\ -1,\ i,\ -i,\ j,\ -j,\ k,\ -k\},\ \cdot)$ za koju vrijedi $i^2=-1$, $ij=k=-ji$ kao i druge relacije dobivene cikličkom zamjenom slova $i,\ j,\ k$.

7. Dokaži da je kvaternionska grupa Qu izomorfna s podgrupom $S_8\{a, b\}$ permutacija elemenata 1, 2, 3, 4, 5, 6, 7, 8, koju proizvode permutacije $a=(1234)\,(5678)$, $b=(1537)\,(2846)$ i da je $S_8\{a,\ b\}=(I,\ a,\ b,\ ab=(1836)\,(2745),\ ba=(1638)\,(2547),\ a^2=b^2=(13)\,(24)\,(57)\,(68),\ a^3=(1432)\,(5876),\ b^3=(1735)\,(2648)\}$; provjeri jednakosti: $a^4=b^4=I$; $a^2=b^2$, $aba=b$, $bab=a^3$, $(aba)\,b=a^3\,b^2=a$, $a^3\,b=b^2\,ab=ba$, $b^3\,a=a^2\,ba=ab$.

8. Dokaži da se skup svih podgrupa grupe Qu sastoji od onih 6 podgrupa kojima su izvodnice: 1, odnosno -1, odnosno i, odnosno j, odnosno k, odnosno $\{i, j\}$.

9. Svaka podgrupa od Qu je invarijantna.

10. Da grupa $(G,\ \cdot)$ bude izomorfna s grupom Qu nužno je i dovoljno da je generiraju dvije izvodnice a, b, perioda 4 i da vrijedi:

$$a^2=(ab)^2=b^2.$$

11. Za svaki prirodni broj n ima ciklička grupa C_n upravo $\varphi(n)$ generatora (isp. 6, § 17.6.2).

14. DESCARTESOVO MNOŽENJE GRUPA. DIREKTNI PRODUKT (SUMA)

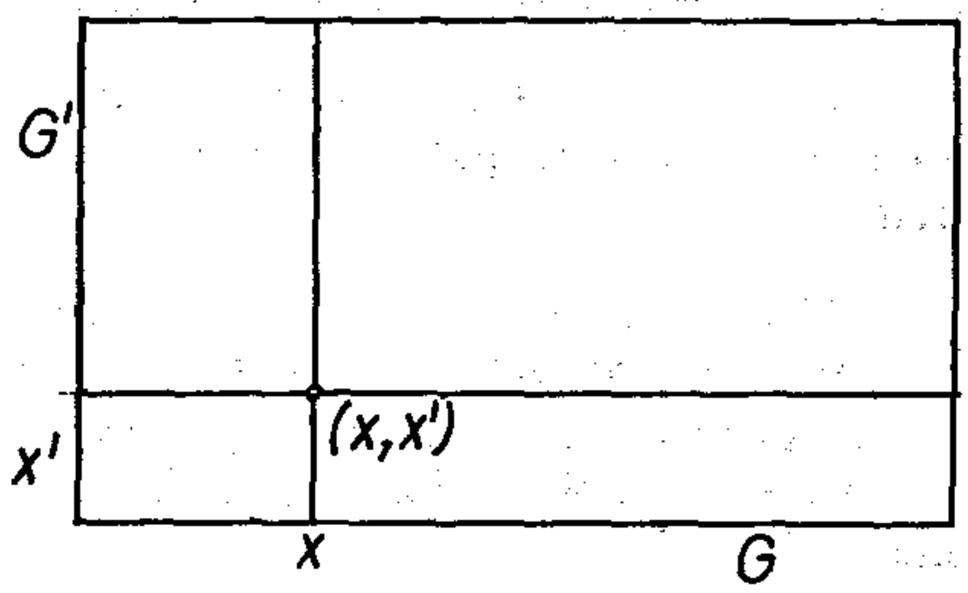
14.0. U toku čitava izlaganja mogli smo se uvjeriti od kako je osnovne važnosti **Descartesovo** ili *kombinatorno množenje skupova.* Na prirodan način množe se ne samo goli skupovi nego i organizacije koje skupovi nose.

14.1. Definicija Descartesova množenja grupoida (grupa). Neka je $(G, \cdot)$, $(G', \cdot)$ uređen par dvaju grupoida (mogu specijalno biti grupe, jedan ili oba).

Sa

(1) $(G \times G', \cdot)$ označujemo

Descartesov produkt grupoidâ $(G, \cdot)$, $(G', \cdot)$, *i to kao množimu svih uređenih* dvojki $(\dot{G}, \dot{G}')$, *pri čemu se računanje iz zadanih grupoida prenosi* ***koordinatno*** *na produkt:*[1)]



Sl. 17.14.1.

(2) $$(x, x') \cdot (y, y') = (x \cdot y,\ x' \cdot y').$$

Specijalno se definira *Descartesov kvadrat* $(G \times G, \cdot)$ *grupoida* $(G, \cdot)$, stavljajući $G' = G$.

U aditivnoj formi: ako je $(x, x'), (y, y') \in G \times G'$ tada po definiciji:

(2+) $$(x, x') + (y, y') = (x + x',\ y + y').$$

Analogna definicija za više faktora iskazuje se na očigledan način.

14.1.2. Descartesov produkt grupa (opći slučaj). Neka je I neprazan skup: za svako $i \in I$ neka $(G_i, *_i)$ bude grupa; produkt grupâ

(3) $$(G_i, *_i)(i \in I)$$

jest skup G svih jednoznačnih funkcija f kojima je I oblast a imaju svojstvo da je $f_i \in G_i$ za svako $i \in I$; ako je I beskonačno, tada zahtijevamo da nužno bude $f_i = 1_i =$ neutralni element u G_i i to za svako $i \in I$ osim eventualno za konačno mnogo izuzetaka; operacija $*$ u skupu G definira se *koordinatno*, tj. pomoću

$$(f * f')_i = f *_i f_i'$$

za svako $i \in I$ i za svaku uređenu dvojku f, f' članova iz (1).

Lako se dokazuje da je $(G, *)$ određena grupa.

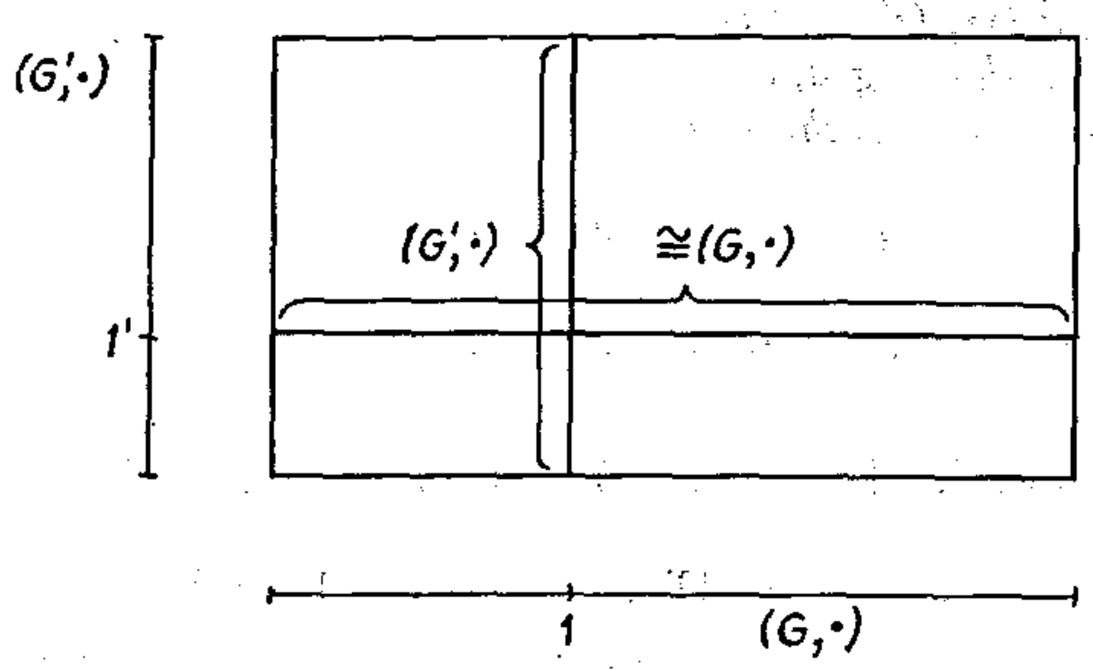
[1)] Ovaj je dodatak važan! Imaj na umu *koordinatno* zbrajanje (množenje) diferencija (razlomaka). Naime: $(x-x')+(y-y')=(x+y)-(x'+y')$, $(x:x')\cdot(y:y')=\frac{xy}{x'y'}$.

14.1.3. Definira se i *potpuni Descartesov produkt grupâ* (3) bez ograničenja da uz konačno mnogo izuzetaka $i \in I$ bude $f_i = 1_i$.

—→ **14.2. Teorem.** ***Descartesov produkt dva grupoida (dvije grupe) je grupoid (grupa); svako od ovih svojstava: asocijativnost, komutativnost, imati neutral, regularnost, biti podgrupa, biti u relaciji obratnosti (inverznosti) prenose se s oba faktora na produkt. Specijalno, ako je*** $\mathbf{1}$ ***odnosno*** $\mathbf{1}'$, ***neutral u*** $(G, \cdot)$, ***odnosno u*** $(G', \cdot)$, ***tada je*** $(\mathbf{1}, \mathbf{1}')$ ***neutral u produktu.***

Ako su x, x^{-1} ***u obratnosti (recipročitetu) u prvom, a*** x', x'^{-1} ***u recipročitetu u drugom grupoidu, tada su*** (x, x'), (x^{-1}, x'^{-1}) ***međusobno recipročni u produktu.***

Obje polazne strukture $(G, \cdot)$, $(G', \cdot)$, ***ukoliko imaju svoje neutrale*** $\mathbf{1}$, $\mathbf{1}'$, ***izomorfno su smještene u produktu: preslikavanje*** $\dot{G} \to (\dot{G}, \mathbf{1}')$ ***predstavlja izomorfno smještavanje od*** $(G, \cdot)$ ***na podstrukturu*** $(G \times \{\mathbf{1}'\}; \cdot)$, ***a radnja*** $\dot{G}' \to (\mathbf{1}, \dot{G}')$ ***je izomorfno smještavanje od*** $(G', \cdot)$ ***na podstrukturu*** $(\{\mathbf{1}\} \times G', \cdot)$ ***produkta.*** Shematski:



Sl. 17.14.2.

Specijalno, ***ako su faktori*** $(G, \cdot)$, $(G', \cdot)$ ***grupe, tada je produkt grupa, a izomorfni smještaji*** $G \times \{\mathbf{1}'\}$, $\{\mathbf{1}\} \times G'$ ***od*** G ***i*** G' ***su invarijantne podgrupe Descartesova produkta zadanih grupa*** G, G'.

Dokaz teorema je jednostavan i izlazi iz prirodnosti Descartesova množenja strukturâ.

Dokažimo da (1) predstavlja grupoid: *rezultat* ili *proizvod dvaju članova iz* (1) *opet je u* (1). Pa neka su faktori u (2) proizvoljni elementi iz (1); to znači da je $x, y \in G$, dakle i $x \cdot y \in G$, jer je $(G, \cdot)$ grupoid; isto tako $x', y' \in G'$; a to opet, po definiciji, znači da (1) predstavlja grupoid.

Dokažimo da je $(1, 1')$ neutral u (1).
Stvarno

$$(x, x') \cdot (1, 1') \overset{def}{=} (x \cdot 1,\ x' \cdot 1') = (\text{zbog}\ \ x \cdot 1 = x,\ x' \cdot 1' \cong x') \equiv (x, x').$$

Dakle je $(1, 1')$ desni neutral u (1). Isto se tako vidi da je $(1, 1')$ lijevi neutral u produktu, ako je 1, odnosno $1'$ lijevi neutral u prvom odnosno drugom faktoru.

Svojstvo suprotnosti također je očigledno, jer po definiciji imamo

$$x \cdot x^{-1} = 1 = x^{-1} x$$

$$x' \cdot x'^{-1} = 1' = x'^{-1} x';$$

odatle po definiciji Descartesova množenja izlazi

$$(x, x') \cdot (x^{-1}, x'^{-1}) = (x \cdot x^{-1}, x' \cdot x'^{-1}) = (1, 1') = (x^{-1} x, x'^{-1} x'),$$

tj. $(x, x') \cdot (x^{-1}, x'^{-1}) = (1, 1') = (x^{-1}, x'^{-1})(x, x')$.

A to po definiciji obratnosti znači da je

$$(x, x')^{-1} = (x^{-1}, x'^{-1}).$$

Najzad, onaj dodatak o izomorfiji proizlazi direktno iz definicija.

Primijetimo da je osiguran bar jedan izomorfni smještaj svakog faktora u produktu; naravno da je posebno pitanje da li ima i drugih osim onih navedenih.

14.3. Plodnost Descartesova množenja vidjeli smo i u procesu prirodnog izraštanja niže strukture u višu, npr. proširenje grupoida do grupe. Tako smo npr. u § 13.2. vidjeli na kako prirodan način grupoid $(N, \cdot)$ preraštava u grupu $\overline{(N, \cdot)}$ pozitivnih racionalnih brojeva. Naime, pojedine situacije u zadanom skupu ili neposredno oko njega mogu se bolje sagledati kad se promatra pripadni Descartesov kvadrat, kub, uopće kvadar od proizvoljno mnogo dimenzija. Pojedine prilično jednostavne situacije u višim kvadrima G^{In} odrazuju se natrag u istom skupu G ukazujući na simptome i pojave unutar samoga G, na koje, iz uže perspektive unutar G, ne bi bilo lako naići.

14.4. Jedan od važnih problema smještavanja. Metoda parcelacije i identifikacije. — **14.4.0.** Ako je zadana jedna struktura, npr. grupoid $(G, \cdot)$, onda je važno znati kakve sve on *podstrukture sadrži.* Tako smo npr. vidjeli da Descartesov kvadrat grupoida $(D_{\neq}, \cdot)$ cijelih regularnih racionalnih brojeva sadrži u sebi podgrupu koja je *izomorfna s grupom* $(Q_{\neq}, \cdot)$ *svih racionalnih regularnih brojeva* (isp. pogl. 17, § 13.2).

14.4.1. Pri tom se *metoda podjele ili particije* pokazuje vrlo plodnom: *skup nosilac promatrane strukture razbije se na* (*disjunktne*) *dijelove pa se promatra obitelj svih tih dijelova, parcelâ, kao nov nosilac naslijeđene strukture; računanje s parcelama indicirano je računanjem s pripadnim članovima.* Npr. za Descartesov kvadrat $(I\omega \times I\omega, +)$ promatrajmo skupove $(m, n) + I\omega = \{(m, n), (m+1, n+1), (m+2, n+2), \ldots\}$; oni parceliraju taj kvadrat, pa se s tim razredima računa po naslijeđenom pravilu o računanju na kvadratu $(I\omega \times I\omega, +)$.

⟶ **14.4.2. Metoda identifikacije** sastoji se u tom, da sve članove pojedine parcele P slijevamo u jedno jedino biće p — poznato eventualno od ranije — i shvatajući elemente iz parcele ili razreda P kao *različite forme istog bića p.* Tada se metoda pokazuje praktičnom i dijaletički povezuje tvorevine nižeg stupnja s tvorevinama višeg stupnja. To je matematici vrlo čest slučaj.

Čitajući gornji tekst, neka se ima na umu npr. prelaz od prirodnih pozitivnih brojeva na 0 i negativne brojeve ili na prelaz od racionalnih brojeva na realne brojeve, itd.

14.5. Direktni produkt grupa. — 14.5.0. Pogledajmo gornju shemu u § 14.2. i uočimo izomorfni smještaj $(G \times \{1\})$ faktora $(G, \cdot)$ te smještaj $\{1\} \times G'$ faktora $(G', \cdot)$ u produktu

$$(G, \cdot) \times (G' \cdot). \tag{1}$$

Nađimo totalan output (rezultat, iznos)

$$G \times \{1'\} \cdot \{1\} \times G' \tag{2}$$

kao skup svih elementarnih iznosa:

$$(\dot{G}, 1') \cdot (1, \dot{G}') = (\dot{G} \cdot 1, \ 1' \cdot G') = (\dot{G}, \ \dot{G}'). \tag{3}$$

Dakle je produkt tih dvaju podgrupoida

$$(G \times \{1'\}, \cdot), \ (\{1\} \times G'; \cdot) \tag{4}$$

upravo čitav grupoid $(G \times G', \cdot)$.

14.5.1. Nadalje, ti podgrupoidi (4) imaju jedan jedini član zajedno — neutral $(1, 1')$.

14.5.2. Nadalje je svaki element od (1) moguće prikazati na jedan jedini način kao produkt, u obliku (3), po jednog člana iz horizontalnog i po jednog člana iz vertikalnog podgrupoida (4) (v. sliku 17.14.2).

Naime, neka je $(x, x') \in G \times G'$; neka je

$$(\dot{G}, \ 1') \cdot (1, \ \dot{G}') \equiv (x, \ x')$$

$$(\dot{G} \cdot 1, \ 1' \cdot \dot{G}^{-1}) = (x, \ x')$$

$$(\dot{G}, \ \dot{G}') = (x, \ x')$$

$$\dot{G} = x, \ \dot{G}' = x'.$$

14.5.3. *Ako su faktori* $(G, \cdot)$, $(G', \cdot)$ *grupe, tada su izomorfni smještaji* (4) *čak normalni ili invarijantni djelitelji produkta* (1).

Vrijedi čak i više: *ne samo da je svaki element iednog od skupova u* (4) *komutativan s drugim od skupova* (4) *kao* ***cjelinom*** *nego je on komutativan sa svakim njegovim elementom* ***individualno;*** naime:

$$(x, \ 1') \cdot (1, \ x') = (x \cdot 1, \ 1 \cdot x') = (1 \cdot x, \ x' \cdot 1) = (1, \ x') \cdot (x, \ 1).$$

Na osnovu toga postavlja se

—→ **14.5.4. Definicija grupe kao direktnog produkta** (isp. pogl. 13, § 4,7). Kaže se da je grupa *direktni produkt* ako je izomorfna s Descartesovim produktom dviju ili više grupa (broj faktora može biti i beskonačan).

Ako je grupa izomorfna s Descartesovim produktom dviju grupa, onda je ta definicija, kao što smo vidjeli, ekvivalentna s ovom definicijom:

14.5.5. Definicija. Kaže se da je grupa G *direktan proizvod* (produkt, suma), *svojih dviju podgrupa* G_1, G_2 i piše $G = G_1 \times G_2$ odnosno $= G_1 \oplus G_2$ ako su ispunjena ova tri uslova:

(I) *Obje podgrupe su invarijantne.*

(II) *Imaju jedino neutral kao zajedničku tačku.*

(III) *Svaki element grupe predočen je na jedan jedini način kao iznos* $g_1 g_2$ pri čemu je $g_1 \in G_1$, $g_2 \in G_2$.

Uslov (III) *može se nadomjestiti traženjem da bude* $G \equiv G_1 \cdot G_2$.

Naime, ako je

$$g = g_1 g_2 \equiv g_1' g_2'$$

i pri tom

$$g \in G,\ \{g_1, g_1'\} \subset G_1,\ \{g_2, g_2'\} \subset G_2$$

tada iz $g_1 g_2 = g_1' g_2'$ izlazi (kako?)

$$g'^{-1}_1 g_1 = g'_2 g_2^{-1}.$$

No u toj jednadžbi stoji lijevo određen član iz G_1 a desno s njim jednak član iz G_2; dakle tu stoji jedini zajednički član od G_1, G_2 tj. neutralni član 1 (uslov II) pa je $g_1'^{-1} g_1 = 1 = g_2' g_2$ dakle izlazi $g_1 = g_1'$, $g_2 = g_3'$; time je i jednoznačnost faktorizacije iz (III) dokazana.

14.5.6. Stvar se prenosi i na više faktora G, G', G'', ..., samo tada uslov (I) glasi da *svaki faktor u produktu svih ostalih faktora ima jedino neutral kao zajedničku tačku.*

Primjena direktnog produkta (sume) dolazi u teoriji linearnih operatora (pogl. 13, § 4.7; pogl. 27, § 6).

14.5.7. Nerastavljive grupe. To su grupe G za koje osim trivijalnih faktorizacijâ $G = 1 \times G$, $G = G \times 1$ nema drugih faktorizacija. Tako npr. grupa S_3 je nerastavljiva jer ima samo jedan netrivijalan normalni divizor. Svaka grupa sastavljena od prostog broja elemenata je nerastavljiva.

Interes gornjih razmatranja izlazi iz ovog teorema:

Za konačne grupe i za komutativne grupe s konačno mnogo izvodnica faktorizacija u nerastavljive normalne divizore je, do izomorfije i redoslijeda faktora, određena jednoznačno (isp. 17 § 20.9.2).

14.5.8. Potpuno rastavljive grupe. To su grupe koje se mogu prikazati kao direktan proizvod od konačnog broja pravih podgrupa.

14.6. Zadaci o Descartesovu množenju i o direktnom proizvodu.

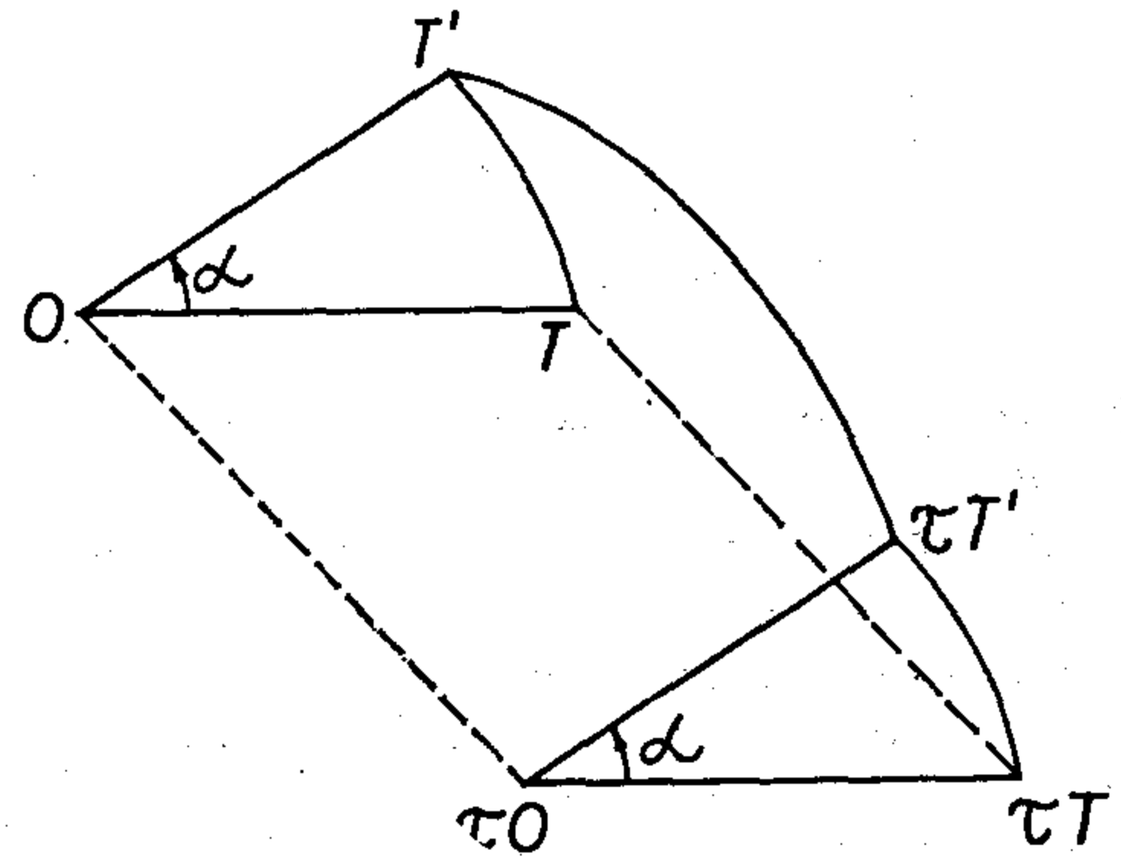
1. Nađi Descartesov proizvod ovih grupa: 1) $(D, +)$, $(D, +)$; 2) $(R, +)$, $(R, +)$; 3) C_2, C_3; 4) C_2, C_2, C_2; 5) C_2, C_3, C_5; 6) $C_2 \times C_2 \times C_2 \times C_2$; 7) $(2^D, \cdot)$, $(3^D, \cdot)$, $(5^D, \cdot)$; 8) $((-1)^D, \cdot)$, $(2^D, \cdot)$, $(3^D, \cdot)$, ... $(p^D, \cdot)$, ... (p prost broj > 1).
2. Je li ova grupa proizvod od dvije netrivijalne normalne podgrupe: 1) $(Q \setminus \{0\}; \cdot)$; 2) $(R \setminus \{0\}, \cdot)$; 3) $(R(i), +)$, $R(i)$ je skup svih kompleksnih brojeva; 4) V_4 (17, § 7.13); 5) grupa kocke (17, § 7.11); 6) $(D, +)$; 7) $(Q, +)$; 8) C_{p^2}; 9) C_{pn}; 10) Euklidski prostor $(E_n; +)$ (isp. 17, § 0.1.21) 11) $(R_{nn}; \cdot)$, gdje R_{nn} označuje skup svih matrica poretka (n, n) i s vrijednostima u R?

3. 1) Ako su m, n relativno prosti prirodni brojevi, tada je $C_m \times C_n$ izomorfno s C_{mn}; 2) Ako prirodni broj n nije prost, može se ciklička grupa C_n prikazati kao direktni proizvod grupâ oblika $C_p{}^k$ (p prosto).

15. KONJUGACIJA ILI SPREZANJE POSREDSTVOM ZADANOG ELEMENTA GRUPE. ENDOMORFIZMI GRUPE

15.0. Uvodni primjer. Ako promatramo određenu *rotaciju* r ravnine, pa ako ravninu podvrgnemo stanovitoj *translaciji* t, nastaje pitanje u kakvoj će vezi biti tačke tT, rT', gdje je $T' = rT$.

Očigledno je, da rotacija pomaknute tačke tT za isti kut α oko pomaknutog središta tO daje pomaknutu sliku tT'; možemo kraće reći da *iz rotacije* r *nastaje* ***pomaknuta*** *rotacija*. (Vidi sl.)



Sl. 17.15.0.

No prelaz od

$$tT \text{ na } tT'$$

možemo izvesti i u ovim etapama: od tT *natrag do* T (*translacija* t^{-1}) pa rotacija r oko O, pa translacija t, dakle u svemu

$$trt^{-1}.$$

Dakle se rotacija oko tO prikazuje i kao *sastavljeno preslikavanje*

$$trt^{-1}.$$

15.1. Definicija konjugacije. Ako su t, x dva elementa grupe $(G, \cdot)$, tada se element txt^{-1} zove *t-konjugatom elementa* x, pa se kaže da on iz x nastaje *konjugacijom ili sprezanjem posredstvom elementa t ili t-transformacijom*; kaže se također da je *element* x, *ekvivalentan, ili konjugiran ili spregnut*, sa txt^{-1}.

Drugim riječima, ako je $x, y \in G$, tada se kaže da je x *konjugirano sa* y *u odnosu na* G, ako postoji $t \in G$ tako da bude $x = tyt^{-1}$.

Odmah se dokazuje

—→ **15.1.1.** Teorem. *Svojstvo konjugiranosti je određena relacija ekvivalentnosti, tj. svojstvo je refleksivno, simetrično i tranzitivno, pa se grupa raspada u određen skup razreda (klasa); svaki razred konjugiranosti obuhvata sve elemente grupe koji su međusobno konjugirani.*

Dokaz. 1. x je konjugirano sa x. Stvarno je $x = 1 \cdot x \cdot 1^{-1}$.

2. Ako je x konjugirano sa y, onda je, obrnuto, i y konjugirano sa x. Naime, iz $x = tyt^{-1}$, $t \in G$ izlazi $t^{-1} x t = y$, tj. $y = zxz^{-1}$ sa $z = t^{-1} \in G$.

3. Svojstvo konjugiranosti je prelazno: *ako je x konjugirano sa y, a y sa u, onda je x konjugirano sa u.* No, te pretpostavke kažu da je $x = tyt^{-1}$ s nekim $t \in G$, odnosno da je $y = vuv^{-1}$ s nekim $v \in G$. Ubacimo li to y u izraz za x, izlazi $x = t(vuv^{-1})t^{-1}$ i dalje $x = (tv)u(v^{-1}t^{-1}) = (\text{v. } 8.4.1) = (tv)u(tv)^{-1}$, tj. aua^{-1}, gdje je $a \in G$, jer je $a = tv$. Dakle je x konjugirano sa u. Time je teorem 15.1.1. potpuno dokazan.

15.1.2. *Za svako $t \in G$ preslikavanje*

$$x \to txt^{-1} \ (x \in G) \tag{1}$$

je određeno izomorfno preslikavanje čitave gripe $(G, \cdot)$ na čitavu samu sebe prevodeći svaku invarijantnu grupu I opet u I. Drugim riječima, preslikavanje (1) *je određen automorfizam grupe $(G, \cdot)$.*

Najprije, preslikavanje (1) je *jednoznačno* u čitavoj grupi G; to je preslikavanje i *obostrano jednoznačno*, jer ako su x, x' dva *različita* elementa iz G, tada su *različiti* i tx, tx', a odatle izlazi također $txt^{-1} \neq tx't^{-1}$. Još preostaje da vidimo da je t-konjugat *produkta* jednak *produktu* t-konjugatâ. No, $t(xx')t^{-1} = t(x)t^{-1}(x')t = (\text{po asocijaciji}) = (txt^{-1})(tx't^{-1})$, za čim se i ide. Da je $tIt^{-1} = I$ za svaku invarijantnu podgrupu $(I, \cdot)$, dokazano je ranije (v. teorem 11.2).

15.1.3. Korolar. *Ako je F subgrupa grupe $(G, \cdot)$, tada za svako $t \in G$ skup tFt^{-1} čini određenu subgrupu u $(G, \cdot)$, izomorfnu sa F,* tj. *t-konjugat svake podgrupe $F \subset G$ opet je jedna podgrupa izomorfna sa F;* drugim riječima, *svakoj podgrupi $F \subset G$ pripada određena obitelj izomorfnih podgrupa*

$$tFt^{-1} \ (t \in G).$$

U slučaju kad je F *invarijantna* podgrupa I, tada je $tIt^{-1} = I$ za *svako* $t \in G$.

15.2. Unutrašnji automorfizmi ili endoautomorfizmi grupe.

15.2.1. Definicija. Svako preslikavanje $x \to axa^{-1}$ grupe G, pri čemu je $a \in G$, zove se *unutrašnji automorfizam* te grupe. *Automorfizmi* koji nisu unutrašnji zovu se *vanjski.*

Tako npr. u cikličkoj grupi $C_3 = \{e^{i3i2\pi/3}; \cdot\}$ preslikavanje $1 \longleftrightarrow 1$, $e^{i2\pi/3} \longleftrightarrow e^{i4\pi/3}$ je *vanjski automorfizam.*

15.2.2. Teorem. *Svi automorfizmi grupe $(G, \cdot)$ obrazuju grupu; označit ćemo je s $a(G)$; svi endoautomorfizmi obrazuju određenu invarijantnu podgrupu $i(G)$ te grupe $a(G)$.*

Prvi dio teorema je očigledan; dokažimo drugi dio. Dokažimo, najprije, da svi endoautomorfizmi obrazuju zaista *grupu*. Stvarno, neka je t, $u \in G$; tada pripadni *unutrašnji* automorfizmi glase

$$txt^{-1}\,(x \in G)$$

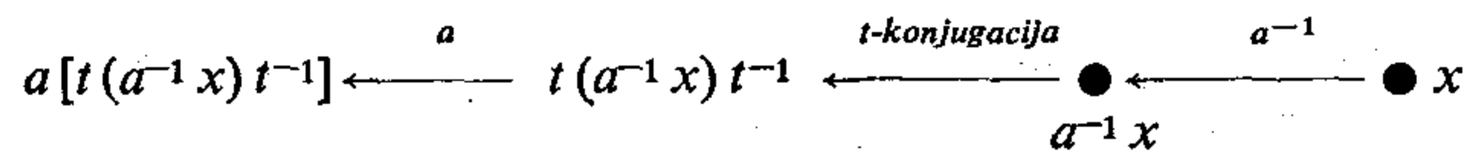
$$uxu^{-1}\,(x \in G),$$

slaganjem prvog i drugog preslikavanja izlazi

$$u\,(txt^{-1})\,u^{-1}, \quad \text{a to je} \quad (ut)\,x\,(ut)^{-1},$$

dakle zaista automorfizam izveden elementom $u \cdot t$ grupe G.

Još treba dokazati da svi endoautomorfizmi čine *invarijantnu* podgrupu u grupi $a(G)$ *svih automorfizama* zadane grupe $(G, \cdot)$. To znači da je za svaki automorfizam a od G na G i za *svako* $t \in G$ pripadni endomorfizam $x \to txt^{-1}$ takav da izvođenje: preslikavanja a^{-1}, pa endomorfizma (*t-konjugacije*), pa a, daje opet određen endomorfizam; shematski:



Imamo, dakle, preslikavanje $x \to a\,[t\,(a^{-1}\,x)\,t^{-1}]$; no kako je a homomorfizam, ovo je dalje $= (at)\,a\,(a^{-1}\,x)\,at^{-1}) = (at)\,xa\,(t)^{-1} = atx\,(at)^{-1}$. Dakle, traženo preslikavanje glasi:

$$x \to (at)\,x\,(at)^{-1}.$$

No, to je konjugacija izvedena elementom at iz G. Dakle se zaista radi o invarijantnoj podgrupi.

15.3. Zatvorene grupe. U općem slučaju je $i\,G \subset a\,G$. No, može se desiti da je $i\,G = a\,G$. Tom jednakošću definiraju se tzv. *zatvorene grupe*: kod njih je *svaki automorfizam izvediv konjugacijom.* Tako se npr. može dokazati da je svaka konačna nekomutativna prosta grupa zatvorena (v. Zassenhauss, p. 42).

⟶ **15.4. Razredi (klase) konjugiranosti.** — **15.4.1.** Skup svih međusobno konjugiranih elemenata zadane grupe zove se *razred* (*klasa*) *spregnutosti te grupe.*

15.4.2. Množina svih razreda konjugiranosti grupe $(G, \cdot)$ označujemo s $Cl\,G$. Kardinalni broj množine $Cl\,G$ označuje se s $r\,G$ ili naprosto s r. Odmah se vidi da je podskup grupe određen razred onda i samo onda ako je on *najobuhvatniji* dio međusobno konjugiranih elemenata grupe.

15.4.3. Tako npr. dijedarska grupa D_4 što pripada kvadratu ima ove razrede (r_4 je rotacija oko glavne osi kvadrata za $2\pi/4$):

$$\{1\}, \quad \{r_4, r_4^3\}, \quad \{r_4^2\}, \quad \{u_1, u_3\}, \quad \{u_2, u_4\};$$

pri tom u_i označuje simetriju prema i-toj sporednoj osi kvadrata, tj. prema osi kvadrata koja je u ravnini kvadrata. Dakle je $r\,D_4 = 5$.

15.4.4. Grupa G_K kocke ima 24 člana, a sastoji se iz ovih razredâ (ispod svakog razreda napisan je broj članova toga razreda):

$$\begin{array}{ccccc} \{e\}, & R_2, & R_3, & R_4, & R_4^2 \\ 1 & 6 & 8 & 6 & 3 \end{array}$$

Razred R_2 sastoji se od rotacijâ kocke oko spojnice središtâ mimohodnih bridova kocke; slično se R^i_k sastoji od svih članova grupe G_K koji su poretka $\frac{k}{i}$; tako npr. R_3 se sastoji od svih rotacija kocke u samu sebe oko svake dijagonale kocke.

15.4.5. Lema. *Ako je R razred, onda je i $R^{-1}=\{x^{-1};\ x\in R\}$ određen razred. Za svaki cio broj m skup R^m je razred konjugiranosti.*

Naime, iz $x, y\in R$ izlazi $y=gxg^{-1}$ za neko $g\in G$; odatle je $y^{-1}=(gxg^{-1})^{-1}=$ $=$(v. § 8.1.3)$=(g^{-1})^{-1}x^{-1}g^{-1}=gx^{-1}g^{-1}$; dakle su i x^{-1}, y^{-1} međusobno konjugirani; prema tome, R^{-1} leži u nekom razredu K. Dokažimo još da je $R^{-1}=K$ tj. da vrijedi

$$k\in K \Rightarrow k\in R^{-1} \quad \text{dakle} \quad k^{-1}\in R.$$

No zbog $R^{-1}\subset K$, element k iz K je oblika $k=gr^{-1}g^{-1}$ za neko $r^{-1}\in R^{-1}$ i neko $g\in G$; dakle je

$$k^{-1}=grg^{-1} \quad \text{tj.} \quad k^{-1}\in R \quad \text{za čim i idemo.}$$

Dokažimo da je R^m određen razred. U prvom redu, iz $x, y\in R$ izlazi da su i x^m, y^m konjugirani. Naime iz $x, y\in R$ izlazi najprije $y=gxg^{-1}$ za neko $g\in G$. Odatle

$$y^2=(gxg^{-1})(gxg^{-1})=(gx)(g^{-1}g)(xg^{-1})=(gx)\cdot 1\,(xg)=gx^2g^{-1}.$$

Induktivno, $y^{n+1}=(gx^ng^{-1})(gxg^{-1})=gx^{n+1}g^{-1}$ za svaki prirodni broj n. Odatle prelazeći na inverzne elemente izlazi da je $y^m=gx^mg^{-1}$ za svaki cio broj m. Dakle zaista $R^m=\{r^m;\ r\in R\}$ leži u nekom razredu K. Treba još dokazati da je $R^m=K$ tj. da vrijedi

$$k\in K \Rightarrow k\in R^m.$$

No, kako $k\in K$ i $r^m\in K$ za svako $r\in R$, to će također biti $k=gr^mg^{-1}$ za neko g (ovo $g\in G$ zavisi od x^m). No, vidi se da je $gr^mg^{-1}=(grg^{-1})^m$ tj. $k=(grg^{-1})^m$ što zbog $grg^{-1}\in R$ znači zaista da je $k\in R^m$.

15.4.6. Lema. *Ako su R_1, R_2 dva razreda konjugiranosti grupe G pa ako njihov proizvod R_1R_2 sadrži neki član r razreda R, tada R_1R_2 sadrži čitav razred R; dakle je R_1R_2 ili razred ili unija (zbir) nekih razreda.*

Po pretpostavci je $r\in R_1R_2\cap R$; dakle $r=r_1r_2$ gdje je $r_1\in R_1$, $r_2\in R_2$. No, odatle je $grg^{-1}=g(r_1r_2)g^{-1}=(gr_1g^{-1})(gr_2g^{-1})$. Dakle je

$$grg^{-1}=(gr_1g^{-1})(gr_2g^{-1}),\ (g\in G).$$

Lijevo je opći član od R; desno u prvoj zagradi stoji opći član od R_1 a u drugoj zagradi stoji opći član od R_2; dakle je zaista $R\subset R_1R_2$.

15.5. Razredi konjugiranosti i invarijantne podgrupe. Ako je I invarijantna podgrupa grupe G, tada iz $i \in I$ izlazi $gig^{-1} \in I$ za svako $g \in G$ a time $G(i) \subset I$; tu $G(i)$ označuje razred konjugiranosti u kojem leži i. ***Dakle je I ili određen razred ili unija određenih razreda konjugiranosti.***

⟶ **15.6.** Teorem. *Podgrupa F grupe G što je proizvodi neki razred R ili nekoji razredi R_1, R_2; ... grupe G je invarijantna podgrupa grupe G.*

Dokaz. Neka je $r \in R$; tada je opći član f podgrupe F oblika

$$f = (g_1 r g_1^{-1})^{\varepsilon_1} (g_2 r g_2^{-1})^{\varepsilon_2} \cdots (g_n r g_n^{-1})^{\varepsilon_n};$$

pri tom je

$$\{g_1, g_1, \ldots, g_n) \subset G, \ \{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n\} \subset \{-1, 1\}.$$

Ako nađemo gfg^{-1}, tada gornji prikaz daje (uklapajući $g^{-1}g$ između zagrada):

$$gfg^{-1} = g(g_1 r g_2)^{\varepsilon_1} g^{-1} \cdot g(g_2 r g_2^{-1})^{\varepsilon_2} g^{-1} \cdots g(g_n r g_n^{-1})^{\varepsilon_n} g^{-1}.$$

Zbog $g(g_\nu r g_\nu^{-1})^{\varepsilon_\nu} g^{-1} = ((gg_\nu)\, r\, (gg_\nu)^{-1})^{\varepsilon_\nu}$, zaključujemo da je također $gfg^{-1} \in F$, tj. podgrupa F je invarijantna.

Analogno se dokazuje invarijantnost podgrupe što je generiraju dva ili više razreda konjugiranosti.

15.7. Normalizator zadana podskupa M grupe.

15.7.1. Definicija. Neka je M pun podskup grupe G; skup svih elemenata g grupe G za koje je $gMg^{-1} = M$ zove se *normalizator od M unutar G* i označuje se sa $N_{M,G}$, odnosno sa N_M. Posebno, za svako $x \in G$ imamo normalizator $N_x = \{g;\ g \in G,\ gxg^{-1} = x\}$.

15.7.2. Lema. *Normalizator N_M svakog nepraznog dijela M grupe G je određena podgrupa grupe G; specijalno, za svako $g \in G$ normalizator N_g je podgrupa od G. Ako je M podgrupa od G, onda je N_M najveća podgrupa od G u kojoj je M invarijantan divizor.*

Dokaz. Najprije iz $x, y \in N_{MG}$ izlazi $x \cdot y \in N_{MG}$. Naime, $x \in N_M$ znači da je $xMx^{-1} = M$; odatle y-sprezanjem:

$$y(xMx^{-1})y^{-1} = yMy^{-1}.$$

Desna strana je M jer je $y \in N_M$; lijeva strana je $= (yx)M(yx)^{-1}$; to znači da yx-sprezanjem množina M prelazi u samu sebe. A to upravo znači da je $yx \in N_M$; slično $xy \in N_M$.

Dokažimo da N_M zadovoljava i 4. aksiom o grupi: $x \in N_M \Rightarrow x^{-1} \in N_M$. No, $x \in N_M$ znači $xMx^{-1} = M$; a odavde x^{-1}-sprezanjem izlazi tražena jednakost $M = x^{-1}Mx$, tj. $x^{-1} \in N_M$.

15.7.3. Primjer. $G = S_3 = \{123, 132, 213, 231, 312, 321\}$, $g = 132$; kad x prolazi redom S_3, tada $x \cdot 132 \cdot x^{-1}$ postaje redom:

132, 132, 321, 321, 213, 213

tako da imamo tablicu

x	123	132	213	231	312	321
$x\,123\,x^{-1}$	132	132	321	321	213	213

Skup rješenja jednadžbe $x \cdot 123 \cdot x^{-1} = 123$ glasi

$$N_{123} = \{123,\ 132\}.$$

15.8. O skupovima koji su konjugirani sa zadanim skupom M.

15.8.1. Neka je opet M pun dio od G; kaže se da je skup $g\,Mg^{-1}$ *konjugiran sa* M. Nastaje pitanje koliko ima skupova koji su sa M konjugirani. Pa neka je

$$g\,Mg^{-1} = h\,Mh^{-1} \tag{1}$$

gdje su g, h iz G; iz te jednadžbe dobije se h^{-1}-konjugiranjem

$$(h^{-1}g)\,M\,(g^{-1}h) = M,\ \text{tj.}\ (h^{-1}g)\,M\,(h^{-1}g)^{-1} = M\ \text{dakle}\ h^{-1}g \in N_M\ \text{dakle}$$

$$g \in h\,N_M. \tag{2}$$

Prema tome, iz (1) izlazi (2). Idući obratnim putom dokazuje se da i (2) $\Rightarrow$ (1). Na taj smo način dokazali

15.8.2. Teorem. *Za svaki neprazan dio M grupe G normalizator N_M je podgrupa; svakom položaju $h\,N_M$ grupe N_M odgovara jedan jedini skup $h\,Mh^{-1}$ koji je konjugiran sa M; različnim (disjunktnim) položajima grupe N_M odgovaraju različni skupovi $h\,Mh^{-1}$ koji općenito nisu disjunktni. Broj različnih skupova $g\,Mg^{-1}$ jednak je indeksu $G : N_M$ tj. jednak je glavnom broju svih položaja $g\,N_M$ grupe N_M. Specijalno svaki element $g \in G$ ima upravo $G : N_g$ elemenata koji su sa g konjugirani (oni čine klasu $G(g)$).*

Tako npr. za $G = S_3$, $g = 132$ tablica iz § 15.7.3. pokazuje da je $G(132) = \{132, 213, 321\}$; taj je razred sastavljen od svih transpozicija množine $\{1, 2, 3\}$.

15.9. Centralizator dijela M grupe G. — 15.9.1. Centralizator dijela M grupe G je presjek svih normalizatora N_m kad $m \in M$; označuje se sa Z_M; dakle definiramo

$$Z_M = \bigcap_m N_m\ (m \in M). \tag{1}$$

15.9.2. Lema. $Z_M = \{g;\ g \in G,\ gm = mg$ *za svako* $m \in M\}$; *drugim riječima, centralizator Z_M je sastavljen od svih članova grupe koji komutiraju sa* **svakim** *elementom iz M; Z_M je grupa; specijalno, Z_G je centar grupe* (v. 17, § 9.5).

Najprije, $n \in Z_M \Rightarrow nm = mn$ za svako $m \in M$; naime, $n \in Z_M$ daje $n \in N_m$ dakle $nmn^{-1} = m$, a odatle izlazi tražena relacija $nm = mn$. Dokažimo obrat. Pa neka je $gm = mg$ za svako $m \in M$; dakle je $gmg^{-1} = m$; tj. $g\,Mg^{-1} = M$ tj. $g \in N_M$; time je $g \in N_x$ za svako $x \in M$, dakle je $g \in Z_M$.

Kao presjek grupâ N_m, $(m \in M)$, Z_M je grupa.

15.10. Zadaci o konjugiranju, razredima, normalizatorima i centralizatorima.

1. Odredi razred $S_3(321)$ svih elemenata grupe S_3 permutacija množine $\{1, 2, 3\}$ koji su konjugirani sa 321. Isto pitanje i za svaki drugi član $p \in S_3$. Dokaži: grupa S_3 ima 3 razreda konjugiranosti i da za $k \in \{1, 2, 3\}$ svi elementi grupe S_3 periode k čine određen razred.
2. Dokaži: S_4 ima upravo 5 razreda: 1) $\{e\}$, 2) transpozicije (cikluse dužine 2); 3) cikluse dužine 3, 4) cikluse dužine 4 i 5) proizvode disjunktnih transpozicija.
3. Odredi sve razrede konjugiranosti ove grupe: 1) S_5, 2) D_3, 3) D_{2n}, 4) D_{2n+1}, 5) G_T (grupa tetraedra), 6) G_K, 7) Go, 8) G_I (grupa ikozaedra); 9) Qu (v. 17, § 13.5.6).
4. Periode konjugiranih elemenata grupe podudaraju se.
5. Nađi normalizator $N_{M,G}$ za ove vrijednosti M, G: 1) $\{123, 132\}$, S_3; 2) $\{123, 132, 213\}$, S_3; 3) $\{m\}$, $m \in G\,(=D_4)$; 4) A_4 kao podgrupa od grupe kocke; 5) M je ciklička grupa poretka 4 u grupi G_K kocke.
6. Nađi centralizator $Z_{M,G}$ u zadatku 5.
7. Dokaži: 1) Ako je $k\,G$ konačan neparan broj, tada je $k\,G - r\,G$ djeljivo sa 16 ($r\,G$ je broj razreda grupe G); 2) $r\,D_{2n} = n+3$; 3) $r\,D_{2n+1} = n+2$; 4) $r\,K_T = 4$; 5) $r\,Go = r\,G_K = 5 = r\,S_4$; 6) $r\,G_I = r\,G_{Dod} = 5$; 7) $r\,Qu = 5$.
8. Odredi sve invarijantne podgrupe grupe G iz zad. 1 i prikaži ih kao uniju razredâ grupe G.
9. Neka G označuje bilo koju grupu iz zad. 1; odredi pridruživanje: 1) $g \in G \to N_g$; 2) $g \in G \to N_{G\times\{g\}}$; 3) $g \in G \to Z_{G\times\{g\}}$.
10. Dokaži: 1) skup razreda podgrupe upisan je u skup razreda grupe, tj. svaki razred konjugiranosti podgrupe nalazi se u određenom razredu same grupe; 2) broj članova svakog razreda dijeli indeks centra grupe.
11. Odredi grupu G koju generiraju elementi a, b, c pri čemu je $a^2 = 1$, $ab = ba = c$; neka također vrijede analogne jednadžbe dobivene cikličkom zamjenom u a, b, c. Dokaži da se grupa unutrašnjih (svih) automorfizama sastoji od identiteta (od 6 članova).
12. Odredi sve automorfizme četvorne grupe. Koji su unutrašnji, a koji vanjski?
13. Koliko ima raznih unutrašnjih automorfizama u grupi: 1) kvadrata; 2) kocke; 3) C_n?
14. Odredi maksimalan skup neizomorfnih grupa po 8 elemenata kao i skup svih automorfizama svake od tih grupa.
15. Navedi nekoliko grupa i njihovih automorfizama.

16. JOŠ O INVARIJANTNIM PODGRUPAMA I IZOMORFIJI

16.1. Znajući sada što znači preslikavanje $x \to txt^{-1}$ za određeno t i činjenica da je za invarijantnu podgrupu $(I, \cdot)$ iz $(G, \cdot)$ karakteristično da je $t\,It^{-1} = I$ za svako $t \in G$, dobivamo jasan uvid u značenje *invarijantnih* pod-

grupa. Tako npr. ako je G grupa *svih* kretanja u zadanoj ravnini, tada je jasno da *sve* pripadne translacije, odnosno sve rotacije tvore dvije *invarijantne* podgrupe u G, ukoliko se tu uopće radi o *grupama* (a stvarno se radi o grupama; to je jasno za translacije; za rotaciju se stvar također može dokazati! Dokaz nije sasvim jednostavan).

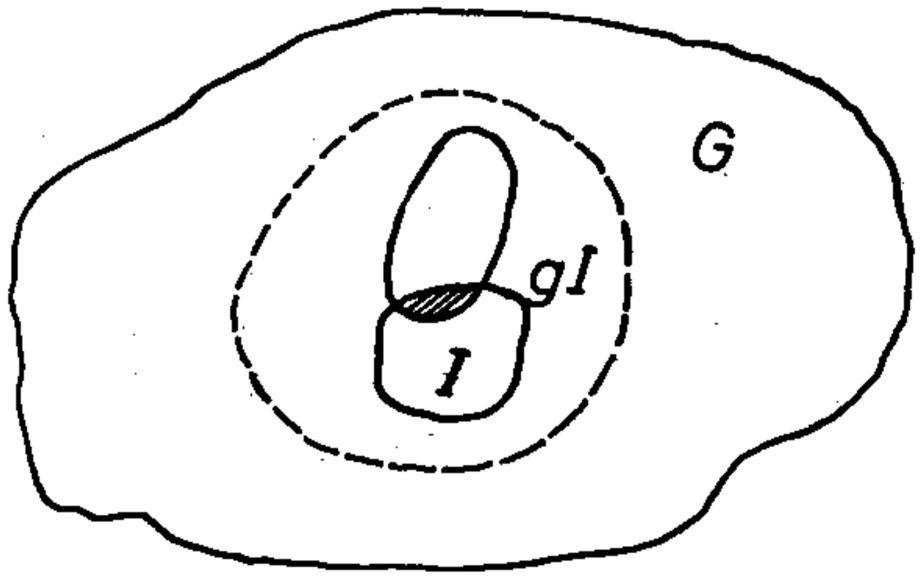
16.2. Jasno je da je presjek dviju ili više *invarijantnih podgrupa* opet *invarijantna podgrupa*. Presjek *svih* invarijantnih podgrupa je jedinična podgrupa, koja je, naravno, invarijantna.

16.3. Također je očigledno ovo: *ako je I invarijantna podgrupa od $(G, \cdot)$, a $(F, \cdot)$ neka grupa za koju je $I \subset F \subset G$, tada je I invarijantna podgrupa i podgrupe $(F, \cdot)$.*

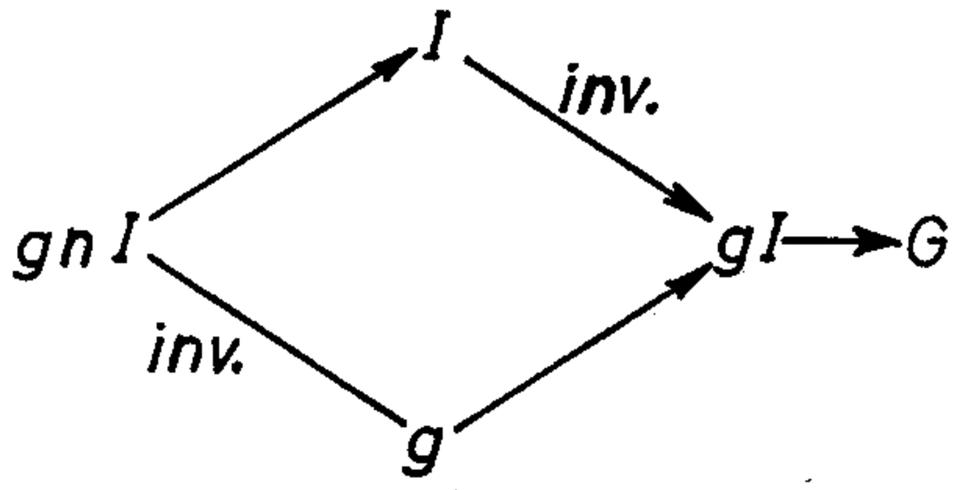
16.4. Vidi se i ovo: *ako je I invarijantna podgrupa,* a F bilo kakva *podgrupa u* $(G, \cdot)$ tada je IF *određena grupa* (ne mora biti invarijantna).

Stvarno, dovoljno je pokazati da je $IF \cdot IF = IF$ te $(IF)^{-1} = IF$ (isp. teorem 9.2.1). No, $IF \cdot IF = FI \cdot IF = F(I \cdot I)F = (FI)F = (IF)F = I(FF) = IF$, tj. zaista $FI \cdot FI = FI$.

U drugu ruku $(IF)^{-1} = F^{-1}I^{-1} = FI = IF$. Q. E. D.



Sl. 17.16.5.



Sl. 17.16.5.1.

16.5. Promatrajmo sliku 16.5: tu je *grupa* $(G, \cdot)$ s podgrupama g i I; k tome je I *invarijantna*; isjenčani skup je $g \cap I$, tj. presjek grupa g, I; taj je presjek invarijantna podgrupa podgrupe $(g, \cdot)$; stvarno, neka je $t \in g$, dakle i $t^{-1} \in g$; tada za svako $x \in g \cap I$ vrijedi, u jednu ruku, $txt^{-1} \in I$, jer je I invarijantna podgrupa; u drugu ruku je $txt^{-1} \in g$, jer su t, x, t^{-1} članovi u g; dakle je $txt^{-1} \in g \cap I$ za svako $x \in g \cap I$ i svako $t \in g$. To znači da je zaista $g \cap I$ invarijantna podgrupa u $(g, \cdot)$.

No, i gI je jedna grupa, kao što smo dokazali u pogl. 17, § 11.8, tako da imamo grupe na sl. 17.16.5.1.

Pri tom se strelica $\rightarrow$ čita »*jest podgrupa u*«; strelica $\xrightarrow{inv}$ čita se: »*invarijantna podgrupa u*«.

16.6. No, uz te parove vezane znakom $\xrightarrow{inv}$ pridružene su pripadne kvocijentne grupe: $(gI)/I$ i $g/(g \cap I)$.

16.7. *Zanimljivo je da su te dvije grupe izomorfne*: pridruživanje položaja

$$\dot{g}I \longrightarrow \dot{g}(g \cap I) \quad (\dot{g} \in g) \tag{1}$$

je *izomorfija između kvocijentnih grupa.*

To se odmah vidi, no tvrdnju ćemo ipak i dokazati. Najprije jedna stvar. Svi položaji grupe $g \cap I$ u g svakako su oblika $(1)_2$, no da li se sa $(1)_1$ iscrpljuju, u gI, svi položaji $(\dot{g}\dot{I})\ I$ grupe I kad $\dot{g} \in g$, $\dot{I} \in I$? Odgovor je: da, jer je $(\dot{g}\dot{I})\ I = \dot{g}(\dot{I}I) = \dot{g}I$, (naime $\dot{I}I = I$, jer je $\dot{I} \in I$).

Naredno pitanje: da li je preslikavanje (1) homomorfija? Jest, jer iz $g \in g$, te $g' \in g$ za pripadne položaje $(1)_1$ i $(1)_2$ izlazi:

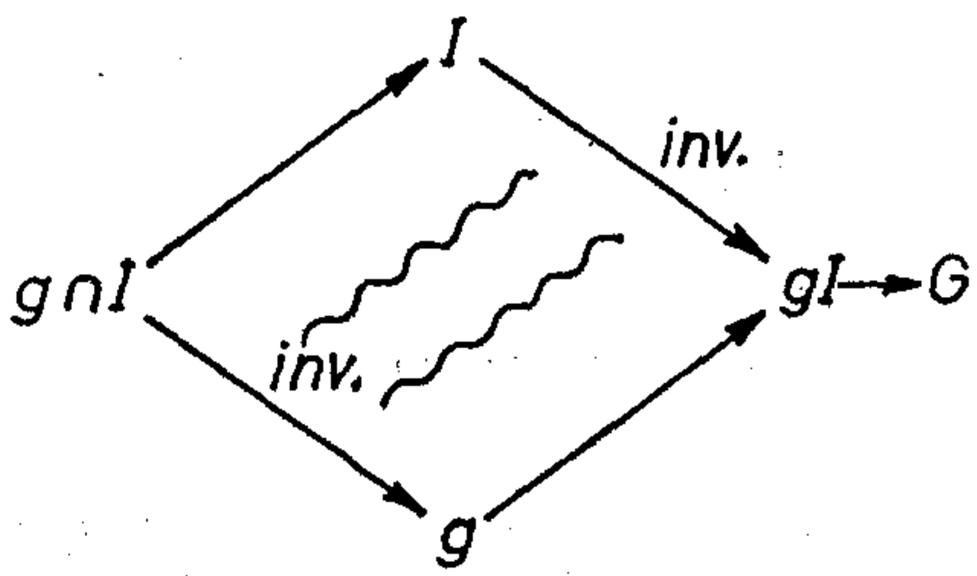
$$\dot{g}I \cdot g'I = \dot{g}g'I \text{ (jer je } I \text{ invarijantna podgrupa u } gI),$$

$$\dot{g}(g \cap I) \cdot g'(g \cap I) = gg'(g \cap I) \text{ (jer je } g \cap I \text{ invarijantna podgrupa u } g).$$

Još preostaje dokaz da različitim položajima $(1)_1$ odgovaraju različiti položaji $(1)_2$, tj. da iz $\dot{g}I \neq g'I$ izlazi $\dot{g}(g \cap I \neq g'(g \cap I)$. Kad bi, naime, bilo $\dot{g}(g \cap I) = g'(g \cap I)$, značilo bi to specijalno da je za neko $a, b \in g \cap I$ ispunjeno $\dot{g}a = g'b$, dakle $\dot{g} = g'ba^{-1}$ sa $b, a^{-1} \in g \cap I$ dakle specijalno i $b, a^{-1} \in I$; time bi bilo $\dot{g}I = (g'ba^{-1})\ I = g'(ba^{-1}I) = g'I$ tj. $\dot{g}I = g'I$, protivno pretpostavci.

Na taj smo način dokazali da vrijedi ovaj

⟶ **16.8. Teorem** (vidi skicu) **(prvi teorem o izomorfizmu).** ***Ako su u nekoj grupi*** $(G, \cdot)$ ***zadane dvije proizvoljne podgrupe*** $(g, \cdot)$, $(I, \cdot)$, ***od kojih je posljednja invarijantna, tada su u shemi svi naznačeni skupovi grupe i k tome*** $g \cap I$ ***invarijantna podgrupa od*** g, ***a*** I ***invarijantna podgrupa od*** gI; ***pripadne kvocijentne grupe***



Sl. 17.16.8.

$$g/(g \cap I),\ gI/I \tag{2}$$

su izomorfne; preslikavanje

$$\dot{g}(g \cap I) \to \dot{g}I,$$

pri čemu $\dot{g}$ ***prolazi grupom*** g, ***jest izomorfija između kvocijent-grupa*** (2).

16.9. Korolar. *Neka su* I_0, I_1, *invarijantne podgrupe u* G; *tada je i presjek* $I_0 \cap I_1$ *invarijantna podgrupa u* G, *dakle i u* I_0, I_1, *pa postoje veze*

$$I_n/(I_0 \cap I_1) \cong (I_0 I_1)/I_{1-n} \text{ za } n = 0, 1.$$

⟶ **16.10. Drugi teorem o izomorfizmu.** — Teorem. *Neka je* G *proizvoljna grupa,* I *njena invarijantna podgrupa; neka je* H *invarijantna podgrupa kvocijent-grupe* G/I; *tada je unija* $\cup H$ *svih članova iz* H *također invarijantna podgrupa u polaznoj grupi* G; $\cup H$ *obuhvata* I, *pa imamo izomorfiju*

$$G/\cup H \cong (G/I)/(\cup H/I).$$

Napomena. *Posljednja se jednakost lako pamti; druga strana izlazi iz prve strane »skraćivanjem« kvocijenta $G/\cup H$ sa I.*

16.10.1. Pođimo od grupe G i njene invarijantne podgrupe I. Tada imamo količničku grupu (pripadni skup) G/I (parcelâ koje obrazuju grupu). Neka je H kakva invarijantna podgrupa u toj grupi G/I komadâ; to specijalno znači da se H sastoji od određenog broja parcela (v. shemu 17 § 11.7.); time dobivamo skup $G/I/H$ skupinâ parcelâ i te skupine tvore određenu grupu; no *komadanju* unutar G/I na skupine parcela odgovara određeno komadanje polazne grupe G na komade grupe G što ih obuhvataju te skupine parcelâ: to je unija $\cup H$ svih parcela iz H i položaji te unije $\cup H$ je invarijantna grupa, pa je pripadno komadanje $G/\cup H$ grupe G očigledno povezano s komadanjem množine G/I parcelâ na skupinu H parcelâ H i pomake te skupine: ta su dva komadanja izomorfna.

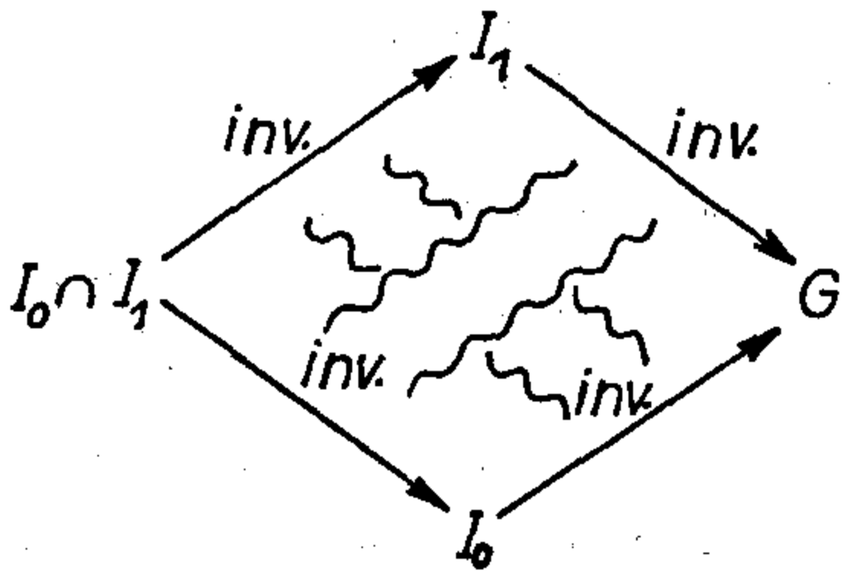
16.10.2. Pokažimo to i formalno. $\cup H$ je svakako invarijantna podgrupa u G (isp. teorem 10. 7. 1); nadalje je

$$G \sim G/I, \quad G/I \sim (G/I)/H \tag{1}$$

(isp. teorem 10.3. i 11.6.3), dakle je

$$G \sim (G/I)/H; \tag{2}$$

prema teoremu 12.5.5. to znači da je $(G/I)/H$ izomorfno s kvocijentnom grupom G/X, gdje je X skup svih elemenata iz G koji se kod homomorfizma (2) prevode u neutralni element H grupe $(G/I)/H$, odnosno koji se kod homomorfizma (1) prevode u neki od članova množine H. No, to znači da je upravo $X = \cup H$, jer je i $\cup H$ upravo skup svih elemenata iz G koji se pri homomorfizmu (1) prevode u jedan od članova skupine H. Na taj je način teorem dokazan.



Sl. 17.16.10.

⟶ **16.11. Glavni teorem o invarijantnim podgrupama.** ***Ako su I_0, I_1 različite maksimalne invarijantne podgrupe grupe $(G, \cdot)$, tada je presjek $I_0 \cap I_1 = I$ invarijantna podgrupa i u $(I_0, \cdot)$ i u $I_1, \cdot)$; neka je $n = 0$ ili 1; faktorske grupe G/I_n i $I_{1-n}/(I_0 \cap I_1)$ su izomorfne, tj.***

$$G/I_0 \cong I_1/I_0 \cap I_1, \quad G/I_1 \cong I_0/I_0 \cap I_1.$$

Preslikavanje

$$\dot{I}_n (I_0 \cap I_1) \to \dot{I}_n I_{1-n}, \tag{1}$$

kad $\dot{I}_n$ prolazi I_n, jest izomorfija.

Dokaz se temelji na teoremu 16.8.

Naime, kako su podgrupe I_0, I_1 invarijantne, produkt $I_0 I_1$ je grupa, a I_0, I_n su njene invarijantne podgrupe.

Prema prethodnom teoremu 16.8. kvocijentne grupe

$$I_n/(I_0 \cap I_1),\ (I_0\, I_1)/I_{1-n} \tag{2}$$

su izomorfne; specijalno, preslikavanje (1) je izomorfizam između grupa (2).

Zato će teorem biti dokazan ako dokažemo da je $I_0\, I_1 = G$. Dokažimo i to! No, skup $I_0\, I_1$ je ne samo grupa nego čak invarijantna podgrupa u grupi $(G, \cdot)$, tj. za svako $x \in G$ vrijedi $x\,(I_0\, I_1) = (I_0\, I_1)\, x$. Stvarno, $x\,(I_0\, I_1) \equiv (x\, I_0)\, I_1$ $= (I_0$ je inv. grupa$) = (I_0\, x)\, I_1 =$ (asoc.$) = I_0\,(x\, I_1) =$ (inv.$) \equiv I_0\,(I_1\, x) =$ (asoc.$) = (I_0\, I_1)\, x$. Dakle je zbilja $I_0\, I_1$ invarijantna grupa u grupi $(G, \cdot)$. No, I_0, I_1 su invarijantne podgrupe u $I_0\, I_1$, i to, prema pretpostavci, maksimalne invarijantne podgrupe.

Kako je

$$I_n \subset_{inv.} I_0\, I_1 \subset_{inv.} G, \tag{3}$$

znači to da znak $\subset$ tu bar jedanput znači $=$. Ako je npr. $I_n = I_0\, I_1$ za $n = 0, 1$, onda to znači da je $I_0 = I_1$, protivno pretpostavci da je $I_0 \neq I_1$. Dakle, u (3) drugi znak $\subset$ znači $=$, tj. $I_1\, I_0 = G$, a to i tražimo. Time je teorem potpuno dokazan.

16.12. Teorem. *Presjek $I = I_0 \cap I_1$ dviju* ***maksimalnih*** *invarijantnih podgrupa G je* ***maksimalna*** *invarijantna podgrupa i od I_0 i od I_1.*

Naime, prema teoremu 16.11, faktorska grupa I_0/I je izomorfna s faktorskom grupom G/I, pa kao i ova mora I_0/I biti prosta; a to prema 17 § 1.13 znači da je I maksimalna podgrupa od I_0.

16.13. Zadaci.

1. U grupi $S_4 \equiv \{1, 2, 3, 4\}$! svih permutacija brojeva 1, 2, 3, 4 nalazi se podgrupa S_3 svih $p \in S_3$ za koje je $p_4 = 4$ kao i podgrupa $F = \{1234, 2314, 3124\}$; 1) je li F invarijantno u odnosu na S_3, odnosno S_4?; 2) je li S_3 invarijantno u odnosu na S_4?
2. Promatraj kvaternionsku grupu Qu (§ 13.5.6.); nađi joj sve podgrupe i uvjeri se da su one sve invarijantne; na primjeru podgrupa što ih generira j odnosno k ilustriraj teoreme 16.11, 16.12.
3. Može li se teorem 16.11 ilustrirati na grupi: 1) tetraedra (odnosno A_4); 2) oktaedra (odnosno S_4)?
4. U grupi $(D, +)$ odredi sve maksimalne invarijantne podgrupe; dokaži da minimalnih nema.
5. Ako je $X \in \{Q, R, R(i)\}$ dokaži da grupa $(X, +)$ nema ni minimalnih ni maksimalnih invarijantnih podgrupa.
6. Množidbena grupa kompleksnih brojeva $\neq 0$ nema maksimalne podgrupe; minimalne su oblika $e^{i\frac{2\pi}{p}D}$, gdje je p proizvoljan prost broj.
7. Ako su I_0, I_1 invarijantne podgrupe od G, te $I_0 \subset I_1$, tada imamo kvocijentne grupe G/I_0, I_1/I_0, G/I_1; time se dobije komadanje od G/I_0 prema I_1/I_0 pa vrijedi $(G/I_0)/(I_1/I_0) \cong G/I_1$ (formalno skraćivanje sa I_0).

8. Ako su I_1, I_2, I_3 invarijantne podgrupe, tada je grupa

$$(I_1 I_2 \cap I_3)/(I_1 \cap I_3)(I_2 \cap I_3)$$

i grupe koje se iz nje dobiju cikličnom zamjenom indeksâ 1, 2, 3 međusobno izomorfne (Remak, 1931).

17. KOMPOZICIONI NIZOVI. NORMALNI NIZOVI

17.0. Priprema. Od interesa je za zadanu grupu $(G, \cdot)$ promatrati njene *najopsežnije* invarijantne podgrupe, tj. takve invarijantne podgrupe kojima je G jedina invarijantna podgrupa grupe G koja ih strogo obuhvata. Tako je npr. u grupi što pripada kvadratu ciklička grupa sa četiri člana maksimalna.

U grupi S_n svih permutacija od n elemenata sve parne permutacije obrazuju tzv. *alternirajuću podgrupu* A_n; ona je *maksimalna* invarijantna podgrupa u S_n. Specijalno, u grupi S_4 svih permutacija od četiri zadana broja 1, 2, 3, 4 alternirajuća grupa A_4 i *četvorna grupa* V_4, što je obrazuju permutacije $e = 1234,\ 2143,\ 3412,\ 4321$, jesu invarijantne podgrupe; prva je *maksimalna*, druga nije jer je V_4 dio podgrupe A_4 (naime sve četiri napisane permutacije su parne).

Sama četvorna grupa V_4 ima ove *tri maksimalne* invarijantne podgrupe:

(1) $\{e, x\}$, gdje je $x \in \{2143, 3412, 4321\}$ i $\{e\} = \{1234\}$.

Na taj način dobivamo ove *nizove grupa* u kojima je *svaki* član osim prvoga *maksimalna invarijantna podgrupa člana pred njim:*

(2) $$S_4 \supsetneq A_4 \supsetneq V_4 \supsetneq \{e, x\} \supsetneq \{e\},$$ pri čemu vrijedi (1).

Svi ti nizovi imaju isti broj članova. To je, svakako, zanimljiva pravilnost. Međutim, pravilnost je još veća i vrijedi za *svaku konačnu grupu.*

Naime, u vezi s maksimalnim invarijantnim podgrupama promatraju se i ***maksimalni** silazni nizovi invarijantnih podgrupa: oni počinju sa G, a svršavaju s jediničnom grupom* $(\{e\}, \cdot)$. Ako je $G_0 = G, G_1, G_2, \ldots, G_n = \{1\}$ jedan takav *maksimalni* niz, onda je $G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_n$ i taj niz ne može biti podniz kakvog drugog strogo silaznog niza invarijantnih podgrupa. Svi ti maksimalni nizovi imaju *isti broj elemenata*; niz pripadnih faktor-grupa

$$G_1/G_0,\ G_2/G_1, \ldots\ G_n/G_{n-1},$$

ne gledajući na redoslijed i izomorfiju, isti je za sve nizove (Jordan 1869, Hölder 1897) (v. § 13.1.6).

Isti zaključak vrijedi ne samo za te tzv. »*glavne nizove*« nego i za tzv. *kompozicione ili Jordan-Hölderove* [*Žordán-Helder*] *nizove* u vezi sa zadanom konačnom grupom: kod ovih je nizova svaki član *maksimalna invarijantna podgrupa* prethodnog člana (a ne mora nužno biti invarijantna podgrupa *svih prethodnih* članova, kao što je slučaj kod glavnih nizova).

Sve ćemo to dokazati u ovom paragrafu.

17.1. Glavni kompozicioni nizovi. Jordan-Hölderov teorem.

17.1.1. Maksimalni invarijantni djelitelj (podgrupa) zadane grupe G je svaki *invarijantni* djelitelj (podgrupa) od G koji nije dio nikoje druge *invarijantne* podgrupe od G (isp. 17 § 11.1.1).

17.1.2. Definicija. **Glavni niz zadane grupe $(G\cdot)$** je svaki *maksimalni strogo silazni niz* $G_0 \supsetneq G_1 \supsetneq \cdots$ *invarijantnih podgrupa* te zadane grupe; faktorske grupe $G_0/G_1, G_1/G_2, \cdots$ zovu se *faktori glavnog niza.*

17.1.3. Definicija. **Kompozicioni ili Jordan-Hölderov niz** zadane grupe $(G,\cdot)$ je svaki *maksimalni strogo silazni* niz $G_0 \supsetneq G_1 \supsetneq \cdots$ koji *počinje* sa zadanom grupom, a svaki preostali član je ***maksimalna** invarijantna podgrupa **prethodnog** člana. Faktorske grupe $G_0/G_1, G_1/G_2, \ldots$ zovu se *faktori kompozicionog niza.*

Naravno, svaki kompozicioni niz završava se jediničnom grupom.

Svaki glavni niz je određen Jordan-Hölderov niz; obrat ne vrijedi. Tako npr. za grupu S_4 niz (2) je kompozicioni niz, ali nije glavni niz jer npr. član $\{e, x\}$ nije invarijantna podgrupa u S_4, mada jest u V_4.

Svaka izreka o Jordan-Hölderovim nizovima vrijedi i za glavne nizove.

Ako je $G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_n$ određen Jordan-Hölderov niz (naravno: $G_0 = G$, $G_n = 1$); tada je određen i niz pripadnih kvocijentnih grupa

$$G_0/G_1, G_1/G_2, \ldots, G_{n-1}/G_n;$$

te kvocijentne grupe zovu se ***faktori** kompozicionog niza.*

17.1.4. Jordan-Hölderov teorem. ***Neka je G proizvoljna konačna grupa; između bilo koja dva kompoziciona niza grupe G može se uspostaviti tolikovanje f* (tj. obostrano-jednoznačno pridruživanje članova jednog niza i članova drugog niza), *tako da pripadne kvocijentne grupe budu izomorfne.*** **To znači ovo: ako su**

$$G_0, G_1, \ldots, G_n$$

$$G_0', G_1', \ldots, G_{n'}$$

dva Jordan-Hölderova niza, tada je $n = n'$ (oba niza imaju jednako mnogo članova); nadalje, postoji permutacija p brojeva (indeksa) $0, 1, \ldots, n$ tako da faktor-grupa G_m/G_{m+1} bude izomorfna s faktor-grupom

$$G'_{p_m}/G_{p_{m+1}}.$$

Gornji teorem dopušta zanimljivo poopćenje. Zato ćemo dokazati to poopćenje (Schreierov teorem), a time i Jordan-Hölderov teorem.

17.2. Normalni nizovi. Schreierov teorem. — 17.2.1. Definicija. *Normalan niz* za zadanu grupu $(G,\cdot)$ jest *svaki* silazni niz koji počinje sa G, a svršava sa $\{1\}$ i u kojem je *svaki član invarijantna podgrupa prethodnog člana.*

17.2.2. Normalan niz *bez ponavljanja* jest svaki normalni niz u kojem *nema jednakih* članova.

17.2.3. Normalnom nizu $G_0 = G \supset G_1 \supset G_2 \cdot \cdot \cdot \supset G_n = \{1\}$ pridružene su faktor-grupe $G_0/G_1, G_1/G_2, \cdot \cdot \cdot, G_{n-1}/G_n$, a zovu se *faktori* promatranog normalnog niza.

17.2.4. *Normalni niz a je proširenje normalnog niza b* ako svaki član ovoga dolazi kao član u nizu *a*.

17.2.5. Dva normalna niza x, y su *izomorfna* simbolički $x \cong y$ ako se između njihovih članova može uspostaviti *tolikovanje*, i to tako da pripadni faktori budu izomorfni.

—→ **17.2.6. Osnovni teorem (Schreier [Šrajer]).** ***Neka je G proizvoljna konačna grupa; tada svaki par normalnih nizova vezanih za grupu G dopušta izomorfna proširenja,*** **tj.** ***i jedan i drugi niz mogu se proširiti tako da nastala dva normalna niza budu izomorfna.***

17.2.7. Naravno, svaki kompozicioni niz je normalan i bez ponavljanja, pa se bez ponavljanja ne može proširiti. Ako su k, l dva kompoziciona niza, tada postoji jedno proširenje k' niza k i jedno proširenje l' niza l, tako da nizovi k', l' budu izomorfni. No, $k = k'$, $l = l'$. To znači da su svi kompozicioni nizovi zadane grupe međusobno izomorfni. To je upravo Jordan-Hölderov teorem.

17.2.8. Primjedba. U osnovnom djelu o grupama: C. Jordan, *Traité des substitutions et des équations algébriques*, Pariz 1870, pokazao je Jordan da je kardinalni broj od G_m/G_{m+1} isti kao i onaj od $G'_{p_m}/G'_{p_{m+1}}$; O. Hölder (Mathematische Annalen 34 (1897), str. 37) dokazao je i spomenuti izomorfizam. Schreier je svoj teorem dokazao u Hamburger Abhandlungen 6 (1928), 300—302.

17.3. Osnovni teorem o invarijantnim podgrupama. Dokaz Šrajerova (Schreier) teorema. — 17.3.1. Neka su

g $\qquad G \supset G_1 \supset \cdot \cdot \cdot \supset G_r = \{e\}$

h $\qquad G \supset H_1 \supset \cdot \cdot \cdot \supset H_s = \{e\}$

dva normalna niza vezana za grupu G; ako je jedan od brojeva r, s jednak 1, *tada je jedan od nizova g, h oblika* $G \supset \{e\}$, *pa je očigledno preostali niz njegovo proširenje — teorem je očigledan.* Za preostale slučajeve dokaz ćemo provesti postupno, i to za $s = 2$ *induktivno po r, a onda induktivno po s.*

17.3.2. Neka je, dakle, $s = 2$; niz h izgleda ovako: $G, H_1, \{e\}$. Teorem vrijedi za slučaj $r = 1$; pretpostavimo da vrijedi i za svaki slučaj kad jedan od nizova ima najviše n članova; dokažimo ga i za slučaj da jedan od nizova ima $1 + n$ članova. Recimo da se radi o gornjem nizu g od $1 + n$ članova. Promatrajmo presjek $G_1 \cap H_1$ i produkt $G_1 \cdot H_1$; to su invarijantne podgrupe u G, pa tako za podgrupu G_1 imamo normalne nizove

(1) $\qquad G_1, G_2, \ldots, G_n \qquad$ sa n članova

(2) $\qquad G_1, G_1 \cap H_1, \{e\} \qquad$ sa 3 člana;

tu se radi o slučaju za koji je, prema pretpostavci, teorem dokazan.

Postoje dakle: proširenje (1)′ od (1) i proširenje (2)′ od (2), tako da bude

(3) $\qquad (1)' \cong (2)'.$

Prema teoremu imamo:

$$G_1 H_1 / H_1 \cong G_1/(G_1 \cap H_1),\ G_1 H_1/G_1 \cong H_1/(G_1 \cap H_1). \tag{3}$$

Prema tome je

$$\{G_1 H_1, G_1, G_1 \cap H_1, \{e\}\} \cong \{G_1 H_1, H_1, G_1 H_1 \cap \{e\}\}. \tag{4}$$

17.3.3. Promatrajmo proširenje $\{G_1 \cdot H_1, (2)'\}$ niza $(4)_1$; tome proširenju $(4)_1'$ odgovara (v. niže, § 17.3.5) neko proširenje i desne strane $(4)_2$ — označimo ga $(4)_2'$, tako da bude

$$(4)_1' \cong (4)_2'.$$

Dakle i

$$\{G, (4)_1'\} \cong \{G, (4)_2'\}. \tag{5}$$

No, $(5)_1$ je određeno proširenje zadanog niza g od $1+n$ članova, a $(5)_2$ je proširenje zadanog niza h od tri člana. Dakle je prelaz od g-nizova sa n članova na g-nizova sa $1+n$ članova učinjen za svaki slučaj kad h-niz ima tri člana. Time je teorem dokazan za proizvoljno r i za $s = 1, 2$.

17.3.4. Sad ćemo primijeniti indukciju na broj s. Teorem je dokazan za svako r te za $s = 1, 2$. Pretpostavimo da je teorem dokazan za svako r te za $s = 1, 2, \ldots, n-1$. Dokažimo ga i za $s = n$. Najprije je jasno da postoji proširenje g' i proširenje $\{G, H_1, e\}'$, tako da bude:

$$g' \cong \{G, H_1, e\}'. \tag{6}$$

Neka je $6\,H_1$ završni dio niza $(6)_2$ koji počinje sa H_1; niz $6\,H_1$ i normalni niz $H_1, H_2, \ldots, H_n$ od n članova imaju, prema induktivnoj pretpostavci, izomorfna proširenja

$$(6\,H_1)',\ \{H_1, H_2, \ldots, H_n\}':$$

$$(6\,H_1)' \cong \{H_1, H_2, \ldots, H_n\}'. \tag{7}$$

Na osnovu niza $(7)_1$ pojavljuje se proširenje $\{G, (6\,H_1)'\}$ normalnog niza $(6)_2$ — označimo to proširenje sa $(6)_2'$; na osnovu izomorfizma (6), zaključujemo prema 17.3.5 da postoji i neko proširenje $(6)_1'$ niz $(6)_1$, tako da bude

$$(6)_1' \cong (6)_2',$$

$$(g')' \simeq \{G, (6\,H_1)'\}. \tag{8}$$

No, iz (7) izlazi

$$\{G, (6\,H_1)'\} = \{G, \{H_1, H_2, \ldots, H_n\}'\},$$

a to je svakako neko h'. Na taj način (8) postaje $(g')' \cong h'$, tj. postoji proširenje $(g')'$ niza g koje je izomorfno s proširenjem h' niza h. A to je i trebalo dokazati. Time je indukcija dokazana i prema r i prema s — teorem je potpuno dokazan, ukoliko još dokažemo da vrijedi ova

17.3.5. Lema o proširenju izomorfnih normalnih nizova. *Neka su g, h dva izomorfna normalna niza grupe G; tada svakom proširenju g' niza g odgovara proširenje h' niza h, tako da g' i h' budu izomorfni.*

Dokažimo da je ta lema ispravna. Pa neka se radi o normalnim nizovima

$$g = (G = G_0, G_1, G_2, \ldots, G_r = \{e\}),\ h = (G = H_0, H_1, H_2, \ldots, H_s);$$

tada zbog $g \cong h$ svakom broju $n = 0, 1, \ldots, r$ odgovara određen broj fn iz niza $0, 1, \ldots, s$, tako da bude

$$G_{n-1}/G_n \cong H_{fn-1}/H_{fn}; \tag{1}$$

zato svakom normalnom nizu grupe G_{n-1}/G_n odgovara izomorfan niz grupe H_{fr-1}/H_{fr}.

No, normalnom nizu faktor-grupe G_{n-1}/G_n odgovara u G_{n-1} određen normalan niz od G_{n-1} do G_n (v. § 12.7.1);[1)] zbog izomorfije (1) odgovara time i u H_{fn-1} od H_{fn-1} do H_{fn} određen izomorfan normalan niz; nizanjem tih nizova dobije se određeno proširenje h' niza h, a očigledno je $g' \cong h'$.

17.3.6. O normalnim nizovima faktorske grupe. — 17.3.6.1. *Neka je I invarijantna podgrupa u grupi G; promatrajmo pripadnu kvocijentnu grupu G/I i bilo koji njen normalni niz*

$$G/I = N_0 \supset N_1 \supset \cdots \supset N_r = \{I\}. \tag{1}$$

Neka je K_i unija članova iz N_i za $i = 0, 1, \ldots, r$. Tako dobivamo normalan niz od G do I, a glasi ovako:

$$K_0 \equiv G,\ K_1,\ K_2, \ldots, K_r = I \tag{2}$$

K_i je invarijantna podgrupa od K_{i-1}.

Prema drugom teoremu o izomorfizmu vrijedi $K_{i-1}/K_i \cong N_{i-1}/N_i$ za $i = 1, 2, \ldots, n$, što znači da su nizovi (1), (2) izomorfni. Prema tome, imamo ovu činjenicu:

17.3.6.2. Lema. *Svakom normalnom nizu faktorske grupe G/I odgovara u G izomorfan niz od G do I.*

17.4. Zadaci.

1. Odredi kompozicione nizove cikličke grupe C_6. Ilustriraj na njima Jordan-Hölderov teorem.
2. Isto pitanje za 1) alternirajuću grupu A_4 (odnosno grupu G_T tetraedra); 2) simetričnu grupu S_4 (odnosno za grupu G_K kocke jer je $S_4 \cong G_K$).
3. Koliko članova ima svaki kompozicioni niz grupe A_n $(n = 3, 4, 5, \ldots)$?
4. Dokaži da kvaternionska grupa Qu ima kompozicioni niz Qu, $\{\pm 1, \pm j\}$, $\{\pm 1\}$, $\{1\}$ i da su pripadne faktorske grupe C_2, C_2, C_2.

18. KOMUTATORI GRUPE. KOMUTANTI GRUPE

18.0. U općem slučaju, za elemente a, b grupe G ne vrijedi $ab = ba$; no u svakom slučaju grupa sadrži x za koje je

$$ab = xba. \tag{1}$$

[1)] Ako je $G_0 = G \supset G_1 \supset \ldots \supset G_n \supset \ldots \supset G_r = \{e\}$ normalni niz grupe G, pa ako je G_n invarijantna podgrupa u G, tada se $G_0, G_1 \ldots G_n$ zove »*normalni niz od G do G_n grupe G*«,

Važno je znati sve »*komutatore grupe*« tj. sve elemente x za koje vrijedi (1) i pri čemu a, b prolaze kroz G. Skup svih komutatora generira podgrupu G' (*komutant ili derivat grupe*) koja je od važnosti za G. Zanimljivo je da grupa G' nastaje u vezi s ispitivanjem *komutativnosti* u grupi G, i da je njena opsežnost mjerilo nekomutativnosti u G; a s druge strane, faktorska grupu G/G' je komutativna (isp. 17 § 18.6).

18.1. Definicija. *Komutator uređene dvojke* a, b članova grupe jest rješenje jednadžbe (1) tj. $aba^{-1}b^{-1}$; označuje se sa $[a, b]$. Dakle $[a, b]=aba^{-1}b^{-1}$.

18.1.1. Lema. $[a, b]=1 \Leftrightarrow ab=ba$.

18.2. Definicija skupa $[G, G]$. *Skup komutatora grupe* G označuje se sa $[G, G]$; tj. $[G, G]=\{aba^{-1}b^{-1};\ a\in G,\ b\in G\}$.

18.3. Definicija komutanta ili derivata G'. *Najmanja* podgrupa grupe G u kojoj leži *svaki* komutator grupe G zove se *komutant, derivat ili izvod* ili *izvedenik grupe* G; označuje se sa G' ili $Der\,G$ ili $D\,G$. *Drugi* komutant (derivat) je komutant prvoga i označuje se G'' ili $D^2\,G$; dakle

$$D^2\,G\equiv G''=D\,(DG).$$

Uopće, za svaki redni broj $\alpha>0$ stavlja se $D^{\alpha+1}\,G=D\,(D^{\alpha}\,G)$; ako redni broj $\lambda>0$ nema neposrednog prethodnika, stavlja se

$$D^{\lambda}\,G=\bigcap_{n} D^{n}\,G,\ (n<\lambda).$$

Također se stavlja $D_0\,G=G$[1].

18.3.1. Primjer. Za permutacije 231, 132 imamo

$$[231,\ 132]=231\cdot 132\cdot 231^{-1}\cdot 132^{-1}=231\cdot 132\cdot 312\cdot 132=312.$$

Tražeći sve komutatore grupe $S_3=\{1, 2, 3\}!$ dobije se upravo grupa A_3 svih parnih permutacija. Dakle je $[S_3,\ S_3]=S_3'=A_3$ (isp. opći teorem 18.7). Dalje je $A_3'=\{123\}$, tj. $S_3''=\{123\}$.

18.4. *Perfektne grupe.* Ako je $G'=G$, grupa je *perfektna* ili *savršena.*

18.5. Lako se dokazuje da je neutralni element komutator i da je invers komutatora opet komutator; vrijedi

$$[1, g]=[g, 1]\equiv 1,\ [a, b]^{-1}=[b^{-1}, a^{-1}],\ g\,[a, b]\,g^{-1}=[gag^{-1}, gbg^{-1}].$$

Odatle izlazi da je derivat G' invarijantna podgrupa. Međutim, grupa G' je invarijantna ne samo prema svakom *unutarnjem* automorfizmu nego je grupa G' invarijantna prema *svakom* automorfizmu α grupe G; naime

$$\alpha\,[a, b]=\alpha\,(aba^{-1}b^{-1})\underline{\underline{\text{def}}}\,\alpha\,a\,\alpha\,b\,\alpha\,a^{-1}\,\alpha\,b^{-1}=(\text{isp. § 12.5.2})=$$

$$\alpha\,a\,\alpha\,b\,(\alpha\,a)^{-1}\,(\alpha\,b)^{-1}\underline{\underline{\text{def}}}\,[\alpha\,a,\ \alpha\,b].$$

---

[1] Analogija s definicijom derivatâ $D^n\,M$ pri čemu je M skup (odnosno funkcija) je očigledna; pri tom se prenosi i odgovarajuća terminologija.

⟶ **18.5.1.** Teorem. *Derivat G' grupe G je karakteristična invarijantna podgrupa.* Pri tom vrijedi

18.5.2. Definicija. Podgrupa G_0 grupe G je *karakteristična,* ako je invarijantna prema *svakom automorfizmu* α grupe G; dakle $\alpha G_0 \subset G_0$ (a ne samo $g G_0 g^{-1} \subset G_0$ za $g \in G$).

18.5.3. Posljedica. *Zadana klasa konjugiranosti grupe G ili leži sva u G' ili leži sva van G'. Derivat G' je unija određenog skupa klasâ grupe G;* ako je $G' = G$ (savršene grupe!), onda je G' unija *svih* razreda grupe G.

Prema tome, za dano $a \in G$ relacija $a \in G'$ daje $g a g^{-1} \in G'$ za *svako* $g \in G$.

⟶ **18.6.** Teorem. ***(i) Derivat G' grupe G je invarijantna podgrupa od G; faktorska grupa G/G' je komutativna.***

(ii) ***Ako je faktorska grupa G/I komutativna, tada je $I \supset G'$.***

Dokaz. Pa neka $a G'$, $b G' \in G/G'$; nađimo pripadni komutator:

$$[a G', b G'] \stackrel{\text{def}}{=} a G'\ b G'\ (a G')^{-1}\ (b G')^{-1} = (ab)\ G'\ (G'^{-1} a^{-1})\ (G'^{-1} b^{-1}) =$$

$$= ab\ G'\ (G'\ a^{-1})\ (G'\ b^{-1}) = ab\ G'\ G'\ (a^{-1} b^{-1}) = ab\ G'\ a^{-1} b^{-1} = aba^{-1} b^{-1} G' = G'.$$

Time je dokazan teorem (*i*). Dokažimo sada (*ii*). Prema pretpostavci, I je invarijantna podgrupa u G za koju je

$$a I \cdot b I = b I \cdot a I \quad (a, b \in G).$$

Odatle izlazi $I(ab) = I(ba)$. To znači da svakom $I_1 \in I$ odgovara određeno $I_2 \in I$ za koje je $I_1 (ab) = I_2 (ba)$ dakle $I_1 (aba^{-1} b^{-1}) = I_2$, tj. $[a, b] = I_1^{-1} I_2$; no $I_1^{-1} I_2 \in I$, jer su $I_1, I_2 \in I$. Dakle iz $a, b \in G$ izlazi $[a, b] \in I$; dakle skup komutatora leži u I; odatle izlazi da i sam komutant G' leži u I, što je i trebalo dokazati.

⟶ **18.7.** Teorem. Za svaki prirodni broj $n > 2$ vrijedi $[S_n, S_n] = S_n' = A_n$ tj. komutatori svih permutacija množine $\{1, 2, \ldots, n\}$ ispunjavaju skup A_n svih parnih permutacija te množine.

Dokaz: A_n je invarijantna podgrupa od S_n pa se S_n/A_n sastoji od dva člana i to iz A_n i množine (12) A_n svih neparnih permutacija. Kao dvočlana grupa, grupa S_n/A_n je komutativna; zato prema teoremu 18.6. (*ii*) imamo $A_n \supset S_n'$. Treba još dokazati i dualnu relaciju $S_n' \supset A_n$. Za $n > 2$ grupa S_n nije komutativna, pa je $S_n' \neq \{e\}$. Grupa S_n' je normalna podgrupa grupe S_n', pa kako je $S_n \subset A_n$, grupa S_n' je netrivijalna podgrupa grupe S_n. Za $n = 4$ lako se vidi da je $S_n' = A_n$. Za $n \neq 4$ zna se da je A_n jedina netrivijalna normalna podgrupa grupe S_n' pa je dakle $S_n' = A_n$ za svako $n > 2$ (isp. 32 § 5.5.5).

18.7. Skup $[G, G]$ komutatora kao dodatak podgrupi. U općem slučaju, skup $[G, G]$ nije ni podgrupoid grupe G, jer *proizvod dvaju komutatora ne mora biti komutator*; tim je zanimljivije da vrijedi.

18.7.1. Teorem. *Svaka podgrupa G_1 grupe G koja obuhvata sve komutatore grupe G je invarijantna podgrupa od G; drugim riječima, ako podgrupa G_1 obuhvata derivat G', onda je G_1 invarijantna podgrupa od G.*

Dokaz. Prema pretpostavci, za $a, b \in G$ vrijedi $[a, b] \in G_1$, pa treba dokazati da je $aG_1 = G_1 a$. Dokažimo najprije da je $aG_1 \subset G_1 a$ tj.

$$ag_1 = xa,\ g_1 \in G_1 \Rightarrow x \in G_1.$$

No, iz te prve relacije izlazi $x = [a, g_1]\, g_1$; kako, po pretpostavci, $[a, g_1]$ leži u podgrupi G_1, leži i x u G_1. Slično se dokazuje dualna relacija $aG_1 \supset G_1 a$. Time je teorem dokazan.

⟶ 18.8. Teorem.

$$(i) \qquad (G/I)' = (G'I)/I,$$

$$(ii) \qquad (G/I)' \cong G'/(G' \cap I);$$

naravno, I označuje bilo koju invarijantnu podgrupu od G; G' je derivat od G.

Dokažimo (i). Elementi grupe G/I su oblika gI, $g'I$ gdje je $g, g' \in G$; zato je $[gI, g'I] = [g, g']I$; odatle zaključujemo da je sam komutant $(G/I)'$ generiran proizvodima članova $[g, g']I$ konačnih nizova: opći član komutanta $(G/I)'$ je oblika

$$[g_1, g_1']I \cdot [g_2, g_2']I \cdots [g_n, g_n']I, \quad \text{tj.}$$

$$[g_1, g_1'][g_2 g_2'] \quad \cdots [g_n, g_n']I.$$

A to je upravo opći član od $(i)_2$; relacija (i) je dokazana.

Dokažimo (ii). Oslonimo se na (i). Kako je G' invarijantna podgrupa, proizvod $G'I$ je grupa (isp. § 16.4); zato možemo primijeniti teorem 16.8. i napisati

$$G'I/I \cong G'/(G' \cap I).$$

Odatle i iz (i) izlazi (ii).

18.8.1. Korolar. *G/I je komutativno* $\Rightarrow I \supset G'$ (isp. teorem 18.6 (ii)).

Dokaz: Obje strane u 18.8 (i) su I; a to znači da je $G'I \subset I$, tj. $G' \subset I$.

18.8.2. Korolar. (i) *Ako je grupa savršena* $(G' = G)$, *onda je svaka njena faktorska grupa savršena*

$$G' = G \Rightarrow (G/I)' = G/I.$$

(ii) *Ako je derivat* $G' = \{1\}$, *tada je komutativna i* ***svaka*** *faktorska grupa* G/I:

$$G' = \{1\} \Rightarrow (G/I)' = \{I\}.$$

Dokaz se dobije pišući G umjesto G' u relaciji 18.8. (ii).

18.9. Zadaci o komutantima ili derivatima.

1. Odredi eksplicitno niz komutanata $G^{(0)} = G, G', G'', \ldots$ za ove grupe G: 1) A_3; 2) A_4; 3) G_{okt}; 4) grupa kretanja euklidske ravnine; 5) Qu.
2. $(G_1 \times G_2)' = G_1' \times G_2'$. Poopći.
3. Direktni produkt prostih necikličkih grupa je savršen onda i samo onda ako je svaki faktor savršen.

4. Za svaki redni broj τ postoji grupa $G=G_\tau$ sa svojstvom da je $G^{(\tau+1)}=G^{(\tau)}$, a da $G^{\tau'}$ nije savršena grupa ni za koje $0<\tau'<\tau$ (A. I. Maljcev, *Mat. Sbornik* (nova serija) 25 (1949) 347—366).

5. Ove tri izreke međusobno su ekvivalentne:

(*i*) $G' \subset ZG$ (centar ZG sastavljen je od svih članova iz G koji komutiraju sa svakim g iz G);

(*ii*) operacija $[a, b]$ uzimanja komutatora je asocijativna:

$$[[a, b], c]=[a, [b, c]] \quad \text{za svako} \quad a, b, c\in G.$$

(*iii*) operacija $[\ ,\ ]$ je distributivna u G:

$$a, b, c\in G \Rightarrow [[a, b], c]=[[a, c], [b, c]].$$

19. RAZRJEŠIVE GRUPE[1)]

Uz problem rješavanja algebarskih jednadžbi pomoću radikala pojavila se edna vrsta grupa — *rješive* ili *razrješive grupe*.

19.1. Definicija. Ako grupa ima derivat ili komutant konačna reda sastavljen jedino od neutralnog elementa, grupa je *rješiva ili rezolubilna.*

19.1.1. Primjer. Je li simetrična grupa S_3 rješiva? Nađimo komutante (isp. § 18.3.1).

$$S_3'=A_3,\ S_3''=A_3'=\{1\};\quad \text{dakle je } S_3 \text{ rješiva grupa.}$$

Isto tako se lako vidi da je

$$S_4'=A_4,\ S_4''=A_4'=V_4\equiv\{(1),\ (12)(34),\ (13)(24),\ (14)(23)\}$$

(četvorna grupa), $S_4'''=V_4'=\{1\}$.

19.2. Može se pokazati da simetrična grupa S_5 nije rješiva; isto vrijedi za S_n gdje je $n>4$. (v. 32, § 5.5.5).

⟶ **19.3. Teorem.** ***Ako je konačna grupa G rješiva, tada ona dopušta bar jedan kompozicioni niz*** **(isp. § 17.1.4)**

$$G_0 \supsetneq G_1 \supsetneq \cdots \tag{1}$$

s komutativnim faktorskim grupama

$$G_0/G_1,\ G_1/G_2, \ldots; \tag{2}$$

i obratno.

Po pretpostavci, grupa G je rješiva; znači da postoji najmanji broj τ sa svojstvom $G^{(\tau)}=\{1\}$; tada imamo niz

$$G^{(0)}(\equiv G),\ G',\ G'', \ldots,\ G^{(\tau)}=\{1\}; \tag{3}$$

prema teoremu 18.6. (*i*) faktorske grupe

$$G^0/G',\ G'/G'', \ldots$$

su komutativne.

[1)] ruski разрешимая (группа), engl. solvable, fr. resoluble, nj. auflösbar.

Obratno, ako je (1) kompozicioni niz a faktorske grupe (2) komutativne, tada prema § 18.6 (*ii*) izlazi da je $G_1 \supset G_0'$; iz istog je razloga $G_2 \supset G_1'$ što s $G_1' \supset G_0''$ daje $G_2 \supset G''$; induktivno se zaključuje da je $G_\nu \supset G^{(\nu)}$ što specijalno za $\nu = \tau$ s $G_\tau = \{1\}$ daje $G^{(\tau)} = \{1\}$. Teorem je dokazan.

—→ **19.4.** Teorem. *Ako je grupa G rješiva, rješiva je svaka podgrupa kao i svaka faktorska grupa grupe G.*

Dokaz. Neka je F podgrupa rješive grupe G. Kako je $F^{(\nu)} \subset G^{(\nu)}$, $G^{(\tau)} = \{1\}$, bit će $F^{(\tau)} = \{1\}$, pa je F rješiva grupa.

Neka je I invarijantna podgrupa od G; dokažimo da je G/I rješiva grupa. Naime,

$$(G/I)' = (G'/G' \cap I) \text{ (§ 18.8. (ii))}$$

$$(G/I)'' = (G'/G' \cap I)' = G''/(G'' \cap (G' \cap I) = G'' \cap I), \ldots$$

$$(G/I)^{(\tau)} = G^{(\tau)}/G^{(\tau)} \cap I = \frac{\{1\}}{\{1\}} = \{1\}, \ (G/I)^{(\tau)} = \{1\}:$$

grupa G/I je rješiva.

19.5. Zadaci.

1. Dokaži rješivost ovih grupa: 1) ciklička grupa C_n; 2) komutativna grupa; 3) grupa kretanja $x' = x\cos\varphi - y\sin\varphi + a$, $y' = x\sin\varphi + y\cos\varphi + b$, pri čemu su φ, a, b proizvoljni realni brojevi; 4) A_2, A_3, A_4; 5) *Qu*; 6) homomorfna slika svake rješive grupe; 7) direktan produkt rješivih grupa; 8) grupa kojoj je rješiva neka invarijantna podgrupa i pripadna faktorska grupa; 9) $G/G^{(n)}$ za bilo koje n; 10) G uz uslov da G ima p^n članova (p prost broj); 11) $kG < 60$ (kG = kardinalni ili glavni broj od G).
2. Feit-J. Thomson najavili su dokaz da je rješiva svaka konačna grupa s neparnim brojem članova (Proc. Nat. Acad. Sci USA 48 (1962) 968—970). Vidjeti Walter Feit-John G. Thomson, *Solvability of groups of odd order*, Pac. J. of Math. 13 (1963), 775—1029; čitav taj rad posvećen je dokazivanju izrečene tvrdnje. To je u historiji matematike dosad najdulji dokaz!

   Time je riješen i poznat Burnside-ov problem pa je dokazano: nikoja *konačna grupa s neparnim brojem članova nije prosta.* (v. Kuroš [2], 433[14–15]).
3. Dokaži neposredno da je grupa A_5 nerješiva.

20. KOMUTATIVNE GRUPE ILI MODULI

20.0. Među najjednostavnije grupe i grupe koje su najbolje izučene spadaju *komutativne grupe ili moduli;* zapisujemo ih obično *aditivno*, pa je dakle $x + y = y + x$. One su važno sredstvo i u izučavanju nekomutativnih grupa. Osnovna je činjenica da svaki modul s konačnim brojem elemenata ili čak s konačnim brojem generatora posjeduje određenu bazu pomoću koje se svaki

član modula izražava jednoznačno; to izvire iz činjenice da je svaka takva grupa direktan proizvod cikličkih grupa (§ 20.8). Na taj način vidimo kako se cikličke grupe pojavljuju kao važan materijal u izgradnji grupa.

20.1. Cikličke grupe su najjednostavniji moduli; svaka ciklička konačna grupa G izomorfna je s multiplikativnom cikličkom grupom G_{kG} brojeva $\cos j\frac{2\pi}{k}+i\sin j\frac{2\pi}{k}$, gdje je $k=k(G)$, $j=0, 1, 2, \ldots, k-1$; svaka beskonačna ciklička grupa izomorfna je sa $(D, +)$.

Odatle se odmah zaključuje da su *ciklične svaka podgrupa G cikličke grupe C kao i faktorska grupa C/G.*

Specijalno, ako je a generator od C, dakle $Da=C$, pa ako m označuje *prvi* prirodni broj sa svojstvom $ma\in G$, tada je ma generator grupe G. U obratnom bi slučaju bilo neko $n\in N$, $na\in G\setminus D(ma)$ pa dakle n ne bi bilo djeljivo sa m nego bi najveća zajednička mjera $d=M(m, n)$ bila $<m$. No, tada postoje cijeli brojevi x, y za koje je $mx+ny=d$ (pogl. 6 § 10.8 (*ii*)) pa bi bilo

$$da=(mx+ny)\,a=mxa+nya$$

dakle $da\in G$ jer mxa, nya leže u grupi G; no relacije $da\in G$, $0<d<m$ protive se definiciji broja m.

20.2. Egzistencija cikličkih grupa u svakoj konačnoj grupi.

Teorem. *Ako je grupa $(G, +)$ konačna i komutativna, tada za svaki prost broj p koji dijeli kG postoji bar jedna ciklička grupa $C_p\supset G$ a time i bar jedan član g_0 iz G za koji je $\pi(g_0)=p$; pri tom $\pi(g_0)$ znači najmanji prirodni broj n za koji je $ng_0=0$ (kad bi grupa bila pisana multiplikativno, onda bi bilo $g_0^n=1$).*

Dokaz. Zadano je $a\in G$; promatrajmo aditivne prikaze od a oblika

$$\sum_g a_g\,g=a; \tag{1}$$

pri tom je koeficijent a_g cio broj iz $\{0, 1, \ldots, \pi(g)-1\}$; prema tome, za svako $a\in G$ promatramo funkciju

$$g\in G\longrightarrow a_g \tag{2}$$

sa svojstvom $a_g\in\pi(g)-1$ i za koju vrijedi (1).

Neka je $N(a)$ broj svih takvih funkcija. Dokažimo da je

$$N(a)=N(0)\quad\text{za svako}\quad a\in G. \tag{3}$$

Stvarno, neka je

$$\sum_g 0_g\,g=0 \tag{4}$$

jedna reprenzentacija neutrala 0; odatle pribrajajući k (4) jednadžbu (1) i radeći s koeficijentima a_g, 0_g modulo $\pi(g)$ dobije se određena reprezentacija od a; to pridruživanje reprezentacijâ od 0 i a je obostrano jednoznačno, kao što se lako vidi. Dakle vrijedi (3).

No, broj svih različnih funkcija (3) jednak je

$$\prod_{g\in G}\pi(g); \tag{5}$$

i svakoj takvoj funkciji f odgovara proizvod $\sum_g f_g g$ koji je određen član $a\in G$ pa vrijedi $f_g = a_g$. Iz tih razloga imamo

$$kG\cdot N(0)=\prod_{g\in G}\pi(g), \tag{6}$$

jer različnim a-ovima iz G odgovara po $N(0)$ promatranih funkcija (2).

Neka prost broj p dijeli kG. Prema (6) dijeli p produkt $(6)_2$ a time i bar jedan od brojeva $\pi(g)$ (pogl. 6. § 13.5); recimo neka za $g_1\in G$ vrijedi $\pi(g_1)=pq$; tada imamo cijeli broj $q=\pi(g_1)\,p^{-1}$ kao i član $g_0=q\,g_1\in G$, pa se vidi da je $\pi(g_0)=p$.

20.2.1. Cauchy je 1845. godine dokazao da teorem 20.2. vrijedi i za nekomutativne konačne grupe (međutim, teorem ne mora vrijediti za beskonačne grupe, kao što to pokazuje grupa $(D, +)$).

20.2.2. Teorem je poopćio Frobenius 1903. dokazavši da za svako $n\,|\,kG$ konačna grupa G sadrži bar jedno rješenje jednadžbe $nx=0$ i da je broj tih rješenja djeljiv sa n; specijalno, za svako $p\,|\,kG$ ima bar jedno $g\in G\setminus\{0\}$ za koje je $pg=0$; vidi se da je tada i $\pi(g)=p$, pa tako zaista iz Frobeniusova rezultata izlazi Cauchyev rezultat.

20.3. *Cilj nam je da dokažemo da je svaka konačna komutativna grupa G proizvod cikličkih grupa.* Stvar ćemo izvesti u nekoliko koračaja promatrajući koliko broj kG ima prostih faktora.

⟶ 20.4. Teorem. ***Ako je $k(G, +)=p^n$, grupa $(G, +)$ je direktni proizvod cikličkih grupa oblika C_p.***

Promatrajmo broj $\pi(G)=\sup\pi(g)$, $(g\in G)$.

(*i*) Slučaj $\pi(G)=p$. Neka je $g_1\in G\setminus\{0\}$; tad imamo cikličku podgrupu $Dg_1=\{0, g_1, 2g_1, \ldots, (p-1)g_1\}$ od p članova:

$$Dg_1\subset G. \tag{1}$$

Ako u (1) vrijedi znak $=$, stvar je gotova; ako u (1) stoji znak $\subset$, neka je $g_2\in G\setminus Dg_1$; tada imamo cikličku podgrupu Dg_2 kao i podgrupu

$$Dg_1+Dg_2 \tag{2}$$

od p^2 članova koji su oblika $e_1g_1+e_2g_2$ s koeficijentima iz $\{0, 1, \ldots, p-1\}$. Vidi se naime da za takve izraze vrijedi

$$e_1g_1+e_1g_2=e_1'g_1+e_2'g_2 \Leftrightarrow e_1=e_1'\wedge e_2=e_2', \tag{3}$$

jer iz prve jednadžbe u (3) izlazi

$$(e_1-e_1')g_1=(e_2'-e_2)g_2. \tag{4}$$

Dakle je $(e_2'-e_2)\,g_2\in Dg_1\cap Dg_2=\{0\}$ i prema tome $(e_2'-e_2)\,g_2=0$ i dalje $e_2'=e_2$. što sa (4) daje i $e_1'=e_1$.

Ako je $(2)=G$, stvar je gotova jer je $(2)=Dg_1\times Dg_2$ (zapravo je $(2)=Dg_1\oplus Dg_2$). Ako je $(2)\subsetneq G$, neka je $g_3\in G\setminus(2)$. Promatrajmo grupu

$$G_3=G_2+Dg_3,\quad \text{gdje je}\quad G_2=Dg_1+Dg_2.$$

Opet se dokazuje da je G_3 podgrupa od p^3 članova; itd.

Nakon $(k\,G/p=)\,s$ koračaja doći ćemo do cilja pa će biti

$$G=Dg_1\oplus Dg_2\oplus\cdots\oplus Dg_s.$$

(*ii*) Slučaj da je teorem 20.4. dokazan za svako G za koje je još i $\Pi\,(G)\leq n-1$; dokažimo onda teorem i za slučaj $\pi\,(G)=n$. Specijalno, za grupu $H=\{g^p;\ g\in G\}$ imamo $\pi\,(H)=n-1$ pa je prema indukcionoj hipotezi

$$H=C_{h_1}\oplus C_{h_2}\oplus\cdots\oplus C_{h_m};$$

neka je $c_i=a_i{}^p$ (pritom je $a_i\in G$) generator cikličke grupe C_{h_i}; promatrajmo proizvode

$$e_1\,a_1+\cdots+e_m\,a_m\ (e_\mu\in\{0,\ 1,\ \ldots,\ ph_\mu-1);$$

lako se dokazuje da oni čine grupu, A_1, od $k\,H\cdot p^m$ članova pa je zato A direktni proizvod grupâ Da_μ $(\mu=1,\ 2,\ \ldots,\ m)$. Ako je $A_1=G$, stvar je gotova; ako pak postoji $b\in G\setminus A_1$, tada je $pb\in H$ dakle i $-pb\in H$ (jer je H grupa); to znači da za neko $g\in A_1$ vrijedi $-pb=pg$. Promatrajmo $b+g$ i odredimo $\pi\,(b+g)$. Svakako je $p\,(b+g)=pb+pg=pb-pg=0$; no zbog b non$\in A_1$ ne može biti $b+g=0$; znači da je $\pi\,(b+g)=p$ pa imamo cikličku grupu $D\,(b+g)$ koja sa A_1 ima jedino 0 zajedno; tako dobijemo opsežniju grupu

$$A_2=A_1\oplus D\,(b+g).$$

Radeći analogno s A_2 kao što smo radili s A_1 imamo ili $A_2=G$ ili $A_2\subset A_3\subset G$, gdje je $A_3=A_2\oplus Da_3$; itd.

Kako je grupa G konačna doći će se nakon konačno mnogo koračaja do traženog rastavljanjâ. Teorem 20.4. je dokazan.

⟶ **20.5.** Teorem. *Neka je glavni broj grupe* $(G,+)$ *produkt od dva relativno prosta broja* m, n *tj.* $k\,G=mn$, $M\,(m,n)=1$; *neka je*

$$A=\{g,\ g\in G,\ \pi\,(g)\,|\,m\}$$

$$B=\{g,\ g\in G,\ \pi\,(g)\,|\,n\};$$

tada su A, B *podgrupe i vrijedi*

$$G=A\oplus B$$

$$k\,A=m,\ k\,B=n.$$

Najprije, zbog $M\,(m,n)=1$ imamo $A\cap B=\{0\}$ jer $g\in A\cap B$ znači da $\pi\,(g)$ dijeli i m i n; dakle je $\pi\,(g)=1$ pa jednadžba

$$\pi\,(g)\,g=0\quad\text{daje}\quad 1\,g=0,\ \text{tj.}\ g=0.$$

Skup A je podgrupoid od G jer $x\in A$, $y\in A$ znači da $\pi(x)$, $\pi(y)$ dijele m, dakle i višekratnik $W(\pi(x), \pi(y))$ dijeli m što sa $\pi(x+y)\,|\,W$ daje traženo $\pi(x+y)\,|\,m$, tj. $x+y\in A$.

Kako je $\pi(x)=\pi(-x)$ i $0\in A$ znači da je A zaista grupa. Isto tako je $(B, +)$ podgrupa od $(G, +)$.

Dokažimo da je svako $g\in G$ u $A+B$. Kako je naime $M(m, n)=1$, možemo naći cijele brojeve c, d za koje je $1=mc+nd$ (6 § 10.8 (*ii*)) pa je zato

$$g=1\,g=(mc+nd)\,g=mcg+ndg;$$

no $mcg\in B$ jer je $n(mcg)=0$ pa dakle $\pi(mcg)\,|\,n$ dakle $mcg\in B$; isto tako je $ndg\in A$: zato gornji rastav od g daje traženo $g\in A+B$. To ujedno ima za posljedicu da je $G=A+B$.

Dokažimo da je svako $g\in G$ na *jedan jedini način* predstavljeno u obliku $a+b$; ako je naime a, $a'\in A$, b, $b'\in B$ te $a+b=a'+b'$ onda je također $a-a'=b'-b$, pa su $a-a'$, $b-b'$ članovi u $A\cap B:=\{0\}$; dakle je $a-a'=0=b'-b$, tj. $a=a'$, $b=b'$. To ujedno znači da je $k\,G=k\,A\cdot k\,B$.

Time smo najzad dokazali da je zaista $G=A\oplus B$.

Dokažimo još da je $k\,A=m$, $k\,B=n$. Upravo smo naveli da je

$$k\,A\cdot k\,B=mn.\ \text{Zbog}\ M(m, n)=1\ \text{mora biti}$$

$$M(k\,A_1\,n)=1=M(k\,B_1\,n),\quad \text{dakle}\ k\,A=m,\ k\,B=n.$$

Stvarno, ako je p prost faktor od $k\,A$, tada prema 20.2. postoji $a_0\in A$ sa svojstvom $\pi(a_0)=p$; time automatski ne može biti $p\,|\,n$ niti $\pi(a_0)\,|\,n$, jer bi inače bilo $a_0\in B$ tj. $a_0\in A\cap B\setminus\{0\}$, protivno činjenici da je $A\cap B=\{0\}$.

Time je teorem 20.5. potpuno dokazan.

⟶ **20.6.** Teorem. *Ako je grupa $(G, +)$ komutativna, a broj $k\,G$ produkt međusobno prostih brojeva $m_1, m_2, \ldots, m_r$ tada iz*

$$G_\rho=\{g;\ g\in G,\ \pi(g)\,|\,m_\rho\}\qquad \text{izlazi}$$

$$(G, +)=G_1\oplus G_2\oplus\cdots\oplus G_r$$

$$k\,G_\rho=m_\rho,\ (\rho=1, 2, \ldots, r).$$

Teorem se dobije postepenim primjenjivanjem teorema 20.5: najprije stavimo $m=m_1$, $n=m_2\cdots m_r$; stavimo nadalje $G_1=A$, pa zatim primjenimo teorem 20.5. na tako dobivenu grupu B, itd.

20.7. Teorem. *Ako je komutativna konačna grupa G takva da je*

$$k\,G=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}\ \text{tada uz}\ G_\rho=\{g;\ g\in G,\ \pi(g)\,|\,p_\rho^{e_\rho}\}\ \text{vrijedi}$$

$$G=\Sigma\oplus G_\rho,\ k\,G_\rho=p_\rho^{e_\rho}\ (\rho=1, 2, \ldots, r).$$

20.7.1. Korolar. *Ako konačna komutativna grupa $(G, \cdot)$ ima svojstvo da za neki prost broj p vrijedi $\pi(g)=p^m$ (m zavisi od g), tada je i $k\,G$ neka potencija prosta broja p.*

20.8. Osnovni teorem o konačnim aditivnim grupama.

Ako na podgrupe G_p iz teorema 20.6. primijenimo teorem 20.4. dolazimo do ovog osnovnog rezultata:

⟶ ***Ako je komutativna grupa konačna, može se ona prikazati kao direktan proizvod konačnih cikličkih grupa oblika C_{p^n} (tj. kardinalni broj svakog C sadrži po jedan prost broj).***

20.9. Baza konačne komutativne grupe. — 20.9.1. Definicija baze. *Baza komutativne konačne grupe* $(G, +)$ je svaki podskup B sa svojstvom da se *svakom* $g \in G$ može pridružiti *jedna jedina* funkcija $b \in B \to g_b$ sa svojstvom

$$\sum_{b \in B} g_b\, b = g, \quad g_b \in \{1, 2, \ldots, \pi(b)\}.$$

20.9.2. Osnovni teorem o egzistenciji baze. ***Svaka konačna komutativna grupa ima bar jednu bazu kojoj elementi imaju periode oblika p^n (prost broj p i prirodni broj n zavise od odgovarajućeg elementa baze).***

Teorem je drugačija formulacija teorema 20.8.

20.9.3. Tip i invarijante komutativne grupe. *Tip konačne komutativne grupe* je skup s ponavljanjem brojeva $\pi(b)$ pri čemu b prolazi nekom bazom ili osnovom grupe o kojoj je riječ u teoremu 20.9.2; sami brojevi $\pi(b)$ zovu se *invarijante grupe*.

⟶ **20.9.4. Teorem.** ***Tip komutativne konačne grupe ne zavisi od izbora onakve baze o kojoj je riječ u 20.9.2; ako su dvije komutativne konačne grupe izomorfne (neizomorfne) imaju one isti tip (različne tipove).***

Teorem je dovoljno dokazati za svaku grupu reda $kG = p^n$; pa neka G ima bazu $A = \{a_1, a_2, \ldots, a_\alpha\}$ kao i bazu $B = \{b_1, b_2, \ldots, b_\beta\}$; možemo numeraciju provesti tako da bude

$$\pi(a_1) \geq \pi(a_2) \geq \ldots, \quad \pi(b_1) \geq \pi(b_2) \geq \cdots \geq \pi(b_\beta).$$

Pretpostavimo da ta dva niza brojeva nisu jednaka, pa neka je *i prvi* indeks za koji je $m_i \neq n_i$ (stavljamo $\pi(a_j) = m_j$, $\pi(b_j) = n_j$); recimo da je $m_i < n_i$. Grupa $m_i G$ imala bi bazu $\{m_i a_1, \ldots, m_i a_{i-1}\}$ kao i bazu $\{m_i b_i, \ldots, m_i b_\beta\}$.

Radi prve baze bilo bi $kG = \frac{m_1}{m_i} \cdot \frac{m_2}{m_i} \cdots \frac{m_{i-1}}{m_i}$; radi druge baze bilo bi $kG \geq \frac{n_1}{m_i} \frac{n_2}{m_i} \cdots \frac{n_{i-1}}{m_i} \cdot \frac{n_i}{m_i}$, odatle bi izlazilo $m_1 m_2 \cdots m_{i-1} \geq n_1 n_2 \cdots n_{i-1} \frac{n_i}{m_i}$, što je nemoguće jer je po pretpostavci $m_1 = n_1, \ldots, m_{i-1} = n_{i-1}$, $\frac{n_i}{m_i} > 1$.

20.9.5. Normiranje tipa. Tip grupe možemo *srediti* tako da mu članove p^n sredimo najprije po padajućim bazama p, a članove s istim p po padajućim eksponentima n. Tako npr. sređen oblik od $(3, 2, 2, 5^2, 5)$ bio bi $(5^2, 5, 3, 2, 2)$.

Ciklička grupa C_{16} ima tip (2^4); ostale komutativne grupe po 16 članova imaju tipove $(2^3, 2)$, $(2^2, 2^2)$, $(2, 2, 2, 2)$.

20.9.6. Realizacija (ostvarivanje) grupe. Ako je zadan tip

$$(p_1^{\alpha_1},\ p_2^{\alpha_2}\cdot\cdot\cdot p_n^{\alpha_n}) \tag{1}$$

(p-ovi su prosti brojevi među kojima može biti i jednakih), tada skup nizova

$$x=(x_1,\ x_2,\ \ldots,\ x_n) \text{ brojeva } x_1,\ \ldots,\ x_n$$

za koje je $x_\nu^{p_\nu^{\alpha_\nu}}=1$ i pri čemu se definira

$$x+y=(x_1y_1,\ x_2y_2,\ \cdot\cdot;,\ x_ny_n)$$

čini aditivnu konačnu komutativnu grupu tipa (1).

20.10. Slobodne komutativne grupe. — **20.10.1** Definicija. Direktni proizvod od proizvoljno mnogo beskonačnih cikličkih grupa zove se *slobodna komutativna grupa*; jednočlana grupa kao i beskonačne cikličke grupe smatramo slobodnima.

20.10.2. Svaki dio X modula $(G, +)$ sa svojstvom da je svaki član $g\in G$ linearna cjelobrojna kombinacija konačna niza članova iz X zove se *skupom izvodnica* (*generatora*) *grupe* G.

20.10.3. *Nezavisnost i zavisnost.* Konačan dio $X:\subset G$ je *linearno nezavisan* ako iz

$$\sum_{x\in X} d_x\cdot x=0\wedge d_m\in D\wedge x\in X \text{ izlazi } d_x=0.$$

20.10.4. Definicija. *Skup X iz G je linearno nezavisan* ako je *svaki konačan* dio iz X linearno nezavisan.

20.10.4.1. Teorem. *Svaki konačni modul $(G, +)$ je linearno zavisan.*

20.10.5. Kaže se da *element x zavisi linearno od $a_1, a_2, \ldots, a_n$* ako za neke *cijele* brojeve $c\neq 0$, $d_1, d_2, \ldots, d_n$ vrijedi $cx=\Sigma d_\nu a_\nu$.

20.10.5.1. Primjedba. Uočimo da se u toj definiciji pojavljuje cio broj $c\neq 0$ koji ne mora biti $=1$, i da je cx cjelobrojan konačan linearan spoj a-ova i to s *cjelobrojnim* koeficijentima.

20.10.6. Definicija. *Rang modula* $(G, +)$ je *maksimalan* broj ρG linearno nezavisnih članova iz G; ako je $k G<\infty$, stavlja se $\rho G=0$; ako u $(G, +)$ ima n linearno nezavisnih članova za svaki prirodan broj n, stavlja se

$$\rho G=k G.$$

20.10.7. Kao i za linearne prostore (isp. 13 § 4.5) tako se i za module (tj. komutativne grupe $(G,+)$) dokazuju ova dva teorema:

(*i*) *Ako je ρG prirodan broj, tada bilo koja dva maksimalna skupa X_1, X_2, $\subset G$ od kojih je svaki linearno nezavisan imaju po jednako mnogo članova: $kX_1=\rho G=kX_2$* (isp. 13 § 4.5.1);

(*ii*) *Ako je X linearno nezavisan skup generatora modula G ranga $\rho G<\infty$, tada je $kX=\rho G$* (isp. § 20.10.4.1).

⟶ **20.10.8. Osnovni teorem o modulima.** ***Svaki modul G (tj. komutativna grupa) s konačnim skupom izvodnica je direktan proizvod cikličkih grupa.***

Dokaz će biti posljedica narednih dvaju teorema.

20.10.8.1. Teorem. *Svaki je modul izomorfan nekoj faktorskoj podgrupi slobodna modula.*

Stvarno, neka je X skup izvodnica iz zadanog modula $(G,+)$; neka je $x \to fx$ bilo kakvo obostrano jednoznačno preslikavanje množine X sa svojstvom da fX i G budu disjunktni. Nad fX izgradimo slobodan modul U formalno kao direktnu sumu modulâ $(Dfx,+)$; preslikajmo U na G pomoću h stavljajući

$$h(d_1y_1+d_2y_2+\cdots+d_ny_n)=d_1f^{-1}y_1+d_2f^{-1}y_2+\cdots+d_nf^{-1}y_n;$$

jasno je da je h homomorfizam od U na G i da je faktorska grupa $U/h^{-1}0$ izomorfna s modulom G.

20.10.8.2. Teorem. *Neka modul X ima konačan broj, s, linearno nezavisnih izvodnica; neka je Y podgrupa od X; tada postoji s-član niz $x_1, x_2, \ldots, x_s$ linearno nezavisnih izvodnica modula X i određen r-član niz prirodnih brojeva*

$$I_1, I_2, \ldots, I_r$$

sa svojstvom da bude $r \leq s$,

$$I\rho \mid I\rho_{+1} \ (\rho = 1, 2, \ldots, r-1),$$

tj. $I\rho$ dijeli $I_{\rho+1}$ i da niz

$$I_1x_1,\ I_2x_2, \ldots, I_rx_r$$

bude sistem linearno nezavisnih izvodnica podmodula Y.

Dokaz. Neka je $z_1, z_2, \ldots, z_s$ proizvoljan niz nezavisnih izvodnica od X, a $v_1, v_2, \ldots, v_m$ proizvoljan niz izvodnica podgrupe Y; kako je $v\mu \in X$ to će za neke cijele brojeve $a \in D$ biti

$$v_\mu = \sum_\sigma a_{\mu\sigma} z_\sigma \ (\mu = 1, 2, \ldots, m;\ \sigma = 1, 2, \ldots, s). \tag{1}$$

Tako dolazimo do matrice a formata (m, s) s cijelim vrijednostima $a_{\mu\sigma}$. Prema Smithovu normalnom obliku postoje kvadratne matrice b, c s cijelim vrijednostima i sa svojstvom da bude $\det b = \det c = 1$ i da matrica $bac\ (=d)$ ima Smithov oblik: $d_{\mu\sigma}=0$ za $\mu \neq \sigma$, brojevi $d_{11}, d_{22}, \ldots, d_{rr}$ gdje je $r = r(a) =$ rang matrice d jesu prirodni brojevi i svaki dijeli narednoga (isp. 27 § 18.6.1). Provedimo transformacije

$$z_\sigma = \sum_{n=1}^{s} c_{\sigma n} x_n \quad (\sigma = 1, 2, \ldots, s) \tag{2}$$

$$y_k = \sum_\mu b_{k\mu} v_\mu;\ (k = 1, 2, \ldots, m;\ \mu = 1, 2, \ldots, m);$$

time veze (1) postaju

$$y_\mu = \sum_\sigma d_{\mu\sigma} x_\sigma, \tag{3}$$

gdje je matrica d jednaka

$$d = bac. \tag{4}$$

Dovoljno je staviti

$$I_1 = d_{11},\ I_{22} = d_{22}, \ldots, I_{rr} = d_{rr},$$

pa da se vidi da je teorem 20.10.8.2 ispravan.

20.10.8.3. Dokaz teorema. 20.10.8. Neka je zadani modul $(G,+)$ generiran *pomoću* s *izvodnica* (s je prirodan broj); neka je X *slobodan* modul koji je generiran od proizvoljna s-člana skupa $\{x_1, x_2, \ldots, x_s\}$; tada imamo prirodni homomorfizam $h: X \to G$ stavljajući

$$h(k_1 x_1 + k_2 x_2 + \cdots + k_s x_s) = k_1 hx_1 + k_2 hx_2 + \cdots + k_s hx_s.$$

Neka je $Y = h^{-1}\{0\}$ *jezgro* toga homomorfizma; tada je X/Y izomorfno sa G. Primijenimo teorem 20.10.8.2. na sadašnje X, Y; tada članovi

$$g_1 = hx_1, \ldots, g_s = hx_s \tag{5}$$

generiraju grupu $(G,+)$, a članovi $I_1 x_1, \ldots, I_r x_r$ generiraju podgrupu Y; specijalno je $I_\rho x_\rho \in Y$, dakle $h(I_\rho x_\rho) = I_\rho hx_\rho = 0$; drugim riječima

$$I_\rho g_\rho = 0 \quad (\rho = 1, 2, \ldots, r). \tag{6}$$

Neka se u nizu $I_1, \ldots, I_r$ broj 1 pojavljuje r_1 puta; dakle je $0 \leq r_1 \leq r$, pa imamo $r - r_1$ generatora $g_{\rho'}$ $(r_1 < \rho' \leq r)$; zbog (6) element $g_{\rho'}$ generira cikličku grupu $(g_{\rho'})$, specijalno za $\rho' \leq r_1$ je $(g_{\nu'}) = \{0\}$ da se takve podgrupe mogu zanemariti. Naprotiv, ako je $r < s$, tada za svako $r < s' \leq s$ grupa $(g_{s'})$ je beskonačna ciklička grupa. Sama grupa G je direktna suma podgrupâ $(g_{s'})$ $(r_1 < s' \leq s)$ i to $r - r_1$ konačnih cikličkih podgrupa $(g_{s'})$ za $(r_1 < s' \leq r)$ i $s - r$ beskonačnih cikličkih podgrupa $(g_{s'})$ za $r < s' \leq s$. Time je teorem dokazan.

20.11. *Zadaci o modulima.*

1. Navedi nekoliko komutativnih grupa (modula) i nekoliko nekomutativnih grupa.

2. Homomorfna slika modula $(D,+)$ cijelih brojeva je ciklička grupa; i obrnuto: svaka ciklička grupa je homomorfna slika modula $(D,+)$.

3. 1) Ako je p prost broj, tada je svaka grupa od p ili p^2 članova komutativna; 2) za svaki paran broj $2n > 4$ *postoji* nekomutativna grupa op $2n$ članova; takva je npr. grupa $(G_{2n},+)$ sastavljena od ovih $2n$ različnih članova: $0_1, 0_2, \ldots, 0_n; 1_1, 1_2, \ldots, 1_n$ pri čemu definiramo: $g + 0_n = g = 0_n + g$ za svako $g \in G_{2n}$, $0_i + 0_k = 0_{i+k}$, $0_i + 1_k = 1_{i-k}$, $1_i + 0_k = 1_{i-j}$, $1_i + 1_k = 0_{i-k}$, $1_i + 1_i = 0_n$; pri tom u indeksima računamo mod. n; 3) Ako je A bilo koji skup neka $D_0(A)$ označuje skup svih jednoznačnih funkcija $f: A \to D$ uz uslov da skup $A \setminus f^{-1}0$ bude prazan ili konačan; tada je $(D_0(A),+)$ modul; ako je A beskonačno, tada je $kA = kD_0(A)$; 4) Može li se u prethodnom zadatku umjesto D pisati bilo koji modul $(M,+)$?

4. Za svaki konačni modul $(M,+)$ vrijedi $(kM)\,x=0$ za svako $x\in M$.

5. 1) Direktni proizvod modulâ opet je modul; 2) direktni proizvod modula i grupe Qu kvaterniona je hamiltonovska grupa; 3) svaka hamiltonovska grupa je direktan proizvod modula i grupe Qu; 4) Kaže se da je grupa *hamiltonovska* ako joj je svaka podgrupa invarijantna podgrupa.

6. 1) *Jezgro grupe* G je skup JG svih članova grupe koji komutiraju sa *svakom* podgrupom grupe; 2) Jezgro grupe je komutativna hamiltonovska podgrupa; specijalno ZG (centrum grupe) je u JG.

7. 1) *Adjunkta grupe* G je G/ZG, pri čemu je ZG (centar grupe) $=\{x;\, x\in G,\, xg=gx$ za svako $g\in G\}$; 2) adjunkta modula je jedinična grupa; 3) ako je adjunkta grupe ciklična, grupa je komutativna; 4) odredi adjunktu grupa: V_4, G_T, G_O, Qu.

8. Odredi *bazu* ovih grupâ: 1) V_4; 2) G_T; 3) G_K: 4) G_{Dod}; 5) D_n; 6) S_4.

9. Koliko ima međusobno neizomorfnih komutativnih grupa G ako je kG: 1) 6; 2) 8; 3) 60; 4) p^n; 5) n?

10. Ostvari modul tipa:
1) $(2, 2, 2, 2)$; 2) (2^4); 3) $(2^3, 2)$; 4) $(2^2, 2^2)$; 5) $(2^3, 2^2, 2, 3^2)$.

11. Nađi direktni proizvod: 1) $C_2\times C_2$; 2) $(C_2,\cdot)\times(C_3,+)$;
3) $(C_2,\cdot)\times(D,+)$; 4) $(C_2,\cdot)\times(C_4,\cdot)\times(D,+)$; 5) $(C_3,\cdot)\times(Q,+)$;
6) $(C_3,\cdot)\times(C_5,\cdot)\times(C_6,\cdot)\times(D,+)\times(D,+)\times(Q,+)$; 7) $(C_2,+)\oplus\oplus(C_4,+)\oplus(C_8,+)\oplus(D,+)$; 8) $(2D,+)\oplus(3D,+)\oplus(D,+)$. Koja od dobivenih grupa ima konačno mnogo izvodnica?

12. Odredi rang grupa u zad. 11.

13. Može li se u zad. 11. pisati $\oplus$ umjesto $\times$?

21. SKUP ENDOMORFIZAMA ZADANE GRUPE

21.1. Definicija. *Skup endomorfizama* grupoida $(G,+)$ je skup EG svih homomorfizama od G u *sama sebe* pri čemu za $f, g\in EG$ definiramo

$$(fg)(x)=f(gx)\quad (x\in G).$$

Prema tome operacija $\cdot$ u $(EG,\cdot)$ je uzastopno izvođenje (kompozicija) dvojke preslikavanja.

21.2. *Naslijeđena operacija.* Osim gornje operacije slaganja u EG, može se u EG definirati i operacija $+$ naslijeđena iz $(G,+)$ i staviti

$$f(x)+g(x)=(f+g)\,x\quad (x\in G).$$

Ta definicija ima smisla jer je $fx\in G$, $gx\in G$.

Na taj način u $E(G, +)$ imamo naslijeđenu operaciju $+$ i definiranu operaciju $\cdot$ slaganja endomorfizama; dobije se trojka $(EG, +, \cdot)$ pa imamo pridruživanje

$$(G, +) \to (EG, +, \cdot) \tag{1}$$

za svaki grupoid $(G, +)$ pa dakle i za svaku polugrupu, kvazigrupu, grupu, modul, itd.

21.3. *Osnovno pridruživanje* (1) *je poučno i dalekosežno*; specijalno ističemo kako se u novi skup $(1)_2$ *prenijela* (*inducirala*) operacija iz date ogranizacije (strukture) $(1)_1$ i kako se na prirodan način u *novi* skup *uvela nova* operacija — komponiranje preslikavanja; tako će biti ako u ishodnoj strukturi ima i više operacija.

Na taj način, pridruživanjem (1) idemo od određene strukture na određenu nadgradnju te strukture[1]. Slična se ideja javlja često u matematici — odraz slične pojave u prirodnim i društvenim zbivanjima.

—→ **21.4. Teorem.** ***Ako je*** $(C, +)$ ***bilo koja beskonačna ciklična grupa, tada je*** $(EC, +, \cdot)$ ***kolo*** (***prsten***) ***slično kolu*** $(D, +, \cdot)$ ***svih cijelih racionalnih brojeva, tako da endomorfizmi modula*** $(C, +)$ ***poprimaju ulogu cijelih racionalnih brojeva.***

Dokaz. Neka je c generator grupe $(C, +)$; neka je $h \in EC$; tada je $hc \in C$ dakle $h(c) = d_h c$ za neki cio broj $d_h \in D$ (naime, $Dc = C$, jer je c generator grupe $(C, +)$). Nadalje je, za svako $m \in D$, $h(mc) = mh(c) = m(d_h c) = (md_h) c$. Dakle je

$$h(mc) = (md_h)\, c \,(m \in D). \tag{1}$$

Relacija (1) pokazuje da cio broj d_h određuje homomorfiju h pa je veza

$$h \in EC \to d_h \in D \tag{2}$$

obostrano jednoznačna.

Specijalno, identični endomorfizam $j = j_C$ za koji je $j_c x = x$ za svako $x \in C$ zadovoljava $d_{j_c} = 1$; naime, supstitucija $h \to j_c$ daje prema (1) ovo: $j(mc) = md_j c \Rightarrow$ $\Rightarrow$ $mc = md_j c$ $\Rightarrow$ $(m - md_j) c = 0$ $\Rightarrow$ $m - md_j = 0$ $\Rightarrow$ $(1 - d_j) = 0$ $\Rightarrow$ $1 - d_j = 0 \Rightarrow$ $\Rightarrow$ $1 = d_j = d_{j_c}$.

Isto tako, *nula-endomorfizmu* 0_C za koji je $0_c x = 0$ za svako $x \in C$ odgovara broj 0 u D, tj. $d_{0_c} = 0$.

Dokažimo da pridruživanjem (2) proizvod prelazi u proizvod: suma u sumu:

$$d_{h+h'} \to d_h + d_{h'} \tag{3}$$

a umnožak u umnožak:

$$d_{hh'} \to d_h\, d_{h'}; \tag{4}$$

pri tom $h, h' \in EC$.

---

[1] Tako npr. odmah ćemo vidjeti da je $(ED, +, \cdot)$ izomorfno kolu cijelih racionalnih brojeva (teorem 21.4).

Stvarno, pišući u (1) $h+h'$ umjesto h i okrenuvši jednakost izlazi:

$$(md_{h+h'})\,c=(h+h')\,(mc)=(\text{Def.})\,h\,(mc)+h'\,(mc)=$$

$$md_h\,c+md_{h'}\,c=m\,(d_h+d_{h'})\,c.$$

Dakle je

$$(h+h')\,(mc)=m\,(d_h+d_{h'})\,c$$

za svako $m\in D$. A to znači da vrijedi (3).

Isto tako, supstitucija hh' umjesto h prevodi (1) u $(hh')\,(mc)=(md_{hh'})\,c$, pa radeći kao maloprije sa $h+h'$ dolazimo do uvjerenja da i (4) vrijedi.

Time je teorem 21.4. dokazan.

21.5. Zadaci o endomorfizmima.

EG označuje skup endomorfizama od G.

1. 1) Dokaži da je $(EC_2, +, \cdot)$ 2-člano tijelo; 2) $(EC_p, +, \cdot)$ je p-člano tijelo za svaki prost broj p; to je tijelo izomorfno s tijelom $(Ip, +, \cdot)$; 3) za $p=2$ i $p=3$ navedi eksplicitno članove skupa EC_p kao i radne tablice za $+$ i $\cdot$.

2. 1) Za svaki prirodni broj n vrijedi $(EC_n, +, \cdot)\cong(In, +, \cdot)$;
   2) $(EQ, +, \cdot)\cong(Q, +, \cdot)$; Q je skup racionalnih brojeva;
   3) Koliko ima endomorfizama grupe $(Q, +)$ koji nisu izomorfni.

3. 1) Grupa p^∞ je multiplikativna grupa kompleksnih brojeva oblika $e^{k_n 2\pi i p^{-n}}$ pri čemu je $k_n\in Ip^n$, $n=1, 2, \ldots$ (p je prost broj);
   2) ima li p^∞ konačan skup izvodnica?
   3) Navedi nekoliko članova prstena $(Ep^\infty, +, \cdot)$; on se zove „*prsten cijelih p-adskih brojeva*“.

4. Iz teorema 21.3 izvedi: 1) svaka beskonačna ciklička grupa C ima samo dva rješenja c, c' jednadžbe $Dx=C$; vrijedi $c+c'=0$;
   2) bilo koje dvije beskonačne cikličke grupe međusobno su izomorfne, i svaka je $\cong(D, +)$.

5. Ako je grupa komutativna, skup pripadnih endomorfizama je komutativno kolo s jedinicom.

6. Ako aG (odnosno iG) označuje skup svih automorfizama (unutrašnjih automorfizama) grupe G, odredi $(iG, +, \cdot)$, $(aG, +, \cdot)$ za pojedine grupe $(G, +)$.

7. 1) *Potpuno karakteristična podgrupa* grupe G jest svaka ona podgrupa grupe G_1 od G za koju je $fG_1\subset G_1$ za svako $f\in EG$ (zahtjevom $f\in iG$, odnosno $f\in aG$ određuju se invarijantne, odnosno karakteristične podgrupe). 2) svaka podgrupa cikličke grupe je potpuno karakteristična podgrupa; 3) $(G)^n=\{g^n;\ g\in G\}$ je potpuno karakteristična podgrupa u $(G, \cdot)$, i to za svako $n\in D$; 4) $G_{no n\infty}=\{g;\ g\in G,\ kDg<\infty\}$ je potpuno karakteristična podgrupa od $(G, +)$; 5) ZG je karakteristična no ne mora biti potpuno karakteristična podgrupa od G (isp. A. Kuroš [2] str. 88).

22. GRUPE S OPERATORIMA

22.0. Ideja. Često se uz grupoid, grupu, ... pojavljuje i određen skup Ω sa svojstvom da se svako ω iz Ω može *složiti* (*komponirati*) sa svakim članom iz G; tako npr. za svaku komutativnu grupu $(G, +)$ možemo uzeti $\Omega = D$ jer za svako $d \in D$ i svako $g \in G$ imamo $dg \in G$, premda u općem slučaju d nije u G; pomenuto slaganje je distributivno prema grupovnoj operaciji:

$$\omega(x+y) = \omega x + \omega y, \quad \text{odnosno} \quad \omega(xy) = \omega x \, \omega y,$$

ako je riječ o množidbenoj grupi.

Na takve „grupe s operatorima" prenose se mnogi teoremi o dosadašnjim „grupama bez operatora".

22.1. Definicija. *Grupoid s operatorima* jest svaki grupoid $(G, \cdot)$ zajedno s nekim skupom Ω sa svojstvom da svakom članu ω iz Ω pridružujemo određen endomorfizam grupoida:

$$g \in G \to \omega g \in G \tag{1}$$

[1)]

$$\omega(x \cdot y) = \omega x \cdot \omega y. \tag{2}$$

Ako je riječ o aditivnom grupoidu, tada jednadžba (2) glasi $\omega(x+y) = \omega x + \omega y$. Govori se o Ω-operatorskom grupoidu, grupi itd.

Skup Ω zove se oblast operatorâ.

Tako imamo uređenu dvojku $((G, \cdot), \Omega)$ sastavljenu od grupoida $(G, \cdot)$ i množine Ω.

22.1.1. Primjer. Svakoj komutativnoj grupi $(G, +)$ pridružen je npr. skup D cijelih brojeva kao skup operatora; napose, sama grupa $(D, +)$ je grupa s operatorima iz samog D.

22.2. *Svaki grupoid* $(G, \cdot)$ *možemo shvatiti i kao* Ω*-grupoid* pri čemu je G sastavljeno od identičkog preslikavanja j_G; na taj način, teorija grupa postaje dijelom teorije grupa s operatorima.

22.4. Često se može pretpostaviti da vrijedi

$$\Omega \subset EG$$

(EG označuje skup svih endomorfizama grupe G); na taj način, svaki „operator" ω iz Ω poistovećujemo s nekim endomorfizmom od $(G, \cdot)$. Međutim, zgodnije je da se to poistovećenje ne sprovodi jer npr. *različnim* članovima iz Ω mogu odgovarati i *jednaki* endomorfizmi; nadalje se mogu promatrati razne grupe s *istim* skupom Ω (gornji primjer: *sve* komutativne grupe vezane su za isto $\Omega (= D)$).

22.5. Također se može poći od neprazne obitelji F nepraznih skupova Ω tako da za svako $\Omega \in F$ i svako ω iz Ω imamo endomorfizam $x \to \omega x \, (x \in G)$.

[1)] Umjesto ωg može se pisati $g\omega$, $\omega(g)$, $g(\omega)$, itd.

22.6. Prijelaz od grupe na Ω-grupe. Mnogi pojmovi i teoremi o grupama prenose se na Ω-grupe, tj. na grupe s operatorima; navest ćemo nekoliko primjera.

22.6.1. *Pojam Ω-homomorfizma.* Ω-grupa G' je *Ω-izomorfna* (*Ω-homomorfna*) *s Ω-grupom* G, simbolički $G \cong_\Omega G'$ (odnosno $G \sim_\Omega G'$), ako postoji izomorfno (homomorfno) preslikavanje h od G na čitavo G' sa svojstvom

$$h(\omega x) = \omega(hx), \ (g \in G, \ \omega \in \Omega).$$

Prema tome je $h\omega = \omega h$ (*komutativnost homomorfizma i operatora*); pri tom naravno, i G i G' odnose se na isto Ω.

22.6.2. *Definicija podgrupe Ω-grupe. Podgrupa Ω-grupe* je svaka podgrupa F koja je zatvorena u odnosu na Ω, tj. $\omega F \subset F$ za svako $\omega \in \Omega$.

U toj definiciji traži se da podgrupa F bude usklađena prema Ω, i to baš zahtjevom $\omega F \subset F$.

22.6.3. *Invarijantna podgrupa Ω-grupe* G je svaka invarijantna podgrupa I za koju je $\omega I \subset I$ za svako $\omega \in \Omega$.

22.7. Prsten kao Ω-grupa. Poseban slučaj Ω-grupa G za koje je $\Omega \subset G$ jesu *kola* ili *prsteni* (isp. 6 § 5.2). Naime, svaki element a prstena $(A, +, \cdot)$ inducira endomorfizam $x \to ax$ i endomorfizam $x \to xa$ (u nekomutivnom prstenu, ta su dva endomorfizma općenito različna).

Međutim, sam prsten može imati i drugih operatora pridruženih nekom skupu Ω. Tako se na prirodan način definira Ω-prsten ili Ω-operatorski prsten kao svaki prsten $(A, +, \cdot)$ sa svojstvom da je $(A, +)$ određena Ω-grupa i da iz $a, b \in A$ te $\omega \in \Omega$ izlazi

$$\omega(ab) = (\omega a)b = a(\omega b).$$

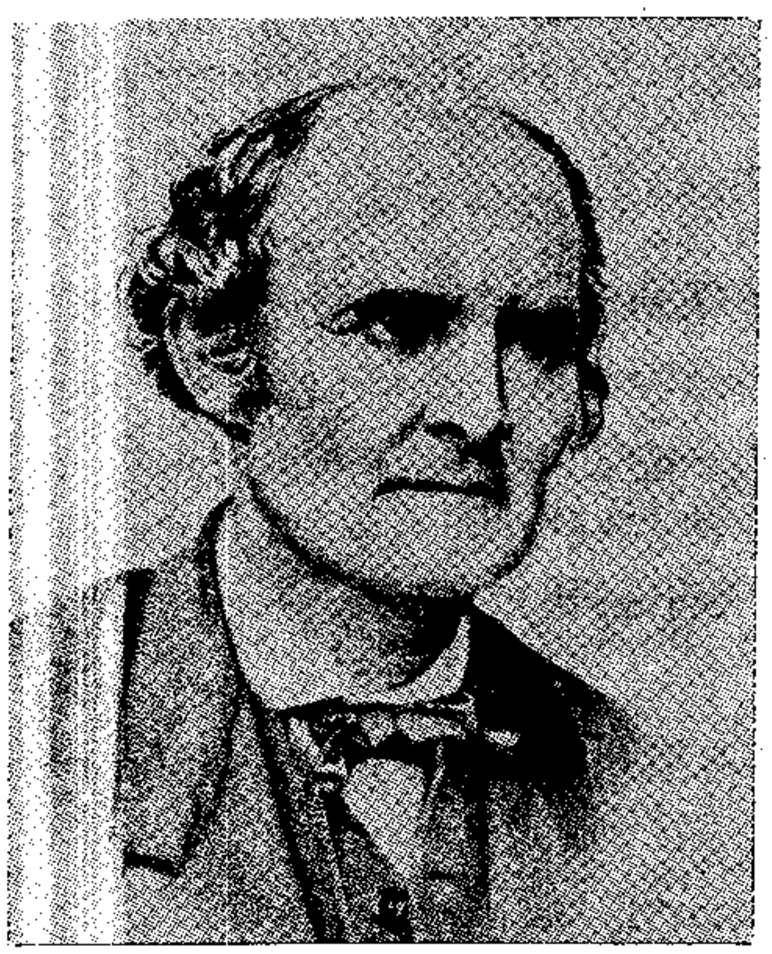
22.8. Zadaci o Ω-operatorskim grupama.

1. Kako bi glasila definicija 1) karakteristične; 2) potpuno karakteristične podgrupe Ω-grupe? (isp. § 21.5.7).
2. Teorem 12.5.5. o homomorfiji prenijeti na Ω-operatorske grupe.
3. Teorem 16.8 o izomorfiji grupa formulirati i dokazati za Ω-grupe.
4. Dopušta li ciklička grupa C_n skup D kao operatore? Može li se pretpostaviti da bude $D \subset C_n$? (isp. § 22.4).

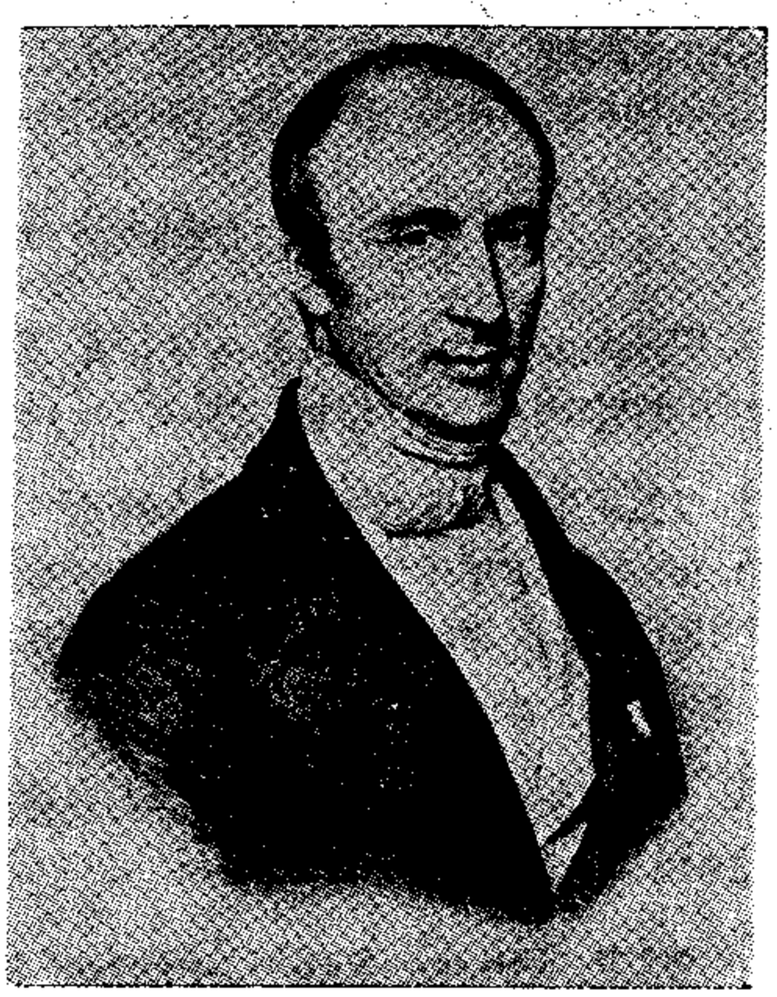
23. OSVRT NA POSTANAK TEORIJE GRUPA

23.1. Bitna ideja u teoriji grupa, naime ideja da se polazi od podataka neke cjeline G pa da se iz njih izgrađuje rezultat i da se onda pitamo da li rezultat leži u G, nalazi se, u specijalnim slučajevima, i u prastaroj matematici. Tako npr. nesvjesno je bilo odavno jasno da je suma (umnožak) dvaju

prirodnih brojeva opet prirodni broj, da *dva uzastopna kretanja* možemo nadomjestiti *jednim* kretanjem; isto tako, pravilnosti na raznim ornamentima, crtežima i sl. nosilac su zanimljivih grupovnih postavki, a život ih je dao prije no što se u 19. stoljeću svjesno uveo pojam grupe, odnosno grupoida.



A. Cayley (1821—1895)



A. L. Cauchy (1789—1857)

23.2. Teorija grupa rodila se u radovima Lagrange-a (1736—1813), (sl. str. 148, Gaussa (1777—1855) (sl. str. 104), Cauchy-a (1789—1857) i naročito Galoisa (1811—1832) (sl. na str. 148). Pri tom se radilo uglavnom o *grupama permutacija* a u vdzi s rješavanjem algebarskih jednadžbi. Specijalno je Galois prenošenjem problematike s algebarskih jednadžbi na problematiku pridruženih grupa otvorio nove putove u matematici. Tehnički naziv »*grupa*« potječe od Galoisa isto kao i pojam invarijantne podgrupe, proste grupe; došao je do vrlo dubokih teorema a otkrio je i konačna tijela elemenata. Treba spomenuti i Talijana P. Ruffini-a (1765—1822) i Norvežanina Abela (1802—1829) (str. str. 147). Galoisova djela objavljena su tek 1846. godine, odnosno 1897. godine; njegov rad je specijalno nastavio C. Jordan (1838—1922) pa se Jordanova knjiga *Traité des substitutions et des équations algébriques*[1] Paris 1870. smatra velikim spomenikom Galoisu.

Faktorske grupe i izomorfije uveo je Jordan. Premda je i Jordan obrađivao uglavnom grupe permutacija, ipak on obrađuje i druge pa i beskonačne grupe.

23.3. Međutim, pojam kompozicije izraštavao je svjesno i u drugim dijelovima ljudskog saznanja; pa se time oblast matematike još više proširivala. Tako je Englez Boole (v. sliku na str. 3) djelom *The mathematical Analysis of Logic*, Cambridge 1847. te djelom *Laws of thought* 1854. (*Zakoni mišljenja*) došao do matematičke logike; Cayley (1821—1895) dolazi oko 1850. do matrica dakle i do nekomutativnih operacija; irski matem. Hamilton (1805—1865) dolazi 1837. god. do algebarske definicije kompleksnih brojeva, do hiperkompleksnih

---

[1] Traktat o supstitucijama i algebarskim jednadžbama. To djelo (ima XVIII + 668 stranica, formata 4°) je prva knjiga o teoriji grupa.

brojeva i vektora (od njega potječe i naziv *vektor* prema lat. *vehere — vući*); Nijemac Grassmann (1809—1877) dolazi do vektora i vektorskih prostora. *Dolazi se do definicije grupe bez obzira kakvi su elementi grupe* (Cayley 1854., Kronecker 1870.), nastaje i teorija skupova (Dedekind i Cantor, v. slike na str. 17. i 18.), počinje se razlikovati konačne i beskonačne grupe i primjećivati da se grupe pojavljuju svuda: u algebri, geometriji, mehanici, fizici, kristalografiji itd. Tako F. Klein (1849—1925) već 1872. god. u svojem glasovitom *Erlanger Programm* (Erlangški program, prema gradu Erlangenu u Njemačkoj u kojem je bio profesor) ističe misao da se klasifikacija geometrije treba vršiti prema vrsti grupâ koje se u pojedinim oblastima geometrije pojavljuju. Radovi Poincaré-a (č. Poenkare, 1854—1912) odnosili su se na grupe u teoriji funkcija kompleksne varijable (automorfne funkcije!), teoriji brojeva, topologiji itd. S. Lie (1842—1899) izučava posebno neprekidne grupe.

Tako se teorija grupa počela naglo razvijati kao da se hoće nadoknaditi izgubljeno vrijeme da se do grupâ kao matematičkog predmeta došlo tako kasno.

Danas je teorija grupa jako vezivno sredstvo u matematici i primjenama matematike; specijalno se njome mnogo služe u kvantnoj mehanici i teoriji polja; u matematici se grupoidi pojavljuju svuda, a izrastavaju sve nove i nove vrste grupoida u vezi s raznim pojavama u matematici i van matematike.

Literatura

Borůvka [1], [2[, Burnside [1], Dubreil, [1], Galois [1], Hall [1], Kuroš [2], Lomont [1], Lugowski [1], L'ubarskij [1], Scorza [1], Specht [1], Speiser [1], von der Waerden [1], Weyl [1], [2], Zassenhaus [1].

POGLAVLJE 18.

KORIJENI JEDINICE. DIJELJENJE KRUGA. PRAVILNI n-VRHOVI

1. POJAM KORIJENA JEDINICE

1.1. Definicija. *Korijeni jedinice* jesu brojevi koji zadovoljavaju bar jednoj jednadžbi oblika

$$x^n = 1; \tag{1}$$

pri tom je n prirodan broj. Specijalno, brojevi koji za zadano n zadovoljavaju (1) zovu se *n-ti korijeni jedinice* ili *korijeni jedinice reda n*; njihov skup možemo označiti sa

$$\{1^{1/n}\} \quad \text{ili} \quad \left\{\sqrt[n]{1}\right\}. \tag{2}$$

Tako je npr. broj 1 jedini korijen jedinice reda 1; korijen jedinice reda 2 jesu brojevi 1, -1; a skup im je $\{+1, -1\}$ ili $\{\pm 1\}$. Nađimo *treće korijene jedinice*, tj. riješimo jednadžbu $x^3 = 1$.

Kako je $x^3 - 1 = (x-1)(x^2+x+1)$ izlazi da su osim 1 i rješenja $\frac{1}{2}(-1 \pm i\sqrt{3})$ jednadžbe $x^2+x+1=0$ treći korijeni jedinice, dakle

$$\{1^{1/3}\} = \left\{1, \frac{-1+i\,3^{1/2}}{2}, \frac{-1-i\,3^{1/2}}{2}\right\}.$$

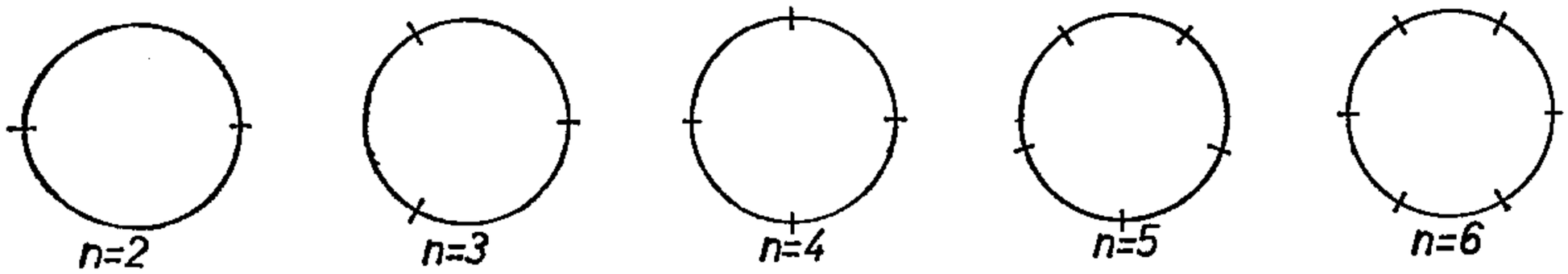
Vidi se da treći korijeni jedinice određuju u brojevnoj ravnini *vrhove pravilnog* 3-*kuta* koji je upisan u jediničnu kružnicu, a jedan mu je vrh u jediničnoj tački. Taj je zaključak *ispravan za svako n*.

1.2. Lema. *n-ti korijeni jedinice glase*:

$$\cos\frac{2\pi}{n}\nu + i\sin\frac{2\pi}{n}\nu \qquad (\nu < n); \tag{3}$$

pri tom različitim brojevima $\nu \in In$ *odgovaraju različiti korijeni jedinice. Svi n-ti korijeni jedinice određeni su svojim položajem u kompleksnoj ravnini kao vrhovi pravilnog n-vrha koji je upisan u jediničnu kružnicu, a jedan je vrh u jediničnoj tački. Brojevi* (3) *čine multiplikativnu grupu.*

Npr. za $n=2, 3, 4, 5, 6$ imamo ove pravilne n-vrhove:



Sl. 18.1.2.

Odmah se vidi (i geometrijski i aritmetički) ovo:

1.3. Lema. *Ako je x_0 bilo koji n-ti korijen jedinice, onda je x_0* i *kn-ti korijen jedinice za svaki mnogokratnik kn broja n;* iz

$$x_0 \in \{1^{1/n}\} \quad \text{izlazi} \quad x_0 \in \{1^{1/kn}\}.$$

To znači da je svaki *pravilni n-vrh* upisan u *svaki pravilni kn-vrh* (uvijek ćemo uzimati da su *n-vrhovi normirani* time što im jedan vrh leži u tački 1 i što je upisan u jediničnu kružnicu).

Promatramo li različite n-vrhove, vidimo da svaki n-vrh ima svojih vrhova koji ne leže ni na kojem n-vrhu sa $n'<n$.

2. PRIMITIVNI (PRVOTNI, PRVOOBRAZNI) I IMPRIMITIVNI (NEPRVOTNI) KORIJENI

Već u jednostavnom slučaju jednadžbe $x^2=1$ vidimo da njen korijen 1 zadovoljava analognu jednadžbu s *nižim* prirodnim eksponentom; naprotiv, za drugo riješenje, -1, to nije slučaj. Kaže se da je -1 *primitivno*, a 1 *imprimitivno* rješenje jedinice reda 2.

2.1. Definicija. *Primitivni ili prvotni n-ti korijen jedinice* jest svako rješenje jednadžbe $x^n=1$ koje ne zadovoljava $x^k=1$ ni za koje $0<k<n$. Ona rješenja koja nisu *prvotna* zovu se *neprvotna* ili *imprimitivna*.

Očigledno je $\varepsilon_n=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$ primitivni n-ti korijen jedinice, jer za svaki cijeli broj $0<k<n$ bit će $\frac{k}{n}<1$; zato je kut $\frac{2\pi k}{n}$ manji od punog kuta 2π rad pa broj $\varepsilon_n^k=\cos\frac{2\pi}{n}k+i\sin\frac{2\pi}{n}k$ ne može biti $=1$ i biti rješenje jednadžbe (1). Tako npr. brojevi $\cos\frac{2\pi}{3}k+i\sin\frac{2\pi}{3}k$ za $k=1, 2$ jesu dva prvotna rješenja kubne jednadžbe $x^3-1=0$. Jednadžba $x^4-1=0$ ima 1 i -1 kao neprvotna, a rješenja jednadžbe $x^2+1=0$ kao prvotna svoja rješenja. Polinom x^6-1 ima samo dva prvotna nula-mjesta, i to broj $\varepsilon_6=\cos\frac{2\pi}{6}+i\sin\frac{2\pi}{6}$ i broj

ε_6^5, koji je zapravo $=\overline{\varepsilon_6}$ (=konjugirano kompleksni od broja ε_6). Broj npr. ε_6^3 nije primitivno rješenje jednadžbe $x^6=1$, jer je on već kvadratni korijen jedinice.

Općenito imamo ovaj zanimljivi

⟶ **2.2.** Teorem. *Za svaki prirodni broj n broj*

$$\varepsilon_n=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$$

je primitivno rješenje jednadžbe $x^n=1$. *Da broj z bude primitivno n-to rješenje jedinice, nužno je i dovoljno da postoji cio broj k za koji je*

$$z=\varepsilon_n^k,\ 0<k<n,\ M(k,n)=1.$$

2.2.1. Uslov je dovoljan. Za svako k za koje je $0<k<n$, $M(k,n)=1$, broj ε_n^k je primitivno rješenje, tj. ni za koje $0<\nu<n$ ne može biti $(\varepsilon_n^k)^\nu=1$. Stavljajući $\alpha=\frac{k\tau}{n}$, značila bi jednakost $(\varepsilon_n^k)^\nu=1$ isto što i $\cos 2\pi\alpha+i\sin 2\pi\alpha=1$, odnosno što i $\cos 2\pi\alpha=1$, odnosno što i uslov da je α cio broj. No, $\alpha=\frac{k\nu}{n}$ ne može biti cio broj, jer bi to zbog pretpostavke $M(k,n)=1$ značilo da je ν djeljivo sa n (isp. Euklidov teorem, pogl. 6, § 11.5). A to je zbog $0<\nu<n$ isključeno.

2.2.2. Uslov je nuždan. Ako je ε_n^ν primitivno rješenje jednadžbe $x^n=1$, onda je $M(\nu,n)=1$.

Dokažimo najprije ovu

2.2.2.1. Lemu. *Ako je z primitivno rješenje jednadžbe* $x^n=1$, *onda iz* $z^s=1$ *izlazi da je s djeljivo sa n* (*očigledan je obrat*: *ako iz* $z^s=1$ *izlazi da je s djeljivo sa n, onda je z primitivno rješenje jednadžbe* $x^n=1$).

Neka je, naime, $s=nq+r$, $0\leq r<n$; količnik q i ostatak r su jednoznačno određeni po osnovnom teoremu o diobi (pogl. 6, § 9.5). Time jednakost $z^s=1$ postaje $z^{nq}\cdot z^r=1$, odnosno, (zbog $z^n=1$): $z^r=1$, a to se zbog $0<r<n$ protivi pretpostavci da je z prvoobrazno.

2.2.3. Pređimo sad na nužnost uslova. Stavimo $M(\nu,n)=d$, $\nu=d\nu'$, $n=dn'$; tada je $\nu n'=\nu' n$, a odatle $\varepsilon_n^{\nu n'}=1$, što prema primitivnosti korijena ε_n^ν znači (v. lema) da je n' djeljivo sa n; kako je i n djeljivo sa n', znači da je $n=n'$, dakle $d=1$, tj. $M(\nu,n)=1$, za čim se i išlo.

Iz teorema 1. proizlazi specijalno

⟶ **2.3.** Teorem. *Jednadžba* $x^n=1$ *ima* $\varphi(n)$ *primitivnih rješenja* (znamo da $\varphi(n)$ kazuje koliko ima brojeva ν za koje je $0\leq\nu<n$, $M(\nu,n)=1$).

——→ **2.4.** Teorem. ***Skup*** $\{1^{1/n}\}$ ***n-tih korijena jedinice je multiplikativna ciklička grupa*** C_n***; svaki generator g grupe, tj. svako g za koje je*** $g^D = C_n$ ***je primitivan n-ti korijen jedinice; i obrnuto, svaki primitivan n-ti korijen jedinice generira grupu*** C_n.

Dokaz. Neka je $g^D = C_n$; prema teoremu 2.2. imamo $g = \varepsilon_n^k$; ne može biti $M = M(k, n) > 1$ jer inače kongruencija $kx \equiv 1 \pmod{n}$ ne bi postojala (6 § 17.5 (*ii*)) pa specijalno zato ne bi bilo $\varepsilon_n = g^d$ ni za koje $d \in D$. Dakle je $M = 1$, pa je zato $g = \varepsilon_n^k$ prema 2.2. primitivno.

Obrnuto: ako je ζ primitivno, tada je $\zeta^D = C_n$; naime, prema 2.2. $\zeta = \varepsilon_n^k$ sa $M(k, n) = 1$, pa svako $c \in C_n$ može biti predstavljeno oblikom $\zeta = \varepsilon_n^{kr}$ jer eksponent kr može biti kongruentan sa svakim od brojeva $\nu \in \{0, 1, \ldots, n-1\}$ za neko cjelobrojno k (isp. 6 § 17,5 (*ii*)).

3. SISTEM $x^k = 1$, $x^n = 1$.

Neka je $d = M(k, n)$ najveća zajednička mjera brojeva k, n; tada znamo da je $x^d - 1$ najveća zajednička mjera polinoma $x^k - 1$, $x^n - 1$ (isp. pogl. 7, § 6.7.4).

Drugim riječima, vrijedi

3.1. Teorem. *Sistem* $x^k = 1$, $x^n = 1$ *ekvivalentan je s jednadžbom* $x^d = 1$, *gdje je* $d = M(k, n)$.

Specijalno, ako su k, n relativno prosti ($d = 1$), *tada je broj* 1 *jedino rješenje promatranog sistema jednadžbi.*

4. JEDNADŽBE $x^n = 1$, $x^s = 1$, $x^{ns} = 1$ za $M(n, s) = 1$

Od interesa je pogledati vezu među korijenima tih triju jednadžbi. Tako npr. vidimo da se korijeni (primitivni) jednadžbe $x^6 = 1$ dobiju tako da se *svaki* (primitivni) korijen jednadžbe $x^2 = 1$ *pomnoži svakim* (primitivnim) korijenom jednadžbe $x^3 = 1$. Zaključak je općenit, kao što pokazuje

——→ **4.1.** Teorem. *Neka su n, n′ dva relativno prosta prirodna broja; tada je*

$$\left\{1^{\frac{1}{n}}\right\}\left\{1^{\frac{1}{n'}}\right\} = \left\{1^{\frac{1}{nn'}}\right\},$$

tj. pomnoži li se bilo koje (primitivno) rješenje z jednadžbe $x^n = 1$ *bilo kojim (primitivnim) rješenjem z′ jednadžbe* $x^{n'} = 1$, *dobije se (primitivno) rješenje* $y = zz'$ *jednadžbe* $x^{nn'} = 1$; *i obrnuto, svako (primitivno) rješenje jednadžbe* $x^{nn'} = 1$ *je navedenog oblika zz′.*

Dokaz. Najprije iz $z^n = 1$, $z^{n'} = 1$ izlazi $(z^n)^{n'} = 1$, $(z'^{n'})^n = 1$, odatle množenjem izlazi $(zz')^{nn'} = 1$. Nadalje, ako su z_1, z_2 dva različita rješenja od $x^n = 1$, bit će $z_1 z_1' \neq z_2 z_2'$, ukoliko je $(z')^{n'} = 1$. Kad bi, naime, bilo $z_1 z_1' = z_2 z_2'$, izlazilo bi odatle $(z_1 z_1')^{n'} = (z_2 z_2')^{n'}$ i dalje $z_1^{n'} = z_2^{n'}$ (jer su z_2, z_2' n′-korijeni jedinice); to

znači da bi bilo $(z_1/z_2)^{n'}=1$ odnosno da bi ne samo broj 1 nego i broj $z_1/z_2 \neq 1$ bio rješenje sistema $x^n=1$, $x^{n'}=1$, protivno teoremu 3.1. (tu dolazi do izražaja pretpostavka $M(n, n')=1$).

Dokažimo još onaj dodatak o primitivnosti: ako je z n-primitivno, a z' n'-primitivno, onda je zz' (nn')-primitivno. To znači da treba izvesti zaključak da iz $(zz')^r=1$ izlazi da je r djeljivo sa nn'. No, potenciramo li posljednju jednadžbu sa n, tada zbog $z^n=1$ izlazi $z'^{rn}=1$; kako je z' primitivno rješenje za $z^{n'}=1$, mora po lemi 2.2.2.1. biti rn djeljivo sa n'; kako je $M(n, n')=1$, mora, dakle, r biti djeljivo sa n'. Analogno se zaključuje da je r djeljivo sa n. Broj r je, dakle, djeljiv relativno prostim brojevima n, n', pa dakle i njihovim produktom nn' (v. pogl. 6, § 9).

Ako broj z nije primitivno rješenje jednadžbe $x^n=1$, tada ni zz' nije primitivno rješenje jednadžbe $x^{nn'}=1$.

Stvarno, imprimitivnost broja z znači da postoji neko ν za koje je $0<\nu<n$, $z^\nu=1$; odatle $(zz')^{\nu n'}=(z_1^\nu)^{n'}$, $(z'^{n'})^\nu=1\cdot 1$; dakle, zz' ne bi bilo primitivno rješenje jednadžbe $x^{nn'}=1$, jer je $0<\nu n'<nn'$. Analogno, ako z' nije n'-primitivno, nije ni broj zz' primitivno rješenje jednadžbe $x^{nn'}=1$. Time je teorem potpuno dokazan.

4.2. *O multiplikativnom svojstvu funkcije* φ. Iz teorema 4.1. izlazi da je $\varphi(nn')=\varphi(n)\varphi(n')$ čim je $M(n, n')=1$.

Naime, prema teoremu 2.2. ima jednadžba $x^{nn'}=1$ tačno $\varphi(nn')$ primitivnih rješenja; ta se rješenja, prema teoremu 4.1, dobiju tako da se svako od $\varphi(n)$ primitivnih rješenja jednadžbe $x^n=1$ pomnoži svakim od $\varphi(n')$ prvotnih rješenja jednadžbe $x^{n'}=1$.

4.2.1. Primjedba. Poučno je i korisno imati jasnu sliku o prethodnom dokazu multiplikavnosti funkcije φ, a time i o dokazu osnovnog obrasca

$$\varphi(n)=n\sum_{p\in P(n)}(1-p^{-1})$$

(v. pogl. 6, § 19) i uporediti taj dokaz s onim u pogl. 6, § 19.1.

5. JEDNADŽBA (POLINOM) PRIMITIVNIH n-TIH KORIJENA JEDINICE

5.1. Neka su

$$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\varphi(n)} \tag{1}$$

sva nula-mjesta od x^n-1, a da nijedno od njih ne zadovoljava $x^\nu=1$, za koje $0<\nu<n$; tada je njihov pripadni normirani polinom

$$\Phi_n(x)=(x-\varepsilon_1)(x-\varepsilon_2)\cdots(x-\varepsilon_{\varphi(n)}). \tag{2}$$

No, svako rješenje od $x^n=1$, ukoliko nije primitivno reda n, primitivno je za posve određen divizor d od broja n; to znači da je

$$x^n-1=\prod_{d\mid n}\Phi_d(x), \quad \text{dakle} \quad \Phi_n=\frac{x^n-1}{\prod\Phi_d}; \tag{3}$$

$d|n$ znači da d dijeli n. Iz identiteta (3) izračunavaju se po redu polinomi Φ_n.

Za $n=1$ izlazi $x-1=\Phi_1(x)$.

Za $n=2$ postaje (3)

$$x^2-1=\Phi_1(x)\,\Phi_2(x)=(x-1)\,\Phi_2(x), \quad \text{dakle} \quad \Phi_2(x)=x+1.$$

Za $n=p$ postaje (3)

$$x^p-1=\Phi_1(x)\,\Phi_p(x), \qquad \text{dakle}$$
$$\Phi_p(x)=1+x+x^2+\cdots+x^{p-1} \qquad \text{za svaki prost broj } p.$$

Polinom $\Phi_6(x)$ izlazi iz

$$x^6-1=\Phi_1(x)\,\Phi_2(x)\,\Phi_3(x)\,\Phi_6(x)=(x-1)\,(x+1)\,(x^2+x+1)\,\Phi_6(x).$$

Dobije se $\Phi_6(x)=x^2-x+1$.

Poznajemo li tzv. *Möbiusovu funkciju*, možemo polinom $\Phi_n(x)$ prikazat na zgodan način.

5.2. Möbiusova funkcija μ.[1] Ona se definira za prirodne brojeve, i to:

$$\mu(1)=1$$
$$\mu(n)=0$$

ako je n djeljivo kvadratom bar jednog broja, inače

$$\mu(n)=(-1)^\nu,$$

gdje je ν broj različitih prostih djelitelja broja n (isp. pogl. 6, § 19.3). Npr.

$$\mu 6=(-1)^2=1, \quad \mu 20=0 \quad \text{jer } 2^2\,|\,20.$$

5.3. Teorem. *Za svaki prirodni broj n vrijedi*

(1) $$\sum_{d\,|\,n}\mu(d)=0.$$

Stvarno, neka je

$$n=p_1^{\alpha_1}\,p_2^{\alpha_2}\cdots p_\nu^{\alpha_\nu}$$

rastav broja n na proste faktore; tada su divizori broja n oblika

(2) $$p_1^{\beta_1}\,p_2^{\beta_2}\cdots p_\nu^{\beta_\nu} \quad \text{za} \quad 0\leq\beta_i\leq\alpha_i.$$

Ako je bar jedan od brojeva $\beta_i>1$, postaje pripadna vrijednost μ nula; zato možemo pretpostaviti da u (2) vrijedi $0\leq\beta_i\leq1$; ako su svi $\beta_i=0$, tada je pripadni divizor $d=1$, dakle $\mu(d)=1$; preostaju još divizori $p_1, p_2, \ldots, p_\nu$, pa ambe $p_1p_2, p_1p_3, \ldots$, tako da je

$$\sum_{d\,|\,n}\mu(d)=\sum_{\lambda=0}^{\nu}(-1)^\lambda\binom{\nu}{\lambda}=(1-1)^\lambda=0.$$

---

[1] August Ferdinand Möbius (1790—1868), njem. matematičar.

5.4. Teorem.

$$\Phi_n(x)=\prod_{d|n}(x^d-1)^{\mu\left(\frac{n}{d}\right)}. \tag{3}$$

Kako su polinomi Φ_d jednoznačno određeni, dovoljno je za dokaz teorema 5.3. vidjeti da polinomi Φ_d obrazovani na način (3) zadovoljavaju identički relaciju 5.1. $(3)_2$ tj. (3) iz § 5.1.

No, 5.1. $(3)_2=\prod_{d|n}\Phi_d(x)=$(po (3))$=\prod_{d|n}\prod_{\delta|d}(x^\delta-1)^{\mu\left(\frac{d}{\delta}\right)}$.

Kako je $d|n$, $\delta|d$, bit će $\frac{n}{\delta}$ djeljivo sa $\frac{d}{\delta}$; drugim riječima, za svako čvrsto δ imat će izraz $(x^\delta-1)$ u gornjem produktu za svoj eksponent ovo: $\sum_e \mu(e)$, pri čemu $e=\frac{d}{\delta}$ prolazi svim divizorima broja $\frac{n}{\delta}$. No, prema teoremu 1. ta je suma $=0$ ili 1, već prema tome da li je $\frac{n}{\delta}>1$ ili $\frac{n}{\delta}=1$; drugim riječima, čitav gornji produkt reducira se na ono što od njega izlazi kad se stavi $\delta=n$, dakle $(x^n-1)^{\mu(1)}=x^n-1$, Q. E. D.

Primjeri.

$$\Phi_6(x)=\prod_{d|6}(x^d-1)^{\mu\left(\frac{6}{d}\right)}=(x-1)^{\mu(6)}(x^2-1)^{\mu(3)}(x^3-1)^{\mu(2)}\cdot(x^6-1)^{\mu(1)}=$$

$$=(x-1)(x^2-1)^{-1}(x^3-1)^{-1}(x^6-1)^1=x^2-x+1.$$

Dakle $\Phi_6(x)=x^2-x+1$.

$$\Phi_p(x)=(x-1)^{\mu(p)}(x^p-1)^{\mu(1)}=(x-1)^{-1}(x^p-1)=$$

$$=x^{p-1}+x^{p-2}+\cdots+x+1.$$

Vrlo važno i duboko svojstvo polinoma $\Phi_n(x)$ iskazuje

5.5. Teorem. *Ni za koji prirodni broj $n>2$ ne može se polinom $\Phi_n(x)$ rastaviti u produkt od dva polinoma s racionalnim koeficijentima: u tijelu Q racionalnih brojeva polinomi $\Phi_n(x)$ su ireducibilni (nesvodljivi) ako je $n=3, 4, \ldots$ Specijalno je $\Phi_p(x)$ nesvodljivo u Q.*

($n=p=$ prost broj: Gauss, 1801; $n=p^k$: Serret 1850; opći slučaj: Kronecker 1854).

5.5.1. Dokažimo teorem za slučaj $n=p^m$ (p je prost broj). Tada je

$$\Phi_{p^m}(x)=\frac{x^{p^m}-1}{x^{p^{m-1}}-1}=x^{(p-1)p^{m-1}}+x^{(p-2)p^{m-1}}+\cdots+x^{p^{m-1}}+1.$$

Kad taj polinom ne bi bio prost nad tijelom racionalnih brojeva mogao bi se on prema Gaussu (7 § 7.4) prikazati kao produkt prostih normiranih polinoma s *cijelim* koeficijentima, npr.

$$\Phi_{p^m}(x)=f_1(x)f_2(x)\cdot\cdot\cdot f_k(x). \tag{2}$$

Odatle posebno za $x=1$ prema (1) izlazi

$$p=f_1(1)f_2(1)\cdot\cdot\cdot f_k(1). \tag{3}$$

Dakle je jedan jedini faktor na desnoj strani jednak, p npr. $f_1(1)=p$; naprotiv bi bilo

$$f_i(1)\in\{-1, 1\} \text{ za } i=2, 3, \ldots, k. \tag{4}$$

No neka je ζ jedno nulamjesto od $f_1(x)$; dakle je i $\Phi(\zeta)=0$ pa se prema 18 § 2.4. svako drugo nulamjesto ζ' od $\Phi(x)$ može prikazati u obliku ζ^r, pri čemu je r prosto prema n; no iz $\Phi(\zeta^r)=0$ izlazi prema (1) da je $f_i(\zeta^r)=0$ za neko $i\in\{1, \ldots, k\}$; ne može biti $i>1$ jer bi iz $f_1(\zeta)=0$, $f_i(\zeta^r)=0$ prema 7 § 7.3 izlazilo $f_1(x)|f_i(\zeta^r)$ dakle specijalno $f_1(1)|f_i(1)$ tj. $p|f_i(1)$, a to zbog (4) znači da je $i=1$; drugim riječima, dokazali smo da iz $f_1(\zeta)=0$ izlazi $f_1(\zeta^r)=0$ za svaki broj r koji je prost prema n; to znači da je $\Phi(x)=f_1(x)$, jer je

$$\Phi(x)=\prod_{\xi}(x-\xi),\ \xi\in\{\zeta^r;\ r\in N,\ M(r,n)=1\}.$$

Slično se može obraditi i opći slučaj: n bilo koji član u N.

6. ELEMENTARNA KONSTRUKCIJA PRAVILNOG 17-KUTA. JEDNADŽBA $x^{17}=1$

6.1. Jednadžba

$$x^{17}-1=0 \tag{1}$$

ima 16 primitivnih rješenja, i to:

$$\varepsilon,\ \varepsilon^2,\ \varepsilon^3,\ \ldots,\ \varepsilon^{16}, \tag{2}$$

gde je

$$\varepsilon=\varepsilon_{17}=\cos\frac{2\pi}{17}+i\sin\frac{2\pi}{17}. \tag{3}$$

6.2. Može li se ε_{17}, tj. ε nacrtati *elementarno*, tj. pomoću *ravnala* (*lineala*) *i šestara*? Naravno, trigonometrijski oblik (3) broja ε još nam ne može ništa kazati u tom pogledu. Zato treba pokušati da se nađe kakva zgodna *algebarska* veza, odnosno algebarski oblik broja ε.

6.3. Najprije je jasno da je

$$\sum_{\nu=0}^{16}\varepsilon^\nu=-1, \tag{4}$$

jer $(4)_1 + 1$ predstavlja sumu svih rješenja jednadžbe (17), dakle 0, jer je 0 koeficijent od x^{16} u (1). No, zbog strukture 2^{2^2} broja 16, najprirodnije je u sumi (4) raspodjeljivati sumande najprije u dvije jednake skupine po 2, svaku od njih u dvije jednake skupine, itd. Također je najprirodnije u jednu početnu skupinu uzeti rješenja ε, ε^2, e^{2^2}, ε^{2^3}, ε^{2^4}, ... itd., jer svako od njih nastaje iz prethodnog *kvadriranjem*, odnosno (geometrijski govoreći) *rotiranjem* za njegov argument. Tako imamo sumu

$$y_0 = \varepsilon + \varepsilon^2 + \varepsilon^4 + \varepsilon^8 + \varepsilon^{16} + \varepsilon^{15}\,(=\varepsilon^{32}) + \varepsilon^{13}\,(=\varepsilon^{64}) + \varepsilon^9 \text{ (zapravo } \varepsilon^{128}). \tag{5}$$

6.4. Označimo li sa y_1 sumu preostalih osam primitivnih rješenja iz (2), bit će

$$y_1 = \varepsilon^3 + \varepsilon^6 + \varepsilon^{12} + \varepsilon^7 + \varepsilon^{14} + \varepsilon^{11} + \varepsilon^5 + \varepsilon^{10}, \tag{6}$$

čime je naznačeno da svaki sumand u (6) nastaje kvadriranjem prethodnoga. Lako se vidi da je $y_0 + y_1 = -1$.

Zbog simetrije prema realnoj osi komponenata ε^i vektora y_0 očito je y_0 realno; također se vidi da je $y_0 > 0$, jer je $\arg \varepsilon_1 < \frac{\pi}{4} > \operatorname{arc} \varepsilon^2$. Isto se tako zaključuje da je $y_1 < 0$; to izlazi i iz $y_0 > 0$ i relacije (4). Može se dokazati da je $y_0 y_1 = -4$, jer produkt $y_0 y_1$ sadrži svaki od faktora ε^2 četiri puta; znači da y_0, y_1 zadovoljavaju kvadratnu jednadžbu $y^2 + y - 4 = 0$, pa dakle za skup $\{y_0, y_1\}$ korijena y_0, y_1 vrijedi

$$\{y_0, y_1\} = \left\{\frac{-1 + 17^{1/2}}{2}, \frac{-1 - 17^{1/2}}{2}\right\}, \tag{7}$$

što na osnovu prethodnoga daje

$$y_1 = \frac{-1 - 17^{1/2}}{2}, \quad y_0 = \frac{-1 + 17^{1/2}}{2}. \tag{8}$$

6.5. Raspodijelimo, po istom principu, sumande za y_0:

u $(5)_1$ na y_{00}, y_{01} i $(6)_1$ u y_{10}, y_{11} pa stavimo

$$y_{00} = \varepsilon + \varepsilon^4 + \varepsilon^{16} + \varepsilon^{13}, \quad y_{01} = y_0 - y_1 = \varepsilon^2 + \varepsilon^8 + \varepsilon^{15} + \varepsilon^9 \tag{9}$$

(naime $\varepsilon^{8.4} = \varepsilon^{15}$)

Radi $\varepsilon^{12.4} = \varepsilon^{14}$, $\varepsilon^{14.4} = \varepsilon^5$, $\varepsilon^{6.4} = \varepsilon^7$, $\varepsilon^{11.4} = \varepsilon^{10}$ imamo

$$y_{10} = \varepsilon^3 + \varepsilon^{12} + \varepsilon^{14} + \varepsilon^5; \quad y_{11} = \varepsilon^6 + \varepsilon^7 + \varepsilon^{11} + \varepsilon^{10}. \tag{10}$$

Lako se može provjeriti da je

$$y_{00} + y_{01} = y_0, \quad y_{00} y_{01} = -1,$$

pa se y_{00}, y_{01} podudaraju s rješenjima jednažbe

$$y^2 - y_0 y - 1 = 0, \qquad \text{dakle da je}$$

$$\{y_{00}, y_{01}\} = \left\{\frac{y_0 + (y_0^2 + 4)^{1/2}}{2}, \frac{y_0 - (y_0^2 + 4)^{1/2}}{2}\right\}. \tag{11}$$

No,
$$y_{00}=(\varepsilon+\varepsilon^{16})+(\varepsilon^4+\varepsilon^{13})=(\varepsilon+\varepsilon^{-1})+(\varepsilon^4+\varepsilon^{-4})=$$
$$=2\cos\frac{2\pi}{17}+2\cos\frac{4\pi}{17}>0,$$

pa zato prema (11) zaključujemo da je

(12) $$y_{00}=\frac{y_0+(y_0^2+4)^{1/2}}{2},\quad y_{01}=\frac{y_0-(y_0^2+4)^{1/2}}{2}.$$

Analogno se dokazuje

(13) $$y_{10}=\frac{y_1+(y_1^2+4)^{1/2}}{2},\quad y_{11}=\frac{y_1-(y_1^2+4)^{1/2}}{2}.$$

6.6. Najzad, rastavimo analogno, sumu $y_{00}=(\varepsilon+\varepsilon^{16})+(\varepsilon^4+\varepsilon^{13})$ i stavimo

(14) $$y_{000}=\varepsilon+\varepsilon^{16},\quad y_{001}=\varepsilon^4+\varepsilon^{13}.$$

Vidi se da je

(15) $$y_{000}+y_{001}=y_{00},\quad y_{000}\cdot y_{001}=y_{10},$$

što znači da y_{000}, y_{001} zadovoljavaju

$$y^2-y_{00}y+y_{10}=0;$$ odatle proizlazi

(16) $$\{y_{000},y_{001}\}=\left\{\frac{1}{2}(y_{00}+D^{1/2}),\quad \frac{1}{2}(y_{00}-D^{1/2})\right\},\quad D=y_{00}^2-4y_{10}.$$

No, lako se dokazuje da je

(17) $$y_{000}=\varepsilon+\varepsilon^{-1}=2\cos\frac{2\pi}{17},\quad y_{001}=\varepsilon^{-4}+\varepsilon^4=2\cos\frac{4\pi}{17}.$$

Dakle $y_{000}>y_{001}$ pa za diskriminantu D prema (15) imamo:

$$D=(y_{000}+y_{001})^2-4y_{000}y_{001}=(y_{000}-y_{001})^2>0.$$

Zato prema (16) izlazi:

(18) $$y_{000}=\frac{1}{2}(y_{00}+D^{1/2}),\quad y_{001}=\frac{1}{2}(y_{00}-D^{1/2}),\quad D=y_{00}^2-4y_{10}.$$

6.7. Sad možemo naći izraz za samo ε. Iz (14) zbog $\varepsilon^{16}=\varepsilon^{-1}$ izlazi najprije $y_{000}=\varepsilon+\varepsilon^{-1}$, što množeći sa ε daje

(19) $$\varepsilon^2-y_{000}\varepsilon+1=0;$$

diskriminanta te jednadžbe je y_{000}^2-4, što je, zbog (17), <0; kako se

$$\varepsilon=\cos\frac{2\pi}{17}+i\sin\frac{2\pi}{17}$$

nalazi u *prvom* kvadrantu, proizlazi iz (19)

$$\varepsilon = \frac{1}{2}[y_{000} + i(4 - y_{000}^2)^{1/2}].$$

6.8. Ukratko, imamo ovaj elegantni lanac za broj ε:

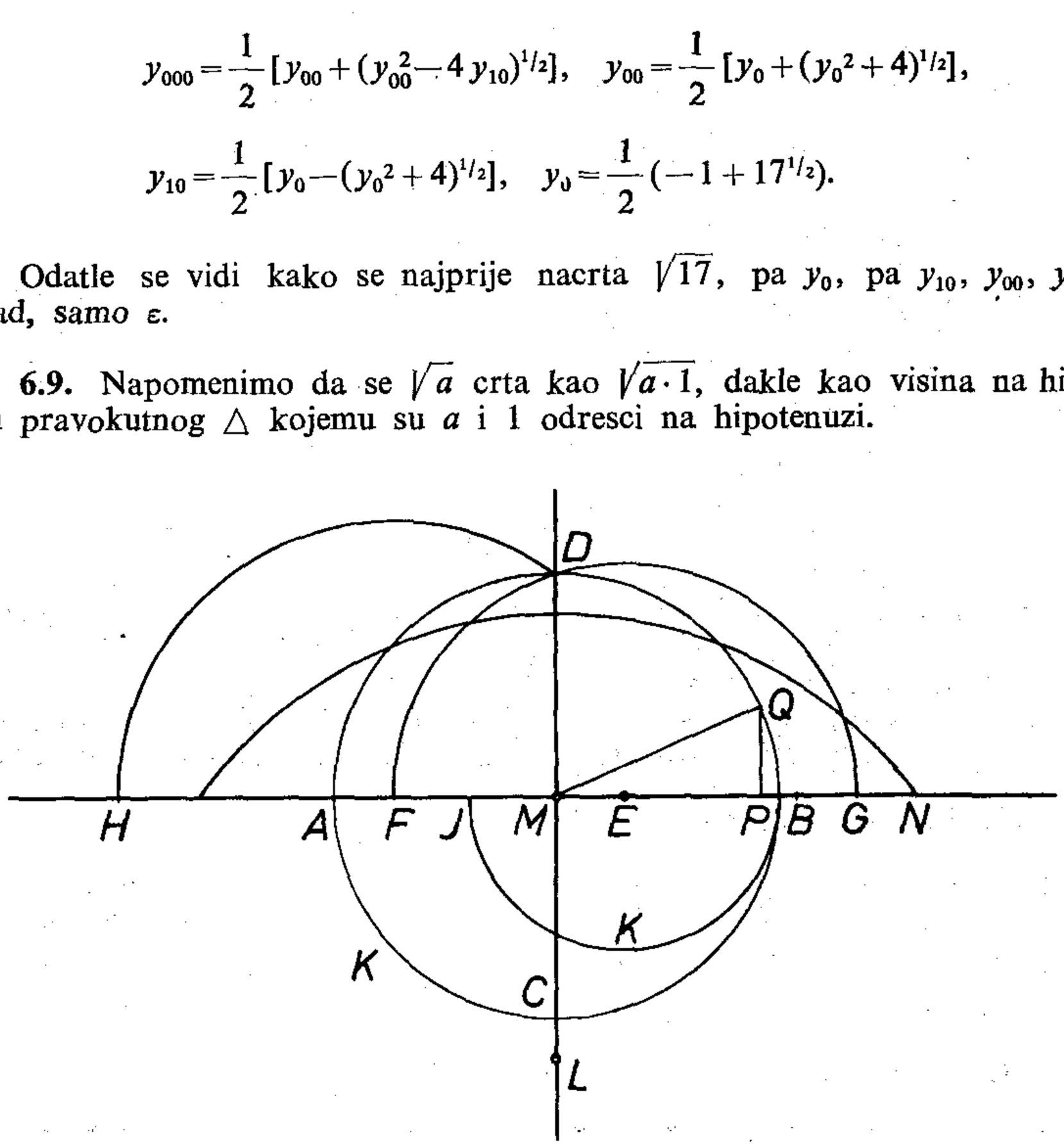
$$\varepsilon = \varepsilon_{17} = \cos\frac{2\pi}{17} + i\sin\frac{2\pi}{17} = \frac{1}{2}[y_{000} + i(4 - y_{000}^2)^{1/2}], \tag{20}$$

$$y_{000} = \frac{1}{2}[y_{00} + (y_{00}^2 - 4y_{10})^{1/2}], \quad y_{00} = \frac{1}{2}[y_0 + (y_0^2 + 4)^{1/2}],$$

$$y_{10} = \frac{1}{2}[y_0 - (y_0^2 + 4)^{1/2}], \quad y_0 = \frac{1}{2}(-1 + 17^{1/2}).$$

Odatle se vidi kako se najprije nacrta $\sqrt{17}$, pa y_0, pa y_{10}, y_{00}, y_{000} i, najzad, samo ε.

6.9. Napomenimo da se $\sqrt{a}$ crta kao $\sqrt{a \cdot 1}$, dakle kao visina na hipotenuzu pravokutnog $\triangle$ kojemu su a i 1 odresci na hipotenuzi.



Sl. 18.6.10.

6.10. Kako se izvodi konstrukcija pravilnog 17-vrha? Lanac elementarnih konstrukcija (20) može se npr. ovako izvesti pa da se u zadanu kružnicu k upiše pravilni 17-kut; radi jednostavnosti neka je radijus kružnice k jednak 1, a M njeno središte. Neka su AB, CD dva okomita dijametra od k. Odredimo E (v. sliku 6.10) tako da bude $ME = 1/4$; Neka su F i G tačke na pravcu AB — koje su i na kružnici oko E kroz D: tada je $MF = EF - ME = \frac{1}{4}(\sqrt{17} - 1) = \frac{1}{2}y_0$, $MG = -\frac{1}{2}y_1$. Neka je H sjecište polupravulje MA i kružnice oko F kroz

D; neka je J sjecište radijusa MA i kružnice oko G kroz D; tada je $MH = y_{00}$, $MJ = GD - MG = y_{10}$. Neka je K sjecište radijusa MC i kružnice kojoj je BI dijametar; tada je $MK = (MJ \cdot MB)^{1/2} = y_{10}{}^{1/2}$. Odabere li se L na pravulji MC tako da K bude središte odreska ML, tada krug oko L radijusom MH određuje na poluzraci MB tačku N, a vidi se da je $HN = HM + MN = 2\,y_{000}$. Drugim riječima, $\frac{1}{4} HN = \cos\frac{2\pi}{17}$; odredi li se na radijusu MB tačka P tako da bude $MP = \frac{1}{4} MB$, tada će, ako je Q tačka u kojoj okomica na AB kroz P siječe gornju polukružnicu k, biti BQ stranica traženog pravilnog 17-kuta.

Primjedba. Gornje razmatranje o pravilnom 17-vrhu uslovljeno je jednakošću $\varphi(17) = 2^{2^2}$; analogno se razmatranje može provesti i za pravilni 257-vrh, jer je $\varphi(257) = \varphi(2^8 + 1) = 2^8$.[1]

6.11. Gaussu je još dok je bio vrlo mlad pošlo za rukom da dokaže ovo: *da bi se pravilni p-vrh* (*p prost broj*) *mogao nacrtati služeći se linearom i šestarom, nužno je i dovoljno da prost broj p bude oblika* $2^{2^n} + 1$, *tj. da p bude fermatovskog oblika* (isp. pogl. 6, § 7.10).

6.12. S takvim prostim brojevima

$$F_n = 2^{2^n} + 1$$

sreo se, naime, Fermat; kako su brojevi $F(0) = 3$, $F(1) = 5$, $F(2) = 17$ $F(3) = 257$, $F(4) = 65537$ prosti brojevi, pomišljao je Fermat (no izričući da za to nema dokaza) da bi i preostali „fermatovski" brojevi bili prosti. Međutim, do danas se ne zna da li postoji ikoji fermatovski prost broj $> F(4)$; zna se, naprotiv, da su brojevi $F(5)$, $F(12)$, $F(23)$, $F(36)$ složeni brojevi.[2]

6.13. Može se dokazati ovaj

Teorem. *Da se jedino pomoću lineala i šestara* (*cirkla*) *može pravilni k-vrh nacrtati, nužno je i dovoljno da broj k bude oblika* 2^α *ili oblika* $2^\alpha p_1 p_2 \ldots p_r$, *gdje su p-ovi različiti prosti brojevi fermatovskog oblika* (isp. sliku na str. 685).

O čitavoj problematici dijeljenja kruga vidjeti knjigu P. Bachmann [2].

7. O elementarnim geometrijskim konstrukcijama (isp. pogl. 5, § 8).

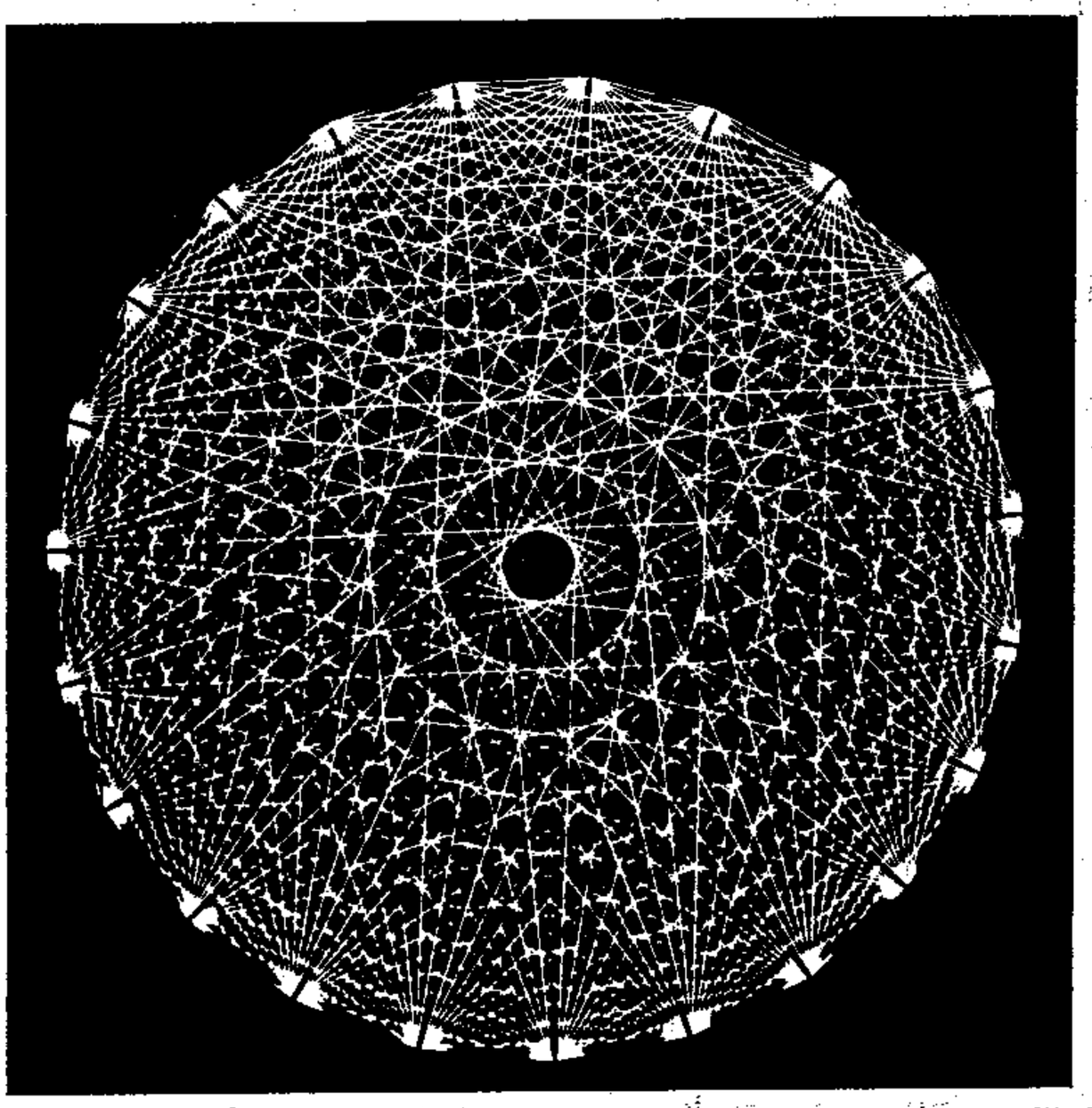
To su one konstrukcije koje se mogu izvesti iz broja 1 služeći se samo linealom (svake, proizvoljno velike dužine) i šestarom (sa svakim mogućim rasponom, odnosno radijusom). Kako se linealom crta *prava* linija, čemu aritmetički odgovara *linearna jednadžba*, a šestarom *kružna linija*, dakle crta drugog stepena, moći će se algebarski problem riješiti *elementarno onda i samo onda ako se on može svesti na rješavanje konačnog broja jednadžbi* 1. *i* 2. *stupnja*.

---

[1] O konstrukciji pravilnog $(2^8 + 1)$ — vrha vidjeti: F. J. Richelot (*Journal fur die reine und angewandte Mathematik*, 9 (1832), str. 1—26, 146—161, 209—230, 337—358).

[2] O tom vidjeti M. Kraitchik, Théorie des nombres, Pariz, 1922, p. 22.

7.1. Problem udvostručenja kocke je stari grčki problem (također nazivan delfijski problem), a sastoji se u tome da se odredi kocka (brid x) dva-put veća od zadane (brid a). Iz $x^3=2a^3$ izlazi $x=a\,2^{1/2}$. Očigledno da se $\sqrt[3]{\ }$ ne može svesti na kvadratni korijen iz racionalna broja. Zato je duplikaciju kocke nemoguće izvesti elementarno. Hipokrates (5. st. pr. n. e.) je *prostorni problem* duplikacije kocke sveo na *planimetrijski* problem o uklapanju između brojeva 1 i 2 dviju srednjih geometrijskih proporcionala x i y, jer iz $1:x=x:y=y:2$ izlazi $x^3=2$.



Sl. 18.7.1. Pravilni 23-kut sa svim dijagonalama. Koncentrični krugovi su optičke varke.

Na sličan način, polazeći od bilo kojeg pravilnog $n-\angle$, dobija se odgovarajuća tvorevina

7.2. Trisekcija kuta (isp. pogl. 5, § 8.7). Zadan je kut 3α, nacrtaj onda i triput manji kut α. Kako je

$$\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha,$$

odnosno

$$8\cos^3\alpha - 6\cos\alpha - 2\cos 3\alpha = 0,$$

to, stavljajući $x=2\cos\alpha$, izlazi

$$x^3 - 3x - 2a = 0, \tag{1}$$

gdje je $a=\cos 3\alpha$ veličina zadana kutom α. To je jednadžba za trisekciju kuta 3α. Npr. za $3\alpha=60^0$ izlazi $a=\cos 60^0=1/2$, pa jednadžba za trisekciju kuta od 60^0 glasi $x^3-3x-1=0$. Kako je ova jednadžba bez ikojeg racionalnog rješenja, to prema 5 § 8.4. izlazi da se kut od 60^0 ne može elementarno podijeliti na tri jednaka dijela, tj. *kut od* 20^0 *ne može se nacrtati elementarno.*

7.2.1. Mogu se navesti i razni drugi kutovi 3α koje ne možemo elementarno podijeliti na 3 jednaka dijela. Stavimo li naime prema (1)

$$a = \cos 3\alpha = r/s, \tag{2}$$

gdje su r, s cijeli brojevi koji su međusobno prosti, tada bi iz (1) izlazilo

$$y^3 - 3s^2 y = 2rs^2 \tag{3}$$

gdje je $y = sx$.

No, (3) je jednadžba s cijelim koeficijentima; zato bi svako njeno racionalno rješenje y bilo cjelobrojno; znači da bi svakom *racionalnom* rješenju x jednadžbe (1) uz uslov (2) nužno odgovaralo *cjelobrojno* rješenje y jednadžbe (3).

7.2.2. Međutim, lako je navesti međusobno proste cijele brojeve r, s za koje je (3) bez ikojeg cjelobrojnog rješenja y; dovoljno je npr. uočiti bilo koji prost broj $p > 2$ i staviti $s = ps'$, pri čemu je s' cio broj nedjeljiv sa p; tada bi nužno y bilo djeljivo sa p dakle bi $(3)_1$ bilo djeljivo sa p^3 a $(3)_2$ ne bi bilo djeljivo sa p^3 (nego samo sa p^2).

Tako npr. za $s = 3$, $r = 2$ određen je elementarno oštri kut 3α iz $\cos 3\alpha = 2/3$; međutim, sam kut α ne može se nacrtati elementarno.

8. Zadaci u vezi s korijenima jedinice.

1. Odredi korijene jedinice reda 3, 4, 5, 6, 7, 8, 9, 10. Koji od njih leže u otvorenom prvom, odnosno otvorenom drugom kvadrantu?
2. Nađi prvoobrazne ili primitivne korijene jedinice reda 3, 4, 5, 6, 7, 8, 9, 10, 12, 24.
3. Koji su od ovih brojeva korijeni jedinice? 1, -1, $\sqrt{2}$, $\cos 30^0$, $\cos 30^0 + i \sin 30^0$, $\cos\frac{2\pi}{17} + i\sin\frac{2\pi}{17}$, $e^{i\frac{2\pi}{35}}$, $1 - e^{i\frac{2\pi}{35}}$; odredi im stepen.
4. Neka je ε_n prvoobrazni korijen jedinice reda n; 1) nađi $\sum_{k=0}^{n=1} \varepsilon_n^k$; konkretiziraj za $n = 3, 5, 10$; 2) kolika je ta suma za neprimitivni korijen jedinice? 3) Odredi $\sum_{k=0}^{n=1} \varepsilon_{2n}^k$.
5. Neka je ε n-ti korijen jedinice: 1) odredi $1 + 2\varepsilon + 3\varepsilon^2 + \cdots + n\varepsilon^{n-1}$, 2) $1 + 4\varepsilon + 9\varepsilon^2 + \cdots + n^2\varepsilon^{n-1}$.
6. Da li je $\left\{1^{\frac{1}{n}}\right\}$ određena grupa? Napravi tablicu množenja!
7. Pomoću rješenja jednadžbe $x^{10} - 1 = 0$ konstruiraj $\cos 18^0$, $\sin 18^0$.
8. Neka je $e_k = e^{i\frac{k2\pi}{n}}$; dokaži: 1) $\prod_{k=0}^{n=1} (a + be_k) = a^n + (-1)^{n-1} b^n$,

   2) $\prod_{k=0}^{n-1} (e_k^2 - 2e_k \cos\varphi + 1) = 2(1 - \cos n\varphi)$,

   3) $\prod_{k=0}^{n-1} \frac{(x + e_k)^n - 1}{x} = \prod_{k=1}^{n-1} [x^n - (e_k - 1)^n]$.

9. Neka je $1, x_2, x_3, \ldots, x_n$ spektar rješenja jednadžbe $x^n = 1$; dokaži $\prod_{k=2}^{n} (1 - x_k) = n$.

10. Dokazati 1) $x^{2n} - 1 = (x^2 - 1) \prod_{k=1}^{n-1} (x^2 - 2x \cos \frac{k\pi}{n} + 1)$;

2) $x^{2n+1} - 1 = (x \varepsilon 1) \prod_{k=1}^{n} (x^2 \varepsilon 2x \cos \frac{2k\pi}{2n+1} + 1)$; (tu ε znači + odnosno −)

3) $x^{2n+1} + 1 = \prod_{k=0}^{n-1} (x^2 - 2x \cos \frac{2k+1)\pi}{2n} + 1)$;

4) $\prod_{k=1}^{n-1} \sin \frac{k\pi}{2n} = n^{1/2} 2^{-n+1}$; 5) $\prod_{k=1}^{n} \sin \frac{k\pi}{2n+1} = (2n+1)^{1/2} 2^{-n}$.

11. Neka je $\varepsilon^2 + \varepsilon + 1 = 0$; neka je x_1, x_2, x_3 spektar polinoma $x^3 + px + q$; ako je $A = x_1 + x_2 \varepsilon + x_3 \varepsilon^2$, $B = x_1 + x_2 \varepsilon^2 + x_3 \varepsilon$, dokazati da je A, B spektar kvadratne jednadžbe $y^2 + 27qy - 27p^3 = 0$.

12. Neka je $z_0, z_1, \ldots, z_{n-1}$ proizvoljan niz kompleksnih brojeva i $\varepsilon^{i\frac{2\pi}{n}} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$; dokaži da je $\sum_{k=0}^{n-1} \left| \sum_{\nu=0}^{n-1} z_\nu \varepsilon^{\nu k} \right|^2 = \sum_{k=0}^{n-1} \left| z_k \right|^2$.

13. Riješi 1) $\bar{x} = x^{n-1}$ 2) $(x+1)^n - (x-1)^n = 0$

3) $(x+i)^n - (x-i)^n = 0$.

14. Dokaži da za Möbiusovu funkciju μ vrijedi: $\mu(n)$ je suma svih prvobiaznih korijena jedinice reda n.

15) Odredi $\Phi_n(x)$ za $n = 3, 4, 5, 6, 12, 20$.

16. Nađi 1) $\Phi_n(1)$; 2) $\Phi_n(-1)$.

17. Ako je ε prvoobrazni korijen jedinice reda n nađi $\left| \sum_{k=0}^{n-1} \varepsilon^{k^2} \right|$.

18. Nađi sumu svih produkata po dva primitivna korijena jedinice reda n.

19. Neka su k, n međusobno prosti prirodni brojevi; ako P_n označuje sve primitivne korijene jedinice reda n, tada: $P_n{}^k$ svih x^k, kada $x \in P_k$ upravo je jednak P_n, tj. $P_n = P_n{}^k$; 2) $x \in P_n \Rightarrow \sum_{\nu=0}^{n-1} x^{m\nu} = 0$ za svaki cio broj m.

20. Iz 19. izvedi ovo: skup S generatora cikličke grupe C_n ima svojstvo da je $S = \{x^k;\ x \in S\}$ za svaki cijeli broj k koji je prost prema n.

Literatura

Bachmann [1], [2]

POGLAVLJE 19.

SIMETRIČNE FUNKCIJE

U ovom poglavlju bit će govora o funkcijama od proizvoljno mnogo promjenljivih

$$x_1, x_2, \ldots, x_n; \tag{1}$$

n je kojigod prirodan broj. Pri tom ćemo imati dva bitno različita slučaja, već prema tome da li će argumenti funkcije biti proizvoljni brojevi ili će pak pripadati skupu (1).

Inače, praktički cilj razmatranja ovog poglavlja sastojat će se u saznanju da je *svaka simetrična racionalna funkcija f od nula-tačaka* (1) *polinoma a* također *racionalna* funkcija *koeficijenata* a_ν toga polinoma, tj. da se može shvatiti kao funkcija nula-tačaka *posredstvom koeficijenata toga polinoma*:

$$f(x_1, x_2, \ldots, x_n) = f_1(a_1(x_1, x_2, \ldots, x_n), a_2(x_1, x_2, \ldots, x_n), \ldots).$$

1. POJAM I PRIMJERI SIMETRIČNIH FUNKCIJA

1.1. Definicija. Funkcija $f(x_1, x_2, \ldots, x_n)$ od n promjenljivih $x_1, x_2, \ldots, x_n$ je *simetrična* ako je njena vrijednost ista za sve permutacije varijabli, dakle ako je

$$f(x_1, x_2, \ldots, x_n) = f(x_{p_1}, x_{p_2}, \ldots, x_{p_n})$$

za svaku permutaciju p skupa 1 (n) brojeva 1, 2, ..., n.

Kako se svaka permutacija može dobiti pomoću transpozicija, možemo reći *da je funkcija simetrična ako pri transpoziciji njenih varijabli funkcija ostaje ista.*

Npr. izraz $2+3$, x_1+x_2, $x_1^k+x_1^k+\cdots+x_m^k$ je simetričan s obzirom na veličine 2, 3, odnosno x_1, x_2, odnosno $x_1, x_2, \ldots, x_m$. Naprotiv, izrazi $2-3$, $x_2^2-x_1$ to nisu.

Specijalno se govori o *simetričnim polinomima*, o *simetričnim racionalnim funkcijama* (izrazima), itd.

1.2. Osnovne simetrične funkcije σ. Od važnosti su ove simetrične funkcije[1]:

$$s_1 = x_1 + x_2 + \cdots + x_n, \quad s_2 = x_1^2 + x_2^2 + \cdots + x_n^2$$

i općenito

$$s_k = s_k(x_1, x_2, \ldots, x_n) = x_1^k + x_2^k + \cdots + x_n^k$$

za svaki cio broj k; posebno se stavlja $s_0 = n$.

Nadalje je izraz

$$\prod_{i=1}^{n} (t - x_i)$$

simetričan polinom veličina $x_1, x_2, \ldots, x_n$. Napiše li se on kao polinom s obzirom na t:

$$\prod_{\nu=1}^{n} (t - x_\nu) = \sigma_0 t^n + \sigma_1 t^{n-1} + \cdots \sigma_{n-1} t + \sigma_n,$$

koeficijenti $\sigma_0, \sigma_1, \ldots,$ zavise od $x_1, x_2, \ldots, x_n$ i imamo teorem:

1.2.1. Teorem (Viète, 1615; isp. sl. na str. 134)

$$\sigma_0 = 1$$

$$\sigma_1 = -(x_1 + x_2 + \cdots + x_n) = -\sum_{\nu=1}^{n} x_\nu$$

$$\text{(V)} \qquad \sigma_2 = x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n = \sum_{\nu_1 < \nu_2} x_{\nu_1} x_{\nu_2},$$

pri čemu ν_1, ν_2, prolazi svim ambama skupa $\{1, 2, , \ldots, n\}$,

$$\sigma_3 = -\sum x_{\nu_1} x_{\nu_2} x_{\nu_3}$$

$$\sigma_\nu = (-1)^\nu \sum x_{\nu_1} x_{\nu_2} \cdots x_{\nu_\nu};$$

tu $\nu_1 \nu_2 \cdots \nu_\nu$ prolazi svim podnizovima po ν članova iz niza $1, 2, \ldots, n$.

Npr. $\sigma_n = (-1)^n x_1 x_2 \cdots x_n$.

Svi izrazi σ_ν su očigledno simetrične funkcije x-ova; kako se te funkcije pojavljuju u tako osnovnoj ulozi, naime kao koeficijenti jednadžbi sa zadanim rješenjima, imaju funkcije σ_ν osnovnu ulogu.

1.2.2. Definicija. Funkcije $\sigma_1, \sigma_2, \ldots, \sigma_n$ definirane pomoću (V) zovu se *osnovne ili elementarne simetrične funkcije zadanih veličina* $x_1, \ldots, x_n$; stavlja se $\sigma_0(x_1, x_2, \ldots, x_n) = 1$, $\sigma_r(x_1, \ldots, x_n) = 0$ za $r = n+1, n+2, \ldots$

---

[1] Zanimljivo je spomenuti kako se slučaj od beskonačno mnogo varijabli može bitno razlikovati od slučaja kad radimo s konačno mnogo varijabli. Tako npr. funkcija $s_1 = x_0 + x_1 + x_2 + \cdots$ ne mora biti simetrična ako ima ∞ mnogo x-ova; npr. ako je

$$x_n = (-1)^n/(n+1) \quad \text{za} \quad n = 0, 1, 2, \ldots,$$

tada izraz s_1 nije simetričan; može se permutiranjem članova sume s_1 dobiti za sumu s_1 bilo koji naprijed dat realan broj (isp. Ž. Marković, [1], sv. 1, p. 111; Vidav [1], 1, § 75; p. 424).

Npr. veličinama x_1, x_2, x_3 pripadaju ove osnovne simetrične funkcije:

$$\sigma_1 = -x_1 - x_2 - x_3$$
$$\sigma_2 = \quad x_1 x_2 + x_1 x_3 + x_2 x_3$$
$$\sigma_3 = -x_2 x_2 x_3.$$

1.3. *Funkcije* $s_m(x_1, x_2, \ldots, x_m)$. Stavlja se

$$s_m = s_m(x_1, \ldots, x_n) = x_1^m + x_2^m + \cdots + x_m^n.$$

1.4. Važna je simetrična funkcija (isp. 11 § 11.5.1)

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix}^2 = \prod_{i>j}^{n} (x_i - x_j)^2 = V_n[x_1 \cdots x_n]^2,$$

što je dalje jednako (množeći stupce sa stupcima):

$$= \begin{vmatrix} n & s_1 & s_2 & \cdots & s_{n-1} \\ s_1 & s_2 & s_3 & \cdots & s_n \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ s_{n-1} & s_{n-2} & \cdots & & s_{2n-2} \end{vmatrix}; \quad \text{isp. § 1.3.}$$

Kao funkcija osnovnih simetričnih veličina $\sigma_1 \cdots \sigma_n$ pokazuje se gornji dvostruki produkt kao diskriminanta polinoma

$$\prod_{i=1}^{n} (x - x_i) \text{ (isp. 20 § 3.3.2).}$$

1.5. Jednostavni simetrični polinomi (ili Σ-polinomi). Neka je $k \leqslant n$ te $\alpha_1, \alpha_2, \ldots, \alpha_k$ bilo kakav niz od k prirodnih brojeva; tada se jednostavna simetrična funkcija

$$[\alpha_1, \alpha_2, \ldots, \alpha_k] \quad \text{ili} \quad \sum x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k} \quad \text{ili} \quad s_{\alpha_1 \alpha_2 \cdots \alpha_k}$$

definira kao suma svih monoma oblika $x_1^{p_1} x_2^{p_2} \cdots x_n^{p_n}$, pri čemu $p_1, \ldots, p_n$ prolazi skupom svih permutacijâ n-članog niza $\alpha_1, \alpha_2, \ldots, \alpha_k, \overbrace{0, 0, \ldots, 0}^{n-k}$. Npr.

$$[1] = s_1, \quad [k] = s_k,$$
$$[1, 1] = \sigma_2, \quad [111] = -\sigma_3, \quad \underbrace{[11 \cdots 1]}_{\nu} = (-1)^\nu \sigma_\nu$$

za svako $\nu \in \{1, \ldots, n\}$;

$$[1, 2] = x_1 x_2^2 + x_1 x_3^2 + \cdots + x_1 x_n^2 + \cdots x_{n-1} x_n^2;$$

prema 3 § 9.3.2 tu ima $\dfrac{n!}{(n-2)!} = (n-1)\, n$ članova.

Interesantnost jednostavnih simetričnih funkcija proizlazi iz

1.5.1. Leme. *Svaki simetrični polinom suma je određenih jednostavnih simetričnih polinoma.*

Npr. $$3 x_1^2 x_3 + 3 x_1 x_3^2 + x_3 + x_1 = 3[1, 2] + [1];$$

tu dolaze samo varijable x_1, x_3.

2. VEZA MEĐU FUNKCIJAMA s_k I OSNOVNIM SIMETRIČNIM FUNKCIJAMA σ_ν. NEWTONOVE FORMULE

2.1. *Slučaj varijabli*: x_1, x_2. Osnovne su simetrične funkcije

$$\sigma_1 = -(x_1 + x_2), \quad \sigma_2 = x_1 x_2.$$

Dokazat ćemo induktivno da je $s_k = (x_1^k + x_2^k)$ *za svako cjelobrojno* $k > 0$ *moguće izraziti pomoću* σ_1, σ_2 *služeći se prvim trima računskim operacijama.*

Najprije, stvar je istinita za $k = 1$, jer je $s_1 = -\sigma_1$. Dokažimo da je izreka istinita za $k = l+1$ ako je istinita za $k = l$. Stvarno,

$$s_{l+1} = x_1^{l+1} + x_2^{l+1} = (x_1^l + x_2^l)(x_1 + x_2) - x_1 x_2 (x_1^{l-1} + x_2^{l-1}),$$

dakle

(*) $$s_{l+1} = s_l \cdot s_1 - \sigma_2 s_{l-1};$$

kako je svaki član u posljednjem binomu polinom s obzirom na σ_1, σ_2, to je i sam taj binom, tj. s_{l+1} cjelobrojni polinom prema σ_1, σ_2.

2.1.1. Primjer. Nađi sumu kuba korijenâ kvadratne jednadžbe $x^2 - 5x + 2 = 0$. Ako su korijeni te jednadžbe x_0, x_1, onda se, dakle, radi o tome da nađemo $s_3(x_0, x_1) = x_0^3 + x_1^3$, a da ne tražimo same korijene x_0, x_1: za to nam dostaju osnovne funkcije $\sigma_1 = -5$, $\sigma_2 = 2$.

Prema obrascu (*) imamo

$$s_3 = s_2 s_1 - \sigma_2 s_1 = (\text{po istom zakonu}) = (s_1 \cdot s_1 - \sigma_2 s_0) s_1$$

$$-\sigma_2 s_1 = -\sigma_1^3 + 3\sigma_1 \sigma_2 = 95, \text{ tj. } s_3 = 95.$$

2.2. Opći slučaj. Newtonovi obrasci. — 2.2.1. Newtonove formule. One govore o vezi funkcija s_i s funkcijama σ_k. Pođimo na izvor osnovnih simetričnih funkcija $\sigma_1, \sigma_2, \ldots, \sigma_n$ i promatrajmo ovaj polinom sređen po padajućim potencijama:

(1) $$f(t) = \prod_{i=1}^{n} (t - x_i) = \sum_{i=0}^{n} \sigma_i t^{n-i};$$

tu je $\sigma_0 = 1$. (Primijetimo, da je simbolika takva da je eksponent varijable t jednak razlici stupnja n i indeksa odgovarajućeg koeficijenta).

No, iz (1) za derivat

(2) $$f'(t) = nt^{n-1} + (n-1)\sigma_1 t^{n-2} + \ldots = \sum_{k=0}^{n} (n-k)\sigma_k t^{n-k-1}$$

izlazi identički

(3) $$f'(t) = \sum_{k=1}^{n} \frac{f(t)}{t - x_k}.$$

Direktnom diobom ili Hornerovom diobom vidi se da je

(4_ν) $$\frac{f(t)}{t - x_\nu} = t^{n-1} + (\sigma_1 + x_\nu) t^{n-2} + (\sigma_2 + \sigma_1 x_\nu + x_\nu^2) t^{n-3} + \ldots +$$
$$+ (\sigma_{n-1} + \sigma_{n-2} x_\nu + \ldots + \sigma_1 x_\nu^{n-2} + x_\nu^{n-1}).$$

Tu ν prolazi svim rednim brojevima 1, 2, ..., n. Saberemo li sve jednakosti (4_ν) $(\nu = 1, \ldots, n)$, dobivamo zbog (3):

$$f'(t) = nt^{n-1} + (n\sigma_1 + s_1)t^{n-2} + (n\sigma_2 + \sigma_1 s_1 + s_2)t^{n-3} + (n\sigma_3 + \sigma_2 s_1 + \sigma_1 s_2 + s_3)t^{n-4} +$$

$$+ \cdots + (n\sigma_{n-1} + \sigma_{n-2} s_1 + \sigma_{n-3} s_2 + \cdots + s_{n-1}). \tag{5}$$

Izjednačujući desne strane u (2) i (5), odnosno izjednačujući po redu koeficijente od t^{n-1}, t^{n-2}, ... t, t^0 u $(2)_2$ i $(5)_2$, dobivamo ovaj sistem jednadžbi

$$\begin{aligned} n\sigma_1 + s_1 &= (n-1)\sigma_1 \\ n\sigma_2 + \sigma_1 s_1 + s_2 &= (n-2)\sigma_2 \\ \sigma_{k-1} s_1 + \sigma_{k-2} s_2 + \cdots + \sigma_1 s_{k-1} + s_k &= -k\sigma_k \quad (k = 1, 2, \ldots, n-1). \end{aligned} \tag{6}$$

Iz toga sistema neposredno izlazi ono što smo tražili, tj.

2.2.2. Teorem. (Newtonove formule[1] isp. 2, § 4.2).

$$\begin{aligned} s_1 &= -\sigma_1 \\ \sigma_1 s_1 + s_2 &= -2\sigma_2 \\ \sigma_2 s_1 + \sigma_1 s_2 + s_3 &= -3\sigma_3 \\ &\cdots\cdots\cdots\cdots \\ n\sigma_\nu + \sigma_{\nu-1} s_1 + \sigma_{\nu-2} s_2 + \cdots + \sigma_1 s_{\nu-1} + s_\nu &= (n-\nu)\sigma_\nu \quad (\nu = 1, 2, \ldots, n-1). \end{aligned} \tag{7}$$

2.2.3. Obrasce (7) izveli smo za $\nu \leq n$. Međutim, isti obrasci vrijede i za $\nu \geq n$, uz dogovor, naravno, da je $\sigma_k = 0$ za $k > n$. Dokaz je vrlo jednostavan, jer je očigledno da naš polinom (1) zadovoljava

$$x_\nu^r f(x_\nu) = 0 \text{ za svako } r \geq 0 \text{ i svako } \nu = 1, 2, \ldots, n \text{ ili eksplicite}$$

$$\sum_{i=0}^{n} \sigma_i x_\nu^{n+r-i} = 0.$$

Sumirajući tih n jednadžbi za $\nu = 1, 2, \ldots, n$, dobivamo željene izraze (7), ali ovaj put i za vrijednost $k = n + r$ za svako $r = 0, 1, 2, \ldots$, tj.

$$\sum_{i=0}^{n} \sigma_i s_{n+r-i} = 0 \text{ pri } \sigma_0 = 1,\ s_0 = n,\ r = 0,\ 1, 2, \ldots \tag{7'}$$

2.2.4. Iz sistema (7), (7') zaključujemo po redu da je eksplicite

$$\begin{aligned} s_1 &= -\sigma_1 \\ s_2 &= \sigma_1^2 - 2\sigma_2 \\ s_3 &= -\sigma_1^3 + 3\sigma_1\sigma_2 - 3\sigma_3 \\ s_4 &= \sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 + 4\sigma_1\sigma_3 - 4\sigma_4 \\ &\cdots\cdots\cdots\cdots\cdots\cdots, \end{aligned} \tag{8}$$

Međutim, u (8) se ne vidi zakon kako se obrazuju desne strane. Zato je od interesa da izrazimo s-ove i drugačije pomoću σ-ova.

---

[1] I. Newton, Arithmetica universalis, 1673/84; štampano 1707.

Nađimo s_k iz svih k jednadžbi sistema (7), koje su s obzirom na $s_1, s_2, \ldots, s_k$ linearne, a koeficijenti im obrazuju determinantu koja je $=1$; neposredno se vidi da po Cramerovu pravilu (isp. 9 § 1.9) izlazi

2.2.4. Teorem. *Za svaki prirodni broj* k vrijedi

$$s_k = -\begin{vmatrix} \sigma_0 & & & \sigma_1 \\ \sigma_1 & \sigma_0 & & 2\sigma_2 \\ \sigma_2 & \sigma_1 & \sigma_0 & 3\sigma_3 \\ \cdots & \sigma_i & & \cdots \\ \sigma_{k-1} & \sigma_{k-2} & & \sigma_{1\,k}\,\sigma_k \end{vmatrix}, \quad \sigma_0 = 1.$$

Nenapisani članovi determinante svi su jednaki 0. Npr.

$$s_2 = -\begin{vmatrix} 1 & \sigma_1 \\ \sigma_1 & 2\sigma_2 \end{vmatrix} = \sigma_1^2 - 2\sigma_2,$$

kao što i inače znamo.

2.2.5. Prema Waringu[1] vrijedi također

$$s_k = \sum (-1)^{\lambda_1+\lambda_2+\cdots+\lambda_n} \frac{(\lambda_1+\lambda_2+\cdots+\lambda_n-1)!}{\lambda_1!\,\lambda_2!\cdots\lambda_n!}\,\sigma_1^{\lambda_1}\sigma_2^{\lambda_2}\cdots\sigma_n^{\lambda_n}; \tag{10}$$

sumacija se proteže na sve cijele brojeve $\lambda_1, \lambda_2, \ldots, \lambda_n$ koji su ≥ 0 i za koje je $\lambda_1 + 2\lambda_2 + \cdots + n\lambda_n = k$.

(Isp. Obreškov [1], sv. 1, p. 111; Perron [1], sv. 1, p. 153).

3. OSNOVNI TEOREM O SIMETRIČNIM POLINOMIMA

—→ 3.1. Teorem[2]. ***Svaki simetrični polinom*** $p(x_1, x_2, \ldots, x_n)$ ***može se prikazati kao polinom*** $P(\sigma_1, \sigma_2, \ldots, \sigma_n)$ ***osnovnih simetričnih funkcija*** $\sigma_1, \sigma_2, \ldots, \sigma_n$ ***taao da je dakle,***

$$p(x_1, x_2, \ldots, x_n) = P(\sigma_1, \sigma_2, \ldots, \sigma_n)$$ **(isp. § 1.2.2.).**

—→ Korolar. 32. ***Svaki simetrični polinom*** p ***nulišta (nulamjestâ) nekog algebarskog normiranog polinoma*** q ***može se izraziti i kao polinom*** P ***koeficijenata toga polinoma*** q***; ako*** p ***ima cjelobrojne koeficijente, ima i*** P ***cjelobrojne koeficijente.***

3.2.1. Dodatak. Teorem i korolar su istiniti i onda ako su koeficijenti polinoma p elementi bilo kojeg komutativnog prstena s jediničnim elementom.

3.3. Dokaz teorema 3.1. Waringova metoda.

---

[1] E. Waring, Meditationes algebraicae, Cambridge, 1782.

[2] Uz teorem dolaze imena: G. Cramer, A. Vandermonde, E. Waring, K. Gauss, L. Cauchy.

Stvarno, promatrajmo simetrični polinom p; njega ćemo, prema Waringu srediti leksikografski ovako: neka su

$$A = a x_1^{\alpha_1} x_2^{\alpha_2} \cdot \ldots \cdot x_n^{\alpha_n}, \quad B = b x_1^{\beta_1} x_2^{\beta_2} \cdot \ldots \cdot x_n^{\beta_n}$$

bilo koja dva različita člana polinoma p; pri tom su eksponenti cijeli i ≥ 0; kako nije $\alpha_i = \beta_i$ $(i = 1, 2, \ldots, n)$, postoji posve određen broj $k \leq n$ za koji je $\alpha_k \neq \beta_k$, dok je $\alpha_i = \beta_i$ za svako $i < k$; stavit ćemo član A *ispred člana* B onda i samo onda ako je $\alpha_k > \beta_k$.

Na taj način svakom polinomu p pripada posve određen ***početni član*** koji u *zavisnosti od p možemo naznačiti sa* $R_0 p$.

Pretpostavimo da je baš promatrano $A = R_0 p$; tada je niz eksponenata $\alpha_1 \geq \alpha_2 \geq \cdots$ silazan; u obrnutom slučaju, bilo bi npr. $\alpha_i < \alpha_{i+1}$; kako je polinom p simetričan, sadržavao bi on uz član A i član A', koji se iz A dobije permutiranjem u njemu varijabli x_i, x_{i+1}; naravno da bi A' bilo ispred A u gornjem uređivanju, protivno pretpostavci da je A početni član. Tako npr. kad bi bilo $A = 3 x_1^2 x_2^3$, bilo bi $A' = 3 x_2^2 x_1^3 = 3 x_1^3 x_2^2$, dakle A' ispred A.

Ako je, dakle,

$$A = R_0 p = a x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} \tag{1}$$

početni član u simetričnom polinomu p, tada cijeli brojevi $\alpha_i - \alpha_{i+1}$ $(i = 1, 2 \ldots n-1)$ nisu negativni. Nadalje se vidi da je izraz

$$a \cdot \sigma_1^{\alpha_1 - \alpha_2} \cdot \sigma_2^{\alpha_2 - \alpha_3} \cdot \ldots \cdot \sigma_{n-1}^{\alpha_{n-1} - \alpha_n} \cdot \sigma_n^{\alpha_n} \tag{2}$$

simetričan polinom s obzirom na $x_1, x_2, \ldots, x_n$ i da mu je početni član $= A$ ili $-A$. Uistinu, lako se vidi da je početni član produkta dvaju polinoma jednak produktu početnih članova tih polinoma; no početni članovi u faktorima polinoma (2) jesu po redu:

$$a,\ (-x_1)^{\alpha_1 - \alpha_2},\ (x_1 x_2)^{\alpha_2 - \alpha_3},\ (-x_1 x_2 x_3)^{\alpha_3 - \alpha_4},\ \ldots,\ ((-1)^n x_1 x_2 \cdot \ldots \cdot x_2)^{\alpha_n}; \tag{3}$$

produkt izrazâ (3) je $(-1)^\alpha A$, gde je

$$\alpha = (\alpha_1 - \alpha_2) + (\alpha_3 - \alpha_4) + \cdots + n \alpha_n; \tag{4}$$

tako npr. eksponent od x_1 u tom produktu je

$$(\alpha_1 - \alpha_2) + (\alpha_2 - \alpha_3) + \cdots + (\alpha_{n-1} - \alpha_n) + \alpha_n = \alpha_1.$$

Drugim riječima, polinom

$$p - (-1)^\alpha \cdot (2), \tag{5}$$

koji nastaje kao diferencija dvaju simetričnih polinoma p, $(-1)^\alpha \cdot (2)$ i sam je simetričan, a njegov početni član $R_0(5)$ je mlađi od $R_0 p$.

3.3.1. *Rekurzioni postupak u dokazivanju teorema* 3.1. (E. Waring, 1782):

prvi korak: naći i napisati vodeći član $R_0 p$ prema (1);
drugi korak: naći (2) i (4);
treći korak: naći polinom (5).

3.3.2. Uzimajući sada u promatranje početni član polinoma (5) i provodeći analogno razmatranje, dolazi se do novog simetričnog polinoma s još mlađim članom. Proces će se završiti nakon konačno mnogo koračaja time da se dođe do „najmlađeg" člana: konstante. A to zapravo znači da je zadani polinom prikazan pomoću osnovnih funkcija $\sigma_1, \sigma_2, \ldots, \sigma_n$.

3.3.3. Primjer. Polinom $p(x, y) = x^2 + y^2 + 3x^2y + 3xy^2$ prikaži pomoću $\sigma_1 = -x - y$, $\sigma_2 = xy$. Tu je $R_0 p = 3x^2 y$, $n = 2$, $x_1 = x$, $x_2 = y$, $\alpha = 1 + 2 \cdot 1 = 3$, $(-1)^\alpha = -1$; monom (2) glasi $-3\sigma_1\sigma_2$ pa (5) daje $p(x, y) + 3\sigma_1\sigma_2 =$ (računaj)! $= x^2 + y^2 = \sigma_1^2 - 2\sigma_2$. Odgovor na pitanje glasi

$$x^2 + y^2 + 3x^2y + 3xy^2 = \sigma_1^2 - 3\sigma_1\sigma_2 - 2\sigma_2.$$

3.4. Jedinstvenost prikaza u osnovnom teoremu. Racionalna nezavisnost osnovnih simetričnih funkcija. — 3.4.1. Lema. *Nema nikoje racionalne funkcije* R *koja nije* $\equiv 0$, *za koju bi bilo*

$$(1) \qquad R(\sigma_1(x_1, x_2, \ldots, x_n), \sigma_2(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)) = 0$$

za sve moguće vrijednosti $x_1, x_2, \ldots, x_n$.

Pretpostavimo da, obrnuto, takva racionalna funkcija R postoji. Množeći (1) nazivnikom od R, dobili bismo za brojnik B analogni identitet:

$$(2) \qquad B(\sigma_1(x_1, \ldots), \sigma_2(x_1, \ldots) = 0$$

za *sve izbore* $x_1, x_2, \ldots$, mada B kao funkcija od σ_ν nije $\equiv 0$, tj. iako postoji bar jedan izbor za $\sigma_1, \ldots, \sigma_n$, recimo $\sigma_1', \ldots, \sigma_n'$, za koje je

$$(3) \qquad B(\sigma_1', \sigma_2', \ldots, \sigma_{n'}) \neq 0.$$

No, promatramo li polinom $x^n + \sigma_1' x^{n-1} + \ldots + \sigma'_{n-1} x + \sigma'_n$ i njegova nulamjesta (nula-tačke) $x_1', x_2', \ldots, x_n'$ pa njih u (2) uvrstimo umjesto x-ova, postaje $(2)_1$ izrazom $(3)_1$ pa identitet (2) u tom slučaju daje $(3)_1 = 0$, protivno relaciji (3).

Iz leme 3.4.1. proizlazi *jednoznačnost* u prikazivanju simetričnog polinoma $p(x_1, x_2, \ldots, x_n)$ pomoću $\sigma_1, \ldots, \sigma_n$: kad bi, naime, postojala dva takva prikaza, recimo $P(\sigma_1, \sigma_2, \ldots)$, $P_1(\sigma_1, \sigma_2, \ldots)$, onda bi njihova razlika bila identički $= 0$ kao funkcija x-ova, a ne bi bila $\equiv 0$ kao funkcija sigmâ, što se protivi sadržini gornje leme.

3.5. Primjedba o vrstama zavisnosti. Za funkcije $\sigma_1, \sigma_2, \ldots, \sigma_n$, koje inače zavise od $x_1, x_2, \ldots, x_n$, dokazali smo da su one *racionalno nezavisne*, a specijalno i *polinominalno nezavisne*; one su, dakle, i posebno *linearno nezavisne*. Može se, međutim, dokazati da su funkcije $\sigma_1, \sigma_2 \cdots$ nezavisne u tom smislu da ne postoji nikakva *neprekidna funkcija* f s derivacijama prvog reda za koju bi bilo identički

$$f(\sigma_1, \sigma_2, \ldots, \sigma_n) = 0$$

za *sve izbore x-ova*. Da bismo se u to uvjerili, dovoljno je da se uvjerimo da *funkcionalna determinanta a-ova* po *x-ovima nije* $\equiv 0$.

3.5.1. Može se pokazati (v. Perron [1], sv. I. p. 143) da je ta funkcionalna determinanta jednaka

$$\det\left[\frac{\partial \sigma_i}{\partial x_k}\right] = (-1)^n \sum_{i<k\leqslant n} (x_i - x_k),$$

dakle nije $\equiv 0$.

3.5.2. Da se vidi kako ima smisla promatrati razne vrste vezâ (zavisnosti), pogledajmo funkcije $\cos x$, $\sin x$; one su *funkcionalno*, pa čak i *polinomijalno* zavisne, jer je $\cos^2 x + \sin^2 x - 1 = 0$; naprotiv, te funkcije nisu *linearno* zavisne, jer iz $a\cos x + b\sin x \equiv 0$ (a, b brojevi) nužno izlazi $a = b = 0$.

3.6. Nadopuna osnovnog teorema o simetričnim funkcijama. Nadopuna će se odnositi na stepen dobivenog polinoma, kao i na izobaričnost tog polinoma, ovo u slučaju da je ishodni simetrični polinom *homogen*.

3.6.1. Teorem. *Stupanj polinoma* $P(\sigma_1, \sigma_2, \ldots, \sigma_n)$, *što pripada simetričnom polinomu* $p(x_1, x_2, \ldots, x_n)$, *jednak je* ***najvišem*** *eksponentu u kojem se neka varijabla* x_1 *pojavljuje u* p (Cayley).

Dokaz. Uočimo jednu od varijabli polinoma p, recimo x_1; promatrajmo osnovne simetrične funkcije $\sigma_1', \ldots, \sigma'_{n-1}$ *preostalih* varijabli[1]; te su funkcije *linearno* vezane s osnovnim simetričnim funkcijama $\sigma_1, \ldots, \sigma_n$ *zadanih* promjenljivicâ, jer je očigledno

$$\begin{aligned}
\sigma_1 &= -x_1 + \sigma_1' \\
\sigma_2 &= -x_1\sigma_1' + \sigma_2' \\
&\cdots\cdots\cdots \\
\sigma_{n-1} &= -x_1\sigma'_{n-2} + \sigma'_{n-1} \\
\sigma_n &= -x_1\sigma'_{n-1}.
\end{aligned} \tag{1}$$

Zato je prema jednakosti $p(x_1, x_2, \ldots, x_n) = P(\sigma_1, \ldots, \sigma_n)$ iz teorema 3.1:

$$p(x_1, x_2, \ldots, x_n) \equiv P(-x_1 + \sigma_1',\ -x_1\sigma_1' + \sigma_2', \ldots, -x_1\sigma'_{n-1}). \tag{1}$$

To znači da najviši stepen od x_1 mora biti *isti* i na lijevoj i na desnoj strani tog identiteta (1). No, najviši stepen od x_1 na desnoj strani je najviši stepen od x_1 u polinomu $P(-x_1, -x_1\sigma_1, \ldots, -x_1\sigma'_{n-1})$, a taj je stepen očigledno jednak stepenu polinoma P.

3.7. O težini monoma. U nekim dijelovima matematike varijablama se dodjeljuje stanovit broj, zvan *težina varijabli*; produktu varijabli dodaje se težina koja je suma težina pojedinih faktora produkta; tako npr. ako varijable z_1, z_2, z_3, z_4 imaju težine p_1, p_2, p_3, p_4, tada izraz $5 z_1^2 z_2^3 z_3 z_4^6$ ima težinu $2p_1 + 3p_2 + p_3 + 6p_4$.

Dodijelimo varijablama $x_1, x_2, \ldots, x_n$ broj 1 kao težinu; onda ćemo *osnovnim simetričnim funkcijama* $\sigma_1, \ldots, \sigma_n$ *pridijeliti kao težine njihove indekse*

---

[1] Prema tome stavljamo $\sigma_i' = \sigma_i(x_2, x_3, \ldots, x_n)$.

1, 2, . . . , n; drugim riječima, kako je σ_ν homogen polinom stepena ν, pridijelit ćemo funkciji σ_ν njen stupanj kao težinu varijable σ_ν.

Prema tome, monomu $a\,\sigma_1^{\alpha_1}\sigma_2^{\alpha_2}\cdot\cdot\sigma_n^{\alpha_n}$ pripada težina $\alpha_1+2\,\alpha_2+\cdot\cdot\cdot+nd_n$.

3.7.1. Definicija. *Težina polinoma je najveća težina njegovih članova. Ako svaki član polinoma ima istu tešinu, kaže se da je polinom izobaričan.*

3.7.2. Teorem. *Ako je* $p(x_1, x_2, \ldots, x_n)$ ***homogen*** *simetričan polinom stepena* s, *polinom* P, *za koji je*

$$p \equiv P(\sigma_1, \sigma_2, \ldots, \sigma_n), \tag{1}$$

jest izobaričan i težine s (Brioschi)[1].

Dokaz. Najprije, homogenost stupnja s polinoma $p(x_1, x_2, \ldots, x_n)$ izražava se identitetom (s obzirom na λ):

$$p(\lambda x_1, \lambda x_2, \ldots, \lambda x_n) = \lambda^s p(x_1, x_2, \ldots, x_n). \tag{2}$$

S druge strane, zamijenimo li u identitetu (1) svako x_i sa λx_i, postaje on

$$\lambda^s p(x_1, x_2, \ldots, x_n) \equiv P(\lambda\sigma_1, \lambda^2\sigma_1, \ldots, \lambda^n\sigma_n), \tag{3}$$

jer je svaka osnovna funkcija σ_ν homogen polinom stepena ν. No, ako je $a\,\sigma_1^{\alpha_1}\sigma_2^{\alpha_2}\cdot\cdot\sigma_n^{\alpha_n}$ bilo koji član polinoma $P(\sigma_1, \ldots, \sigma_n)$, onda odgovarajući član u polinomu glasi:

$$a(\lambda\sigma_1)^{\alpha_1}\cdot\cdot(\lambda^n\sigma_n)^{\alpha_n} = a\,\lambda^{\alpha_1+2\alpha_2+\cdots+n\alpha_n}\sigma_1^{\alpha_1}\cdot\cdot\sigma_n^{\alpha_n}. \tag{4}$$

No, prema (3) svaki član polinoma $(3)_2$ sadrži λ^s kao faktor u najvišoj potenciji; drugim riječima, λ se kao faktor u svakom članu polinoma $(3)_2$ javlja u jednu ruku upravo kao λ^s, a u drugu ruku, prema $(4)_1$, tačno kao $\lambda^{\alpha_1+2\alpha_2+\cdots+n\alpha_n}$, što znači da je

$$s = \alpha_1 + 2\,\alpha_2 + \cdot\cdot\cdot + n\,\alpha_n.$$

Kako je posljednja suma baš jednaka *težini* promatranog člana polinoma P, time je teorem potpuno dokazan.

Teoreme 3.1., 3.6.1. i 3.7.2. možemo ukratko izreći kao

—→ **3.8. Osnovni teorem o simetričnim funkcijama.** ***Svaki simetrični polinom*** $p(x_1, \ldots, x_n)$ ***varijablâ*** $x_1, \ldots, x_n$ ***može se napisati na jedan i samo jedan način kao polinom*** $P(\sigma_1, \ldots, \sigma_n)$ ***osnovnih simetričnih funkcija tih varijablâ; stepen dobivenog polinoma je jednak stepenu zadanog polinoma s obzirom na jednu jedinu, inače koju god varijablu*** x_i. ***Ako je polazni polinom*** $p(x_1, \ldots, x_n)$ ***homogen i stepena*** μ, ***dobiveni je polinom*** $P(\sigma_1, \ldots, \sigma_n)$ ***izobaričan i težine*** μ (isp. 19 § 1.2.2).

Kako se Cayleyev i Brioschijev teorem mogu upotrijebiti pri određivanju polinoma P za zadano p, neka posluži ovaj

---

[1] F. Brioschi [Brioski], (1824—1897), talijanski matematičar.

3.8.1. Primjer. Jednostavni simetrični polinom $p=[2, 1, 1]=\Sigma x_1^2 x_2 x_3$ izrazi pomoću osnovnih funkcija $\sigma_1, \sigma_2, \ldots$; tu se sumacija podrazumijeva u tom smislu da umjesto niza $x_1 x_2 x_3$ uzmemo sve moguće nizove po tri nejednaka elementa iz niza $x_1, x_2, \ldots, x_n$ zadanih n veličina.

Kako je polinom p stepena 2 s obzirom na x_1, bit će prema Cayleyu polinom P kvadratan; a kako je p homogeno, bit će prema Brioschiju P izobaričan, i to težine 4; dakle je P nužno oblika

$$P=A\,\sigma_1\,\sigma_3+B\,\sigma_2^2+C\,\sigma_4, \qquad \text{dakle}$$

(1)
$$\sum x_1^2 x_2 x_3=A\,\sigma_1\,\sigma_3+B\,\sigma_2^2+C\,\sigma_4.$$

Birajući broj n varijablâ te vrijednosti tih varijablâ može se dalje odrediti vrijednost koeficijenata A, B, C. Naime, važno je da ti koeficijenti ne zavise od n.

Za $n=3$ izlazi

$$\sigma_4=0, \quad \text{pa za } x_1=0,\ x_2=x_3=1$$

izlazi

$$\sigma_1=-2, \quad \sigma_2=1, \quad \sigma_3=0,$$

pa gornja formula (1) daje

$$0=0+B\cdot 1+0, \quad \text{tj.} \quad B=0.$$

Za $x_1=-1,\ x_2=x_3=1$ dobivamo

$$\sigma_1=-1, \quad \sigma_2=-1, \quad \sigma_3=1=A\cdot -1\cdot 1,$$

dakle

$$x_1^2 x_2 x_3+x_2^2 x_1 x_3+x_3^2 x_1 x_2=A\cdot -1\cdot 1, \quad \text{tj.} \quad -1=-A, \quad \text{tj.} \quad A=1.$$

Za $n=4,\ x_1=x_2=x_3=x_4=1$ dobije se

$$\sigma_1=-4, \quad \sigma_2=6, \quad \sigma_3=-4, \quad \sigma_4=1:$$

$$\sum x_1^2 x_2 x_3=x_1^2 x_2 x_3+x_1^2 x_2 x_4+x_2^2 x_1 x_3+x_2^2 x_1 x_4+x_3^2 x_1 x_2,$$

dakle

$$12=16+C, \quad \text{tj.} \quad C=-4.$$

Drugim riječima,

$$\sum x_1^2 x_2 x_3=\sigma_1\,\sigma_3-4\,\sigma_4,$$

i to *bez obzira na broj n veličinâ* $x_1, \ldots, x_n$.

4. RACIONALNE SIMETRIČNE FUNKCIJE

Neka je

(1)
$$R(x_1, \ldots, x_n)=\frac{A(x_1, \ldots, x_n)}{B(x_1, \ldots, x_n)}$$

racionalna simetrična funkcija veličinâ $x_1, \ldots, x_n$; naravno, A i B su polinomi koje možemo smatrati *neskrativima*. Kako je funkcija (1) simetrična, ostat će ona ista pri svim permutacijama veličinâ $x_1, \ldots, x_n$; odatle specijalno izlazi da polinom B ne može biti $=0$ ni za koju permutaciju varijablâ $x_1, \ldots, x_n$. Može se desiti da je i B simetrično, no u općem slučaju B nije simetričan polinom; označimo li tada sa $B_1, B_2, \ldots, B_q$ sve moguće različite polinome što iz B nastaju permutirajući x-ove, očigledno je da je

$$R(x_1, \ldots, x_n) = \frac{A B_1 B_2 \cdots B_q}{B B_1 B_2 \cdots B_q} \tag{2}$$

i da je nazivnik u $(2)_2$ simetričan polinom x-ova. Kako je i R simetrično, simetričan je i brojnik u $(2)_2$. Dokazali smo, dakle,

4.1. Teorem. *Svaka racionalna simetrična funkcija veličina $x_1, \ldots, x_n$ može se prikazati kao kvocijent od dva **simetrična polinoma** tih istih veličina.*

Zato se izučavanje racionalnih simetričnih *funkcija* svodi na izučavanje simetričnih *polinoma*.

5. SIMETRIČNE FUNKCIJE I ALGEBARSKE JEDNADŽBE

Gornji osnovni teorem 3.8. o simetričnim polinomima možemo ovako izreći:

⟶ **5.1. Teorem.** ***Svaki simetrični polinom nulatačaka algebarskog normiranog polinoma $b = x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$ može se prikazati kao polinom koeficijenata $b_0, b_1, b_2, \ldots, b_{n-1}$ tog polinoma. Općenitije, svaka racionalna simetrična funkcija nulatačaka algebarskog polinoma***

$$c = c_0 + c_1 x + c_2 x^2 + c_n x^n$$

može se prikazati kao racionalna funkcija koeficijenata toga polinoma.

Prvi dio teorema je očigledan, jer su, prema Viète-u (§ 1.2.1), b-ovi osnovne simetrične funkcije nulatačaka normiranog polinoma. U drugu ruku, polinom c ima ista nulamjesta kao polinom c/c_n što nastaje iz c dijeleći ga koeficijentom c_n najstarijeg člana. Neka je tada R racionalna funkcija nulištâ $x_1, \ldots, x_n$ polinoma c/c_n: tada je $R = A/B$, gdje su A, B simetrični polinomi od $x_1, \ldots, x_n$; prema osnovnom teoremu, A i B su polinomi s obzirom na koeficijente $\frac{c_0}{c_n}, \frac{c_1}{c_n}, \ldots$ polinoma c/c_n; dakle su A i B, a time i njihov kvocijent R, racionalne funkcije koeficijenata zadanog polinoma c.

6. RACIONALNE FUNKCIJE KORIJENA ALGEBARSKE JEDNADŽBE

6.1. Neka su $x_\nu (\nu = 1, 2, \ldots, n)$ nula-tačke algebarskog polinoma $p(x)$ stepena n. Neka je $R(x_1) = \frac{A(x_1)}{B(x_1)}$ racionalna funkcija nulatačke x_1. Dokazat ćemo da se $R(x_1)$ može dobiti iz x_1 i pomoću *prve tri računske operacije*.

Možemo pretpostaviti da ni jedan od brojeva $A(x_\nu)$, $B(x_\nu)$ nije $=0$; tada je, naravno,

$$R(x_1)=\frac{A(x_1)B(x_2)\cdot\cdot\cdot B(x_n)}{B(x_1)B(x_2)\cdot\cdot\cdot B(x_n)}. \tag{1}$$

No, tu su brojnik i nazivnik simetrične cijele racionalne funkcije nulatačaka. Specijalno je nazivnik simetrična cijela racionalna funkcija nulatačaka polinoma p; zato je on cijela racionalna funkcija *koeficijenata toga polinoma* (isp. § 5.1.). I funkcija

$$B(x_2)B(x_3)\cdot\cdot\cdot B(x_n) \tag{2}$$

je simetričan polinom nula-tačaka polinoma $\frac{p(x)}{x-x_1}$; ovome su koeficijenti polinomi s obzirom na x_1. Odatle proizlazi da je (2) cijela racionalna funkcija od x_1, a time prema (1) i $R(x_1)$ je cijela racionalna funkcija $P(x_1)$ od x_1, tj. $R(x_1)$ se iz x_1 može dobiti i pomoću prve tri računske operacije. Tvrdimo da možemo suponirati da je stepen od $P(x_1)$ manji od stepena n zadanog polinoma p; možemo, naime, uvijek napisati po osnovnoj lemi o diobi polinoma (poglavlje 7 § 4.1):

$$P(x)=p(x)\,q(x)+r(x), \quad \text{sa } 0=r \quad \text{ili} \quad 0\leq \operatorname{st} r<\operatorname{st} p.$$

Odatle za $x=x_1$ izlazi, zbog $p(x_1)=0$:

$$P(x_1)=r(x_1),$$

za čim se i ide.

Zaključak je općenit:

—→ **6.2.** Teorem. *Svaki racionalni izraz $R(x_1, x_2, \ldots, x_n)$ nulatačaka algebarskog polinoma $p(x)$ može se dobiti iz tih nula-tačaka već pomoću tri prve racionalne operacije.*

Naime, izraz $R(x_1, \ldots, x_n)$ kao racionalna funkcija od x_1 može se predstaviti kao polinom s obzirom na x_1, recimo

$$R(x_1, x_2, \ldots, x_n)=R_0+R_1\cdot x_1+\cdot\cdot\cdot+R_{n-1}\,x_1^{n-1},$$

gdje su $R_0, \ldots, R_{n-1}$ racionalni izrazi prema $x_2, \ldots, x_n$. Svaki od njih je, iz istog razloga, polinom s obzirom na x_2, što znači da se $R(x_1, x_2, x_3, \ldots)$ može izraziti kao polinom s obzirom na x_1, x_2 s koeficijentima koji racionalno zavise od preostalih nula-tačaka x_3, $x_4\cdot\cdot\cdot$ Zaključujući slično na x_3 itd., dolazimo do uvjerenja da je teorem istinit.

6.3. Primjedba. Valja dobro imati na umu da se kod gornjih teorema radi o (racionalnim) funkcijama koje su definirane samo u skupu nula-tačaka polinoma p. Naravno da u općem slučaju *racionalna* funkcija u nekom skupu S nije isto što i *cijela racionalna funkcija* u tom skupu S; no racionalna funkcija u posebnom skupu Sp nula-tačaka polinoma p *uvijek je jednaka jednom polinomu u istom skupu Sp.*

7. RACIONALIZACIJA NAZIVNIKA (IMENIOCA)

7.1. Zadana je cjeloracionalna funkcija $c(x)$ s koeficijentima c_ν u nekom tijelu K (npr. Q); nadalje je zadana razlomljeno-racionalna funkcija $a(x)/b(x)$ sa koeficijentima a_i, b_j iz K i sa svojstvom da su $b(x)$, $c(x)$ međusobno prosti.

Tada se traži da se uz uslov $c(x_1)=0$ vrijednost

(1) $$a(x_1)/b(x_1)$$

napiše kao *cjeloracionalan izraz s koeficijentima iz K.*

Neka je $x_1, x_2, \ldots, x_n$ spektar polinoma $c(x)$; kako je $b(x_\nu)\neq 0$ bit će

(2) $$\frac{a(x_1)}{b(x_1)}=\frac{a(x_1)\,b(x_2)\cdots b(x_n)}{b(x_1)\,b(x_2)\cdots b(x_n)}.$$

Novi nazivnik u (2) je simetrična funkcija od $x_1, \ldots, x_n$; zato se on može cjeloracionalno izraziti pomoću koeficijenata $c_1, \ldots, c_n$, pa je vrijednost novog nazivnika u (2) neki član B iz K; zato je

(3) $$\frac{a(x_1)}{b(x_1)}=B^{-1}\cdot a(x_1)\,b(x_2)\cdots b(x_n).$$

U (3) se javlja i simetrična cjeloracionalna funkcija

(4) $$b(x_2)\cdots b(x_n)$$

veličinâ $x_2, \ldots, x_n$; zato se (4) može cjeloracionalno izraziti pomoću odgovarajućih osnovnih simetričnih funkcija

(5) $$\sigma'_{\nu'}(x_2, \ldots, x_n)\ (\nu'=1, 2, \ldots, n-1).$$

No, osnovne funkcije $\sigma_\nu=\sigma_\nu(x_1, x_2, \ldots, x_n)$ i funkcije (5) vezane su relacijama (1) iz § 3.6.1, iz kojih izvire

(6) $$\begin{aligned}\sigma_1' &= \sigma_1+x_1=c_{n-1}+x_1\\ \sigma_2' &= \sigma_2+x_1\sigma_1'=\alpha_2+x_1\sigma_1+x_1^2=c_{n-2}+c_{n-1}x_1+x_1^2\\ &\ldots\ldots\ldots\ldots\ldots\ldots\\ \sigma_{n-1}' &= \sigma_{n-1}+x_1\sigma_{n-2}'=c_1+c_2x_1.\end{aligned}$$

To znači da se (4) a time i $(4)\cdot a(x_1)$ može izraziti cjeloracionalno pomoću c_ν, x_1; stavimo li $(4)=A(x_1)$, tada prema (3) imamo

$$\frac{a(x_1)}{b(x_1)}=B^{-1}\cdot a(x_1)\cdot A(x_1),$$

pa je cilj postignut.

7.2. Primjer. Racionaliziraj $\frac{1}{3+x_1}$ ako je $x_1^3-2x_1-2=0$. Imamo

$$\frac{1}{3+x_1}=\frac{(3+x_2)(3+x_3)}{(3+x_1)(3+x_2)(3+x_3)},$$

$$(3+x_1)(3+x_2)(3+x_3)=27+9(x_1+x_2+x_3)+3(x_1x_2+x_1x_3+x_2x_3)+$$
$$+x_1x_2x_3=27-9\sigma_1+3\sigma_2-\sigma_3.$$

Prema Viète-ovim formulama imamo

$$\sigma_1=0,\quad \sigma_2=-2,\quad \sigma_3=-2,$$

pa posljednji izraz daje $B=23$. Dakle je

$$\frac{1}{3+x_1}=\frac{1}{23}(3+x_2)(3+x_3).$$

$$(3+x_2)(3+x_3)=9-3\sigma_1'+\sigma_2'=9-3(\sigma_1+x_1)+(\sigma_2+x_1\sigma_1+x_1^2)=$$
$$=9-3x_1+(-2+x_1^2)=7-3x_1+x_1^2\equiv A(x_1).$$

Dakle je

$$\frac{1}{3+x_1}=\frac{1}{23}(7-3x_1+x_1^2)=\frac{7}{23}-\frac{3}{23}x_1+\frac{1}{23}x_1^2.$$

8. Zadaci o simetričnim funkcijama i vezama među koeficijentima i ništištima (nulatačkama) polinoma.

1. Nađi osnovne simetrične funkcije ovih veličina: 1) x, y, z; 2) x_1, x_2, x_3, x_4; 3) x_1, x_2, x_3, x_4, x_5; 4) 2, 5, 6; 5) $-1, 1, 0$; 6) $1, 2, 3, 4, \ldots, n$.

2. Za gornje veličine nađi ove funkcije: 1) s_2; 2) s_3; 3) [1, 1, 2]; 4) [2, 1]; 5) [1, 2, 3]; 6) [−1]; 7) [−1, 2].

3. Koliko članova ima polinom [2, 1], ako on ima 2, 3, 4, 5, 6, ..., n varijabla?

3.[a] Isto pitanje za polinom [1, 2, 3].

4. Koje su od ovih funkcija simetrične a koje nisu: 1) $3x^2+3y^2-xy$; 2) $x+2y^2$; 3) $x+2y^2+y$; 4) $x+2y^2+y+2y^2$; 5) $x+2y^2+y++2x^2-3xy$; 6) $3x+3y+3z-2x^2y-2y^2x-2x^2z-2xz^2-2yz^2--2y^2z+xyz$; 7) $\begin{vmatrix} x & y & z \\ x^2 & y^2 & z^2 \\ x^3 & y^3 & z^3 \end{vmatrix}$; 8) $(x_1+x_2)(x_1+x_3)(x_1+x_4)$ $(x_2+x_3)(x_2+x_4)(x_3+x_4)$; 9) $(x_1-x_2-x_3)(x_2-x_3-x_1)(x_3-x_1-x_2)$.

5. Simetrične funkcije iz zad. 3 prikaži kao sumu Σ-funkcija.

6. Neka je S_n skup simetričnih polinoma u $x_1, x_2, \ldots, x_n$ s koeficijentima u skupu 1) N; 2) D; 3) Q; 4) R; 5) A; 6) $R(i)$. Da li je a] $(S_n, +)$, b] $(S_n, -)$, c] $(S_n, \cdot)$ d] $(S_n, :)$ grupoid?

7. Izrazi pomoću osnovnih simetričnih funkcija ove izraze:
1) [2]; 2) [3]; 3) [1, 2]; 4) [1, 3]; 5) [1, 2, 3]; 6) [2, 2, 1]; 7) [4, 1, 1]; 8) [2, 2, 2]; 9) [1, 5]; 10) [1, 1, 2, 2]. Konkretiziraj npr. $n=5$.

8. Isto pitanje za ove izraze: 1) $x^3+y^3+z^3-xyz$; 2) $x^4+y^4+z^4-$ $-2(xy)^2-2(yx)^2-2(xz)^2$; 3) $(x+y)(y+z)(z+x)$;
4) $(x-y)^2(y-z)^2(z-x)^2$.

9. Izrazi pomoću osnovnih simetričnih funkcija ove simetrične funkcije:
1) $\sum_{i<k}(x_i-x_k)^2$; 2) $\sum_{i<k}(x_i+x_k)^4$; 3) $\sum_{i<k}(x_i+x_k)^3$;
4) $\sum_{i<k}(x_i+x_k-x_m)^2$.

10. Isto pitanje za simetričnu funkciju $\sum_{p}(z_1 x_{p_1}+z_2 x_{p_2}+\cdots+z_n x_{p_n})^2$, pri tom p prolazi skupom svih permutacija brojeva $1, 2, \ldots, n$; nadalje, $z_1, z_2, \ldots, z_n$ je zadan niz brojeva.

11. Naći $s_1, s_2, s_3, \ldots, s_k$ za spektar polinoma: 1) x^2+1; 2) x^3-1.

12. Izračunaj na dva načina izraz s_2, s_3, s_4, s_5 za jednadžbu $x^2-5x+6=0$; proba!

13. Odredi težinu ovih izraza: 1) $x_1 x_2$; 2) $3x_1^2+3x_2^2$; 3) $5x_1x_2-$ $-x_1^2+x_3^3$; 4) $\sigma_2^2+\sigma_3$; 5) $3\sigma_1^3-2\sigma_2^2\sigma_3+\sigma_4$; 6) $\sigma_1\sigma_2\sigma_3-\sigma_3^2$; 7) s_2; 8) $s_3^2-\sigma_4^2+\sigma_1^6$; 9 $\sigma_n s_n+\sigma_{n-1}^2 s_{n-1}^2$; 10) $\sum_{i=1}^{n}\sigma_i s_i$; pri tom su $\sigma_1, \sigma_2, \ldots$ osnovne simetrične funkcije.

14. Odredi ove simetrične funkcije za odgovarajuću jednadžbu:
1) [1, 2], [2, 3] za $x^2-5x+6=0$,
2) [1, 2], [1, 4] za $3x^3-5x^2+1=0$,
3) [3, 3], [3, 4] za $2x^3+5x-1=0$,
4) [3, 3], [3, 4] za $x^4+2x^3+5x-1=0$.

15. Ako je x_1, x_2, x_3 spektar jednadžbe $a_0x^3+a_1x^2+a_2x+a_3=0$ izrazi pomoću a_0, a_1, a_2, a_3 ove simetrične funkcije:
1) $a_0^4(x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2$;
2) $a_0^4(x_1^2-x_2x_3)(x_2^2-x_3x_1)(x_3^2-x_1x_2)$;
3) $a_0^4(x_1^2+x_1x_2+x_2^2)(x_2^2+x_2x_3+x_3^2)(x_3^2+x_3x_1+x_1^2)$;
4) $(x_1^3+2x_1x_2^2)(x_2^3+2x_2x_3^2)(x_3^2+2x_3x_1^2)$;
5) $(x_1-x_2)^2(x_1x_2)^{-1}+(x_2-x_3)^2(x_2x_3)^{-1}+(x_3-x_1)^2(x_3x_1)^{-1}$.

Konkretiziraj za jednadžbu $3x^3-5x^2+1=0$.

16. Neka se odredi uslov tako da među rješenjima $x_1, x_2, \ldots$ jednadžbe postoji ovakva veza: 1) $x^2+3x-5m=0$, $x_1x_2=1$; 2) $x^2+3x-5m=0$, $x_1+x_2=0$; 3) $x^2+5x-5m=0$, $x_1x_2+x_1-x_2=0$; 4) x^3+ax^2+ $+bx+c=0$, $x_1+x_2=x_3$, 5) $x^3+ax^2+bx+c=0$, $x_1-x_2=x_2-x_3$; 6) $x^3+ax^2+bx+c=0$, $x_1x_2=x_3$; 7) $x^3+ax^2+bx+c=0$; $x_1:x_2=$ $=x_2:x_3$; 8) $x^3+px+q=0$, $x_1x_2=x_3^{-1}$; 9) $x^4+3x^3+4x^2+mx-5=0$, $x_1+x_2=x_3+x_4$; 10) $x^4+5x^3+mx^2+3x+5=0$, $x_1x_2=1$;
11) $x^4+ax+b=0$, $x_1x_2+\lambda(x_1+x_2)+\mu=0$, $x_3x_4+\lambda(x_3+x_4)+\mu=0$; tu su λ, μ poznati brojevi.

17. Naći s_3, s_5, s_7 za: 1) $x^3-3x=0$, 2) $x^3-3x-1=0$.

18. Naći $s_1, s_2, \ldots, s_n$ za $x^n+\frac{1}{1!}x^{n-1}+\frac{1}{2!}x^{n-2}+\ldots+\frac{1}{n!}=0$.

19. Za svaku jednadžbu stepena 3 vrijedi $\frac{s_1^5-s_5}{s_1^3-s^3}=\frac{5}{3}(\sigma_1^2-\sigma_2)$.

20. Dokaži:

1) $s_k=\begin{vmatrix} a_1 & 1 & & \\ 2a_2 & a_1 & 1 & \\ 3a_3 & a_2 & a_1 & \\ \cdot & & \cdot & \\ \cdot & & & \cdot \\ \cdot & & & \\ ka_k & a_{k-1} & \cdots & a_2\ a_1 \end{vmatrix}$ 2) $a_k=\frac{1}{k!}\begin{vmatrix} s_1 & 1 & & & \\ s_2 & s_1 & 2 & & \\ s_3 & s_2 & a_1 & 3 & \\ \cdot & & & \cdot & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ s_k & s_{k-1} & & & s_1 \end{vmatrix}$.

Ispisati izraze za slučaj $k=2, 3, 4$.

21. Ako je zbroj korijena jednadžbe stepena 4 jednak 0, tada je

$$\frac{s_5}{5}=\frac{s_2}{2}\cdot\frac{s_3}{3}.$$

22. Odredi jednadžbu stupnja n za koju je: 1) $s_1=s_2=\ldots=s_{n-1}=0$ odnosno 2) $s_2=s_3=\ldots=s_n=0$ odnosno 3) $s_2=1$, $s_3=s_4=\ldots=s_{n+1}=0$.

23. 1) Nađi s_k za jednadžbu $\Phi_n(x)=0$ dijeljenja kruga; 2) za $X_n(x)=0$ vrijedi $\sigma_2, \sigma_3, \sigma_4\in\{0, 1, -1\}$.

24. Za jednadžbu $x^3+px+q=0$ nađi: 1) $[1, 1, -1]=\sum x_1x_2x_3^{-1}$;
2) $\sum x_1(1+x_1)^{-1}$; 3) $\sum x_1^2(1+x_2)^{-1}(1+x_3)^{-1}$; 4) $\sum x_1x_2^{-1}=[1, -1]$
5) $\sum x_1^2(1+x_1)^{-1}$.

25. Ako je $x_1, x_2, \ldots, x_n$ spektar od $x^n+a_1x^{n-1}+\ldots+a_n=0$ dokaži da se svaki simetrični polinom od $x_2, x_3, \ldots, x_n$ može izraziti kao polinom od x_1.

26. 1) Odredi matricu f za koju je $f_{ik}=\frac{\partial\sigma_i}{\partial x_k}$;

2) nađi $\sum_{k=1}^{n}\frac{\partial\sigma_i}{\partial x_k}$; 3) $\det f$.

27. Ako je $p(x_1, x_2, \ldots, x_n)=P(\sigma_1, \sigma_2, \ldots, \sigma_n)$, tada je

$$\sum_k\frac{\partial p}{\partial x_k}=n\frac{\partial P}{\partial\sigma_1}+(n-1)\sigma_1\frac{\partial P}{\partial\sigma_2}+(n-2)\sigma_2\frac{\partial P}{\partial\sigma_3}+\ldots+\sigma_{n-1}\frac{\sigma P}{\partial\sigma_n}.$$

28. Dokaži $\det\left[\frac{\partial \sigma_i}{\partial x_k}\right]=(-1)^n \prod_{i<k\leqslant n}(x_i-x_k)$.

29. Za cijele racionalne funkcije $a(x)$, $b(x)$ dokaži da je simetrična funkcija $\sum_i b(x_i)$ korijena x_i jednadžbe $a(x)=0$ upravo koeficijent od x^{-1} u razvoju po x funkcije $\frac{a'(x)\,b(x)}{a(x)}$.

Obradi posebno slučaj kad $a(x)$ znači a^n-1.

30. Odredi simetričnu funkciju $\prod_i (1-x_i)$, pri čemu x_i prolazi spektrom cijele racionalne funkcije $a(x)$; obradi specijalno slučaj

$$a(x)=1+x+x^2+\cdots+x^{n-1}.$$

31. Racionaliziraj nazivnik u $\frac{2x_1+1}{3x_1+2}$ ako x_1 zadovoljava jednadžbu:

1) $3x^2+5x-1=0$; 2) $x^3+2x^2+5x-1=0$;

3) $x^4+x^3+2x^2+5x-1=0$.

Literatura

Faddeev-Sominskij [1]; Kuroš [1]; Obreškov [1], [2]; Perron [1]; Plemelj [1]; Serret [1]; Weber [1].

POGLAVLJE 20.

O ELIMINACIJI. REZULTANTA. DISKRIMINANTA

Idejna postavka. Često se postavlja pitanje kako *eliminirati* (ukloniti, isključiti) stanovitu veličinu ili veličine iz zadanih relacija. Idejno je prirodno da *uočimo veličinu koju želimo ukloniti, izračunamo je iz jedne relacije, a onda s tim rezultatom idemo u drugu relaciju.*

Time ćemo uočenu veličinu ukloniti, isključiti.

Primjer. Neka je

$$3x+4=0$$

$$x^2-5ax-a=0.$$

Tu se pojavljuje x u obje relacije. Iz prve izlazi $x=-3^{-1}4$, pa zato druga postaje $3^{-2}4^2+5a3^{-1}4-a=0$; u njoj više nema x.

Specijalno se dešava da je *zadano više relacija* nego što ima veličinâ; u tom slučaju općenito sistem nema rješenja. A da rješenje postoji, potrebno je da budu ispunjeni *dodatni zahtjevi.* Tako je npr. jasno da općenito sistem $a(x)=0, b(x)=0$ nema rješenja. Skup od više jednadžbi nego što ima nepoznanica u općem slučaju također neće imati rješenja.

1. REZULTANTA ILI ELIMINANTA DVAJU ALGEBARSKIH POLINOMA

1.1. Zadani su algebarski polinomi

$$a(x)\equiv a_0+a_1x+a_2x^2+\cdots+a_\alpha x^\alpha,$$

$$b(x)\equiv b_0+b_1x+b_2x^2+\cdots+b_\beta x^\beta$$

stupnja α, odnosno β. Kad će oni imati zajedničku nulatačku, odnosno kad će jednadžbe

$$a(x)=0,\ b(x)=0 \tag{1}$$

biti zadovoljene istim brojem x?

Naravno, uz te jednadžbe postoje i jednadžbe

$$x^m a(x)=0$$

$$x^n b(x)=0$$

za bilo koje brojeva m, n koji su $\neq 0$.

Posebno bismo tako dobili jednadžbe:

$$
\begin{aligned}
x^{\beta-1}\, a(x) &= 0\\
x^{\beta-2}\, a(x) &= 0\\
&\ldots\ldots\\
x\, a(x) &= 0\\
a(x) &= 0\\
x^{\alpha-1}\, b(x) &= 0\\
x^{\alpha-2}\, b(x) &= 0\\
&\ldots\ldots\\
b(x) &= 0,
\end{aligned}
$$

odnosno eksplicite

$$
\begin{array}{ll}
a_\alpha x^{\alpha+\beta-1} + a_{\alpha-1} x^{\alpha+\beta-2} + \cdots + a_0 x^{\beta-1} & = 0\\
0\, x^{\alpha+\beta-1} + a_\alpha\, x^{\alpha+\beta-2} + \cdots + a_1 x^{\beta-1} + a_0 x^{\beta-2} & = 0\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\
\qquad\qquad a_\alpha x^\alpha + a_{\alpha-1} x^{\alpha-1} + \cdots + a_1 & = 0\\
b_\beta x^{\alpha+\beta-1} + b_{\beta-1} x^{\alpha+\beta-2} + \cdots + b_0 x^{\alpha-1} & = 0\\
0\, x^{\alpha+\beta-1} + b_\beta\, x^{\alpha+\beta-2} + \cdots + b_1 x^{\alpha-1} + b_0 x^{\alpha-2} & = 0\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\
\qquad\qquad b_\beta x^\beta + b_{\beta-1} x^{\beta-1} + \cdots + b_0 & = 0.
\end{array} \tag{3}
$$

Tu imamo $\alpha+\beta$ linearnih homogenih veza za $\alpha+\beta$ veličinâ

$$x^{\alpha+\beta-1},\ x^{\alpha+\beta-2}, \ldots, x^2, x, 1. \tag{4}$$

Kako ove veličine (4) nisu sve $=0$, znači to da *determinanta sistema* jednadžbi (3) mora biti jednaka 0 (isp. 13 § 7.3). Ta determinanta zove se *rezultanta ili eliminanta polinomâ a i b*; označuje se sa $R(a; b)$; dakle

1.2. (Definicija). *Rezultanta ili eliminanta algebarskih polinoma*

$$a(x) = a_0 + a_1 x + \cdots + a_\alpha x^\alpha,$$
$$b(x) = b_0 + b_1 x + \cdots + b_\beta x^\beta, \quad \text{gdje je}$$

$\alpha = \operatorname{st} a$, $\beta = \operatorname{st} b$, označuje se sa $R(a, b)$ i glasi ovako:

$$
R(a,b) \overset{\text{def}}{=\!=}
\overset{\longleftarrow\ \operatorname{st} a + \operatorname{st} b\ \longrightarrow}{
\begin{vmatrix}
a_\alpha, & a_{\alpha-1}, & a_{\alpha-2}, \ldots a_1, & a_0, & 0, & 0, \ldots\\
0 & a_\alpha & , a_{\alpha-1}, \ldots & a_1, & a_0, & 0, \ldots\\
0 & 0 & \ldots\ldots\ldots\ldots & & & \\
\ldots & \ldots & \ldots\ldots\ldots\ldots & & & \\
0 & 0 & 0 \ \ldots 0 & a_\alpha & \ldots a_1, & a_0\\
b_\beta, & b_{\beta-1}, & b_{\beta-2} \ldots b_1, & b_0 & 0 & 0 \ldots\\
0 & b_\beta & b_{\beta-1} \ldots\ldots b_1 & b_0 & 0 & \ldots\\
\ldots & \ldots & \ldots\ldots\ldots\ldots & & & \\
0 & 0 & 0 \ \ldots 0 & b_\beta & \ldots b_1, & b_0
\end{vmatrix}} \tag{5}
$$

U slučaju da je a konstanta $\neq 0$, stavlja se $R(a,b)=a^{\text{st}\,b}$; ako je b konstanta $\neq 0$, stavlja se $R(a,b)=b^{\text{st}\,a}$; ako je a konstantno i $\neq 0$ te ako je b konstanta $\neq 0$, stavlja se $R(a,b)=1$. Time je $R(a,b)$ definirano za svako $a\,\text{non}\equiv 0$ i svako $b\,\text{non}\equiv 0$. Npr.

$$R(3x-2,\ 4x^2-5x+1)=\begin{vmatrix} 3 & -2 & 0 \\ 0 & 3 & -2 \\ 4 & -5 & 1 \end{vmatrix}=3\cdot -7+4\cdot 4=-5.$$

Zato funkcije $3x-2,\ 4x^2-4x+1$ nemaju nikojeg zajedničkog nulamjesta.

1.3. Dobili smo ovaj rezultat: *ako polinomi* $a(x)$, $b(x)$ *imaju koju nulatačku zajedničku, onda njihova rezultanta mora biti* $=0$.

1.4. Dokažimo da važi i obrat: *ako je* $R(a(x),b(x))=0$, *tada skup jednadžbi* $a(x)=0$, $b(x)=0$ *ima bar jedno rješenje.*

No, to što determinanta R iščezava, znači da je volumen paralelepipeda nad stupcima determinante jednak 0 pa zato u prostoru $E_{\alpha+\beta}$ od $\alpha+\beta$ dimenzija postoji jedan nenulti niz (vektor)

$$v=v_0, v_1, \ldots, v_{\alpha+\beta-1} \tag{6}$$

koji je okomit na svakom stupcu determinante R; to znači da sistem linearnih jednadžbi

$$v_0 R_{i,0}+v_1 R_{i,1}+\cdots+v_{\alpha+\beta-1} R_{i,\alpha+\beta-1}=0 \quad (i=0,1,2,\ldots,\alpha+\beta-1) \tag{7}$$

dopušta nenulto rješenje.

Pomnožimo jednadžbe (7) po redu sa $x^{\alpha+\beta-1}, x^{\alpha+\beta-2}, \ldots, x^2, x, 1$ pa ih saberimo; izlazi jednadžba

$$\begin{aligned}(v_0 x^{\beta-1}+v_1\ x^{\beta-2}+\cdots+v_{\beta-1})\ \ a(x)+ \\ +(v_\beta x^{\alpha-1}+v_{\beta+1} x^{\alpha-2}+\cdots+v_{\alpha+\beta-1})\,b(x)=0\end{aligned} \tag{8}$$

za svako x.

Tvrdimo da među prvih β članova niza (6) ima bar jedan koji je $\neq 0$. U obrnutom slučaju bilo bi

$$v_0=0=v_1=\cdots=v_{\beta-1}, \tag{9}$$

pa bi se identitet (8) reducirao na identitet

$$(v_\beta x^{\alpha-1}+v_{\beta+1} x^{\alpha-2}+\cdots)\,b(x)\equiv 0,$$

a ovo dalje, zbog $b\,\text{non}\equiv 0$, na identitet

$$v_\beta x^{\alpha-1}+v_{\beta+1} x^{\alpha-2}+\cdots+v_{\alpha+\beta-2} x+v_{\alpha+\beta-1}\equiv 0,$$

a ovo dalje na

$$v_\beta=0,\ v_{\beta+1}=0,\ldots,\ v_{\alpha+\beta-1}=0. \tag{10}$$

Taj niz v bio bi nula-niz, protivno pretpostavci.

Na isti način zaključujemo da ni niz (10) nije sastavljen od samih 0. Drugim riječima, za polinome

$$f(x)=v_0 x^{\beta-1}+v_1 x^{\beta-2}+\cdots+v_{\beta-1}$$

$$g(x)=v_\beta x^{\alpha-1}+v_{\beta+1} x^{\alpha-2}+\cdots+v_{\beta+\alpha-1}$$

vrijedi

$$f \text{ non}\equiv 0,\ g \text{ non}\equiv 0,\quad \text{st}\, f<\text{st}\, b,\quad \text{st}\, g<\text{st}\, a.$$

Prema (8) vrijedi identitet

$$a(x) f(x)=-b(x) g(x).$$

To znači da je svaki linearni faktor od $a(x)$ divizor od b ili od g; no zbog $\text{st}\, a>\text{st}\, g$ ne može svaki linearni faktor od a biti linearni faktor od g; postoji, dakle, bar jedan linearni faktor od a koji je linearni faktor i od b; to znači da polinomi a, b *imaju bar jedan zajednički linearni faktor*, tj. bar jednu zajedničku nulatačku. A to smo upravo željeli saznati.

Time smo dokazali ovaj

—→ **1.5. Teorem.** ***Nuždan i dovoljan uslov da dva algebarska polinoma $a(x)$, $b(x)$ imaju bar jednu zajedničku nula-tačku, odnosno da sistem algebarskih jednadžbi***

$$a(x)\equiv a_0+a_1 x+a_2 x^2+\cdots+a_\alpha x^\alpha=0$$

$$b(x)\equiv b_1+b_1 x+b_2 x^2+\cdots+b_\beta x_\beta=0$$

bude zadovoljen bar jednim brojem x, sastoji se u tome da rezultanta $R(a,b)$ tih polinoma a, b bude $=0$.

Može se pokazati da vrijedi ovaj

1.6. Ooći teorem. *Neka su $a(x), b(x)$ dva algebarska polinoma; neka je aMb njihov najveći zajednički divizor, a $R(a,b)$ rezultanta tih polinoma a, b. Tada je:* $\text{rang}\ R(a,b)=st\, a+st\, b-st\,(a\,Mb)$. (Isp. Perron I. str. 205).

2. SVOJSTVA REZULTANTE

2.1. Vrijednost rezultante $R(x-k,\ b(x))$ je $b(k)$.

Neka je k konstanta. Tada je

$$R(x-k, b(x))=\begin{vmatrix} 1 & -k & & & \\ 0 & 1 & -k & & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & & & 1 & -k \\ b_\beta & b_{\beta-1}+\cdots & b_1 & & b_0 \\ k^\beta & k^{\beta-1} & k & & + \end{vmatrix} = \text{(stupce množi po redu sa } k^\beta, k^{\beta-1}, \ldots, k \text{ i sve dodaj posljednjem stupcu)} =$$

$$= \begin{vmatrix} 1 & -k & \cdots & 0 \\ 0 & 1 & -k \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ b_\beta & b_{\beta-1} & \cdots b_1 & b(k) \end{vmatrix} = (\text{razvij po posljednjem stupcu}) = b(k).$$

Dakle je $$R(x-k, b(x)) = b(k).$$

Rezultanta od $x-k$ i $b(x)$ za svaku konstantu k iznosi $b(k)$, tj.

$$b_\beta \cdot (k-b_{(1)})(k-b_{(2)}) \cdots (k-b_{(\beta)}),$$

gdje je $b_{(1)} \cdots b_{(\beta)}$ potpun niz nulatačaka polinoma b; naravno, $\beta = \operatorname{st} b$; b_β je najugledniji koeficijent polinoma b. Dakle je

$$R(x-k, b(x)) = b(k) = b_\beta (-1)^\beta (b_{(1)}-k)(b_{(2)}-k) \cdots (b_{(\beta)}-k).$$

Prema tome, možemo slutiti da će i u općem slučaju rezultanta $R(a(x), b(x))$ u svojoj suštini biti produkt od izrazâ

$$a_\alpha^\beta (a(b_{(1)})(a(b)_{(2)}) \cdots (a(b_{(\beta)}),$$

odnosno

$$b_\beta^\alpha (b(a_{(1)})(b(a_{(2)}) \cdots (b(a_{(\alpha)}).$$

To ćemo moći i dokazati (v. § 2.3).

2.2. Teorem. *Operator R uzimanja rezultante je distributivan prema množenju polinoma:*

(1) $$R(ab, c) = R(a, c)\, R(b, c) \text{ i } R(p \cdot q \cdot r \cdots, u) = R(p, u) \cdot R(q, u) \cdot R(r, u) \cdots$$

Dokaz. Za polinome $a(x) = \Sigma a_i x^i$, $b(x) = \Sigma b_i x^i$, $\operatorname{st} a = \alpha$, $\operatorname{st} b = \beta$ produkt ab je polinom $(ab)(x) = \sum_{i=0}^{\alpha+\beta} (ab)_i x^i$, pri čemu su koeficijenti tog produkta po redu

$$(ab)_0 = a_0 b_0,\ (ab)_1 = a_0 b_1 + a_1 b_0,$$

(2) $$(ab)_2 = a_0 b_2 + a_1 b_1 + a_2 b_0, \ldots$$

$$(ab)_k = \sum_{i+j=k} a_i b_j, \ldots, (ab)_{\alpha+\beta} = a_\alpha b_\beta.$$

Rezultanta polinomâ ab, c je po definiciji:

(3) $$R(ab, c) = \begin{vmatrix} (ab)_{\alpha+\beta} & (ab)_{\alpha+\beta-1} \cdots (ab)_0 & \cdots & \\ \cdots & \cdots & \cdots & \} \gamma \\ & (ab)_{\alpha+\beta} \cdots (ab)_0 & & \\ & c_\gamma \cdots c_0 & & \\ & \cdots & & \} \alpha+\beta \\ & c_\gamma \cdots c_0 & & \end{vmatrix}$$

Izvršimo nekoje transformacije na toj determinanti kako bismo u retke $\gamma+1, \gamma+2, \ldots, \gamma+\alpha$, uveli koeficijente produkta (bc).

Najprije je očigledno (prvi redić c-ova pomnoži sa b_β, a vani sa b_β^{-1}) gornja determinanta =

$$= b_\beta^{-1} \left| \quad b_\beta c_\gamma \;\; b_\beta c_{\gamma-1} \cdots b_\beta c_0 \cdots \right| \Big\}\gamma$$

svi nenapisani elementi determinante podudaraju se s odgovarajućim elementima determinante (3). No, ako rediće $\gamma+2$, $\gamma+3$ množimo po redu sa $b_{\beta-1}, b_{\beta-2}, \ldots, b_0$ i pribrojimo ih rediću $\gamma+1$, vrijednost determinante se ne mijenja, a sam rezultat postaje

$$b_\beta^{-1} \left| (bc)_{\beta+\gamma} \quad (bc)_{\beta+\gamma-1} \cdots (bc)_1 \quad (bc)_0 \right| \begin{matrix} \Big\}\gamma \\ \\ \Big\}\alpha+\beta-1 \end{matrix}$$

Formalno stvar izgleda kao da u prvom retku c-ova umjesto c_k pišemo $(bc)_{\beta+k}$, a pred determinantu izlučimo faktor b_β^{-1}.

Ponavljajući taj isti postupak α puta, zaključujemo da je (nenapisana mjesta su zauzeta nulama):

$$(4) \qquad R(ab, c) = b_\beta^{-\alpha} \left| \begin{matrix} (ab)_{\alpha+\beta} \cdots (ab)_1, (ab)_0 \cdots & & \\ \cdots & & \Big\}\gamma \\ \cdots (ab)_{\alpha+\beta} \cdots \cdots (ab)_1, (ab)_0 & & \\ (bc)_{\beta+\gamma} \cdots (bc)_1, (bc) \cdots & & \\ \cdots & & \Big\}\alpha \\ (bc)_{\beta+\gamma} \cdots \cdots (bc)_1 (bc)_0 & & \\ c_\gamma \cdots c_0 & & \\ \cdots & & \Big\}\beta \\ c_\gamma \cdots c_0 & & \end{matrix} \right|$$

No, lako se vidi da je ta determinanta jednaka

$$(5) \qquad \left| \begin{matrix} a_\alpha \cdots a_0 & & \\ \cdots & & \\ a_\alpha \cdots a_1, a_0 & & \Big\}\gamma \\ c_\gamma \cdots c_0 & & \\ \cdots & & \\ c_\gamma \cdots c_0 \cdots & & \Big\}\alpha \\ 1 \ldots 0 & & \\ \cdots & & \\ 0 \quad \underbrace{\cdot 1}_{\beta} & & \Big\}\beta \end{matrix} \right| \rightarrow \left| \begin{matrix} b_\beta \cdots b_0 & & \Big\}\alpha+\gamma \\ \cdots & & \\ b_\beta \cdots b_0 & & \\ c_\gamma \cdots c_0 & & \Big\}\beta \\ \cdots & & \\ c_\gamma \cdots c_1, c_0 & & \end{matrix} \right|$$

Označimo te dvije determinante sa X, Y; tada vidimo da je

$$X = R(a, c)$$

(dovoljno je X razviti po posljednjih β redića). Također tvrdimo da je

$$Y = b_\beta^\alpha R(b, c)$$

(dovoljno je Y razviti po prvih α redića).

Na taj način jednakost (4) postaje

$$R(ab, c) = b_\beta{}^{-\alpha} XY = b_\beta{}^{-\alpha} R(a, c)\, b_\beta^\alpha R(b, c) = R(a, c)\ R(b, c).$$

A to se i tvrdi prvom relacijom u (1). Druga relacija u (1) dobije se iz prve pomoću indukcije.

2.3. Nov izraz za rezultantu: zavisnost od nula-tačaka. Sad možemo rezultantu $R(a, b)$ izraziti pomoću vrijednosti što ih b uzima u spektru $\operatorname{sp} a$ nula-tačaka od a.

Naime, znamo da je $$a(x) = a_\alpha \prod_{k=1}^{\alpha} (x - a_{(k)}).$$

Zato je prema (1):

$$R(a; b) = R\left(a_\alpha \prod_{i=1}^{\alpha} (x - a_{(i)}); b\right) = R(a_\alpha; b) \cdot \prod_{i=1}^{\alpha} R(x - a_{(i)}; b) =$$

$$= (\text{zbog } R(a_\alpha, b) = a_\alpha^\beta \text{ i teorema } 1) = a_\alpha^\beta \prod_{i=1}^{\alpha} b(a_{(i)}), \text{ tj. imamo}$$

2.3.1. Teorem.

$$R(a(x), b(x)) = a_\alpha^\beta \prod_{i=1}^{\alpha} b(a_{(i)}). \tag{1}$$

No, za polinom $b(x)$ imamo rastav

$$b(x) = b_\beta \prod_{j=1}^{\beta} (x - b_{(j)}), \quad \beta = \operatorname{st} b.$$

Uvrstimo li tu $a_{(i)}$ umjesto x, pa dobiveni izraz unesemo u obrazac (1), dobivamo

$\longrightarrow$ **2.4.** Teorem.

$$R(a(x), b(x)) = a_\alpha^\beta \prod_{i=1}^{\alpha} \prod_{j=1}^{\beta} b_\beta \cdot (a_{(i)} - b_{(j)}).$$

$$R(a(x), b(x)) = a_\alpha^\beta b_\beta^\alpha \prod_{\substack{i=1,\ldots,\alpha \\ j=1,\ldots,\beta}} (a_{(i)} - b_{(j)}). \tag{2}$$

Drugim riječima: *rezultanta polinomâ a i b dobije se tako da se od svakog člana spektra prvog polinoma oduzme svaki član spektra drugog polinoma, dobivene razlike međusobno pomnože i rezultat još pomnoži sa* $a_\alpha^\beta b_\beta^\alpha$.

2.4.1. Primjedba. Vrlo se često obrazac (2) uzima kao *definicija rezultante*. Iz obrasca (2) odmah se vidi da je poništavanje rezultante nuždan i dovoljan uslov pa da polinomi $a(x), b(x)$ imaju zajedničku nula-tačku.

—→ **2.5.** Teorem. Ako je $a_\alpha \neq 0$, $b_\beta \neq 0$, tada je

$$R(a(x), b(x)) = \begin{vmatrix} a_\alpha & a_{\alpha-1} & \cdots & & a_0 & & \\ 0 & a_\alpha & \cdots & & & & \\ \cdot & \cdot & \cdot & & & & \\ 0 & \cdots & 0 & a_\alpha & \cdots & a_1 & a_0 \\ b_\beta & b_{\beta-1} & \cdots & b_0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & & & & \\ & & & b_\beta & \cdots & b_1 & b_0 \end{vmatrix} = a_\alpha^\beta b_\beta^\alpha \prod_{\substack{\alpha' \in [1,\alpha] \\ \beta' \in [1,\beta]}} (a_{(\alpha')} - b_{(\beta')}),$$

pri čemu je

$$\sum_0^\alpha a_j x^j = a_\alpha \prod_{\alpha'} (x - a_{(\alpha')})$$

$$\sum_0^\beta b_j x^j = b_\beta \prod_{\beta'=1}^{\beta} (x - b_{(\beta')}).$$

Naime, iz definicije izraza $R(a, b)$ i veza (2) izlazi gornja jednakost.

Na taj način vidimo zanimljivu vezu među koeficijentima i nula-tačkama dvaju algebarskih polinoma.

2.6. Izobaričnost rezultante. Teorem *Rezultanta*

$$R(a, b) \text{ polinomâ } a(x) = \sum_{i=0}^{\alpha} a_i x^i, \; b(x) = \sum_{i=0}^{\beta} b_i x^i$$

je izobarična funkcija veličinâ

(1) $$a_0, a_1, \ldots, a_\alpha$$

(2) $$b_0, b_1, \ldots, b_\beta$$

i težina joj je $\alpha \cdot \beta$; *tu je* $\alpha = \operatorname{st} a$, $\beta = \operatorname{st} b$. *Pri tom definiramo da je težina od* a_k jednaka $\alpha - k$, *a od* b_k *jednaka* $\beta - k$.

Stvarno, promatrajmo determinantu $R(a, b)$; u odnosu na veličine (1) ta je determinanta algebarki homogeni polinom stupnja β; u odnosu na koeficijente (2) ona je isto tako homogen polinom stupnja α.

Opći član determinante $R(a, b)$ oblika je

(3) $$K_{r_1 \cdots r_\beta, s_1 \cdots s_\alpha} a_{r_1} a_{r_2} \ldots a_{r_\beta} b_{s_1} b_{s_2} \ldots b_{s_\alpha};$$

K je konstanta: težina toga člana (3) iznosi

(4) $$(\alpha - r_1) + (\alpha - r_2) + \cdots + (\alpha - r_\beta) + (\beta - s_1) + \cdots + (\beta - s_\alpha);$$

pri tom je $a_{\alpha-r_1}$ iz prvog retka i stupca $\alpha-r_1+1$

$a_{\alpha-s_2}$ iz retka drugog i stupca $\alpha-r_2+2$

. . . . . .

$b_\beta-s_1$ iz retka $\beta+1$ i stupca $\beta-s_1+1$

$\beta_\beta-s_2$ iz retka $\beta+2$ i stupca $\beta-s_2+2$

. . . . . .

Kako je u (3) zastupljen svaki od stupaca $1, 2, \ldots, \alpha+\beta$, znači da je

$$(\alpha-r_1+1)+(\alpha-r_2+2)+\cdots+(\alpha+r_\beta+\beta)+$$

$$+(\beta-s_1+1)+(\beta-s_2+2)+\cdots+(\beta-s_\alpha+\alpha)=1+2+3+\cdots+(\alpha+\beta).$$

Odatle, prema izrazu (4) za težinu p člana (3), imamo

$$p=1+2+\cdots+(\alpha+\beta)-(1+2+\cdots+\beta)-(1+2+\cdots+\alpha)=$$

$$=\frac{(\alpha+\beta)(\alpha+\beta-1)}{2}-\frac{\beta(\beta+1)}{2}-\frac{\alpha(\alpha+1)}{2}=\alpha\beta.$$

Dakle je uistinu težina svakog člana rezultante jednaka $\mathrm{st}\,a\cdot\mathrm{st}\,\beta$.

3. DISKRIMINANTA KAO POSEBNA REZULTANTA

3.0. Idejna postavka. *Diskriminanta* polinoma $a(x)$ ima da služi kao sredstvo da saznamo da li taj polinom a ima ili nema bar jednu višestruku nula-tačku, tj. da li polinom a i njegov derivat a' imaju koju nula-tačku zajedničku.

3.1. Definicija. Pod *diskriminantom polinoma* $a(x)=\sum_{i=0}^{\alpha} a_i x^i$ razumijevamo produkt od $\frac{(-1)^{\frac{\alpha(\alpha-1)}{2}}}{a_\alpha}$ i rezultante $R(a,a')$; označuje se sa $\mathrm{Dis}(a)$; dakle je

$$\mathrm{Dis}\,(a_0+a_1x+\cdots+a_\alpha x^\alpha)=(-1)^{\frac{\alpha(\alpha-1)}{2}}\begin{vmatrix} 1 & a_{\alpha-1}\cdots a_0\cdots & \\ 0 & a \quad a_{\alpha-1}\cdots a_1\,a_0\cdots & \\ \cdots & \cdots & \end{vmatrix}\Big\}\mathrm{st}\,a-1$$

$$\begin{vmatrix} a_\alpha\cdots & a_1\,a_0 \\ \alpha & (\alpha-1)\,a_{\alpha-1}\cdots a_1 \\ 0 \quad \alpha & a_\alpha \cdots 2\,a_2\;a_1 \\ \cdots & \cdots \\ \alpha\,a_\alpha\cdots & 2\,a_2\;a_1 \end{vmatrix}\Big\}\mathrm{st}\,a$$

3.2. Primjeri: st $a = 1, 2, 3$.

3.2.1. Dis $(a_0 + a_1 x) = 1$.

$$\text{Dis}\,(a_0 + a_1 x + a_2 x^2) = (-1)^{\frac{2\cdot 1}{2}} \begin{vmatrix} a_1 & a_1 & a_0 \\ 2a_2 & a_1 & 0 \\ 0 & 2a_2 & a_1 \end{vmatrix} = a_1^2 - 4a_0 a_2.$$

3.2.2. Dis $(x^3 + px + q) = (-1)^{\frac{3\cdot 2}{2}} \begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 3 & 0 & p & 0 & 0 \\ 0 & 3 & 0 & p & 0 \\ 0 & 0 & 3 & 0 & p \end{vmatrix}$ = (razvijajući po 3. re-

diću) $= -3(-1)^{3+1} \begin{vmatrix} 0 & p & q & 0 \\ 1 & 0 & p & q \\ 3 & 0 & p & 0 \\ 0 & 3 & 0 & p \end{vmatrix} - p(-1)^{3+3} \begin{vmatrix} 1 & 0 & q & 0 \\ 0 & 1 & p & q \\ 0 & 3 & p & 0 \\ 0 & 0 & 0 & p \end{vmatrix} =$

$$= -3\left(p(-1)^{1+2} \begin{vmatrix} 1 & p & q \\ 3 & p & 0 \\ 0 & 0 & p \end{vmatrix} + q(-1)^{1+3} \begin{vmatrix} 1 & 0 & q \\ 3 & 0 & 0 \\ 0 & 3 & p \end{vmatrix}\right) - p^2 \begin{vmatrix} 1 & 0 & q \\ 0 & 1 & p \\ 0 & 3 & p \end{vmatrix} =$$

$$= 3p^2 \begin{vmatrix} 1 & p \\ 3 & p \end{vmatrix} - 3q \cdot 1 \cdot 3 \cdot (-1)^{2+1} \begin{vmatrix} 0 & q \\ 3 & p \end{vmatrix} - p^2 \begin{vmatrix} 1 & p \\ 3 & p \end{vmatrix} =$$

$$= -6p^3 - 27q^2 + 2p^3 = -4p^3 - 27q^2.$$

Dakle je

$$\text{Dis}\,(x^3 + px + q) = -4p^3 - 27q^2.$$

Težina svakog člana u tom izrazu je 6, jer je težina od p jednaka 2, a od q jednaka 3 (naime, $2 = 3-1$, $3 = 3-0$, gdje su 1, odnosno 0 eksponenti od x-koeficijenata od p, odnosno q). *To izobarično svojstvo diskriminante omogućava da se ona lakše zapamti.*

3.2.3. Lako se može provjeriti da je

$$\text{Dis}\,(a_0 + a_1 x + a_2 x^2 + a_3 x^3) = a_1^2 a_2^2 - 4a_0 a_2^3 - 4a_1^3 a_3 + 18 a_0 a_1 a_2 a_3 - 27 a_0^2 a_3^2.$$

Taj je polinom izobaričan; težina mu je 6. Za slučaj $a_3 = 1$, $a_2 = 0$, $a_1 = p$, $a_0 = q$ postaje taj izraz $-4p^3 - 27q^2$.

3.3. Kako diskriminanta polinoma zavisi od njegovih nula-tačaka?

3.3.1. Po definiciji je

$$\text{Dis}\,(a(x)) = (-1)^{\frac{\alpha(\alpha-1)}{2}} a_\alpha^{-1} R(a, a');$$

no, prema § 2.4. vrijedi

$$R(a, a') = a_\alpha{}^{\alpha-1} \prod_{\alpha' \in [1,\ \alpha]} a'(a_{(\alpha')}).$$

S druge strane iz

$$a(x) = a_\alpha \prod_{\alpha'=1}^{\alpha} (x - a_{(\alpha')})$$

lako izlazi da je

$$a'(x) = \sum_{\alpha'=1}^{\alpha} \frac{a(x)}{x - a_{(\alpha')}};$$

odatle dalje

$$a'\, a_{(\alpha')}) = a_\alpha \prod_k a_{(\alpha')} - a_{(k)});$$

tu je $k \neq \alpha'$ te $k \in [1, \alpha]$.

Uvrstimo li tu po redu $\alpha' = 1, \ldots, \alpha-1, n$ i sve dobivene jednadžbe međusobno pomnožimo, tada vidimo da na desnoj strani dalaze faktori

$a_{(\alpha')} - a_{(k)}$, $a_{(k)} - a_{(\alpha')}$; produkt im je

$-(a_{(\alpha')} - a_{(k)}{}^2)$; takvih produkata ima $\binom{\alpha}{2}$;

to znači da je

$$\prod_{\alpha'} a'(a_{(\alpha')}) = a_\alpha{}^\alpha (-1)^{\binom{\alpha}{2}} \prod_{\alpha' < k} (a_{(\alpha')} - a_{(k)})^2,$$

pa gornji izraz za diskriminantu daje ovaj

3.3.2. Teorem.

$$\mathrm{Dis}\, a(x) = a_\alpha{}^{2\alpha-2} \prod_{\alpha' < k} (a_{(\alpha')} - a_{(k)})^2;$$ pri tom je $\alpha', k \in [1, \alpha]$.

Odatle se očigledno vidi da je $\mathrm{Dis}\, a = 0$ onda i samo onda ako u spektru nula-tačaka: $a_{(1)}, a_{(2)}, \ldots, a_{(\alpha-1)}$, $a_{(\alpha)}$ ima jednakih članova, tj. ako polinom a ima višestrukih nula-tačaka.

⟶ **3.3.3.** ***Osnovno svojstvo diskriminante sastoji se u ovom: da polinom*** $a(x)$ ***ima bar jednu višestruku nula-tačku, nužno je i dovoljno da njegova diskriminauta iščezava. Drugim riječima, ako je sistem*** $a(x) = 0$, $a'(x) = 0$, ***moguć, tada je*** $\mathrm{Dis}\, a = 0$; ***i obrnuto.***

3.3.4. *Nejednakost* $\mathrm{Dis}\, a \neq 0$ *znači isto što i činjenica da* $a(x)$ *ima upravo* $\alpha = \mathrm{st}\, a$ različitih nula-tačaka.

Sjetimo se da kod kvadratnih i kubnih polinoma s koeficijentima iz R *predznak* diskriminante odlučuje da li su nula-tačke *realne* (u R) ili nisu u R.

3.3.5. Zanimljiva je formula

$$\mathrm{Dis}\,(a(x) \cdot b(x)) = \mathrm{Dis}\, a \cdot \mathrm{Dis}\, b \cdot R^2(a, b).$$

4. DVIJE JEDNADŽBE S DVIJE NEPOZNATE VELIČINE

4.1. Zadane su dvije jednadžbe

$$a(x, y) = 0 \tag{1}$$

$$b(x, y) = 0. \tag{2}$$

Treba odrediti x i y, tj. odrediti uređenu dvojku (x, y) tako da vrijedi (1) i (2). Govoreći *geometrijski*, jednadžbom (1) zadana je neka krivulja A; jednadžbom (2) zadana je također neka krivulja B. Tada se radi o tome da se nađu *zajedničke tačke* (x, y) *tih krivulja.* Gledajući stvar *analitički*, put kako da dođemo do rješenja (x, y) jednadžbi (1), (2), odnosno da nulatačke (x, y) funkcijâ (operatorâ) a i b, bio bi ovaj;

Najprije se ukloni jedna nepoznata veličina (*npr.* x), *pa se onda nađe preostala nepoznanica.*

4.2. *Ako su funkcije a i b algebarski polinomi, tada se eliminacija* (*uklanjanje*) *nepoznanice*, ***formalno,*** *lako provede.*

Tako npr. ako se radi o jednadžbama oblika

$$a_1 x + a_2 y + a_3 = 0$$

$$b_1 x + b_2 y + b_3 = 0,$$

pri čemu su a-ovi i b-ovi nezavisni od x, y, tada rezultanta (eliminanta) tih jednadžbi s obzirom na x kao nepoznanicu koju želimo ukloniti glasi:

$$\begin{vmatrix} a_1 & a_2 y + a_3 \\ b_1 & b_2 y + b_3 \end{vmatrix}.$$

Njeno poništavanje dovodi do *rezultata eliminacije*

$$a_1 (b_2 y + b_3) - b_1 (a_2 y + a_3) = 0,$$

odakle se odmah nađe y.

4.3. Postupak je općenit. Ako npr. iz (1) i (2) želimo ukloniti x, tada shvatamo a i b kao algebarske polinome u x i pišemo:

$$a(x, y) = a_0 (y) + a_1 (y)\, x + a_2 (y)\, x^2 + \cdots + a_\alpha (y)\, x^\alpha$$

$$b(x, y) = b_0 (y) + b_1 (y)\, x + b_2 (y)\, x^2 + \cdots + b_\beta (y)^\beta.$$

Rezultanta R tih *x-polinoma* ne sadrži više x, ali je, naravno, *određena funkcija od y*; time što (1) i (2) postoje u isto vrijeme izlazi da je

$$R(a(x, y),\ b(x, y)) = 0. \tag{3}$$

To je jednadžba oblika

$$R(y) = 0. \tag{3}$$

Za svako y iz (3) imaju obje zadane jednadžbe (1), (2) zajedničko rješenje x, pa se tako dobiju *sve nula-tačke* (x, y) *zadanih polinoma* a, b.

4.4. Primjer. Riješi jednadžbe

$$a(x,y) \equiv (x-2)(x+5)(x^2y-2x+y^2-1) = 0 \tag{1}$$

$$b(x,y) \equiv (x+4)(x+2)(xy-2) = 0. \tag{2}$$

Najprije se vidi da na skupu (1) leži čitava pravulja $x=2$ kao i čitava pravulja $x=-5$, jer za svako y leže tačke $(2,y)$ i $(-5,y)$ na (1). No sa $x=2$ jednadžba (2) je ekvivalentna s jednadžbom

$$(y+2)(2y-2) = 0,$$

odakle izlazi $y=-2$ ili $y=1$.

Tako smo našli već dvije tačke $(2, -2)$ i $(2, 1)$ koje zadovoljavaju i (1) i (2). Slično se vidi da su i $(-5, -2), (-5, -2/5)$ dva rješenja jednadžbi (1), (2).

Iskorištavajući linearne faktore funkcije $b(x,y)$, zaključujemo analogno da su rješenja također $(-4, -7/17)$ te $(x, -2)$ gdje x poništava $-2x^2-2x+4-1$, dakle $x=\frac{1}{2}(1\pm\sqrt{7})$. Sva preostala rješenja jednadžbi (1), (2) nalaze se na krivuljama

$$x^2y-2x+y^2-1=0 \tag{3}$$

$$xy-2=0. \tag{4}$$

Riješimo (3), (4) uklanjajući npr. x. Rezultat eliminacije je poništavanje rezultante tih jednadžbi, odnosno polinoma

$$\begin{vmatrix} y & -2 & y^2-1 \\ y & -2 & 0 \\ 0 & y & -2 \end{vmatrix} = 0,$$

tj,

$$y^2(y^2-1)=0.$$

Odatle zaključujemo na rješenje oblika $(x, 0), (x, 1), (x, -1)$.

No, slučaj $x=0$ ne dolazi u obzir, jer bi iz (3) i (4) izlazilo da je pripadno x beskonačno, i to $+\infty$ i $-\infty$. A to nam kazuje da se obje krivulje (3) i (4) asimptotski približuju x-osi, i to kad po x-osi idemo u beskonačnost u jednom smjeru i u drugom smjeru. Najzad, rješenja oblika $(x, 1)$ i $(x, -1)$ jesu $(2, 1), (-2, -1)$.

Prema tome, imamo ova rješenja jednadžbi (1), (2):

$$(2, -2),\ (2, 1),\ (-5, -2),\ (-5, -2/5),\ (-4, -7/17),$$

$$(\tfrac{1}{2}(1\pm\sqrt{7}), -2),\ (-2, -1).$$

4.5. Primjer.

$$xy^2-y^2+x-1=0$$
$$xy\ -y+x-1=0.$$

Uklonimo y; rezultat je

$$R(x)\equiv\begin{vmatrix} x-1 & 0 & x-1 \\ x-1 & x-1 & 0 \\ 0 & x-1 & x-1 \end{vmatrix}=0,$$

tj.

$$2(x-1)^3=0$$
$$x=1.$$

No, za $x=1$ jednadžbe su zadovoljene za svako y. Drugim riječima, zadane krivulje obuhvataju čitavu pravulju $x=1$.

5. BEZOUTOV TEOREM O ELIMINANTI[1)]

Ako iz jednadžbi

(*)
$$a(x,y)=0$$
$$b(x,y)=0$$

eliminiramo y, izlazi jednadžba oblika

$$R_y(x)=0.$$

Uklonimo li x iz gornjih jednadžbi (*), rezultat eliminacije je oblika

$$R_x(y)=0.$$

Bézoutov teorem odnosi se na stupanj od $R(x)$ u slučaju kad su $a(x,y)$ i $b(x,y)$ *algebarski polinomi u odnosu na* x, y: tada je

(1)
$$\operatorname{st} R_x(a(x,y), b(x,y))\leq \operatorname{st} a\cdot \operatorname{st} b$$

(2)
$$\operatorname{st} R_y(a(x,y), b(x,y))\leq \operatorname{st} a\cdot \operatorname{st} b.$$

Nadalje, koeficijenti obiju *eliminanata* polinomâ $a(x,y)$ $b(x,y)$ *leže u kolu što ga određuju koeficijenti tih dvaju polinoma.*

Dokaz te izrečene *činjenice o koeficijentima* je trivijalan, jer se eliminanta ispisuje u obliku determinante kojoj su elementi polinomi u x, odnosno u y, s koeficijentima zadanih polinoma a, b.

Mnogo je dublji dokaz relacija (1), (2).

On se svodi na *izobarnost rezultante* (v. § 2.6.). Naime, poredajmo članove od a i b po potencijama od x:

$$a(x,y)=a_0+a_1x+a_2x^2+\cdots+a_\alpha x^\alpha$$
$$b(x,y)=b_0+b_1x+\cdots+\qquad +b_\beta x^\beta.$$

[1)] Bézout /Bezu/ (1730—1780), francuski matematičar.

Tada je rezultanta $R_x(a, b)$

tih x-polinoma izobaran polinom koeficijenata $a_0, a_1, \ldots, a_\alpha, b_0, b_1, \ldots, b_\beta$. No, težina nijednog od tih koeficijenata ne premašuje njegov stupanj s obzirom na varijablu x. A to znači da stupanj y-polinoma $R_x(a, b)$ ne premašuje njegovu težinu, koja je prema § 2.6. jednaka $\alpha\beta$. Time je taj važni teorem dokazan. Naravno da u relacijama (1), (2) umjesto $\leq$ može stajati znak $<$. No, ipak za *svaki par* prirodnih brojeva α, β postoje algebarski polinomi $a(x, y), b(x, y)$ stepena α, odnosno β, tako da njihove pripadne eliminante budu stupnja *upravo* $\alpha \cdot \beta$.

6. BROJ ZAJEDNIČKIH NULA-MJESTA ALGEBARSKIH POLINOMA $a(x, y)$, $b(x, y)$. BEZOUTOV TEOREM

6.1. Govoreći *geometrijski*, radi se o presjeku skupova

$$a(x, y) = 0.$$

$$b(x, y) = 0.$$

Ako funkcije a, b imaju zajednički divizor $c(x, y)$, onda svaka tačka množine

$$c(x, y) = 0$$

zadovoljava zadanim jednadžbama. Tih tačaka ima beskonačno mnogo. Zato ćemo promatrati slučaj da su funkcije $a(x, y), b(x, y)$ relativno proste:

$$a(x, y) \,\mathrm{M}\, b(x, y) = 1.$$

Tada vrijedi važan

—→ **6.2. Bézoutov teorem.** *Ako su $a(x, y), b(x, y)$ dva algebarska polinoma bez zajedničkog divizora, tada oni imaju upravo toliko zajedničkih elemenata koliko je produkt stepenâ tih polinoma. Pri tom se svaka nula-tačka broji onoliko puta kolika joj je kratnost. Nadalje, nula-tačke ne moraju biti realne, nego i kompleksne, pa k tome ležati i u beskonačnosti.*

Dokaz gornjeg Bézoutova teorema počiva na spomenutom Bézoutovu teoremu o stupnju eliminante polinoma $a(x, y), b(x, y)$.

Primjene tog teorema su brojne. Teorem je razrađen u djelu Bézout: *Théorie générale des équations algébriques*, Pariz 1799. (*Opća teorija algebarskih jednadžbi.*) Teorem su upotpunjavali Liouville, Mertens, Kronecker itd. Analogan teorem postoji i za skupove jednadžbi s tri i više nepoznanica.

6.3. Kako se definira kratnost nula-tačke funkcije od dva i više argumenata. Znamo što znači da je z nula-tačka kratnosti k za funkciju $f(x)$ (isp. pogl. 5, § 2.2 i pogl. 5, § 4.2.7). Kako se analogna definicija prenosi na funkcije od dvije i više varijabli?

Definicija. Neka je $f(x_0, x_1, \ldots)$ funkcija od dvije ili više varijabli; aki *niz* vrijednosti tih varijabli za koji f postaje 0 zove se *nula-mjesto funk-*ze f. To je nula-mjesto *jednostavno* ako ono nije nula-mjesto *svih* derivata da 1. funkcije f. Ako je nula-tačka od f ujedno nula-tačka i od *svih* derivata da 1. funkcije f, kaže se da je ta nula-tačka *kratnosti* ≥ 2. Uopće, nula-ska z funkcije f od jedne ili više varijabli je kratnosti $>k$ ako je ta nula-ska ujedno nula-tačka *svih derivata* reda $1, 2, \ldots, k-1$ funkcije f; kratnost i je upravo k ako joj je kratnost $\geq k$, ali nije $\geq k+1$; to znači da nula-ska z ne poništava bar jedan derivat k—og reda funkcije f, ali poništava sve rivate reda $<k$.

7. Zadaci o rezultanti, diskriminanti i eliminaciji.

1. Nađi rezultantu $R(a, b)$ ovih parova polinomâ:

1) $3x-5$, $6x+1$; 2) $1-5x$, $3+6x$; 3) $1+x$, $1+x+x^2$;
4) $3x-1$, $5x^2+4x-2$; 5) $1+2x$, $3x^2-2+3x$; 6) x^3-3x^2+2x+1, $2x^2-x-1$; 7) $2x^3-3x^2+2x+1$, x^2+x+3; 8) $2x^3-3x^2-x+2$. x^4+2x^2-3x+4; 9) $3x^3+2x^2+x+1$, $2x^3+x^2-x-1$;
10) $2x^4-x^3+3$, $3x^3-x^2+4$; 11) $a_0x^2+a_1x+a_2$, $b_0x^2+b_1x+b_2$.
12) X_m, X_n; 13) x^m-1, X_n.

2. Za koje λ imaju parovi ovih polinoma bar jedno zajedničko nula-mjesto? 1) $2x+\lambda$, $\lambda x-1$; 2) $3\lambda x+5$, $6\lambda x-8$; 3) $\lambda x-5$, $2x^2+3x+\lambda$; 4) $\lambda x-5$, $2x^2+\lambda x+5$; 5) $\lambda x-5$, λx^2+3x+5; 6) $x^3-\lambda x+2$, $x^2+\lambda x+2$; 7) $x^3-2\lambda x+\lambda^3$, $x^2+\lambda^2-2$; 8) $x^3+\lambda x^2-9$, $x^3+\lambda x-3$; 9) $x^3+3x^2+2x+\lambda$, x^2-3x+2.

3. Nađi diskriminantu ovih izraza: 1) $3x$; 2) $3x+5$; 3) x^2+3x+5; 4) x^3+3x^2+5x; 5) x^3+3x+5; 6) $x^4+3x^3+5x^2$; 7) x^4+3x^2+5, 7′) x^4+3x+5; 8) x^3-x^2-2x+1; 9) x^3+2x^2+4x+1;
10) $3x^3+3x^2+5x+2$; 11) $x^4-x^3-3x^2+x+1$; 12) $2x^4-x^3-4x^2+x+1$; 13) $x^5-5ax^3+5a^2x-b$; 14) $(x^2-x+1)^3-\lambda(x^2-x)^2$;
15) $ax^3-bx^2+(b-3a)x+a$; 16) x^n+a; 17) x^n+px+p; $a_0x^{m+n}+a_1x^m+a_2$; 19) $1+x+x^2+\cdots+x^{n-1}$;
20) $(x-a)^n+(x-b)^n$,

4. Ukloni x iz ovih jednačaba: 1) $2x-3y+5=0$, $5x+6y-7=0$; 2) $2x-3y+5=0$, $x^2+y^2-100=0$; 3) $2x-3y+5=0$, $x^2-3y^2=16$; 4) $x^2-xy+y^2=3$, $x^2y+xy^2=6$; 5) $y=x^2-3x+1$, $y=2x^2+5x-1$; 6) $y=x^3-2x^2-6x+8$, $y=2x^3-8x^2+5x+2$.

5. Riješi:

1) $y^2-7xy+4x^2+13x-2y-3=0$, $y^2-14xy+9x^2+28x-4y-5=0$;
2) $y^2+x^2-y-3x=0$, $y^2-6xy-x^2+11y+7x-12=0$;
3) $5y^2-6xy+5x^2-16=0$, $y^2-xy+2x^2-y-x-4=0$;

4) $y^2+(x-4)y+x^2-2x+3=0$, $y^3-5y^2+(x+7)y+x^3-x^2-5x-3=0$;
5) $2y^3+4xy^2-(2x^2-12x+8)y+x^3+6x^2-16x=0$,
$4y^3-(3x+10)y^2-(4x^2-24x+16)y-3x^3+2x^2-12x+40=0$.

6. Odredi vrijednost parametra λ, tako da naredni polinom ima bar jedno nula-mjesto koje nije jednostruko: 1) $x^2+\lambda$; 2) $x^3+\lambda$; 3) $x^k+\lambda$; 4) $x^3-5x+\lambda$; 5) $x^4-4x+\lambda$; 6) $x^3-8x^2+(13-\lambda)x-(6+2\lambda)$; 7) $x^4-4x^3+(2-\lambda)x^2+2x-2$; 8) $x^3-3\lambda x+\lambda$; 9) $x^3-\lambda^2x+5$.

7. Dokaži: 1) $\operatorname{Dis}((x-\lambda)f(x))=\operatorname{Dis}f\cdot f(\lambda)^2$; 2) $\operatorname{Dis}(f(x)\cdot g(x))=\operatorname{Dis}f\cdot\operatorname{Dis}g\cdot(R(f,g))^2$; 3) $R(f,g)$ je jednako determinanti kojoj su stupci koeficijenti ostataka pri diobi polinoma $x^k\cdot g(x)$ sa $f(x)=x^n+f_{n-1}x+f_{n-2}x^{n-2}+\ldots+f_n$ $(k=0,\ 1,\ 2,\ldots n-1)$ (Hermite-ov teorem); 4) $R(f,g)$ je jednako determinanti kojoj su stupci koeficijenti polinoma stepena $\leq n-1$ i to $h_k(x)=(f_nx^{k-1}+f_{n-1}x^{k-2}+\ldots+f_{n-k+1})g(x)-(g_nx^{k-1}+g_{n-1}x^{k-2}+\ldots g_{n-k+1})f(x)$ za $k=1,\ 2,\ldots,\ n$ (Bézout-ov teorem). Dokaži da je $h_1=f_ng-g_nf$, $h_k=xh_{k-1}+f_{n-k+1}g-g_{n-k+1}f$; 5) Ako je $\operatorname{st}f=n>\operatorname{st}g=m$, tada je $R(f,g)$ jednako determinanti kojoj su stupci koeficijenti polinoma $c_k(x)$ stepena $\leqq n-1$, gdje je $c_k=x^{k-1}g$ za $1\leq k\leq n-m$, $c_k=(f_nx^{k-n+m-1}+f_{n-1}x^{k-n+m-2}+\ldots f_{2n-m-k+1})x^{n-m}g-(g_mx^{k-n+m-1}+g_{n-1}x^{k-n+m-2}+\ldots+g_{2n-k-m+1})f$; dokaži da je $c_{n-m+1}=f_nx^{n-m}f-g_mf$

$$c_k=xc_{k-1}+f_{2n-k-m+1}x^{n-m}f-g_{2n-k-m+1}f.$$

8. Odredi diskriminantu ovih posebnih mnogočlana:

1) $E_n(x)=n!\left(1+\frac{x}{1}+\frac{x^2}{2!}+\ldots+\frac{x^n}{n!}\right)$; 2) X_n (Legendre-ov polinom);

3) L_n (Laguerre-ov polinom; 4) T_n (polinom Čebiševa);

5) $P_n(x)=(-1)^n(1+x^2)^{n+\frac{1}{2}}D^n(1+x^2)^{-\frac{1}{2}}$;

6) $P_n(x)=(-1)^nx^{2(n+1)}-x^{-1}D^ne^{x-1}$; 7) $(-1)^ne^{\frac{x^2}{2}}De^{\frac{-x^2e}{2}}$.

9. Dokaži: 1) $\operatorname{Dis}f(x^m)=m^{mn}(-1)^{\frac{m(m-1)n}{2}}(f_0f_n)^{m-1}(\operatorname{Dis}f)^m$, $n=\operatorname{st}f$; specificiraj: $m=1,2,3$; 2) $\operatorname{Dis}(f(g(x)))=(\operatorname{Dis}f)^m\prod_{i=1}^{n}\operatorname{Dis}(g-x_i)$, $m=\operatorname{st}g$, spektar od f je $x_1,x_2,\ldots.x_n$; $f_n=1=g_m$; 3) $\operatorname{Dis}a=\operatorname{Dis}a^T$, gdje je $a=a_0+a_1x+a_2x^2+\ldots+a_nx^n$, $a^T=a_n+a_{n-1}x+a_{n-2}x^2+\ldots a_1x^{n-1}+a_0x^n$.

Literatura

Faddeev-Sominskij [1]; Kuroš [1]; Obreškov [1]. [2]; Perron [1]; Plemelj [1]; Serret [1]; Weber [1]

POGLAVLJE 21.

TRANSFORMACIJA JEDNADŽBI

1. UVODNA RAZMATRANJA

Često se iz *zadane* jednadžbe dolazi do *drugih* jednadžbi, koje su jednostavnije i koje znamo riješiti, pa iz njihovih rješenja zaključujemo na rješenja zadane jednadžbe, odnosno zadanih jednadžbi. Naravno da će najjednostavnije biti ako se iz zadane jednadžbe prelazi na *ekvivalentnu* jednadžbu.

Tako npr. pođemo li od jednadžbe

$$a(x)=0 \tag{1}$$

i supstitucije

$$y=t(x), \tag{2}$$

tada će nula-mjesta

$$z_1,\ z_2,\ \dots \tag{3}$$

polinoma a prijeći u brojeve

$$t_1=t(z_1),\ t_2=t(z_2),\ \dots \tag{4}$$

Jednadžba

$$(t-t_1)(t-t_2)\cdots=0 \tag{5}$$

ima upravo brojeve (4) za svoja rješenja. Zato se jednadžba (5) naziva *rezolventom ili t-transformatom jednadžbe* (1). *Čitava se ideja sastoji u tome da se može desiti da rezolventa bude jednostavnija,* da je možemo *napisati i riješiti,* a da onda preko (2) idemo i na rješenja same zadane jednadžbe (1). Važno je da se *rezolventa može odrediti već na osnovu koeficijenata zadane jednadžbe.*

Stvar ćemo razjasniti na nekoliko tipova transformacija (linearne, razlomljeno-linearne, cijele racionalne i racionalne transformacije).

2. TRANSLACIJE

2.1. Zadana je funkcija $a(x)$; treba naći jednadžbu kojoj se ništišta (nula-tačke) dobiju *umanjujući svaku nula-tačku funkcije* a za određen broj h.

Supstitucijom

$$t = x - h$$

svaka je nula-tačka x od a umanjena za h i prelazi u t.

No, iz $t = x - h$, izlazi $x = t + h$, pa funkcija $a(x)$ prelazi u $a(t+h)$, gdje je t varijabla. Kako oznaka varijable nije od važnosti, možemo govoriti i ovdje o x kao nezavisnoj varijabli pa tako vidimo da funkcija $a(x+h)$ *ima za svoje nula-tačke upravo nula-tačke od* $a(x)$ *umanjene za* h.

Drugim riječima, *krivulja*

$$y = a(x+h)$$

nastaje iz krivulje

$$y = a(x)$$

translacijom za $-h$ *duž x-osi*; operativno: [1]

$$\mathrm{Sp}\, a(x+h) = \mathrm{Sp}\, a(x) - h.$$

Tako npr. kvadratna jednadžba $a_2 x^2 + a_1 x + a_0 = 0$ supstitucijom $t = x - h$ prelazi u

$$a_2 (t+h)^2 + a_1 (t+h) + a_0 = 0$$

$$a_2 t^2 + (2 a_2 h + a_1) t + (a_2 h^2 + a_1 h + a_0) = 0.$$

Ta se jednadžba pojednostavnjuje ako je

$$2 a_2 h + a_1 = 0, \text{ tj. ako je } h = -2^{-1} a_2^{-1} a_1,$$

jer dobivamo *čistu* kvadratnu jednadžbu.

Sličan zaključak vrijedi za algebarske jednadžbe st. > 2.

2.2. Teorem. *Ako je* $a(x) = 0$ *algebarska jednadžba stupnja* n, *tada se supstitucijom* $t = x - n^{-1} a_n^{-1} a_{n-1}$ *dobije jednadžba u kojoj je koeficijent od* t^{n-1} *jednak* 0. Drugim riječima, *translacijom krivulje* $y = a(x)$ *duž x-osi za broj* $-a_{n-1}/(n\ a_n)$ *gubi se koeficijent od* x^{n-1}.

2.3. Postupak kako da se odredi polinom $a(t+h)$ iz $a(t)$. Naravno, ako je $a(x)$ polinom n-og stupnja, onda je i $a(t+h)$ stupnja n po t; pa stavimo da je $a(t+h) = b(t)$:

$$a(t+h) = b(t) = b_0 + b_1 t + b_2 t^2 + \cdots b_n t^n. \tag{1}$$

Kako je $x = t + h$, postaje (1):

$$a(x) = b_0 + b_1 (x-h) + b_2 (x-h)^2 + \cdots + b_n (x-h)^n.$$

---

[1] Sa $\mathrm{Sp}\, f(x)$ označujemo neuređen niz nula-tačaka funkcije f, svaka se od njih pojavljuje onoliko puta koliki joj je red.

Odatle zaključujemo ovo: podijelimo li polinom $a(x)$ sa $x-h$, dobije se x-polinom stupnja $n-1$ i broj b_0 kao ostatak, tj. (o oznaci v. pogl. 7, § 4.1):

$$E_2(a(x),\ x-h)=b_0.$$

Ako polinom $E_1(a(x),\ x-h)$ podijelimo sa $x-h$, dobit ćemo kao ostatak koeficijent b_1, itd. (isp. pogl. 7, § 4.1).

2.4. Algoritam o dijeljenju $a(x)$ sa $x-h$ ili sintetička divizija po Horneru. — **2.4.1.** Podijelimo li polinom $a(x)=a_0+a_1x+\cdots+a_\alpha x^\alpha$ sa $x-h$ dobije se polinom $b(x)$ stupnja $\alpha-1$ i određen broj r kao ostatak (naime ili je $r=0$ ili je st $r=0$). To znači da je identički $a(x)=(x-h)b(x)+r$ i specijalno $a(h)=r$ (isp. pogl. 7, § 4.2).

No, koeficijente $b_0,\ b_1,\ldots,\ b_{\alpha-1}$ možemo lako izračunati. Naime, imamo

$$a_0+a_1x+\cdots+a_\alpha x^\alpha=(x-h)(b_0+b_1x+\cdots+b_{\alpha-1}x^{\alpha-1})+r$$

$$a_0+a_1x+\cdots+a_\alpha x^\alpha=b_0x+b_1x^2+\cdots+b_{\alpha-2}x^{\alpha-1}+b_{\alpha-1}x^\alpha$$

$$-hb_0-hb_1x-hb_2x^2-\cdots-hb_{\alpha-1}x^{\alpha-1}+r.$$

Odatle izjednačivanjem odgovarajućih koeficijenata na lijevoj i desnoj strani izlazi:

$$\begin{aligned}
a_\alpha &= b_{\alpha-1}\\
a_{\alpha-1} &= -hb_{\alpha-1}+b_{\alpha-2},\ \text{tj.}\ b_{\alpha-2}=hb_{\alpha-1}+a_{\alpha-1}\\
a_{\alpha-2} &= -hb_{\alpha-2}+b_{\alpha-3},\ \text{tj.}\ b_{\alpha-3}=hb_{\alpha-2}+a_{\alpha-2}\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
a_0 &= -hb_0+r\ ,\ \text{tj.}\ r=hb_0+a_0.
\end{aligned}$$

2.4.2. Istu stvar možemo pregledno i shematski predstaviti ovako: (niz svih koeficijenata od a ispisani *po starini*)

	a_α	$a_{\alpha-1}$,	$a_{\alpha-2}$,	$\ldots$,	a_{i+1},	$\ldots$,	a_2, a_1,	a_0
h	$a_\alpha=b_{\alpha-1}$,	$b_{\alpha-2}$,	$b_{\alpha-3}$,	$\ldots$,	b_i ,	$\ldots$,	b_1, b_0,	r

$$b_i=hb_{i+1}+a_{i+1}.$$

Drugi redić pokazuje i koeficijente kvocijenta $b(x)$ i ostatak r. Prvi član je $b_{\alpha-1}=a_\alpha$; svaki preostali član z u drugom retku dobije se tako da se prethodni član pomnoži sa h i umnošku pribroji član iz 1. retka koji je iznad z.

Taj postupak odnosno shema zove se (*Hornerov*) *sintetički postupak* dijeljenja.[1] Npr. polinom $a(x)=1-5x+6x^3+2x^4$ dijelimo sa $x-4$ po ovoj shemi

---

[1] W. G. Horner (1773—1827; Englez) objavio je gornju metodu 1819. godine; no, metoda se nalazi već 1804. kod Talijana Ruffini-a (1755—1822), a kažu da se nešto slično nalazi oko 5. stoljeća ranije kod Kineza Čin Čiu Šao.

	2	6	0	—5	1
4					
	2	14	56	219	877

Dakle je $a(x)=(x-4)(2x^3+14x^2+56x+219)+877$. Posebno je $a(4)=877$. U to se i inače lako uvjerimo!

2.4.3. Postupak dijeljenja sa $x-h$ možemo ponoviti i na dobivenu kvocijentu $b(x)$; ostatak pri dijeljenju je broj $b(h)$ pa je

$b(x)=(x-h)q(x)+b(h)$, što zbog $a(x)=(x-h)b(x)+a(h)$ daje

$a(x)=(x-h)^2 q(x)+(x-h)b(h)+a(h)$; itd.

2.4.4. Razvoj polinoma $a(x)$ oko tačke h. Imamo

$$a(x)=a(h)+a'(h)(x-h)+\frac{a''(h)}{2!}(x-h)^2+\ldots+\frac{a^{(\alpha)}(h)}{\alpha!}(x-h)^{\alpha}.$$

Koeficijent $a(h)$ je ostatak pri dijeljenju polinoma $a(x)$ sa $x-h$;

koeficijent $a'(h)$ je ostatak pri dijeljenju polinoma $\frac{a(x)-a(h)}{x-h}$ sa $x-h$;

koeficijent $\frac{a''(h)}{2!}$ je ostatak pri dijeljenju polinoma $\frac{a(x)-a(h)-a'(x-h)}{(x-h)^2}$

sa $x-h$

. . . . . .

Prema tome, iteracijom (Hornerove) sintetičke divizije sa $x-h$ dobiju se koeficijenti razvoja od $a(x)$ po potencijama od $x-h$; ti koeficijenti leže na sporednoj dijagonali b-ova u ovoj trokutnoj tablici b-ova;

	a_α	$a_{\alpha-1}$	$\ldots$	a_1	a_0
h	b_{11}	b_{12}		$b_{1\alpha}$	b_{10}
	b_{21}	b_{22}	$\ldots$	b_{21}	b_{20}
	.	.		.	
	.			.	
	.				
	$b_{\alpha-11}$	$b_{\alpha-10}$			
	$b_{\alpha 0}$				

2.4.5. Primjer: Napiši

$a(x)\equiv 5-3x^2+2x^4=b_0+b_1(x-3)+b_2(x-3)^2+b_3(x+3)^3+b_4(x-3)^4$;

odredi b-ove.

Shema izgleda ovako:

h	2	0	-3	0	5
3	2	6	15	45	$\boxed{140} = b_0$
	2	12	51	$\boxed{198} = b_1$	
	2	18	$\boxed{105} = b_2$		
	2	$\boxed{24} = b_3$			
	$\boxed{2} = b_4$.				

Traženi koeficijenti $b_0, b_1, \ldots, \ldots, b_4$ smješteni su po sporednoj dijagonali, pa je

$$a(x) = 140 + 198(x-3) + 105(x-3)^2 + 24(x-3)^3 + 2(x-3)^4.$$

Primjedba. Ako su koeficijenti ili h (ili oboje) brojevi s više cifara, onda se gornji postupak dijeljenja može obavljati tako da se najprije izvrši množenje a onda zbrajanje; takav se slučaj u praksi pojavljuje specijalno ako je h decimalan broj između 0 i 1. Npr.

h				
	35	-16	932	594
$\boxed{-8}$	$35 \cdot h \rightarrow$	-280		
		$-296 \cdot h \rightarrow$	2368	
			$3300 \cdot h \rightarrow$	-26400
				-25806

Tu je dobiveno da je

$$35x^3 - 16x^2 + 932x + 594 = (x+8)(35x^2 - 296x + 3300) - 25806.$$

2.4.6. Primjer. Oslobodi se kubnog člana u jednadžbi

$$a(x) = 2x^4 + 5x^3 + 4x - 1 = 0.$$

Dovoljno je staviti

$$t = x - 5 \cdot (4 \cdot 2)^{-1} = x - 0{,}625, \quad \text{odnosno}$$

$$x = t + 0{,}625.$$

Na taj način gornji zadatak svodi se na ovaj

2.4.6.1. Zadatak. *Umanji rješenje jednadžbe* $a(x) = 0$ *za broj* 0,625 *i nađi pripadnu jednadžbu radeći s tačnosti na* 2 *decimale.*

Prema gornjem rezultatu treba odrediti $a(t+0{,}625)$. Shema računanja izgleda ovako (pri tom množimo skraćeno na 2 dec.):

$h=-0{,}625$

2	5	0	4	−1
2	−1,25			
	3,75	−2,34	1,46	
			5,46 →	−3.41
				−4,41

2	−1,25		
	2,50 →	−1,56	
		−3,90 →	2,44
			7,90

2 →	−1,25	
	1,25 →	0,78
		−4,68

2
0
2

Tražena jednadžba glasi

$$-4{,}41+7{,}90\,t-4{,}68\,t^2+2\,t^3=0.$$

Drugim riječima, radeći na dvije decimale imamo

$$-1+4\,x+5\,x^3+2\,x^4=-4{,}41+7{,}90\,(x+0{,}625)-4{,}68\,(x+0{,}625)^2+$$
$$+2\,(x+0{,}625)^3.$$

3. TSCHIRNHAUSOVA TRANSFORMACIJA [1]

3.1. Ako je t linearna funkcija od x, onda se jednadžba $a(x)=0$ uvođenjem nepoznanice t može pojednostaviti npr. u tom smislu da koeficijent od t^{n-1} bude 0.

Promatrajmo sada zamršeniju transformaciju, stupnja 2:

$$t=c_0+c_1\,x+c_2\,x^2\equiv c\,(x), \tag{1}$$

pa pokušajmo npr. kubnu jednadžbu

$$a\,(x)\equiv a_0+a_1\,x+a_2\,x^2+a_3\,x^3=0 \tag{2}$$

---

[1] E. W. Tschirnhaus ili Tschirnhausen [Čirnhaus, Čirnhausen] (1681—1708); transformacija se pojavila u časopisu Acta Eruditorum 2 (1683), 204.

svesti na *binomski* oblik

(3) $$t^3 + \text{konst} = 0,$$

Neka su x_1, x_2, x_3 rješenja jednadžbe $a(x)=0$; tada rezolventa glasi:

(4) $$(t-t_1)(t-t_2)(t-t_3)=0,$$ gdje je

(5) $$t_i = c(x_i) \quad (i=1,\ 2,\ 3).$$

Označimo produkt u (4) sa $R(t)$, tj.

(6) $$R(t) \equiv (t-t_1)(t-t_2)(t-t_3) = R_0 + R_1 t + R_2 t^2 + t^3.$$

3.2. Odredimo nove koeficijente R_0, R_1, ...

Stavimo:

$$s_k = \sum_i x_i^k, \quad S_k = \sum_i t_i^k.$$

Tada prema *Newtonovim obrascima* (§ 2.2.2) postoje ove veze između *s*-ova, odnosno *S*-ova i *R*-ova (stavljajući $i' = \text{stupanj} - i$):

(7)
$$\begin{aligned} s_1 + \sigma_1 &= 0 & S_1 + R_{1'} &= 0 \\ s_2 + \sigma_1 s_1 + 2\sigma_2 &= 0 & S_2 + R_{2'} S_1 + 2R_{2'} &= 0 \\ s_3 + \sigma_1 s_2 + 3\sigma_3 &= 0 & S_3 + R_{1'} S_2 + 3R_{3'} &= 0. \end{aligned}$$

Prema tome, koeficijenti R_0, R_1, ... se lako izražavaju pomoću S_1, S_2, ... U drugu ruku, *S*-ovi se lako izražavaju pomoću *s*-ova; tako npr.

(8) $$S_1 = 3c_0 + c_1 s_1 + c_2 s_2$$ (to se dobiva sabirući j. (5)).

Nađimo S_2; najprije je

(9) $$t_i^2 = c_0^2 + 2c_0 c_1 x_1 + c_1^2 x_i^2 + 2c_0 c_2 x_i^2 + 2c_1 c_2 x_i^3 + c_2 x_i^4 \quad (i=1,\ 2,\ 3).$$

Zbog relacija $a(x_i)=0$, $x_i a(x_i)=0$, ... mogu se odatle potencije x_i^k za $k \geq \text{st } a$ izraziti pomoću potencija nižeg stupnja.

Iz (9) sabiranjem izlazi:

(10) $$S_2 \equiv \sum t_i^2 = 3c_0^2 + 2c_0 c_1 s_1 + c_1^2 s_2 + 2c_0 c_2 s_2 + 2c_1 c_2 s_3 + c_2^2 s_4.$$

No, *s*-ovi se po Newtonovim obrascima lako izražavaju pomoću *a*-ova. To znači da se, najzad, i *R-ovi* mogu izraziti pomoću *a*-ova. Drugim riječima.

—→ *Čirnhausova rezolventa može se napisati a da se i ne traže rješenja polazne jednažbe.*

3.3. Pokušajmo sada transformaciju $c(x)$ odrediti tako da rezolventa bude što jednostavnija, npr. tako da bude

(11) $$R_{1'} = 0 = R_{2'}.$$

No, zahtjev $R_{1'}=0$ znači isto što i $S_1=0$, pa se zato i zahtjev $R_{2'}=0$ svodi na zahtjev $S_2=0$. Drugim riječima, sistem (11) je ekvivalentan sa sistemom $S_1=0=S_2$. S obzirom na odnose (8), (10, to znači da se stvar svodi na rješavanje jednadžbi

$$3\,c_0+s_1\,c_1+s_2\,c_2=0$$

(12)

$$3\,c_0^2+2\,s_1\,c_0\,c_1+s_2\,c_1^2+2\,s_2\,c_0\,c_1+2\,s_3\,c_1\,c_2+s_4\,c_2^2=0$$

(nepoznate veličine su c_0, c_1, c_2; c_0 se iz prve jednadžbe unese u drugu pa se odatle nađe $c_1\,c_2^{-1}$, itd.

Na posve isti način dokazuje se

⟶ **3.4.** Teorem. *Zadana algebarska jednadžba* $a(x)=0$ *može se transformacijom* $t=c(x)$ *stupnja* 2, *odnosno* 3 *transformirati tako da pripadna rezolventa* $R(t)=0$ *zadovoljava uslovu*

$$R_{1'}=0;\quad R_{2'}=0,\quad \text{odnosno još i}\quad R_{3'}=0,$$

tu smo stavljali $i'=\text{st}\,R-i$.

Posebno to znači da u slučaju st $a=3$ ili 4, rezolventa poprima binomski oblik: $R_0+t^3=0$, odnosno $R_0+t^4=0$.

3.5. Izražavanje rješenja zadane jednadžbe pomoću rješenja rezolvente. Prikažimo stvar na slučaju st $c=2$. Imali smo jednakosti (5), (9), tj.

$$t_i=c_0+c_1\,x_i+c_2\,x_i^2 \tag{12}$$

$$t_i^2=(c_0+c_1\,x_i+c_2\,x_i^2)^2. \tag{13}$$

Ako se u (13) iskvadrira, x_i^3 ukloni pomoću $a(x_i)=0$ zatim x_i^4 ukloni pomoću $x_i\,a(x_i)=0$, postaje (13) oblika

$$t_i^2=c_0'+c_1'\,x_i+c_2'\,x_i^2.$$

Ako ovamo iz (12) donesemo x_i^2, dobiva se veza između x_i i t_i, t_i^2 oblika

$$x_i=c_0+l_1\,t_i+l_2\,t_i^2. \tag{14}$$

A to znači da je zadana jednadžba riješena, ukoliko je riješena rezolventa $R(t)=0$. *Kombinirajući taj rezultat s teoremom 3.4.* izlazi ovo:

⟶ **3.6.** Teorem. *Tschirnhausovom transformacijom svodi se algebarska jednadžba stupnja* 2, 3, 4 *na binomski oblik pa joj se rješenje može naći i izraziti pomoću koeficijenata jednadžbe primjenom racionalnih operacija te antikvadriranja i antikubiranja.*

3.7. Opća polinomna transformacija $t=c(x)$. — **3.7.1.** Tschirnhaus se zanosio mišlju da će se *svaka algebarska* jednadžba $a(x)=0$ *moći* svesti na *binomski oblik* i da će za to biti dovoljno povisivati stupanj polinoma $c(x)$. Zna

se da već za slučaj st $a=5$ *takva redukcija nije moguća* (1813: P. Ruffini (1765—1822), 1823: N. H. Abel (1802—1829) [1].

3.7.2. *Problem je ovaj: zadana je jednadžba*

(1) $$a(x)\equiv a_0+a_1x+a_2x^2+\cdots+a_\alpha x^\alpha=0$$ *kao i polinom*

(2) $$c(x)\equiv c_0+c_1x+c_2x^2+\cdots+c_\gamma x^\gamma;$$

treba odrediti normiranu jednadžbu

(3) $$R(t)\equiv R_0+R_1t+R_2t^2+\cdots+R_{\alpha-1}t^{\alpha-1}+t^\alpha=0$$

kojoj je spektar

(4) $$t_1=c(x_1),\ t_2=c(x_2),\ldots,\ t_\alpha=c(x_\alpha);$$ *pri tom je*

(5) $$\operatorname{Sp}a=x_1,\ x_2,\ldots,\ x_\alpha.$$

Problem se rješava analogno kao u posebnom slučaju u § 3.1.

Tražena normirana jednadžba glasi

(6) $$R(t)\equiv(t-t_1)(t-t_2)\cdots(t-t_\alpha)=0$$

i zove se *Tschirnhausenova rezolventa* [2] ishodne jednadžbe u odnosu na *Tschirnhausenovu polinomsku transformaciju* (2).

Rezolventa (3) nastaje eliminacijom od x iz jednadžbi $a(x)=0$, $t=c(x)$.

3.7.3. *Rezolventa* (3) *može se odrediti pomoću koeficijenata u* (1) *i* (2), *a da ni ne rješavamo jednadžbe* (1). Naime, služeći se Newtonovim formulama mogu se traženi koeficijenti $R_0, R_1, \ldots$ izraziti pomoću veličinâ

(7) $$S_i=t_1^i+t_2^i+\cdots+t_\alpha^i\quad(i=1,\ 2,\ldots,\ \alpha);$$

isto tako izražavaju se veličine

(8) $$s_i=x_1^i+x_2^i+\cdots+x_\alpha^i\quad(i=1,\ 2,\ldots,\ \alpha)$$

pomoću koeficijenata

(9) $$a_0,\ a_1,\ldots,\ a_\alpha$$

ishodne jednadžbe (1). Na taj način, posredstvom s_k, S_i izražavaju se *traženi koeficijenti* R_j *pomoću zadanih koeficijenata* (9). *U toj činjenici leži važnost Tschirnhausenove transformacije.*

3.7.4. Dokažimo da se veličine S_i u (7) izražavaju *racionalno* pomoću veličina s_k u (8). Naime, za $j=1,\ 2,\ldots,\ \alpha$ imamo

(10) $$t_j=c_0+c_1x_j+c_2x_j^2+\cdots+c_\gamma x_j^\gamma;$$

---

[1] Ipak, spomenimo da se jednadžba stupnja 5 može transformacijom stupnja 4 svesti na tzv. Bring-Jerrardov oblik $t^5+t+\text{konst}=0$ (Bring, 1786; Jerrard, 1834).

[2] Stvar je u časopisu Acta Eruditorum 2 (1683), str. 204—207 obradio njemački matematičar E. W. Tschirnhausen ili Tschirnhaus [č. Čirnhauzen ili Čirnhaus] (1651—1708),

iz $a(x_j)=0$ izlazi

$$x_j^{\alpha} = -a_{\alpha}^{-1}(a_0 + a_1 x_j + \cdots + a_{\alpha-1} x_j^{\alpha-1}). \tag{11}$$

Množeći jednadžbu (11) sa x_j i dovodeći u nju izraz (11) za x_j^{α} vidi se da je $x_j^{\alpha+1}$ izraženo pomoću veličina

$$x_j,\ x_j^2, \ldots,\ x_j^{\alpha-1}. \tag{12}$$

Množeći dobiven izraz za $x_j^{\alpha+1}$ sa x_j dokazuje se analogno da se i $x_j^{\alpha+2}$ može izraziti linearno pomoću veličina (12). Induktivno, vidi se *da se za svaki prirodni broj n potencija* x_j^n *može izraziti linearno pomoću veličina* (12).

3.7.5. Odatle specijalno izlazi da se u transformaciji (2) može pretpostaviti da je $\gamma \leq \alpha-1$, tj. da je $\mathrm{st}\, c < \mathrm{st}\, a$. To ćemo odsada i pretpostavljati: $\gamma = \alpha-1$.

3.7.6. U drugu ruku, zbrojimo li jednadžbe (10) za $j=1, 2, \ldots, \alpha$ dobije se veza $S_1 = \alpha c_0 + c_1 s_1 + \cdots + c_{\alpha-1} s_{\alpha-1}$. Isto tako, kvadrirajući jednadžbu (10) i uklanjajući potencije x_j^n za koje je $n \geq \alpha$ vidi se da t_j^2 možemo izraziti linearno pomoću veličina (12) i s koeficijentima koji zavise od a_i, c_k. Stvar se prenosi i na potencije t_j^3, $t_j^4, \ldots$; *sve se one linearno izrazuju pomoću* (12) *s koeficijentima koji zavise od zadanih koeficijenata u* $a(x)$, $c(x)$.

Time je teoretski tražena rezolventa $R(x)=0$ određena.

3.7.7. Određivanje spektra Sp *a* iz Sp *R*. Znamo li spektar Sp R rezolvente R može se naći i spektar Sp a ishodne jednadžbe. Naime, upravo vidjesmo da se veličine $t_j,\ t_j^2, \ldots,\ t_j^{\alpha-1}$ izražavaju linearno pomoću (12), recimo

$$t_j^i = c_0^{(i)} x_j + c_1^{(i)} x_j + c_2^{(i)} x_j^2 + \cdots + c_{\alpha-1}^{(i)} x_j^{\alpha-1} \quad (i = 1,\ 2, \ldots,\ \alpha-1); \tag{13}$$

koeficijenti $c_k^{(i)}$ zavise od koeficijenata od $a(x)$ i $c(x)$; posebno je $c_k^{(1)} = c_k$. U (13) imamo $\alpha-1$ linearnu jednadžbu s nepoznanicama (12); specijalno za $i=1$ izlazi $t_j = c(x_j)$; sistem ima rješenje.

Za zadano $j \in \{1, 2, \ldots, \alpha\}$ možemo sistem (13) riješiti npr. tako da eliminiramo $x_j^{\alpha-1}$ pa $x_j^{\alpha-2} \ldots, x_j^2$.

Ako u spektru Sp R ima članova koji se ponavljaju, npr. ako se t_1 ponavlja k puta, tada to znači da jednadžbe $a(x)=0$, $t_1 = c(x)$ imaju k korijena koji zadovoljavaju najvećoj zajedničkoj mjeri $M(x)$ polinomâ $a(x)$, $c(x)-t_1$. No, $M(x)$ se iz tih polinoma određuje elementarno; naravno, $\mathrm{st}\, M(x) = k$. Ako zadana jednadžba nema višestrukih korijena, tada je $k < \alpha$ pa se elementarno dolazi do faktora $M(x)$ ishodnog polinoma $a(x)$; time se i *rješavanje jednadžbe* $a(x)=0$ *svodi na rješavanje faktorskih jednadžbi* $M(x)=0$, $a(x)/M(x)=0$.

3.7.8. Rezolventa u obliku determinante.

Pođimo od jednadžbe

$$t_j = c_0 + c_1 x_j + c_2 x_j^2 + \cdots + c_{\alpha-1} x_j^{\alpha-1} \quad (\text{tj. } t_j = a(x_j)); \tag{14}$$

odatle:

$$x_j t_j = c_0 x_j + c_1 x_j^2 + \cdots + c_{\alpha-1} x_j^{\alpha}$$

što s obzirom na (11) pokazuje da se izraz $x_j t_j$ prikazuje linearno u veličinama (12); isto vrijedi za $x_j^2 t_j$ pa za $x_j^3 t_j, \ldots$; recimo neka je za $i \in \{0, 1, 2, \ldots, \alpha-1\}$

$$x_j^i t_j = c_{i0} a_{i1} x_j + c_{i2} x_j^2 + \cdots + c_{i\alpha-1} x_j^{\alpha-1}, \text{ tj.}$$

$$c_{i0} + c_{i1} x_j + \cdots + (c_{ii} - t_j) x_j^i + \cdots + c_{i\alpha-1} x_j^{\alpha-1} = 0 \quad (i = 0,\ 1,\ 2, \ldots,\ \alpha-1.$$

To je sistem homogenih linearnih jednadžbi, pa iz njega izlazi

$$(15) \qquad \begin{vmatrix} c_{00}-t_j & c_{01} & \cdots & c_{0\alpha-1} \\ c_{10} & c_{11}-t_j & \cdots & c_{1\alpha-1} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ c_{\alpha-10} & c_{\alpha-11} & \cdots & c_{\alpha-1\,\alpha-1}-t_j \end{vmatrix} = 0.$$

Ta je determinanta uistinu jednaka 0 kao što se vidi kada prvom stupcu pribrojimo drugi stupac umnožen sa x_j, treći stupac umnožen sa $x_j^2, \ldots$, posljednji stupac umnožen sa $x_j^{\alpha-1}$; time prvi stupac postaje 0. To znači da je i sama determinanta $= 0$. Drugim riječima, članovi t_j spektra $\mathrm{Sp}\, R$ su ništišta funkcije

$$(16) \qquad \begin{vmatrix} c_{00}-t & c_{01} & \cdots & c_{0\alpha-1} \\ \cdots & \cdots & \cdots & \cdots \\ c_{\alpha-10} & \cdots & \cdots & c_{\alpha-1\,\alpha-1}-t \end{vmatrix}$$

Ako u $\mathrm{Sp}\, R$ nema jednakih članova, onda vidimo da je $(16) = (3)_1$, jer je k tome i $\mathrm{st}\,(3)_1 = \mathrm{st}\,(16)$.

Međutim, relacija $(16) = (3)_1$ vrijedi i u slučaju kada u $\mathrm{Sp}\, R$ ima jednakih članova, jer se ovaj slučaj prikazuje kao granični slučaj prethodnoga. Naime, neka su $z_1, z_2, \ldots, z_\alpha$ nezavisne varijable, a $\sigma_1, \sigma_2, \ldots, \sigma_\alpha$ pripadne osnovne simetrične funkcije; tada su općenito veličine

$$(17) \qquad t_i = c(z_i) \quad (i = 1,\ 2, \ldots,\ \alpha)$$

nejednake pa poništavaju funkciju (16). No veličine c_{ik} koje se u (16) pojavljuju jesu cijele racionalne funkcije u odnosu na $\sigma_1, \ldots, \sigma_\alpha$, a simetrični polinomi u odnosu na $z_1, z_2, \ldots, z_\alpha$; variranjem veličina z_i relacija $(16) = 0$ ostaje na snazi uvijek, iz razloga neprekidnosti i to bez obzira da li među pripadnim veličinama (17) ima i jednakih veličina.

4. RECIPROČNA TRANSFORMACIJA. RECIPROČNE JEDNADŽBE

4.1. Reciproćna transformacija je oblika $t = x^{-1}$. Njome jednadžba $a(x) = 0$ prelazi u $a(t^{-1}) = 0$.

4.2. Reciproćne jednadžbe. To su jednadžbe koje su ekvivalentne sa svojim recipročnim transformatom: $a(x) = 0$ treba biti ekvivalentno sa $a(x^{-1}) = 0$.

To znači: ako je x_k rješenje od $a(x)=0$, onda je i x^{-1} rješenje, i to *iste kratnosti*. Tako npr. jednadžba $3x^4-2x^3+5x^2-2x+3=0$ očigledno je recipročna; recipročnom transformacijom prelazi ona u

$$3x^{-4}-2x^{-3}+5x^{-2}-2x^{-1}+3=0.$$

4.2.1. Ta jednadžba zadovoljava relacijama simetrije

$$a_k=a_{k'}, \tag{1}$$

gdje je $k'=\operatorname{st}a-k$, za $k=0, 1, \ldots, \operatorname{st}a$.

Za svaki polinom a sa svojstvom (1) *jednadžba* $a(x)=0$ *je simetrična.*

Uistinu

$$a(x^{-1})=a_0+a_1x^{-1}+a_2x^{-2}+\cdots+a_nx^{-n}=x^{-n}(a_0x^n+$$
$$+a_1x^{n-1}+\cdots+a_{n-1}x+a_n)= \text{ (zbog (1)) } =x^{-n}(a_{0'}x^n+$$
$$+a_{1'}x^{n-1}+\cdots+a_{(n-1)'}x+a_{n'})=x^{-n}a(x), \text{ tj.}$$

$$a(x^{-1})=x^{-n}a(x), \text{ odnosno } x^na(x^{-1})=a(x). \tag{2}$$

A to znači da su jednadžbe $a(x)=0$ i $a(x^{-1})=0$ ekvivalentne. Dakle je $a(x)=0$ recipročna jednadžba.

Odmah se vidi da iz (2) proizlazi (1). Naime, (2) znači da je

$$x^n(a_0+a_1x^{-1}+\cdots+a_nx^{-n})=a_0+a_1x+\cdots+a_nx^n.$$

Izjednačujući odgovarajuće koeficijente na obje strane na toj jednadžbi, dolazimo upravo do (1).

4.2.2. I u slučaju *kose simetrije*:

$$a_k=-a_{k'} \quad (k=0, 1, \ldots, \operatorname{st}a) \quad k'=\operatorname{st}a-k \tag{3}$$

jednadžba je recipročna. Dokaz se provodi kao u slučaju simetrije (1), jer

$$a(x^{-1})=a_0+a_1x^{-1}+\cdots+a_{n-1}x^{-(n-1)}+a_nx^{-n}=\text{(zbog (3))}=$$
$$=(-a_{0'}-a_{1'}x^{-1}-\cdots-a_{n'}x^{-n})=$$
$$=x^{-n}(a_nx^n+\cdots+a_0)=x^{-n}a(x).$$

Prema tome, imamo:

$$a(x^{-1})=-x^{-n}a(x), \text{ tj.} \tag{4}$$
$$x^na(x^{-1})=-a(x).$$

Odatle proistječe tražena recipročnost jednadžbe $a(x)=0$. Dodajmo da iz odnosa (4) proizlaze relacije (3). Dokaz je sličan onome da iz (2) izlazi (1).

4.3. Dva tipa recipročnih jednadžbi. Na taj smo način došli do dviju vrste recipročnih jednadžbi: onih za koje vrijedi simetrija (1) — to su *recipročne jednadžbe tipa I* — i onih za koje vrijedi *kosa simetrija* (3) — *recipročne*

jednadžbe tipa II. Može se pokazati da drugih recipročnih jednadžbi i nema: *svaka recipročna jednadžba* $a(x)=0$ *je takva da vrijedi ili* (1) *ili* (3).

Uistinu, neka je α kratnost broja 1 kao rješenje simetrične jednadžbe $a(x)=0$; isto tako neka je β kratnost broja -1; naravno da može biti $\alpha=0$; to znači da broj 1 nije nula-tačka polinoma $a(x)$. Preostale nula-tačke dolaze spareno: neka z_1 i z_1^{-1} imaju kratnost k_1; z_2, z_2^{-1} kratnost k_2, itd.

Tada je

$$a(x)=a_n\cdot(x-1)^{\alpha}(x+1)^{\beta}(x-x_1)^{k_1}(x-x_1^{-1})^{k_1}(x-x_2)^{k_2}(x-x_2^{-1})^{k_2}\cdots=$$
$$=a_n\cdot(x-1)^{\alpha}(x+1)^{\beta}(x^2-[x_1+x_1^{-1}]x-1)^{k_1}(x^2-[x_2+x_2^{-1}]x-1)^{k_2}\cdots,$$

tj.

$$a(x)=a_n\cdot(x-1)^{\alpha}(x+1)^{\beta}(x^2-[x_1+x_1^{-1}]x-1)^{k_1}\cdots \tag{5}$$

Naravno, $\alpha+\beta+2k_1+2k_2+\cdots=\operatorname{st}a=n$.

Stavimo li u gornji rezultat x^{-1} umjesto x, izlazi

$$a(x^{-1})=a_n(x^{-1}-1)^{\alpha}(x^{-1}+1)^{\beta}(x^{-2}-[x_1+x_1^{-1})x^{-1}-1)^{k_1}\cdot(x^{-2}-[x_2+x_2^{-1}]x^{-1}-1)\ldots$$

No,

$$(x^{-1}-1)^{\alpha}=x^{-\alpha}(1-x)^{\alpha}=x^{-\alpha}(-1)^{\alpha}(x-1),\ (x^{-1}+1)^{\beta}=x^{-\beta}(1+x)^{\beta},$$

$$(x^{-2}-[x_1+x_1^{-1}]x^{-1}-1)^{k_1}=x^{-k_1}(1-[x_1+x_1^{-1}]x-x^2),\ldots$$

Na taj način, a na osnovu (5), izlazi

$$a(x^{-1})=(-1)^{\alpha}x^{-\alpha-\beta-2k_1-2k_2}\cdots a(x)=(-1)^{\alpha}x^{-n}a(x).$$

Množenjem sa x^{-n} izlazi:

$$x^n a(x^{-1})=(-1)^{\alpha}a(x); \tag{6}$$

pri tom je α kratnost broja 1 kao nula-tačke polinoma a. To znači, ako je α parno (npr. $\alpha=0$), tada relacija (6) postaje (2), a to znači da vrijedi simetrija (1); ako je α neparno, tada (6) glasi (4) pa imamo kosu simetriju (3). Dakle, za svaki recipročni polinom $a(x)$ vrijedi ili (1) ili (3).

Često se umjesto o recipročnim jednadžbama govori o *simetričnim jednadžbama.* Međutim, ispravnije je da se govori o *recipročnim* jednadžbama, pogotovu što može nastupiti i *kosa simetrija* koeficijenata, tj. relacija (3).

4.4. Kako se rješavaju recipročne jednadžbe. — 4.4.1. *Stupanj: paran; tip I.* Uzmimo primjer jednadžbe stupnja 4 i tipa I; opći joj je oblik

$$a_0+a_1x+a_2x^2+a_1x^3+a_0x^4=0. \tag{7}$$

Odatle

$$a_0(1+x^4)+a_1(x+x^3)+a_2x^2=0\ |\cdot x^{-2}$$
$$a_0(x^{-2}+x^2)+a_1(x^{-1}+x)+a_2=0. \tag{8}$$

Provedimo *zamjenu*:

(9) $$x^{-1}+x=t,$$

dakle

$$x^{-2}+x^2=t^2-2.$$

Time jednadžba (8) postaje

$$a_0(t^2-2)+a_1 t+a_2=0.$$

Odatle se nađe t, a nadalje iz (9) i traženo x. Primijetimo da se jednadžba (9) svodi na kvadratnu jednadžbu.

Slično se radi sa *svakom recipročnom jednadžbom* tipa I i parnog stepena $2n$:

Jednadžbu

(10) $$a_0+a_1 x+a_2 x^2+\cdots+a_n x^n+a_{n-1} x^{n+1}+\cdots+a_1 x^{2n-1}+a_0 x^{2n}=0$$

možemo pisati i ovako, pomnoživši je sa x^{-n}:

(11) $$a_0(x^{-n}+x^n)+a_1(x^{-(n-1)}+x^{n-1})+\cdots+a_{n-1}(x^{-1}+x)+a_n=0.$$

Supstitucijom (9) svodi se njeno rješavanje na rješavanje jednadžbe stupnja n i na n kvadratnih jednadžbi. Pri tom znajmo da je $x^{-k}+x^k$ izrazivo u t kao polinom stupnja k, a na osnovu obrasca:

$$x^{-(k+1)}+x^{k+1}=(x^{-k}+x^{-k})(x^{-1}+x)-(x^{-(k-1)}+x^{k-1}) \text{ za } k=1,\ 2,\ldots$$

Ta se jednakost neposredno provjerava.

Npr. $$x^{-3}+x^3=t^3-3t$$

$$x^{-4}+x^4=t^4-4t^2+2.$$

4.4.2. *Recipročna jednadžba neparnog stupnja i tipa I.* Neka je $\operatorname{st} a=2s+1$; tada prema obrascu (2) imamo:

$$x^{2s+1}a(x^{-1})=a(x).$$

Odatle, stavljajući $x=-1$:

$$-a(-1)=a(-1),\ \text{tj.}\ a(-1)=0.$$

To znači da je -1 nula-tačka polinoma $a(x)$; dakle je $a(x)$ djeljivo sa $x+1$; pa neka je $g(x)=a(x)(x+1)^{-1}$. Tvrdimo da je $g(x)$ *recipročan polinom parnog stepena i tipa I.*

Naravno, $\operatorname{st} g=2s=\operatorname{st} a-1$; dokažimo da je $g(x)$ recipročno i tipa *I*, tj. da je

(12) $$x^{2s}g(x^{-1})=g(x).$$

No, $$x^{2s}g(x^{-1})=x^{2s}a(x^{-1})(x^{-1}+1)^{-1}=x^{2s}a(x^{-1})x(1+x^{-1})^{-1}=$$

$$=x^{2s+1}a(x^{-1})(x+1)^{-1}=a(x)(x+1)^{-1}=g(x).$$

Dakle, uistinu vrijedi (12).

4.4.3. *Recipročne jednadžbe tipa II.* Za njih je

$$x^{\mathrm{st}\,a}\,a(x^{-1}) = -a(x).$$

Odatle za $x=1$ izlazi $1^{\mathrm{st}\,a}\,a(1) = -a(1)$, tj. $a(1)=0$.

Dakle je broj 1 jedno rješenje jednadžbe $a(x)=0$, pa je polinom $a(x)$ djeljiv sa $x-1$, tj. funkcija $h(x)=a(x)(x-1)^{-1}$ je jedan polinom. Lako se vidi da je $h(x)=0$ recipročna jednadžba tipa II.

⟶ **4.4.4. Gornja analiza pokazuje specijalno ovo:** ***ako je jednadžba*** $a(x)=0$ ***recipročna, tada treba najprije ustanoviti da li među brojevima*** -1, 1 ***ima koje njeno rješenje; zatim treba odrediti kratnost*** α ***od*** -1 ***i kratnost*** β ***od*** 1. ***Jednadžba***

$$a(x)(x+1)^{-\alpha}(x-1)^{-\beta}=0$$

je opet recipročna, ali joj ne zadovoljava ni -1 ***ni*** $+1$. ***Zato je ona tipa I i parnog stupnja. Rješava se kao maloprije u t.*** 1.

4.4.5. Primjedba. Iz relacija (3) u § 4.2.2. vidi se ovo: ako je $\mathrm{st}\,a$ paran broj $2s$, tada je

$$-a_s = a_{s'} = a_s, \quad \text{tj.} \quad a_s = 0.$$

Primjer:

$$x^6-4x^5+3x^4-3x^2+x-1=0.$$

5. TRANSFORMACIJE POMOĆU RACIONALNIH FUNKCIJA

5.1. Uzmimo da se radi o *homografiji*

$$t=\frac{ax+b}{cx+d}.$$

Kako je

$$\frac{ax+b}{cx+d}=\frac{a}{c}-\frac{ad-bc}{c^2\left(x+\frac{d}{c}\right)},$$

to se gornja transformacija svodi na *slaganje ovih transformacija*: x se uveća za d/c *pa se pomnoži sa* c^2, *provede recipročna* transformacija pa pomnoži sa $-(ad-bc)$ i doda a/c.

5.2. Promatrajmo opću racionalnu transformaciju

$$t=R(x), \quad R(x)=\frac{P(x)}{Q(x)}.$$

Možemo uzeti da su P i Q *relativno prosti*; $a(x)$, $Q(x)$ neka su također relativno prosti. To znači da je posebno $Q(a_{(t)})\neq 0$ za svaku nula-tačku

$a_{(i)}$ polinoma $a(x)$. Prema Bézoutovu identitetu (isp. pogl. 7, § 5. 4) postoje polinomi $u(x)$, $v(x)$, za koje je

$$a(x)u(x)+Q(x)v(x)=1.$$

Odatle, množeći sa $P(x)$, izlazi:

$$a(x)u(x)P(x)+Q(x)P(x)v(x)=P(x).$$

Neka je (prema osnovnoj lemi o dijeljenju primjenjenoj na polinome $P\cdot v$, a):

$$P(x)v(x)=a(x)q(x)+r(x),\ r=0 \text{ ili } \operatorname{st} r<\operatorname{st} a.$$

Time prethodna jednakost postaje

$$auP+(aq+r)Q=P,$$

odnosno

$$a(uP+qQ)+rQ=P.$$

Posebno, za nula-tačku od a, tj. za

$$x=a_{(1)},\ a_{(2)},\ \ldots,\ a_{(n)},$$ imamo odatle

$$a(a_{(i)})(u(a_{(i)})P(a_{(i)})+q(a_{(i)}))Q(a_{(i)})+r(a_{(i)})Q(a_{(i)})=P(a_{(i)}).$$

Zbog $a(a_{(i)})=0$ znači da je

$$r(a_{(i)})=P(a_{(i)}/Q(a_{(i)}).$$

Drugim riječima, *zadana razlomljena funkcija* $P(x)/Q(x)$ i *nađeni polinom* $r(x)$ stupnja $<\operatorname{st} a$ prevode *svaku nula-tačku* $a_{(i)}$ *od* a u *isti broj*; zato je *rezolventa jednadžbe* $a(x)=0$ s obzirom na transformaciju $t=P(x)/Q(x)$ ista kao i s obzirom na polinomijalnu transformaciju $t=r(x)$.

Zato promatranje *razlomljenih transformacija* pomoću *racionalnih* funkcija ne daje *ništa novo* u odnosu prema transformacijama pomoću cijelih racionalnih funkcija.

6. Zadaci o transformacijama jednadžbi.

Kao i inače, za polinom $a(x)=a_0+a_1x+\ldots+a_nx^n$, gdje je $a_n\neq 0$ znači Sp a (spektar od a) neuređen niz brojeva $x_1, x_2, \ldots, x_n$ za koje je $a(x)=a_n\prod(x-x_k)$; naravno $\operatorname{Sp} a+h=x_1+h_1,\ x_2+h,\ldots,\ x_n+h$; $\operatorname{Sp} a\cdot h=x_1h,\ x_2h,\ldots,\ x_nh$ itd.

1. Zamjenom $t=x-h$ oslobodi se člana koji stoji uz najuglednijeg člana u ovim jednadžbama: 1) $2x^2+5x-6=0$, 2) $x^3+2x^2+5x-6=0$, 3) $x^4+x^3+2x^2+5x-6=0$; 4) $x^4+x^3+2x^2+5x+6=0$; 5) $x^4-x^3-2x^2-5x+6=0$; 6) $x^5+3x^4=0$; 7) $x^8+6x^7-x+1=0$.
2. Sredi po t izraz $a(t+h)$ za $h=2$ i polinome koji znače lijevu stranu u zadacima 1.
3. Podijeli sa $x-5$ lijevu stranu u jednadžbi iz zad. 1.

4. Odredi jednadžbu $g(x)=0$ za koju je $\mathrm{Sp}\, g=\mathrm{Sp}\, f-5$; pri tom je f lijeva strana u jednadžbi zadatka 1.

5. Isto pitanje uz uslov $\mathrm{Sp}\, g=-\mathrm{Sp}\, f$.

6. Isto pitanje uz uslov $\mathrm{Sp}\, g=-\mathrm{Sp}\, f+1$.

7. Isto pitanje zahtijevajući $\mathrm{Sp}\, g=3\,\mathrm{Sp}\, f$.

8. Isto pitanje uz uvjet $\mathrm{Sp}\, g=3\,\mathrm{Sp}\, f+1$.

9. Isto pitanje za zahtjev $\mathrm{Sp}\, g=(\mathrm{Sp}\, f)^2$.

10. Nađi Tschirnhausovu rezolventu za ove jednadžbe i ove transformacije; odredi obratne transformacije:
1) $x^3-x+2=0$, $t=x+x^2$, 2) $x^4-3x+1=0$, $t=x^3+x$;
3) $x^4+5x^3+6x^2-1=0$, $y=x^3+4x^2+3x-1$;
4) $x^3-x^2-2x+1=0$, $y=2-x^2$; 5) $x^3-2x-3=0$, $t=1-2x-x^2$;
6) $x^3-x-1=0$, $t=\dfrac{x-3}{x}$.

11. Zadana je jednadžba $x^3-3x+5=0$; nađi jednadžbu kojoj zadovoljavaju vrijednosti izraza: 1) x_i^2; 2) $(x_i-x_k)^2$; 3) x_k^2; 4) x_k^3; 5) $x_i x_k$ $(i\neq k)$; 6) $x_i x_k^{-1}$ $(i\neq k)$.

12. Preobrazi: 1) $a(x)=0$ supstitucijom (smjenom) $t=x+x^{-1}$;
2) $x^3+2x^2-3x-2=0$, $t=(1-x^2)^{-1}$;
3) $x^3+3x-2=0$, $t=\dfrac{t-1}{t^2+1}$;
4) $x^3+3x+2=0$, $t=\dfrac{t+1}{t^2+1}$.

12.[a] Odredi polinomsku transformaciju $t=t_0+t_1x+\cdots$ koja je ravnopravna s transformacijom u zad. 12.

13. Preobrazi $f(x)=0$ stavljajući 1) $t=x^2$; 2) $t=x^3$.

14. Odredi preslikavanje $t=a+bx+cx^2$ tako da slijedeća jednadžba prijeđe u binomski oblik:
1) $x^3+2x^2-5=0$; 2) $x^3+3x-5=0$; 3) $x^3+x^2+3x-5=0$.

15. Neka je x_1, x_2, x_3, x_4 spektar polinoma x^4+px^2+qx+r; odredi jednadžbu kojoj su brojevi $\frac{1}{4}(x_1+x_2-x_3-x_4)^2$ jednostruki korijeni.

Literatura

Faddeev-Sominskij [1]; Kuroš [1]; Obreškov [1], [2]; Perron [1]: Plemelj [1]; Serret [1]; Weber [1].

POGLAVLJE 22.

KONGRUENCIJE VIŠEG STEPENA

1. KONGRUENCIJE VIŠEG STEPENA. POJAM

1.1. Povratimo se na kolo D cijelih brojeva pa promatrajmo kolo $D[x]$ polinomâ u x s koeficijentima iz D.

No, sad ćemo uzimati da je $x \in D$ i pustiti da x neodređeno varira po D; prema tome, kad se sad kaže $x \in D[x]$, onda to znači da je a određen član iz $D[x]$ oblika $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ i da za svako $x \in D$ imamo vrijednost $a(x)$.

1.2. Promatrat ćemo kongruencije, ali s modulom m, koji je zasad broj $\neq 0$ (a ne npr. kakav polinom višeg stepena).

1.3. Definicija. Za polinom — funkciju $a(x)$ relacija

$$a(x) \equiv 0 \pmod{m} \tag{1}$$

značit će da je broj $a(x)$ djeljiv brojem m. Svaki broj x za koji vrijedi (1) zove se *rješenje kongruencije* (1).

1.4. Definicija. Sredi li se polinom $a(x)$ po stepenima od x, recimo $a(x) = a_0 + a_1 x + \cdots + a_n x^n$, pa ako je $a_n \not\equiv 0 \pmod{m}$, kaže se da je kongruencija *a stupnja n*.

Koeficijent a_n zove se *najstariji* ili *najugledniji* koeficijent polinoma $a(x)$ mod m.

Tako je npr.

$$12x - 4x^3 + 9x^4 \equiv 0 \pmod{3}$$

kongruencija stupnja 3; koeficijenti $\equiv 0 \bmod 3$ mogu se izostaviti; izlazi

$$-4x^3 \equiv 0 \pmod{3}, \quad \text{dakle}$$

$$x^3 \equiv 0 \pmod{3}$$

$$x \equiv 0 \pmod{3}.$$

Kongruencija $x^6 \equiv 1 \pmod{7}$

je stupnja 6; rješenja su joj 1, 2, 3, 4, 5, 6, ili, što je isto, 1, 2, 3, −3, −2, −1 (ovo je lakše provjeriti).

1.5. Uopće, prema Fermatovu poučku za svaki prost broj p ima kongruencija

$$x^{p-1} \equiv 1 \pmod{p} \tag{2}$$

upravo p rješenja koja su međusobno inkongruentna; zadovoljava je svaki cijeli broj koji je prost prema p.

1.6. Teorem. *Ako je*

$$a(x_0) \equiv 0 \pmod{m}, \tag{3}$$

onda je

$$a(x) \equiv (x - x_0)\, q_0(x) \pmod{m}; \tag{4}$$

i obratno: *iz* (4) *izlazi* (3).

Tu se vidi analogija s jednadžbama.

Dokaz se temelji na osnovnom obrascu o dijeljenju. Naime, podijelimo li $a(x)$ sa $x - x_0$, izlazi

$$a(x) = (x - x_0)\, q(x) + c \text{ (konstanta)},$$

odakle za $x = x_0$ dobivamo

$$a(x_0) = c, \text{ tj.}$$

$$a(x) = (x - x_0)\, q(x) + a(x_0). \tag{5}$$

Iz (5) se odmah očitava teorem 1.6.

1.7. Lagrangeov teorem. *Kongruencija* $a(x) \equiv 0 \pmod{p}$ *ima* $\leq$ st a *nekongruentnih rješenja.*

To zaključujemo postepeno iz 1.6. razlažući polinom $a(x)$ po rješenjima x_0, x_1, ... Naime, ako je $x_i \not\equiv x_0$ i $a(x_i) \equiv 0 \pmod{p}$, tada prema 1.6. imamo

$$a(x) \equiv (x - x_i)\, q_i(x) \pmod{p}. \tag{6}$$

Odatle posebno izlazi

$$a(x_0) \equiv (x_0 - x_1)\, q_1(x) \pmod{p}$$

$$0 = \underbrace{(x_0 - x_1)}_{\not\equiv 0}\, q_1(x_0) \pmod{p}$$

$$0 \equiv q_1(x_0) \pmod{p}.$$

Primjenom obrasca 1.6: (piši $q_0(x)$ umjesto $a(x)$) izlazi odatle:

$$(x - x_0)\, q_{00}(x_0) \equiv q_1(x) \pmod{p},$$

tj. množeći sa $(x - x_1)$;

$$(x - x_0)(x - x_1)\, q_{00}(x) \equiv (x - x_1)\, q_1(x) \pmod{p}.$$

A to s obzirom na (6) za $i = 1$ postaje

$$(x - x_0)(x - x_1)\, q_{00}(x) \equiv a(x) \pmod{p}. \tag{7}$$

Ako je, dalje, x_2 novo rješenje kongruencije (3), koje je $\not\equiv x_0$ i $\not\equiv x_1$, tada analogno iz (7) zaključujemo (stavi $x = x_1$) da je

$$q_{00}(x_2) \equiv (\text{mod } p),$$

dakle prema 1.6. opet

$$q_{00}(x) = (x - x_2)\, q_{000}(x), \ (\text{mod } p).$$

Množenjem te kongruencije sa $(x-x_0)(x-x_1)$ izlazi analogno

$$a(x) \equiv (x-x_0)(x-x_1)(x-x_2)\, q_{000}(x) \ (\text{mod } p), \qquad \text{itd.}$$

Kako je $\text{st}\, a_0 > \text{st}\, q_0 > \text{st}\, q_{00} > \cdots$, jasno je da se najkasnije poslije $\text{st}\, a$ koračaja dolazi na konstantu.

Time je Lagrangeov teorem dokazan.

1.8. *Pretpostavka da je modul prost broj je nužna*; već najjednostavniji slučaj *linearnih* kongruencija pokazuje da broj rješenja, za složen modul, može biti $> \text{st}\, a$. Tako npr. kongruencija stupnja 1:

$$6x - 8 \equiv 0 \ (\text{mod } 4)$$

ima dva nekongruentna rješenja 0 i 2 (ona je stvarno zadovoljena za svako parno $x \in D$).

1.9. Korolar. *Ako kongruencija* $a(x) \equiv 0 \ (\text{mod } p)$ *ima* $> \text{st}\, a$ *nekongruentnih rješenja, onda su svi koeficijenti polinoma a djeljivi sa p.*

To je neposredna posljedica Lagrangeova teorema.

1.10. Teorem. *Ako su brojevi* $m_1, m_2, \ldots, m_k$ *dva po dva međusobno prosta, tada iz*

(7) $$a(x) \equiv 0 \ (\text{mod } m_1 m_2 \ldots m_k)$$ *izlazi:*

(8_i) $$a(x) \equiv 0 \ (\text{mod } m_i) \ i = 1, 2, \ldots, k.$$ *I obratno.*

Ako je $N(m)$ *broj rješenja kongruencija* (7), *a* $N(m_i)$ *broj rješenja kongruencije* (8_i), *tada je*

(9) $$N(m) = N(m_1)\, N(m_2) \ldots N(m_k).$$

Da iz (7) izlazi (8) i obratno, to je osnovni teorem o dijeljenju međusobno prostim brojevima. Iz istog razloga stoji (9). Naime, neka je $r(m_i)$ skup rješenja kongruencije (8_i) za dano $i = 1, 2, \ldots, k$; neka je $r_i \in r(m_i)$; ako tada odredimo x iz sistema $x \equiv r_i, \ (\text{mod } m_i)$, mijenjajući r_i, dobiva se svaki put drugo rješenje za (7).

Primjer. Neka je

$$a(x) = x^3 + 3x^2 + 4x + 2;$$

imamo kongruenciju

$$a(x) \equiv 0 \ (\text{mod } 12);$$

ona je ekvivalentna sa sustavom kongruencijâ

$$a(x) \equiv 0 \ (\text{mod } 3)$$

$$a(x) \equiv 0 \ (\text{mod } 4).$$

Znači da je

$$x \equiv 2 \pmod 3$$

$$x \equiv 3 \pmod 4.$$

Odatle je $x = 2 + 3k = 3 + 4m$, tj. $x = 12t - 1$.
Dakle je $x = 11$ traženo rješenje (samo je jedno).

1.11. Svođenje kongruencije na module p^e. Na osnovu prethodnog teorema svodi se kongruencija $a(x) \equiv 0 \pmod m$ na niz pripadnih kongruencija kojima je modul p_i^{ei}, gdje $m = \prod_{p \in P_m} p$.

1.12. Dalja redukcija: modul prost broj. Kongruencija (1) za $m = p^e$ svodi se na analognu kongruenciju sa $m = p$. Najprije je jasno da svako rješenje x kongruencije

(10) $$a(x) \equiv 0 \pmod{p^e}$$ zadovoljava

(11) $$a(x) \equiv 0 \pmod p.$$

No, i obratno mogu se iz rješenjâ kongruencije (11) izgraditi rješenja za (10). Stvarno, ako x_1 zadovoljava (11), znači to da je $x = x_1 + py_1$ sa $y_1 \in D$. Odredimo x, tj. y_1 tako da vrijedi

(12) $$a(x) \equiv 0 \pmod{p^2}$$ (dakle najprije $e = 2$).

No, u (12) možemo razložiti polinom $a(x)$ prema Taylorovoj formuli oko $x = x_1$; time se (12) reducira na

$$a(x_1) + py_1 a'(x_1) \equiv 0 \pmod{p^2},$$

jer su ostali članovi $\equiv 0 \pmod{p^2}$.

Odatle

(13) $$\frac{a(x_1)}{p} + y_1 a'(x_1) \equiv 0 \pmod p.$$

Ako je

(*) $$a'(x_1) \not\equiv 0 \pmod p,$$

daje (13) jedno jedino rješenje $y_1 \equiv y_1' \pmod p$. To znači da je

$$y_1 = y_1' + py_2,$$

gdje je y_2 zasad neodređen cio broj. Znači da imamo

(14) $$x = x_1 + py_1' + p^2 y_2 = x_2 + p^2 y_2.$$

Sad možemo slično odrediti y_2 stavljajući taj izraz za x u kongruenciju

$$a(x) \equiv 0 \pmod{p^3}$$

i radeći kao maloprije izlazi:

$$a(x_2) + p^2 y_2 a'(x_2) \equiv 0 \pmod{p^3}$$

(15) $$\frac{a(x_2)}{p^2} + y_2 a'(x_2) \equiv 0 \pmod p.$$

Zbog (*) i $x_1 \equiv x_2 \pmod p$ izlazi da je

$$a'(x_2) \not\equiv 0 \pmod p,$$

pa iz (14) imamo potpuno određeno rješenje $y_2 \equiv y_1' \pmod p$. To znači da je $y_2 = y_2' + py_3$, pa idući natrag ka x u (14), dobivamo

$$x = x_2 + p^2 y_2' + p^3 y_3,$$

tj.

$$x = x_3 + p^3 y_3 \text{ itd.},$$

dok se ne dođe do određenog rješenja $x = x_e + p^e y_e$ za polaznu kongruenciju (10).

To je bilo tako uz uslov (*). Ako (*) ne vrijedi, tada iz (13) očitavamo ovo: ako je $a(x_1)$ djeljivo sa p^2, onda se za y_1 može uzeti koji god broj; ako nije $p^2 \mid a(x_1)$, tada nijedno rješenje kongruencije (11) ne zadovoljava (10).

1.13. Zadaci o kongruencijama n-og stupnja.

1. Odrediti stupanj ovih kongruencija:

   1) $45947\,x^2 - 354\,x + 1 \equiv 0 \pmod{11}$;

   2) $(3^{12} - 1)\,x^4 - 3^5\,x^3 + x^2 + 5 \equiv 0 \pmod{13}$;

   3) $10!\,x^{10} + 9!\,x^9 + \cdots + 2!\,x^2 + x + 1 \equiv 0 \pmod{100}$;

   4) $\binom{10}{5} x^4 + \binom{10}{4} x^4 + \cdots \equiv 0 \pmod 2$.

2. Dokaži da je kongruencija $a(x) \equiv 0 \pmod p$ ravnopravna s nekom kongruencijom $b(x) \equiv 0 \pmod p$ pri čemu je $\operatorname{st} b < p$. Razjasni stvar s kongruencijom $3\,x^8 + 4\,x^7 + 6\,x^6 - 3\,x^2 + x - 5 \equiv 0 \pmod 5$.

3. Riješi $f(x) \equiv 0 \pmod m$, gdje je $f(x) = 4\,x^4 + 5\,x^3 + 6\,x^2 + 7\,x + 8$ te $m = 3, 4, 5$.

4. Neka kongruencija $a_0\,x^n + a_1\,x^{n-1} + \cdots + a_{n-1}\,x + a_n \equiv 0 \pmod p$ ima n rješenja (1) $x_1, x_2, \ldots, x_n$; dokaži da je $a_1 \equiv -a_0 S_1 \pmod p$, $a_2 \equiv a_0 S_2 \pmod p, \ldots, a_k \equiv (-1)^k a_0 S_k \pmod p$; pri tom S_k znači sumu produkata članova od podniza iz (1) s k članova.

5. Neka $M(a_n, m) = 1$ i $a(x) = a_0 + a_1\,x + \cdots + a_n\,x^n$; odredi normiran polinom $b(x)$ stupnja n koji je ravnosilan kongruenciji $a(x) \equiv 0 \pmod m$. Promatraj specijalno $a(x) = 6\,x^8 + 5\,x^2 - 7$, $m = 77$.

6. Riješi $3\,x^3 + 5\,x^2 - 6\,x + 1 \equiv 0 \pmod m$ za $m = 2, 3, 4, 5, 6, 7, 8, 9, 10$.

7. Riješi 1) $6\,x \equiv 12 \pmod{18}$;

   2) $2\,x^2 + 6\,x \equiv 12 \pmod{18}$;

   3) $x^3 + 2\,x^2 + 6\,x \equiv 12 \pmod{(18)}$;

   4) $6\,x^3 + 27\,x^2 + 17\,x + 20 \equiv 0 \pmod{30}$.

2. KORIJENI JEDINICE. SVOJSTVEN POKAZATELJ.

2.1. Definicija. *n-ti korijeni jedinice ili n-ti ostaci jedinice prema modulu m jesu rješenja kongruencije*

$$x^n \equiv 1 \pmod{m}. \tag{1}$$

Pri tom brojeve koji su $\equiv \bmod m$ ne smatramo kao nejednaka rješenja kongruencije (1). Tako npr. treće korijene jedinice mod 4 tražimo među brojevima 0, 1, 2, 3 i vidi se da je to samo 1.

Znamo za osnovni Fermat-Eulerov teorem, prema kojemu je

$$a^{\varphi(m)} \equiv 1 \pmod{m} \quad \text{za svako } a \in D \text{ pri } M(a, m) = 1. \tag{2}$$

Na taj način imamo n-tih ostataka jedinice bar za brojeve $n = \varphi(m)$.

Dokažimo da iz

$$a M m = 1 \tag{3}$$

izlazi da je broj a određen ostatak jedinice ne obazirući se pri tom na osnovnu formulu (2). Promatrajmo niz

$$a, a^2, a^3, a^4, \ldots \tag{4}$$

Taj je niz beskonačan. Zato u njemu mora biti brojeva koji su $\equiv \bmod m$ (dolaze na isti vrh brojevnog m-vrha). Neka je a^k prvi član u (4) koji je kongruentan s nekim $a^{k'}$ iz (4) uz $k' < k$. To znači da je

$$a^k \equiv a^{k'} \pmod{m}$$

i odatle, dijeleći sa $a^{k'}$

$$a^{k-k'} \equiv 1 \pmod{m}. \tag{5}$$

Dijeljenje je bilo dopušteno jer je $M(a^{k'}, m) = 1$. Dakle, broj a uistinu zadovoljava kongruenciju oblika (1) za $k - k'$, pri čemu smo k i k' definirali na jednoznačan način. Lako se može dokazati da je $k - k'$ *prvi* prirodni broj za koji vrijedi (5).

Zanimat će nas taj eksponent.

2.2. Svojstven eksponent. Ako je $M(a, m) = 1$, neka $m(a)$ znači *prvi* prirodni broj n za koji broj a zadovoljava (1), tj. po definiciji

$$a^{m(a)} \equiv 1 \pmod{m}, \text{ no } a^n \not\equiv 1 \pmod{m} \text{ za } n = 1, 2, \ldots, m(a) - 1.$$

Tako npr. odredimo 9(4). Radi se o kongruenciji

$$4^n \equiv 1 \pmod{9}.$$

Treba naći prvo n odatle. Idemo po redu:

$$4^1 \equiv 4 \pmod{9}.$$

Odatle, množeći sa 4:

$$4^2 \equiv 16 \equiv -2 \pmod{9}.$$

Odatle, množeći sa 4:

$$4^3 \equiv -8 \equiv 1 \pmod 9.$$

Dakle je $n=3$, tj. $9(4)=3$.

2.3. Lema. *Ako je* $M(a, m)=1$ i $a^n \equiv 1 \pmod m$, *tada je* $m(a) \mid n$, tj. $m(a)$ *dijeli* n.

Pri tom se predmnijeva $n \geq 1$; naravno da je $n \geq m(a)$. Neka je

$$n = m(a) \cdot q + r \text{ sa } 0 \leq r < m(a).$$

Tada kongruencija (1) postaje (zbog $a^n = (a^{m(a)})^q \cdot a^r = 1^q \cdot a^r$):

$$a^r \equiv 1 \pmod m, \quad \text{dakle} \quad r = 0,$$

po definiciji broja $m(a)$.

To znači da je zaista $m(a) \mid n$.

2.4. No, prema Fermat-Eulerovu teoremu imamo $a^{\varphi(m)} \equiv 1 \pmod m$; pri tom $\varphi(m)$ kazuje koliko skup $\Phi(m)$ ima članova ($\Phi(m)$ je skup brojeva 0, 1, 2, . . . , $<m$ koji su prosti prema m). Na osnovu 2.3. imamo ovo:

2.5. $m(a) \mid \varphi(m)$ za svaki relativno prosti broj a prema m.

Naravno, postavlja se problem da se pronađu oni brojevi a iz $\Phi(m)$ za koje je $m(a)=\varphi(m)$. Ima li ih uvijek? Zvat ćemo ih *primitivni* ili *prvoobrazni korijeni jedinice modulo m.*

2.6. No, najprije ovo: kako je a prosto prema m, i svi brojevi

$$a, a^2, a^3, a^r, \ldots, a^{m(a)}$$

prosti su prema m; svaki od njih ima svoj svojstven eksponent modulo m. Odredimo ga, tj. nađimo $m(a^r)$. Po definiciji, to je *najmanji* prirodni broj n sa svojstvom $(a^r)^n \equiv 1 \pmod m$; no prema 2.3. izlazi odatle da je $m(a) \mid rn$ i da je pri tom n najmanji mogući broj. No, najmanji kratnik rn broja $m(a)$ nastupa za $n = \dfrac{m(a)}{M(r, m(a))}$. Stvar je jasna ako je $r\,M\,m(a)=1$. No, opći slučaj svodi se na taj; označimo li, naime, $r\,M\,m(a)=\mu$, tada je rn najmanji kratnik od $m(a)$ onda i samo onda ako je $\dfrac{nr}{\mu}$ najmanji kratnik od $\dfrac{m(a)}{\mu}$, a to zbog $\dfrac{r}{\mu} M \dfrac{m(a)}{\mu} = 1$ znači da je $n = \dfrac{m(a)}{\mu}$.

Time smo dokazali da vrijedi

2.7. Teorem

$$m(a^r) = \frac{m(a)}{r\,M\,m(a)} \quad \text{za } r = 1, 2, \ldots, m(a)-1;$$

posebno, $m(a^r)=m(a)$ za svaki od $\varphi(m(a))$ brojeva 0, 1, 2, . . . , $m(a)$ koji su prosti prema $m(a)$. Npr. za slučaj $m=9$, $a=3$ imali smo $9(4)=3$; a prema tome rezultatu izlazi i $9(4^2)=9(4)$, jer je $2\,M\,9(4)=1$. I stvarno je $(4^2)^3 \equiv 1$, ali nije $(4^2)^i \equiv 1$ za $i=1$ ili 2.

2.8. *Ako je* $m(a)=rs$ *tada je* $m(a^r)=s$.

2.9. *Ako je* $m(a)\,M\,m(b)=1$, *tada je* $m(ab)=m(a)\,m(b)$.

Stvarno, po definiciji je $a^{m(a)}\equiv 1$, dakle i $a^{m(a)\,m(b)}\equiv 1$.
Isto tako je $b^{m(a)\,m(b)}\equiv 1$, dakle i $(ab)^{m(a)\,m(b)}\equiv 1 \pmod m$.

Prema 2.3. znači to da je

$$m(ab)\,|\,m(a)\,m(b). \tag{6}$$

S druge strane, prema definiciji, imamo $(ab)^{m(ab)}\equiv 1$. Odatle

$$a^{m(ab)\,m(ab)}\equiv 1 \pmod m. \tag{7}$$

Iz (6) zbog $m(a)\,M\,m(b)=1$ slijedi:

$$m(ab)=u\cdot v;\quad u\,|\,m(a),\quad v\,|\,m(b).$$

Na osnovu toga potenciranjem kongruencije (7) brojem $w=\dfrac{m(b)}{v}$ proizilazi

$$a^{m(ab)}\cdot w\equiv 1 \pmod m.$$

Prema tome:

$$m(a)\,|\,m(ab)\cdot w,\ \text{tj. zbog}\ \ m(a)\,M\,w=1,\ m(a)\,|\,m(ab).$$

Analogno

$$m(b)\,|\,m(ab).$$

Ta relacija zajedno sa (6) daje traženu jednakost u iskazu 2.9.

2.10. Lema. *Ako za brojeve* $q_1, q_2, \ldots$, *koji su prosti prema* m, *vrijedi da su brojevi* $m(q_1).\ m(q_2), \ldots$ *dva po dva međusobno prosta, tada je*

$$m(q_1\,q_2\ldots)=m(q_1)\cdot m(q_2)\ldots$$

3. PRIMITIVNI ILI PRVOOBRAZNI KORIJENI JEDINICE PREMA ZADANOM MODULU m.

Vidjeli smo da iz $a\,M\,m=1$ izlazi da je svojstven eksponent $m(a)$ broja a prema m djelitelj broja $\varphi(m)$ (§ 2.3—2.5). Postavlja se pitanje da li ima i takvih a za koje je $m(a)=\varphi(m)$.

3.1. Definicija prvoobraznih korijena jedinice. *Svaki broj* a *koji je prost prema* m *i za koji je* $m(a)=\varphi(m)$, *tj.* $a^{\varphi(m)}\equiv 1\ (mod\ m)$ *i* $a^k\not\equiv 1\ (mod\ m)$ *za* $k=1, 2, \ldots, \varphi(m)-1$, *zove se prvoobrazni ili primitivni korijen jedinice modulo* m.

3.2. Teorem. Karakteristično svojstvo primitivnih korijena. *Ako je* a *prvoobrazni korijen jedinice modulo* m, *tada potencije*

$$a^r, \ldots, \quad pri \quad r\in\Phi(m)$$

predstavljaju $\varphi(m)$ *inkongruentnih brojeva prostih prema* m; *i obratno, ako neki broj* a, *prost prema* m, *ima svojstvo da je svaki broj prost prema* m *kongruentan mod* m s *nekim stepenom broja* a, *onda je* a *prvoobrazan korijen jedinice modulo* m.

Dokaz. Najprije, ako je a primitivan korijen, onda to znači da je $m(a)=\varphi(m)$ i da je $a^n \not\equiv 1 \pmod m$ za svako $n<\varphi m$; specijalno su brojevi a^r ($r\in 1(\varphi m)$) međusobno $\not\equiv$, jer bismo inače iz $a^r\equiv a^s \pmod m$ zaključili da je $a^{r-s}\equiv 1 \pmod m$ za neke brojeve $r, s\in 1(\varphi(m))$; jasno je da je $r-s<\varphi m$; dakle bi bilo $a^k\equiv 1$ za broj $k=r-s<\varphi m$, protivno definiciji broja $m(a)$.

S druge strane, ako broj a ima svojstvo da je svaki broj $r'\in\Phi(m)$ kongruentan mod m s nekim brojem a^r, onda je nužno $m(a)=\varphi(m)$. Naime, u jednu je ruku svaka potencija a^n kongruentna sa $a^{n'}$, gdje je $n\equiv n' \pmod{m(a)}$. U drugu ruku $m(a)\,|\,\varphi(m)$. Ne može biti $m(a)<\varphi(m)$, jer tada ne bismo mogli $\varphi(m)$ brojeva iz $\Phi(m)$ predstaviti pomoću $m(a)$ brojeva $a^{n'}$ sa $n'\leq m(a)$. Time je teorem dokazan.

3.3. Primjeri. — **3.3.1.** Primjer. Nađimo prvoobrazne korijene jedinice modulo 5, tj. rješenja a za koje je $5(a)=\varphi(5)=4$ i $a\,M\,5=1$.

Imamo tablicu:

a	1	2	3	4
$m(a)$	1	4 $\varphi(5)$	4 $\varphi(5)$	2

Dakle je tražena relacija $m(a)=\varphi(m)$ zadovoljena za $a=2, 3$.

3.3.2. Drugi primjer. Nađimo primitivne korijene (ostatke) prema modulu $m=35$.

Imamo

$$\varphi(35)=35\cdot(1-5^{-1})(1-7^{-1})=4\cdot 6=24.$$

Radi se, dakle, o rješenjima prostima prema 35 i za koja je $x^{\varphi(35)}\equiv 1 \pmod{35}$. No, svaki broj koji je prost prema 35, prost je i prema njegovim faktorima 5, 7; dakle mora biti također

$$x^{\varphi(5)}\equiv 1 \pmod 5 \quad \text{tj.} \quad x^4\equiv 1 \pmod 5$$

$$x^{\varphi(7)}\equiv 1 \pmod 7 \qquad x^6\equiv 1 \pmod 5.$$

No, iz te dvije kongruencije izlazi da je

$$(x^4)^3\equiv 1 \pmod 5$$

$$(x^6)^2\equiv 1 \pmod 7, \text{ tj.}$$

$$x^{12}\equiv 1 \pmod{35}.$$

Prema tome, nema nijednog prvoobraznog korijena jedinice mod 35.

Uostalom, o tome bismo se mogli uvjeriti i direktnim izračunavanjem svojstvenih eksponenata brojeva iz $I\,35$. Tako npr. $35(1)=1$; $35(2)=?$

Radimo ovako: $2\equiv 2$ $\qquad 2^3\equiv 8$

$2^2\equiv 4$ $\qquad 2^4\equiv 16$

$$2^5 \equiv 32 \equiv -3 \qquad 2^9 \equiv 22 \equiv -13$$

$$2^6 \equiv -6 \qquad 2^{10} \equiv -26 \equiv 9$$

$$2^7 \equiv -12 \qquad 2^{11} \equiv 18$$

$$2^8 \equiv -24 \equiv 11 \qquad 2^{12} \equiv 36 \equiv \mathbf{1}.$$

Dakle je $35\,(2) = 12$, kao što smo bili i inače dokazali.

3.4. Prema tome, ne mora svako m imati prvoobraznih svojih jedinica. Pogledajmo slučaj $m = p$ (prost broj); dakle je $\varphi(p) = p-1$.

3.5. Teorem. *Postoji $\varphi(p-1)$ primitivnih ili prvoobraznih korijena jedinica modulo p za svaki prost broj p.*

Najprije, prema Fermatovu teoremu rješenja kongruencije

$$x^{p-1} \equiv 1 \pmod{p}$$

jesu brojevi

$$1, 2, 3, \ldots, p-1 \quad \text{(njih } p-1 \text{ na broju).} \tag{1}$$

Njima pripadaju određeni brojevi

$$p\,(1), p\,(2), \ldots, p\,(p-1) \tag{2}$$

kao svojstveni eksponenti.

Za svaki broj d iz niza (2) znači to da je bar za jedno a iz niza (1) ispunjeno $p\,(a) = d$. No, prema teoremu 2.7. znači to da je i za svako $r \in \Phi(d)$ ispunjeno $p\,(a^r) = d$. To znači da svakom članu d iz (2) pripada $\varphi(d)$ članova iz (1) s istim d; drugim riječima, svaki član niza (2) pojavljuje se u tom nizu upravo $\varphi(d)$ puta. Ako je, dakle, $S\,(2)$ skup sastavljen od brojeva iz (2), tada je $\sum_{d \in S(2)} \varphi(d) =$ broj članova u (2) = broj članova u (1), tj. $p-1$. Imamo, dakle,

$$\sum_{d \in S(2)} \varphi(d) = p-1. \tag{3}$$

No, za svako $d \in S\,(2)$ je $a^d \equiv 1 \pmod{p}$, što sa $a^{p-1} \equiv 1 \pmod{p}$ ima prema 2.3. za posljedicu da je $d \mid (p-1)$. S druge strane, prema dobenom svojstvu funkcije φ (pogl. 6, § 19) imamo $\sum_{t \mid (p-1)} \varphi(t) = p-1$, pri čemu t prolazi *svim* djeliteljima broja $p-1$; to znači da ni u sumaciji (3) ne smije izostati nijedan djelitelj broja $p-1$, specijalno ne djelitelj $p-1$. A to znači da se u nizu eksponata (2) zbilja pokazuje i broj $p-1$. Time se on u (2) pokazuje $\varphi(p-1)$ puta, pa je teorem potpuno dokazan.

Primijetimo kako dokaz teorema 3.5. zahtijeva raznovrstan i dosta težak materijal.

3.6. Teorem o složenim modulima. *Za prirodni broj m neka $P\,(m)$ bude skup svih prostih djelitelja broja m. Ako je $g\,M\,m = 1$, pa ako je*

$$m\,(g) = \varphi(m), \tag{4}$$

tada ni za koji prost broj $p \mid m$ *ne može biti*

$$g^{\frac{\varphi(m)}{p}} \equiv 1 \pmod{m}; \tag{5}$$

i obratno, ako ova relacija ne vrijedi ni za koje $p \mid m$, *tada je g prvoobrazan korijen jedinice mod m.*

Jasno je da zbog (4) relacija (5) ne može vrijediti jer je $\varphi(m)p^{-1} < \varphi(m)$. No, vrijedi i obrat, tj. (5) $\Rightarrow$ (4). Naime, kad bi bilo $m(g) < \varphi(m)$, bilo bi $\varphi(m) = m(g) \cdot p \cdot x$, gdje je p prost broj; dakle bilo bi $g^{\frac{\varphi(m)}{p}} = (g^{m(g)})^x$, tj. $g^{\frac{\varphi(m)}{p}} = 1 \pmod{p}$, protivno pretpostavci.

Gornjim se teoremom koristimo da nađemo eventualne prvoobrazne ostatke za složene module.

4. INDEKSI

4.1. Neka je a jedan od $\varphi(p-1)$ primitivnih korijena jedinice mod p brojeva koji pripadaju eksponentu $p-1$ mlo p (isp. teorem 3.5); onda je jasno da u nizu

$$1, a, a^2, a^3, \ldots, a^{p-2} \tag{1}$$

nema kongruentnih brojeva prema modulu p. No, kako uopće ima tek $p-1$ klasa mod p brojeva nedjeljivih sa p, to znači da je svaki broj *b koji nije djeljiv sa p kongruentan s jednim jedinim brojem u nizu* (1), tj.

$$b \equiv a^{\beta} \pmod{p} \quad \text{sa} \quad 0 \leq \beta < p-1. \tag{2}$$

Eksponent β, koji je tako određen, zove se *indeks zadanog broja b s obzirom na bazu a i označuje se* $\mathrm{Ind}_a b$, Prema tome,

$$\mathrm{Ind}_a b = \beta \tag{3}$$

znači isto što i

$$b \equiv a^{\beta} \pmod{p}.$$ Dakle je

$$a^{\mathrm{Ind}_a b} \equiv b \pmod{p}. \tag{4}$$

Na taj način *zadan prvoobrazan ili primitivan korijen jedinice a možemo upotrijebiti za prikazivanje ostalih brojeva u obliku potencije* a^x; *to je slično kao kod logaritama.* I ovdje, kao i kod logaritama, ima brojeva koji izbjegnu takvu zapisivanju (npr. broj 0).

4.2. Primjer.

Za modul 7, $\mathrm{Ind}_3 18 = ?$, $3^x \equiv 18 \equiv 4 \pmod{7}$, $x = ?$

$\mathrm{Ind}_3 18 = ? = \mathrm{Ind}_3 4$

$x = 4$ jer je

$3^4 \equiv 18 \pmod{7}$

$81 - 18 = 63 \equiv 0 \pmod{7}$.

Pozitivne ostatke mlo 7: 1, 2, 3, 4, 5, 6

možemo, dakle, prikazati kao potencije od 3, i to po redu:

$3^0 \equiv 1 \pmod 7$
$3 \equiv 3$
$3^2 \equiv 2$
$3^3 \equiv 6$
$3^4 \equiv 4$
$3^5 \equiv 5$
$3^6 \equiv 1$

x	1	2	3	4	5	6
3^y	3^0	3^2	3^1	3^4	3^5	3^3
$y = \mathrm{Ind}_3 x$	0	2	1	4	5	3

Odatle *očitavamo npr.* $\mathrm{Ind}_3 6 = 3$.

Odredimo $x = \mathrm{Ind}_3 7247$ prema modulu 7.

To znači da treba biti

$$3^x \equiv 7247 \pmod 7.$$

Zato broj 7247 možemo zamijeniti njegovim ostatkom pri dijeljenju sa 7. Taj ostatak je 2; dakle je $\mathrm{Ind}_3 7247 = \mathrm{Ind}_3 2 =$ (prema gornjoj tablici) $= 2$.

4.3. Primjer. Uzmimo $p = 13$; $\varphi(p) = 12$. Broju $12 = \varphi(p)$ pripada baza 2, jer je $2^{12} \equiv 1 \pmod{13}$, dok je $2^n \not\equiv 1 \pmod{13}$ *za* $n < 12$, tj. 2 je primitivni korijen jedinice prema modulu 13.

No, $\varphi(12) = 12\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 2 \cdot 1 \cdot 2 = 4$; zato prema teoremama 3.5. postoje četiri primitivna korijena jedinice prema mod 13; to su 2, 6, 7, 11. Ispitajmo broj 3 i nađimo $13(3)$.

Broj	*ostatak mod* 13
③	3
3^2	−4
3^3	①

Nije prvoobrazan, jer je, eto, $13(3) = 3$, dakle $13(3) < \varphi(13)$. Slično se radi i za preostale brojeve 4, 5, 6, . . . , 12.

Na taj se način može doći do ove tablice:

Baza \ Eksp.	1	2	3	4	5	6	7	8	9	10	11	12	
	Ostaci mlo 13 od potencije a^e												
2	2	4	−5	3	6	−1	−2	−4	5	−3	−6	①	primitivan
3	3	−4	①										imprimitivan
4	4	3	−1	−4	−3	①							imprimitivan
5	5	−1	−5	①									imprimitivan
6	6	−3	−5	−4	2	−1	−6	3	5	4	−2	①	primitivan
7	−6	−3	5	−4	−2	−1	6	3	−5	4	2	①	primitivan
8	−5	−1	5	①									imprimitivan
9	−4	3	①										imprimitivan
10	−3	−4	−1	3	4	①							imprimitivan
11	−2	4	5	3	−6	−1	2	−4	−5	−3	6	①	primitivan
12	−1	①											imprimitivan

Odatle se vidi da su prvoobrazni ostaci mod 13 ovi brojevi:

2, 4, 7, 11.

Preostali su imprimitivni (neprvoobrazni).

Iz te tablice odmah vidimo da je

$$\mathrm{Ind}_2 5 = 9 \qquad \mathrm{Ind}_7 5 = 3$$

$$\mathrm{Ind}_6 5 = 9 \qquad \mathrm{Ind}_{11} 5 = 3$$

4.4. Pravila o indeksovanju. Indeks ili pokazatelj je po svojoj naravi *eksponent*, slično kao i *logaritam*. Zato će za indeksovanje donekle vrijediti pravila koja su slična pravilima za logaritmiranje. Radimo sa prostim brojem p kao modulom. Tu se onda pojavljuje i broj $\varphi(p) = p-1$ kao modul.

4.4.1. Teorem. $Ind\,(b_1 b_2) \equiv Ind\, b_1 + Ind\, b_2$, $(mod\ p-1)$.

Primjedba: Modul nije p, nego $p-1$.

Neka je baza a.

$$a^{\mathrm{Ind}\,(b_1 b_2)} \equiv b_1 b_2, \pmod p$$

$$a^{\mathrm{Ind}\, b_1} \equiv b_1, \pmod p$$

$$a^{\mathrm{Ind}\, b_2} \equiv b_2, \pmod p$$

$$a^{\mathrm{Ind}\, b_1 + \mathrm{Ind}\, b_2} \equiv b_1 b_2, \pmod p.$$

Dakle, $a^{\mathrm{Ind}\, b_1 + \mathrm{Ind}\, b_2} \equiv a^{\mathrm{Ind}\,(b_1 b_2)}, \pmod p$.

No, a je primitivan korijen jedinice mod p, tj. pripada eksponentu $p-1$; zato su pripadni eksponenti kongruentni mlo $p-1$, što smo i htjeli.

4.4.2. Teorem. $Ind\,(b_1 b_2 \ldots b_k) \equiv Ind\, b_1 + \cdots + Ind\, b_k$, mod $(p-1)$.

Specijalno, ako $b_1 = b_2 = \cdots = b_r = b$, tada teorem postaje

4.4.3. Teorem. $\mathrm{Ind}\, b^n \equiv n\, Ind\, b$, $(mod\ p-1)$.

4.4.4. Primjedba o smislu gornjih obrazaca. Gornji teoremi 4.4.1—3. znače ovo: ako promatramo jednu kongruenciju s obzirom na modul p, možemo iz te kongruencije izvesti drugu kongruenciju tako da obje strane kongruencije indeksujemo, a modul p kongruencije zamijenimo modulom $\varphi(p)$. I obratno za antiindeksovanje. Važno je da se i moduli mijenjaju ali samo jednostavno: $p \rightleftarrows \varphi(p)$.

Primijetimo da smo to pravilo dokazali samo za *proste module p*.

4.5. Primjena na linearnu kongruenciju $ax \equiv b$, (mod p).

Indeksovanjem izlazi $\mathrm{Ind}\,(ax) \equiv \mathrm{Ind}\, b, \pmod p$.

$$\mathrm{Ind}\, a + \mathrm{Ind}\, x \equiv \mathrm{Ind}\, b, \pmod{p-1}.$$

$$\mathrm{Ind}\, x = \mathrm{Ind}\, b - \mathrm{Ind}\, a, \pmod{p-1}.$$

Npr. $3x = 4, \pmod 7$

$\mathrm{Ind}_3 x = \mathrm{Ind}_3 4 - \mathrm{Ind}_3 3, \pmod 6$

$\mathrm{Ind}\, x = 4 - 1, \pmod 6$

$\mathrm{Ind}\, x = 3, \pmod 6.$

$x = 3^3, \pmod 7$

$x \equiv -1, \pmod 7.$

4.6. Indeksi po složenim modulima. Ako modul m nije prost broj, onda znamo da ne mora postojati primitivan korijen jedinice prema modulu m (§ 3.3.2). Za takve module ne promatraju se indeksi. No, ima složenih modula za koje postoje primitivni korijeni jedinice; takvi su npr. moduli p^r, $2p^n$, gdje je p prost neparan broj; za njih kao module možemo promatrati indekse (isp. § 3.5).

4.7. Zadaci o korijenima jedinice modulo m i o indeksima.

1. Nađi n-te korijene jedinice modulo m za ove parove brojeva n, m:

   1) 2, 2; 2) 2, 3; 3) 2, m; 4) 3, 3; 5) 3, 5; 6) 3, 10.

2. Nađi svojstven eksponent $m(a)$ za ove parove brojeva a, m:

   1) 3, 5; 2) 4, 9; 3) 15, 29; 4) 30, 77.

3. Nađi $15(7^r)$ za $r = 1, 2, 3, 4, 5, 6, 7.$

4. Nađi prvoobrazne n-te korijene jedinice modulo m za ove dvojke brojeva n, m: 1) 5, 11; 2) 8, 17; 3) 70, 71; 4) 60, 61; 5) 70, 71; 6) 3, 6; 7) 3, 9; 8) 3, 12; 9) 3, 27; 10) 3, pq (p, q su dva prosta broja); 11) 3, 50.

5. Dokaži da jedino za brojeve oblika $m = p^e$, $2p^e$ i 4 imamo prvoobrazne korijene jedinice mod m.

6. Broj primitivnih korijena za modul p^e, gdje je p prost broj >2 jednak je $\varphi(\varphi p^e)$. Dokaži.

7. Za prost broj $p>2$ ima jednako mnogo prvoobraznih korijena za modul p^e i za modul $2p^e$.

8. Neka je p prost neparan broj; dokaži ovo: 1) svaki primitivan korijen a prema broju p^e primitivan je i prema p; 2) ako je g prvoobrazan prema p te ako p^2 dijeli $(g^{p-1}-1)$, tada je g prvoobrazno prema p^e; 3) svaki neparan prvoobrazni korijen mod p^e prvoobrazan je prema $2p^e$; 4) svaki primitivan korijen prema $2p^e$ primitivan je i prema p^e.

9. Nađi: $\mathrm{Ind}_2 8 \pmod 5$; $\mathrm{Ind}_3 8 \pmod 7$; $\mathrm{Ind}_2 8 \pmod{11}$; $\mathrm{Ind}_2 8 \pmod{13}$; $\mathrm{Ind}_3 8 \pmod{17}$; $\mathrm{Ind}_5 8 \pmod{23}$; $\mathrm{Ind}_7 8 \pmod{71}$; $\mathrm{Antiind}_2 2 \pmod 5$; $\mathrm{Antiind}_2 15 \pmod{13}$; $\mathrm{Antiind}_3 8 \pmod{17}$; $\mathrm{Antiind}_5 8 \pmod{23}$.

10. Tablica indeksa. $m=13$, $g=2$.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	3	6	12	11	9	5
1	10	7								

Te dvije tablice (indeksovanje i antiindeksovanje) znače ovo: modul je $m=13$; $g=2$ je (najmanji) prvoobrazni korijen jedinice; N (numerus = broj) ima cifru desetica u stupcu ispod N, a jedinice u retku desno od N; na sjecištu je indeks; npr. $\mathrm{Ind}\,4=2$, $\mathrm{Ind}\,14$ ne postoji. Slično je za tablicu antiindeksovanja: $\mathrm{I}\rightarrow \mathrm{antiind\,I}$; npr. $\mathrm{antiind}\,2=4$, $\mathrm{Antiind}\,14$ ne postoji.

Provjeri gornje tablice.

11. Za proste brojeve 3, 5, 7, 11, 23 odredi najmanje odgovarajuće prvoobrazne korijene g jedinice i sagradi odgovarajuću tablicu indeksovanja i tablicu antiindeksovanja slično kao u zad. 10 za $m=13$, $g=2$.

12. Provjeri pravila o indeksovanju na ovim primjerima tražeći na dva načina indeks ovih izraza: 1) $18\cdot 19 \pmod{17}$; 2) $2^6 \pmod{17}$; 3) $354^3\cdot 254^4 \pmod{13}$.

13. Zadatke iz pogl. 6, § 17.7.1. riješi pomoću indeksovanja i antiindeksovanja.

14. Kongruenciju 1) $x^2\equiv 5 \pmod{13}$, 2) $23\,x^5\equiv 15 \pmod{73}$ riješi isprobavanjem kao i služeći se indeksovanjem.

15. Dokaži: Ako je $2^{2^n}+1$ prost broj p, tada je broj 3 prvoobrazan korijen mod p.

16. Dokaži: Ako su p i $4p+1$ prosti brojevi $\neq 2$, tada je 2 primitivan korijen jedinice mod $4p+1$ (Čebišev). Čebišev je dokazao i ovo: Ako su p, q prosti brojevi i $p=4\cdot 2^m q+1$ i $m>0$, $q>\dfrac{9^{2^n}}{4\cdot 2^m}$, tada je 3 prvoobrazan korijen prema p (Isp. Raboti Čebiševa str. 79).

5. NORMIRANE BINOMNE KONGRUENCIJE

5.1. One su oblika

$$x^n\equiv D, \pmod{p}. \tag{1}$$

Odatle prema 4.4.2. i 4.4.3.:

$$n\,\mathrm{Ind}\,x\equiv \mathrm{Ind}\,D, \pmod{p-1}. \tag{2}$$

Primjer: $$x^2\equiv 2, \pmod{10}.$$

Pokušavajući $x=0, \pm 1, \pm 2, \pm 3, \pm 4, 5$, vidi se da ta kongruencije nije moguća.

Drugi primjer: $x^{554} \equiv 4 \pmod 5$.

Svakako mora biti $M(x, 5) = 1$, jer inače kongruencija nije moguća. No, iz $M(x, 5) = 1$ izlazi $x^{\varphi(5)} \equiv 1 \pmod 5$, tj. x^4 možemo zamijeniti sa 1.

$$x^{554} \equiv 4 \cdot 138 + 2 \equiv (x^4)^{138} \cdot x^2 \equiv 1 \cdot x^2.$$

Time zadana kongruencija glasi:

$$x^2 \equiv 4 \pmod 5.$$

Gledajući koji od brojeva 0, -1, $+1$, -2, 2 zadovoljava, vidi se da su to brojevi -2, 2. Prema tome, polazna kongruencija ima rješenja -2 i 2.

5.2. Teorem. *Da binomna kongruencija* (1) *bude moguća, nužno je i dovoljno da bude*

$$\text{Ind } D \equiv 0, \pmod \delta, \quad \textit{gdje je} \quad \delta = M(n, p-1). \tag{3}$$

To ćemo izreći i nezavisno od indeksa i dokazati jedan Eulerov teorem (§ 5.3).

Neka je najprije ispunjeno (3), dakle

$$\text{Ind } D = h\,\delta, \tag{4}$$

$$D \equiv a^{h\delta}, \pmod p. \tag{5}$$

No $a^{p-1} \equiv 1, \pmod p$.

Zato potencirajući (5) sa $\frac{p-1}{\delta}$ izlazi:

$$D^{\frac{p-1}{\delta}} \equiv a^{h(p-1)}, \pmod p, \quad \text{tj.} \tag{6}$$

$$D^{\frac{p-1}{\delta}} \equiv 1, \pmod p. \tag{7}$$

I obrnuto. Ako D zadovoljava (7), *izlazi odatle, stavljajući* $D \equiv a^{\text{Ind } D} \pmod p$:

$$a^{\frac{p-1}{\delta} \text{Ind } D} \equiv 1, \pmod p;$$

kako je a primitivan korijen modulo p, tj. kako a pripada broju $p-1$, mora $\frac{p-1}{\delta} \text{Ind } D$ biti višekratnik od $p-1$, dakle je $\frac{\text{Ind } D}{\delta}$ cio broj a to baš i tvrdi uslovna relacija (3). Ujedno je dokazan i

5.3. Teorem (Euler). *Da binomna kongruencija* $x^n \equiv D, \pmod p$ *bude moguća, treba, a i dosta je da bude*

$$D^{\frac{p-1}{\delta}} \equiv 1, \pmod p \quad \textit{gdje je} \quad \delta = M(n, p-1). \tag{8}$$

5.4. Primijetimo da je uslovna kongruencija (8) istoga tipa kao (1).

Ako je taj uslov ispunjen, koliko ima inkongruentnih brojeva D za koje je kongruencija (1) moguća? Toliko, koliko kongruencija

$$D^{\frac{p-1}{\delta}} \equiv 1, \pmod{p} \quad \text{ima rješenja!} \tag{9}$$

Za kongruenciju (9) Eulerov uslov (8) daje:

$$\delta' = M\left(\frac{p-1}{\delta}, p-1\right) = \frac{p-1}{\delta}$$

i očito je ispunjen uslov (8) da bude $1^{\frac{p-1}{\delta'}} \equiv 1 \pmod{p}$.

5.5. Pojam ostataka potencija. Brojevi D za koje je (1) moguće (nemoguće) zovu se *ostaci* ili *rezidui*, (*neostaci, nerezidui*) *n-tih potencija modulo p.* Specijalno se često pojavljuju *kvadratni, kubni i bikvadratni ostaci mod p*: to su brojevi koji su kongruentni kvadratu, kubu, odnosno bikvadratu nekog broja.

Na taj se način postavlja *problem da li je zadani broj D ostatak* ili *neostatak* zadanog stupnja n s obzirom na zadani modul p. Mnogo je teže još *pitanje za koje je sve module zadana binomna kongruencija moguća.*

6. TRI GLAVNA PITANJA O OSTACIMA POTENCIJA

Pogledajmo binomnu kongruenciju

$$x^n \equiv c \pmod{m}. \tag{1}$$

Tu se pojavljuju tri broja: n, c i m; nepoznata veličina je x.

Postavljaju se ova četiri osnovna pitanja:

Prvo pitanje. Ako su zadana sva tri broja: stepen n, ostatak c i modul m, da li je kongruencija (1) moguća? Drugim riječima, *da li je c ostatak n-tog stupnja za modul m*?

Drugo pitanje. Odrediti sve n-te ostatke zadanog broja m kao modul (*zadano n, m, odrediti c*).

Treće pitanje. *Zadano n i c, odrediti m*; drugim riječima, za koje je sve module zadani broj c ostatak stupnja n?

Četvrto pitanje. *Zadano c i m, traži se n*, drugim riječima, kojeg je sve stepena zadani broj c ostatak prema modulu m?

Uz ta četiri pitanja vezana je čitava jedna grana matematike. Mi ćemo se u narednom paragrafu dotaknuti najvažnijeg i najjednostavnijeg slučaja: $n = 2$.

7. KVADRATNE KONGRUENCIJE. KVADRATNI OSTACI (NEOSTACI)

Kvadratne kongruencije su među najjednostavnijima. A već se u njima naziru problemi koji se prenose na kongruencije višeg stupnja. Gauss u mladim danima imao je velikih uspjeha na tom polju.

7.1. Kvadratne kongruencije su oblika

(1) $$a x^2 + bx + c \equiv 0 \pmod{m}, \quad \text{pri čemu je} \quad a \not\equiv 0 \pmod{m}.$$

Normirana čista kvadratna kongruencija je oblika

(2) $$x^2 \equiv c \pmod{m}.$$

Ako je kongruencija (2) moguća (nemoguća), veli se da je broj c *kvadratni ostatak* (*neostatak*) *prema modulu* m.

7.1.1. Primjer. Odredimo kvadratne ostatke i neostatke za broj 10 kao modul. Imamo kongruenciju:

(3) $$x^2 \equiv c \pmod{10}, \quad \text{pa u skupu} \quad I10 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

gledamo za koje $c \in I10$ kongruencija (3) ima rješenje, a za koje ga nema. Npr. $c = 1$ je očigledno ostatak, jer je dovoljno u (3) staviti $x = 1, 9$. Pokušavanjem se vidi da broj $c = 2$ nije ostatak: veza $x^2 = 2 \pmod{10}$ nije moguća ni za koje $x \in I10$ (a time ni za druge cijele brojeve). Stvarno, ostaci mod 10 kvadrata cifara jesu 0, 1, 4, 9, 6, 5, 6, 9, 4, 1 i tu se ne pojavljuje cifra 2. To su znali i Arapi kad su primijetili da se kvadrat cijelog broja ne može završavati sa 2.

Drugim riječima kvadratni ostaci mod 10 jesu 0, 1, 4, 5, 6, 9; kvadratni neostaci jesu preostale cifre, tj. 2, 3, 7, 8.

Prema tome, imamo šest ostataka i četiri neostatka (više jednih nego drugih). Je li općenito tako? Npr. za modul 5?

7.2. Lema. *Među brojevima* $1, 2, \ldots, p-1$ *ima jednako mnogo kvadratnih ostataka i kvadratnih neostataka prema modulu* p.

Pišemo li, naime, gornje brojeve u obliku $\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}$, dobivaju se pripadni kvadrati $1, 4, \ldots, \left(\frac{p-1}{2}\right)^2$ i ima ih $\frac{p-1}{2}$. Ti su brojevi ostaci, a preostali su neostaci.

7.3. Lema. *Ako je* c *kvadratni ostatak, odnosno neostatak mod* p, *onda je*

(3) $$c^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \quad \text{odnosno} \quad c^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Naime, po Fermatovu teoremu je

$$c^{p-1} \equiv 1 \pmod{p}, \quad \text{dakle}$$

(4) $$(c^{\frac{p-1}{2}} - 1)(c^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}.$$

Ako je c ostatak (misli se kvadratni ostatak prema promatranom modulu), onda je moguće pisati

$$c \equiv x^2 \pmod{p}.$$

Odatle, množeći eksponente sa $\frac{p-1}{2}$:

$$c^{\frac{p-1}{2}} \equiv x^{p-1} \pmod{p},$$

odnosno zbog $x^{p-1} \equiv 1 \pmod{p}$:

$$c^{\frac{p-1}{2}} \equiv 1 \pmod{p}. \tag{5}$$

Time se dobila tražena relacija za svaki ostatak (jer prema 7.2. imamo $\frac{p-1}{2}$ ostataka). Za kvadratni neostatak c relacija (5) ne vrijedi, pa zato iz (4) zaključujemo da drugi faktor lijeve strane mora biti djeljiv sa p, jer prvi faktor nije djeljiv sa p; to znači da vrijedi tražena druga relacija u (3).

7.4. Legendreov simbol. Definicija. Rečenica: »*c je kvadratni ostatak prema prostom modulu p*« ispisuje se prema Legendreu, kao jednakost, ovako:

$$\left(\frac{c}{p}\right) = 1.$$

Rečenica: »*c nije kvadratni ostatak prema p*« zapisuje se, kao jednakost, ovako:

$$\left(\frac{c}{p}\right) = -1.$$

Npr. $\left(\frac{5}{7}\right) = ?$ Treba gledati kongruenciju $x^2 \equiv 5 \pmod{7}$. Stavljajmo u nju $x = 0, 1, 2, 3, 4, 5, 6$ i gledajmo da li je zadovoljena; nije zadovoljena ni za koje $x \in I\,7$; znači: 5 je kvadratni neostatak mod 7, pa se i piše

$$\left(\frac{5}{7}\right) = -1.$$

7.5. Teorem. $$\left(\frac{-1}{p}\right) = \left(-1\right)^{\frac{p-1}{2}};$$

tj. -1 *je kvadratni ostatak za proste brojeve oblika* $4k+1$, *a neostatak za proste brojeve oblika* $4k+3$ (Fermat, Euler).

Naime, svaki neparni broj je oblika $4k+1$ ili $4k+3$; ako se ti izrazi stave u (3), dobiva se iskazani sud (isp. 7.10.1).

Na osnovu teorema 7.5. dokazuje se ovaj fini

7.5.1. Teorem (Fermat). *Svaki prosti broj oblika* $4k+1$ *suma je od dva kvadrata.*

Npr. za $k = 1, 4$ dobije se $5 = 2^2 + 1^2$, $17 = 4^2 + 1$.

Fermat je teorem dokazao glasovitom metodom *descente indéfinie* (*neodredenim spuštanjem*), svodeći teorem na slučaj $p = 5 = 2^2 + 1^2$.

7.5.2. Spomenimo Lagrangeov teorem: *svaki cijeli broj je suma od četiri kvadrata.*

Teorem 7.5. je specijalan slučaj ovog:

7.6. Eulerov kriterij. *Ako je* $M(c, p)=1$, *tada je*

$$\left(\frac{c}{p}\right)\equiv c^{\frac{p-1}{2}} \pmod p. \tag{6}$$

Dokažimo taj kriterij. Ako je

$$\left(\frac{c}{p}\right)=1, \quad \text{dakle} \quad x^2\equiv c \pmod p, \tag{7}$$

onda odatle, množeći eksponente sa $\frac{p-1}{2}$, izlazi:

$$x^{p-1}=c^{\frac{p-1}{2}} \pmod p. \tag{8}$$

Kako je $c\,M\,p=1$, to je i $x\,M\,p=1$, pa je prema Fermatu lijeva strana u $(8)\equiv 1$, tj.

$$1\equiv c^{\frac{p-1}{2}} \pmod p. \tag{9}$$

Time zbog (7), vidimo da (6) vrijedi za slučaj (7).

Još treba pokazati da (9) $\Rightarrow$ (7), pa će time biti dokazano (6). No, prema (9) zadovoljava c kongruenčiju

$$x^{\frac{p-1}{2}}\equiv 1 \pmod p.$$

A sva rješenja ove kongruencije jesu

$$1^2,\ 2^2, \ldots, \left(\frac{p-1}{2}\right)^2; \tag{10}$$

to znači da je c iz (9) kongruentno jednom od brojeva (10), recimo $r^2\equiv c \pmod p$. A to baš znači da je $\left(\frac{c}{p}\right)=1$. Time je teorem dokazan.

7.6.1. Da li je npr. kongruencija $x^2\equiv 3 \pmod{1949}$ moguća? Prema (6) je $\left(\frac{3}{1949}\right)=3^{974} \pmod{1949}$. No kako ovo izračunati?

Malo niže, u § 6.12, dokazat ćemo da je

$$\left(\frac{3}{1949}\right)=\left(\frac{1949}{3}\right)\cdot(-1)^{\frac{3-1}{2}\cdot\frac{1949-1}{2}}=\left(\frac{649\cdot 3+2}{3}\right)\cdot(-1)^{1974}=\left(\frac{2}{3}\right)=1.$$

Dakle je kongruencija moguća!

7.7. Nekoliko svojstava Legendreova simbola.

1. $\left(\frac{c^2}{p}\right)=1$, posebno $\left(\frac{1}{p}\right)\equiv 1$.

2. Ako je $c\equiv c'\pmod p$, tada je $\left(\frac{c}{p}\right)=\left(\frac{c'}{p}\right)$. Npr. $\left(\frac{1949}{3}\right)=\left(\frac{2}{3}\right)$.

3. $\left(\frac{c_1 c_2 \cdots c_k}{p}\right)=\left(\frac{c_1}{p}\right)\cdot\left(\frac{c_2}{p}\right)\cdots\left(\frac{c_k}{p}\right)$.

Dokažimo ovaj posljednji obrazac. Pišući $p_1=\frac{p-1}{2}$, imamo:

$$\left(\frac{c_1 c_2 \cdots}{p}\right)=\text{(prema (6))}=(c_1 c_2 \cdots)^{p_1}=c_1^{p_1} c_2^{p_1}=\text{(prema (6))}=$$

$$=\left(\frac{c_1}{p}\right)\cdot\left(\frac{c_2}{p}\right)\cdots$$

7.8. Označimo sa r bilo koji broj $1, 2, \ldots, p_1=\frac{p-1}{2}$; neka je $\varepsilon_r r'$ onaj broj kojemu je apsolutna vrijednost najmanja, a kongruentan je sa $cr \bmod p$; prema tome, $r'>0$, $\varepsilon_r=\pm 1$ i imamo sistem:

$$cr\equiv\varepsilon_r r' \pmod p,\ r=1, 2, \ldots p_1. \tag{11}$$

Pomnožimo međusobno sve te kongruencije; izlazi:

$$c^{p_1}\cdot 1\cdot 2\cdot 3\cdots p_1=\varepsilon_1\varepsilon_2\cdots\varepsilon_{p_1}\ 1'\cdot 2'\cdots p_1' \pmod p.$$

No, $1\cdot 2\cdot 3\cdots p_1=1'\cdot 2'\cdots p_1'$ i to je prema p prost broj; zato prethodnu kongruenciju možemo skratiti i dobiti $c^{p_1}\equiv\varepsilon_1\varepsilon_2\cdots\varepsilon_{p_1}\pmod p$, odnosno po (6):

$$\left(\frac{c}{p}\right)=\varepsilon_1\varepsilon_2\cdots\varepsilon_{p_1},\ \pmod p,\ p_1=\frac{p-1}{2}. \tag{12}$$

7.9. Najveće cijelo zadanog broja. Za broj x označimo sa Ex najveći cijeli broj $\leq x$. Npr. $E\,3/2=1$, $E\,10/4=2$. Stavimo $Mx=x-Ex$. Prema tome, za svaki broj x je $x=Ex+Mx$. Nadalje je za svaki cijeli broj n:

$$E(n+x)=n+Ex.$$

Također se vidi da je

$$E\frac{2cr}{p}=E\left[2E\left(\frac{cr}{p}\right)+2M\frac{cr}{p}\right]=2E\frac{cr}{p}+E\left(2M\frac{cr}{p}\right). \tag{13}$$

Ako to primijenimo na formule (11), gdje su c, r, p cijeli brojevi, tada je (13) parno ili neparno, već prema tome da li je broj $b_r=E\left(2M\frac{cr}{p}\right)$ jednak 0 ili 1. Taj je broj $=0$ onda ako je modulo p najmanji pozitivni ostatak broja

cr manji od $p/2$; ako je taj ostatak $>p/2$, onda je $\varepsilon_r=-1$; no za taj slučaj na taj način imamo:

$$\varepsilon_r=(-1)^{E\frac{2cr}{p}}$$ što sa (12) daje:

$$\left(\frac{c}{p}\right)=(-1)^{\sum_r E\frac{2cr}{p}} \quad \left(r=1, 2, \ldots, p_1=\frac{p-1}{2}\right). \tag{14}$$

Dokazali smo da vrijedi:

7.10. Lema (Gauss).

$$\left(\frac{c}{p}\right)=(-1)^{\mu},$$

pri čemu μ *pokazuje koliko brojeva*

$$c\cdot 1,\ c\cdot 2,\ c\cdot 3,\ \ldots,\ cp_1 \tag{15}$$

ima svoje najmanje pozitivne ostatke modulo p veće od p/2.

7.10.1. Kao primjenu Gaussove leme nađimo $\left(\frac{-1}{p}\right)$. Tu se radi o brojevima $-1, -2, -3, \ldots, -\left(\frac{p-1}{2}\right)$; svi njihovi pozitivni ostaci su $>p_1$, jer su preostali ostaci već zauzeti: $0, 1, 2, \ldots, p_1$. Dakle je $\mu=p_1$, pa Gaussova lema daje $\left(\frac{-1}{p}\right)=(-1)^{p_1}$ (teorem 7.5).

7.11. Teorem (Euler).

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}};$$

drugim riječima, broj 2 je kvadratni ostatak za proste brojeve oblika $8k+1$, *a neostatak za proste brojeve oblika* $8k\pm 3$.

Kako je p prost i neparan broj, to je p jednog od ovih oblika:

$$p=8k+1,\ 8k+3,\ 8k+5,\ 8k+7.$$

Promatrajmo prvi slučaj: $p=4k+1$. Dakle, $p_1=4k$ pa niz (15) za $c=2$ daje:

$$2\cdot 1,\ 2\cdot 2, \ldots, 2\cdot 2k,\ 2\cdot(2k+1), \ldots, 2\cdot 4k; \tag{16}$$

svi su oni ostaci mod p.

Brojevi u (16), koji su $>2\cdot 2k$, jesu $2(2k+1), \ldots, 2\cdot(2k+2k)$; ima ih $\mu=2k$; zato je prema 6.10

$$\left(\frac{2}{8k+1}\right)=(-1)^{\mu}=(-1)^{2k}=1.$$

Na sličan se način promatraju brojevi $p=8k+3$, $8k+5$, $8k+7$, i dokazuje da je 2 ostatak i za $8x+7$, a neostatak za $p=8k+3$, $8k+5$. To se kraće zapisuje Legendreovim simbolom kao u teoremu 7.11.

⟶ **7.12. Zakon recipročnosti.** *Ako su p, q prosti neparni brojevi, tada je*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},\ \text{odnosno}\ \left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

Riječima: neka su p, q prosti nejednaki brojevi >2; *ako je jedan od njih oblika* $4k+1$, *onda je q ostatak (neostatak) mod p, već prema tome da li je p ostatak (neostatak) mod q; ako su oba broja* $\equiv 3 \pmod 4$, *tada je q kvadratni ostatak (odnosno neostatak) mod p, već prema tome da li je p kvadratni neostatak (odnosno ostatak) mod q.*

7.12.1. Historijat. Zakon recipročnosti osnovao je Euler oko 1746; ime, oblik i nepotpun dokaz dao je Legendre 1785; potpun dokaz dao je Gauss 1801. (Gaussu su tada bile 24 godine). U toku svojeg života Gauss je našao šest dokaza zakona recipročnosti.

Dugo je Gauss tražio i zakon recipročnosti za bikvadratne ostatke; našao ga je tek kad je otkrio da se svojstva običnih racionalnih cijelih brojeva prenose i na kolo $D+i\,D$ *cijelih kompleksnih brojeva*; kubni zakon recipročnosti vezan je uz kolo „cijelih brojeva“ $D+D\rho$, gdje je ρ nula-tačka polinoma x^2+x+1. Vrlo se mnogo radilo i još se radi na zakonima recipročnosti ostataka stupnja >4.

7.12.2. Ilustracija zakona recipročnosti dana je u § 7.6.1.

7.13. Dokaz zakona recipročnosti. Polazimo od formule

$$\left(\frac{c}{p}\right)=(-1)^{\sum_r E\frac{2cr}{p}}\left(r=1,\,2,\,\ldots,\,p_1=\frac{p-1}{2}\right),$$

koju ćemo malo preobraziti i dokazati da za neparno c nadesno možemo brisati broj 2. Ako je c neparno, tada je $c+p$ parno, pa imamo ove zaključke:

$$\left(\frac{2}{p}\right)=\left(\frac{c}{p}\right)=(\text{po } 7.7.3)=\left(\frac{2c}{p}\right)=(\text{po } 6.7.2,\ \text{jer je } 2c=2c+2p \bmod p)=$$

$$=\left(\frac{2c+2p}{p}\right)=\left(\frac{4\cdot\frac{c+p}{2}}{p}\right)=\left(\text{po } 7.7.3,\ \text{uzimajući } c_1=4,\ c_2=\frac{c+p}{2}\right)=$$

$$=\left(\frac{4}{p}\right)\left(\frac{\frac{c+p}{2}}{p}\right)=1\cdot\left(\frac{\frac{c+p}{2}}{p}\right)=(\text{po (14)})=(-1)^{\sum_r E\frac{(c+p)r}{p}}=(-1)^{\sum_r E\frac{cr}{p}\sum_r r}=$$

$$=\left(\text{tu } r=1,\,2,\,\ldots,\,p_1=\frac{p-1}{2}\right)=(-1)^{\sum_r E\frac{cr}{p}+\frac{p^2-1}{8}}=(-1)^{\frac{p^2-1}{8}}(-1)^{\sum_r E\frac{cr}{p}}=$$

$$=(\text{prema } 6.11)=\left(\frac{2}{p}\right)(-1)^{\Sigma}.$$

Drugim riječima,

(1) $$\left(\frac{2}{p}\right)\left(\frac{c}{p}\right)=(-1)^{\frac{p^2-1}{8}}(-1)^{\sum_r E\frac{cr}{p}},\ \text{odakle zbog}\ \left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}:$$

(2) $$\left(\frac{c}{p}\right)=(-1)^{\sum_r E\frac{cr}{p}}\left(r=1,\,2,\ldots,\,\frac{p-1}{2}\right).$$

To je traženi izraz, jer ćemo iz njega odmah izvesti zakon recipročnosti. Za proizvoljan prost neparan broj $q\neq p$ formule (2) daje (sumacioni indeks označujemo sa p', odnosno q'):

$$\left(\frac{q}{p}\right)=(-1)^{\sum_{p'} E\left(\frac{q}{p}p'\right)}\left(p'=1,\,2,\ldots,\,p_1=\frac{p-1}{2}\right)$$

Analogno

$$\left(\frac{p}{q}\right)=(-1)^{\sum_{q'} E\left(\frac{p}{q}q'\right)}\left(q'=1,\,2,\ldots,\,q_1=\frac{q-1}{2}\right).$$

Odatle množeći:

(3) $$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^s,$$ gdje je

(4) $$s=\sum_{q'} E\left(\frac{pq'}{q}\right)+\sum_{p'} E\left(\frac{qp'}{p}\right)$$

(5) $$p'=1,\,2,\ldots,\,\frac{p-1}{2}$$

$$q'=1,\,2,\ldots,\,\frac{q-1}{2}.$$

Vidimo da se u (3) i (4) pojavljuju produkti pq' i qp' uz značenje (5) za p' i q'. Takva dva broja ne mogu biti jednaka, dakle je $pq'\neq qp'$, jer bi jednakost imala za posljedicu da je $p\,|\,q$ ili $p\,|\,p'$; a to nije moguće.

Prema tome, skup S svih uređenih parova

(6) $(pq',\,qp')$ ima $p_1\cdot q_1$ članova:

(7) $kS=p_1 q_1$ (kS je glavni broj množine S).

Nadalje, za svaki njegov član je ili

(8) $$pq'<qp' \quad \text{ili} \quad pq'>qp'.$$

Neka je S_0 podskup svih članova iz S za koje prvi slučaj nastupa, tj. S_0 se sastoji od svih uređenih dvojki (6) za koje vrijedi prvi dio relacije (8). No, za zadano p', odnos (8) se pojavljuje upravo za ove vrijednosti q':

$q'=1, 2, \ldots, E\frac{q}{p}p'$; tih vrijednosti ima $E\frac{qp'}{p}$; puštajući sada da p' varira od 1 do p_1, dobiju se na taj način svi parovi iz S_0, pa za glavni broj kS_0 množine S_0 imamo:

$$kS_0=\sum_{p'}E\frac{qp'}{p}.$$

Analogno $$kS_1=\sum_{q'}E\frac{pq'}{q}.$$

No, kardinalni broj kS od S je p_1q_1 s jedne strane (obrazac (7)), a s druge strane je $kS=kS_0+kS_1$, jer je $S=S_0\cup S_1$ i $S_0\cap S_1=$ prazno.

Na taj način izlazi:

$$\frac{p-1}{2}\,\frac{q-1}{2}=p_1q_1=kS=kS_0+kS_1=\sum_{p'}E\frac{qp'}{p}+\sum_{q'}E\frac{pq'}{q}=s$$

iz (3) i (4), tj.

$\frac{p-1}{2}\cdot\frac{q-1}{2}=s$. Time je dokazano da je $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{p_1q_1}$.

A to je traženi zakon recipročnosti.

8. JACOBIJEV SIMBOL[1)]

8.1. Legendreov simbol $\left(\frac{c}{p}\right)$ bio je definiran za *proste* brojeve p. Time je simbolom bilo vjerno prikazano da li je c kvadratni ostatak ili neostatak prema prostom modulu p. Formalno se definira analogan simbol i za *složene* module; no za njih treba uvijek posebno ustanoviti kvadratni karakter, tj. svojstvo da li je broj kvadratni ostatak ili neostatak.

8.2. Definicija. Neka je m bilo kakav neparan broj (prost ili složen—bez razlike). Neka tada za svaki cijeli broj c koji je prost prema m znak $\left(\frac{c}{m}\right)$ znači produkt Legendreovih simbola $\left(\frac{c}{p}\right)$ za $p|m$, pri čemu svako p nastupa sa svojom kratnošću. Drugim riječima *definiramo* tzv. *Jacobijev simbol*

$$\left(\frac{c}{p_1p_2\cdots p_r}\right)=\left(\frac{c}{p_1}\right)\cdot\left(\frac{c}{p_2}\right)\cdots\left(\frac{c}{p_r}\right). \tag{1}$$

8.3. Teorem. *Ako je c kvadratni ostatak modulo m, tada je*

$$\left(\frac{c}{m}\right)=1;$$

obrat više ne vrijedi (isp. teorem 7.5).

[1)] C. G. J. Jacobi [Jakobi] (1804—1851), njemački matematičar.

Naime, ako je $x^2 \equiv c \pmod{m}$, izlazi odatle pogotovu

$$x^2 \equiv c \pmod{p} \text{ za svako } p \mid m, \text{ dakle } \left(\frac{c}{p}\right) = 1,$$

dakle i množenjem takvih izraza $\left(\frac{t}{p}\right)$ izlazi opet 1 za $\left(\frac{c}{m}\right)$.

Lako se vidi da je $\left(\frac{2}{3}\right) = -1 = \left(\frac{2}{5}\right)$; dakle je po definiciji

$$\left(\frac{2}{3 \cdot 5}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = -1 \cdot -1 = 1, \quad \text{tj.} \quad \left(\frac{2}{15}\right) = 1.$$

Međutim, broj 2 je neostatak mod 15 (jer kad bi broj 2 bio ostatak mod 15, bio bi on ostatak i mod 3).

8.3.1. *Analogno* se dokazuje da iz $\left(\frac{c}{m}\right) = -1$ izlazi da je c neostatak modulo m.

Prema tome, stvarno značenje Jacobijeva simbola ne ide onako daleko dokle ide stvarno značenje Legendreova simbola. Međutim, formalna pravila za oblast simbola gotovo su *ista*.

Specijalno, imamo ove teoreme:

8.4. Teorem. *Ako je* $c \equiv c' \pmod{m}$, tada je $\left(\frac{c}{m}\right) = \left(\frac{c'}{m}\right)$ (isp. § 7.7.2).

8.5. Teorem. $\left(\frac{1}{m}\right) = 1$ (§ 7.7.1).

8.6. Teorem. $\left(\frac{c\,c'}{m}\right) = \left(\frac{c}{m}\right)\left(\frac{c'}{m}\right)$ (§ 7.7.3).

8.7. Teorem. $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$ (§ 7.5).

8.8. Teorem. $\left(\frac{2}{m}\right) = (-1)^{\frac{-m^2-1}{8}}$ (§ 7.11.).

8.9. Teorem. $\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}}$ (§ 7.12).

Dokaz tih teorema provodi se tako da se uvijek ide na definiciju (1) Jacobijeva simbola i njegovo svođenje na Legendreov simbol.

Dokažimo npr. 8.6.

$$\left(\frac{c\,c'}{m}\right) = \left(\frac{c\,c'}{\prod p}\right) = (\text{def. (1)}) = \prod_p \left(\frac{c\,c'}{m}\right) = \text{po svojstvu 7.7.3. za Legendreov simbol}$$

$$\prod \left(\frac{c}{p}\right)\left(\frac{c'}{p}\right) = \prod_p \left(\frac{c}{p}\right) \prod_p \left(\frac{c'}{p}\right) = (\text{def. (1)}) = \left(\frac{c}{m}\right)\left(\frac{c'}{m}\right).$$

8.10. D o k a z i. Dokažimo npr. 8.8, i to za dva faktora (slično je općenito):

$$\left(\frac{2}{m}\right)=\left(\frac{2}{p_1 p_2}\right)=\left(\frac{2}{p_1}\right)\left(\frac{2}{p_1}\right)=(\text{teorem } 7.11)=(-1)^{\frac{p_1^2-1}{8}}\cdot(-1)^{\frac{p_2^2-1}{8}}= \tag{1}$$

$$=(-1)^{\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}}.$$

No, $\dfrac{m^2-1}{8}=\dfrac{(p_1 p_2)^2-1}{8}=\dfrac{p_1^2 p_2^2-1}{8}=\dfrac{\left(1+8\dfrac{p_1^2-1}{8}\right)\left(1+8\dfrac{p_2^2-1}{8}\right)-1}{8}$

$=\dfrac{p_1^2-1}{8}+\dfrac{p_2^2-1}{8}+$ paran broj. Dakle je uistinu i $\left(\dfrac{2}{m}\right)$ i $(-1)^{\frac{m^2-1}{8}}$ jednako.

Dokažimo i 8.9.

$\left(\dfrac{m}{n}\right)=\prod_{p_i}\left(\dfrac{m}{p_i}\right)=(\text{po } 7.6)=\prod_{p_i}\prod_{q_j}\left(\dfrac{q_j}{p_i}\right)$. Slično $\left(\dfrac{n}{m}\right)=\prod_{q}\prod_{p}\left(\dfrac{p}{q}\right)$.

Pri tom p prolazi potpunim nizom prostih faktora broja m, a q slično za n, tj. $\prod p_i=m$, $\prod q_j=n$.

Odatle množenjem:

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=\prod_{p_i}\prod_{q_j}\left(\frac{q_j}{p_i}\right)\cdot\prod_{q_j}\prod_{p_i}\left(\frac{p_i}{q_j}\right)=(\text{po teoremu } 7.12)=(-1)^k, \text{ gdje je} \tag{2}$$

$k=\sum_i\sum_j\dfrac{p_i-1}{2}\cdot\dfrac{q_j-1}{2}$. No, ovo je dalje $=\sum_i\dfrac{p_i-1}{2}\sum_j\dfrac{q_j-1}{2}=\dfrac{m-1}{2}\cdot\dfrac{n-1}{2}+$

+ paran broj. Dakle je

$$\left(\frac{m}{n}\right)\cdot\left(\frac{n}{m}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}+\text{parno}}=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

Prema tome, teorem 8.9 je dokazan.

P r i m j e r.

$$\left(\frac{35}{88}\right)=\left(\frac{87}{35}\right)\cdot(-1)^{\frac{35-1}{2}\cdot\frac{87-1}{2}}=\left(\frac{17}{35}\right)\cdot-1=-\left(\frac{35}{87}\right)\cdot(-1)^{\frac{17-1}{2}\cdot\frac{35-1}{2}}=$$

$$=-\left(\frac{1}{17}\right)\cdot 1=-1\cdot 1=-1. \text{ Dakle je } \left(\frac{35}{87}\right)=-1.$$

Kongruencija $x^2\equiv 35 \pmod{87}$ nema rješenja.

9. KVADRATNE KONGRUENCIJE

9.1. Oblika su

(1) $$a x^2 + b x + c \equiv 0, \pmod{m}.$$

Naravno da se pretpostavlja da je $a \not\equiv 0, \pmod{m}$. Transformirajmo (1) tako da nastane kvadrat; treba pomnožiti sa a:

(2) $$a^2 x^2 + a b x + a c \equiv 0, \pmod{a m}.$$

Da $(2)_1$ nadopunimo na kvadrat, pomnožimo sa 4:

$$(2 a x + b)^2 - b^2 + 4 a c \equiv 0, \pmod{4 a m},$$

odnosno stavljajući:

$$2 a x + b = y, \quad \text{tj.} \quad y \equiv b, \pmod{2 a}$$

$$b^2 - 4 a c = D \ (D \text{ je } \textit{diskriminanta} \text{ kongruencije } (1));$$

izlazi:

$$y^2 \equiv D, \pmod{4 a m}.$$

Tako se, dakle, *kongruencija* (1) *svela na čistu kongruenciju*

$$y^2 \equiv D \pmod{4 a m} \ \textit{sa}$$

$$y \equiv b, \pmod{2 a}.$$

Ukratko, možemo se ograničiti na čisto kvadratne kongruencije

(3) $$x^2 \equiv D, \pmod{m}.$$

9.2. Dokažimo da možemo pretpostaviti

(4) $D \,\mathrm{M}\, m = 1$, tj. da su D, m međusobno prosti brojevi.

Stvarno, neka je

(5′) $$\delta = \mathrm{M}(D, m), \ D = \delta D', \ m = \delta m';$$

tada je

(5₁) $$\mathrm{M}(D', m') = 1.$$

Stavimo

(6) $$\delta = e^2 f,$$

f bez kvadratnog faktora. Brojevi δ, D', m', e, f jednoznačno su određeni.

Stavimo li izraze (5) i (6) u (3), dobija se

(7) $$x^2 \equiv e^2 f D' \pmod{e^2 f m'}.$$

Odatle se zaključuje da mora biti

$$e^2 \mid x^2, \quad \text{dakle} \quad e \mid x;$$

neka je $x = e y$; tada (7) daje nakon skraćivanja sa e^2:

(9) $$y^2 \equiv f D' \pmod{f m'}.$$

Odatle se analogno zaključuje da je

(10) $$f \mid y^2 \quad \text{te} \quad f \mid y,$$

jer je f bez kvadratnog faktora; dakle je

(10¹) $$y = f z,$$

pa se iz (9) najzad dobiva, dijeleći (9) sa f:

(10) $$f z^2 \equiv D' \pmod{m'}.$$

Iz ove kongruencije izlazi:

$$\mathrm{M}(f, m') \mid \mathrm{M}(D', m'); \quad \text{zbog} \quad D' \,\mathrm{M}\, m' = 1$$

znači to da je

(11) $$f \,\mathrm{M}\, m' = 1.$$

Najzad iz (9) izlazi:

(12) $$y^2 \equiv f D' \pmod{m'}; \quad \text{k tome je } D' f \,\mathrm{M}\, m' = 1,$$

jer je

$$D' \,\mathrm{M}\, m' = 1 \text{ (isp. (5'))} \quad \text{te} \quad f \,\mathrm{M}\, m' = 1 \text{ (prema (11))}.$$

9.3. Prema tome je uistinu kongruencija (3) svedena na rješavanje analogne kongruencije (12) uz dodatni uslov da slobodni koeficijent i modul budu međusobno prosti.

Obratnim putem dolazi se iz (12) do (3): dovoljno je (12) pomnožiti svuda sa e^2, tj. i lijevo i desno i modul.

Zato ograničenje koje smo prije toga stavljali da u $x^2 \equiv c \pmod{m}$ bude $c \,\mathrm{M}\, m = 1$ *stvarno nije nikakvo ograničenje.*

10. Zadaci o binomnim kongruencijama i ostacima potencija.

1. Da li ova kongruencija dopušta rješenje: 1) $x^2 \equiv 1 \pmod{5}$;
   2) $2x^2 \equiv 3 \pmod{7}$; 3) $3x^4 \equiv 5 \pmod{11}$; 4) $15x^7 \equiv 14 \pmod{17}$;
   5) $3x^4 \equiv 2 \pmod{6}$; 6) $x^5 \equiv 44 \pmod{101}$; 7) $x^2 \equiv -2 \pmod{1823}$?
2. Odredi kvadratne ostatke i kvadratne neostatke za modul
   1) 3; 2) 5; 3) 6; 4) 8; 5) 11; 6) 12; 7) 13; 8) 19.
3. Odredi $\left(\frac{-1}{p}\right)$ za $p = 2, 3, 5, 7, 11, 12, 20, 1971$.
4. Odredi $\left(\frac{100}{p}\right)$ za $p = 5, 7, 13$.
5. Odredi $\left(\frac{2}{p}\right)$ za $p = 13, 17, 1961$.

6. Odredi proste brojeve p za koje je $\left(\frac{360}{p}\right)=1$.

7. Odredi proste brojeve p za koje je $\left(\frac{72}{p}\right)=-1$.

8. Odredi $\left(\frac{17}{29}\right)$, $\left(\frac{71}{101}\right)$, $\left(\frac{13}{1961}\right)$.

9. Izračunaj $\left(\frac{1}{6}\right)$, $\left(\frac{2}{6}\right)$, $\left(\frac{3}{6}\right)$, $\left(\frac{5}{6}\right)$, $\left(\frac{100}{6}\right)$, $\left(\frac{6}{100}\right)$.

10. Riješi ove kvadratne kongruencije: $x^2-1\equiv 0 \pmod 8$. (Rez. 1, 3, 5, 7). 1) $x^2+x\equiv 0 \pmod 2$; 2) $x^2+x+1\equiv 0 \pmod 2$; 3) $3x^2+6x-1\equiv 0 \pmod 5$; 4) $17x^2-13x+19\equiv 0 \pmod{12}$; 5) $-256x^2+389x-30\equiv 0 \pmod{30}$.

11. Riješi: 1) $2x^3\equiv 6 \pmod 7$ (Nema rješenja).
2) $2^x\equiv 1 \pmod 7$ (Rez. $6D$, $6D+3$ tj. $3D$).
3) $x^7-3x+2\equiv 0 \pmod 5$ (Rez. 1, 3).
4) $x^x\equiv 2 \pmod 5$ (Rez. $3+20n$, $17+20n$ za $n=0, 1, 2$).

LITERATURA

Albert A. A.

[1] Structure of algebras, New York 1939, 12 + 210.
[2] Introduction to algebraic theories, Chicago 1941, 8 + 138.

Alendoerfer C. B. — Cletus Oakley

[1] Principi matematike (prevela Jelena Stojanović), Beograd 1961, XVI + 411 (gl. 1: logika).

Aljančić Slobodan

[1] Uvod u realnu i funkcionalnu analizu. Građevinska knjiga, Beograd 1968, 6 + 327.

Anđelić T. P.

[1] Teorija vektora, Beograd 1947, 8 + 408.
[2] Tenzorski račun, Beograd, 8 + 320.
[3] Matrice, Beograd 1962, 268 str.

Arow K. J. — Nurwitz L. N. — Uzawa H.

[1] Studies in linear and non-linear programming, Stanford 1958 (ruski, Moskva 1962, 334).

Bachmann P.

[1] Zahlentheorie. Versuch einer Gesamtdarstellung dieser Wissenschaft in ihren Hauptteilen. I - Die Elemente der Zahlentheorie, Leipzig 1892, 12 + 264; II - Die analytische Zahlentheorie; 1894, 18 + 494; III - Die Lehre von der Kreisteilung und ihre Beziehungen zur Zahlentheorie, 1872, 12 + 300; IV - Die Arithmetik der quadratischen Formen, 1. Abt. 1898, 16 + 668; V - Allgemeine Arithmetik der Zahlenkörper, 1905, 22 + 548,
[2] Die Lehre von der Kreisteilung und ihre Beziehungen zur Zahlentheorie, Leipzig 1872, 12 + 300.

Ball, W. W. Rouse

[1] A short account of the History of mathematics, London 1908_4, 24 + 522.

Barsov A. S.

[1] Čto takoe linejnoje programmirovanije, Moskva 1959, 104.

Behnke H. (sa saradnicima)

[1] Grundzüge der Mathematik, I Grundlagen. Arithmetik und Algebra; Göttingen 1962_2, 14 + 572.

Bell E. T.

[1] The development of mathematics, New York—London 1945_2, 12 + 638.

Berezin I. S. — Židkov N. P.

[1] Metodi víčislenij II, Moskva 1962_2, 639.

Bhagavantam S. — Venkatarayudu T.

[1] Theory of groups and its application to physical problems, Andhra Univ., Waltair 1951_2 (ruski, Moskva 1959, 301).

Bieberbach L. — Bauer G.

[1] Algebra, Leipzig—Berlin 1933_5, 10 + 358.

Bilimović Anton

[1] Geometrijske osnove Računa sa diodama I Dioda i afinor. Srpska akademija Nauka. Posebna izdanja 72 (1930) 14 + 232.

Birkhoff Garrett

[1] Lattice theory, New York, 1948_2, 14 + 283.

Birkhoff G. — Mac Lane S.

[1] A survey of modern algebra, New York 1953, 12 + 472.

Blanuša D.

[1] Viša matematika I dio; prvi svezak. Algebra i algebarska analiza, Zagreb I_1 1963, 483, I_2 (1965) s. 927; II_1 (1969) 403.

Bodewig E.

[1] Matrix Calculus, Amsterdam 1959_2, 12 + 452.

Boerner H.

[1] Darstellungen von Gruppen, Berlin — Göttingen — Heidelberg 1955. 12 + 287.

Boole George

[1] The mathematical analysis of logic, Cambridge 1847, 82.

Borevič Z. I. — Šafarevič I. R.

[1] Teorija čisel, Moskva 1964, 568.

Borůvka O.

[1] Uvod do teorie grup, Praha 1944_1, 1952_2.

[2] Grundlagen der Gruppoid — und Gruppentheorie, Berlin 1960, 12 + 198.

Bourbaki N.

[1] Éléments de Mathématiques, Livre II Algèbre: 1. Structures algébriques, Paris 1951_2, 4 + 176; 2. Algèbre linéaire, 134; 3. Algèbre multilinéaire, Paris 1948, 158; 4. Polynomes et fractions rationnelles; 5. Corps commutatifs, Paris 1950, 222; 6. Groupes et corps ordonnés; 7. Modules sur les anneaux principaux, Paris 1952, 160 (ruski prevod 1-3 D. A. Rajkova, Moskva 1962, 516).

Buhštab A. A.

[1] Teorija čisel, Moskva 1966_2, 384.

Burnside W.

[1] Theory of groups of finite order, Cambridge 1897, 1911_2.

Cahen E.

[1] Élements de la théorie des nombres Paris 1899, 8 + 403.

Cantor Moritz

[1] Vorlesungen über Geschichte der Mathematik, I - Leipzig 1880_1, 8 + 804; II - Leipzig 1892, 10 + 963; III - Leipzig 1901_2, 10 + 923.

Cesarec Rudolf

[1] Analitička geometrija linearnog i kvadratnog područja. I - Analitička geometrija u ravnini, Zagreb 1957, 20 + 528.

Cohn P. M.

[1] Universal algebra, New York-London 1965 (ruski prevod 1968, 352).

Church A.

[1] Introduction to mathematical logic 1, Princeton 1956, IX + 376.

Curry Haskell B.

[1] Foundations of Mathematical logic, 1963 (ruski prevod: Osnovanija matematičeskoj logiki, Moskva, 1969, 568).

Demidovič B. P. — Maton I. A.

[1] Osnoví víčislitel' noj matematiki, Moskva 1963, 660.

Denis-Papin M., Kaufmann A.

[1] Cours de calcul matriciel appliqué, Paris 1951, 304.

Deuring Max

[1] Algebren, Ergebnisse der Mathematik und ihrer Grensgebiete, Bd. 4, fasc. 1,

Devidé Vladimir

[1] Matematička logika. Prvi dio (klasična logika sudova), Beograd 1964 (Mat. inst. knj. 3), 288.

Dickson Leonard Eugene

[1] History of the theory of numbers, Washington 1919—20—23, 3 sveska.

[2] Modern elementary theory of numbers, Chicago 1939, 7 + 309.

Dubreil **Paul**

[1] Algèbre I, Équivalences, operations, groupes, anneaux, corps, Paris 1946, 10 + 306; 1954_2, 467 pp.

Dubreil Paul, Dubreil — Jacotin M. L.

[1] Leçons d'algèbre moderne, Paris 1964_2, 7 + 401.

Dubreil — Jacotin M. L., Groisot R.

[1] Leçons sur la théorie des treillis ordonnés et des treillis géométriques, Paris 1958, 8 + 385

Galois E.

[1] Écrits et Mémoires mathématiques d'Evariste Galois. Édition critique intégrale de ses manuscrits et publicatons par Robert Bourgne et J. P. Azra, Préface de J. Dieudonné, Paris 1962, Gauthier—Villars, 22 + 542.

* * *

[1] Encyklopädie der math. Wissenschaften (red. W. F. Meyer), I - Arythmetik und Algebra, Leipzig 1898—1904, 38 + 1197. Drugo izdanje: I Algebra und Zahlentheorie, 1. A -- - Grundlagen, B - Algebra, 1939.

* * *

[2] Enciklopedija elementarnoj matematiki (pod redakcijej P. S. Aleksandroya, A. I. Mar kuševiča i J. J. Hinčina), II - Algebra, Moskva—Lenjingrad 1961, 424.

Faddejev D. K. — Faddejeva V. N.

[1] Vičislitel'nie metodi linejnoj algebri, Moskva—Lenjingrad 1963, 736. (popis literature ispunio je str. 677—734).

Faddeev D. K. — Sominskij I. S.

[1] Sbornik zadač po višej algebre, Moskva 1953_2, 308.

Gantmaher F. R.

[1] Teorija matric, Moskva 1954, 492, odnosno 1966_2, 576.

Gavrilović Bogdan

[1] Teorija determinanata, Beograd 1899, 12 + 278.

Gel'fond A. O.

[1] Transcendentnije i algebraičeskije čisla, Moskva 1952, 224.

Glejzer G. I.

[1] Istorija matematiki v škole, Moskva 1964, 376.

Gribanov V. U. — Titov P. I.

[1] Sbornik upražnenij po teoriji čisel, Moskva 1964, 144.

Greub Werner H.

[1] Linear Algebra, Berlin-Göttingen—Heidelberg, Springer Verlag 1963_2 12 + 338.

Hadley G.

[1] Linear programming, London 1962, 12 + 520.

Hall M. jr.

[1] The theory of groups, New York 1959 (na ruskom: Moskva 1962, 468).

Hasse Helmut — Klobe W.

[1] Aufgabensammlung zur höheren Algebra (Sammlung Göschen, 1082), Berlin 1961_3, 183.

Hasse H.

[1] Vorlesungen über Zahlentheorie, Grundl. d. math. Wiss. 61, Springer V. 1950, 12 + 474.

[2] Zahlentheorie. Akademie-Verlag, Berlin 1963; pp. 611.

[3] Höhere Algebra I - 1963_5, II - 1958_4 (Sammlung Göschen, 931, 932), 150, odn. 158 str.

Hilbert D. — Ackermann W.

[1] Grundzüge der theoretischen Logik, Berlin 1938_2, 8 + 134.

Jacobson Nathan

[3] Structure of rings, Amer. Math. Soc., Prov. 1956, 7 + 263 (ruski, Moskva 1961, 392 s).

Juškevič A. P.

[1] Istorija matematiki v srednije vjeka, Moskva 1961, 448.
(pod uredništvom Juškeviča)

[2] Istorija matematiki 1, 2 Moskva 1970.

Karamata J.

[1] Algebra I, Prvi deo, Beograd 1949, 140; Drugi deo, Beograd 1950, 184.

Karlin S.

[1] Mathematical methods and theory in games, programming and economics, London--Paris Vol I 10 + 433, Vol. II 11 + 386 (ruski, Moskva 1964, 838).

Kašanin R.

[1] Viša matematika, Beograd I (1949_3 7 + 847, II_1 (1949) 8 + 624, II_2 (1950) 7 + 679.

Kočin N. E.

[1] Vektornoje isčislenije i načala tenzornogo isčislenija, Moskva 1951_7, 428.

Kol'man E.

[1] Istorija matematiki v drevnosti, Moskva 1961, 236.

Kowalewski G.

[1] Determinantentheorie, Berlin—Leipzig 1925_2, 4 + 304.

Kraitschik M.

Recherches sur la théorie des nombres 1924. T. 1, 1929, str. 16 + 272; T. 2, Factorisation, 1924, str. 15 + 184; Théorie des nombres, Paris, I - 1922; II - 1929.

Krečmar V. A.

[1] Zadačnik po algebre, Moskva—Leningrad 1950, 440.

Križanič France

[1] Vektorji, matrike, tenzorji, Ljubljana 1962, 272.

Krull W.

[1] Elementare und klassische Algebra vom modernen Standpunkt I (Sammlung Göschen, 930), Berlin 1963_3, 148 str.; II (S. G. 933), Berlin 1959, 132.

[2] Allgemeine Modul-, Ring- und Idealtheorie . . . (Enzykl. d. math. Wiss.) Leipzig-Berlin 1939, Bd I 1. Teil, 11, 1—54 12, 1—53.

Kurepa Đuro

[1] Teorija skupova, Zagreb, 1951, 22 + 444.

[2] Šta su skupovi i kakva im je uloga. Zagred, 1960, 11+190; 1967_2, 4+203; 1970_3, 4+215.

Kurepa Svetozar

[1] Konačno dimenzionalni vektorski prostori i primjene, Zagreb, Tehn. knj. 1967, 788.
[2] Uvod u matematiku. Skupovi. Strukture. Brojevi. Zagreb, Tehn. knj. 1970, 252.

Kuroš A. G.

[1] Kurs višej algebri, Moskva—Leningrad 1952_3, 336.

[2] Teorija grupp, Moskva 1953_2, 468; 1967_3 648.

[3] Lekciji po obščej algebre, Moskva 1962, 396.

Landau E.

[1] Vorlesungen über Zahlentheorie. I - Aus der elementaren und additiven Zahlentheorie, 12 + 360; II - Aus der anal. und geom. Zahlentheorie, 8 + 308; III - Aus der alg. Zahlentheorie und über die Fermatsche Vermutung, 8 + 342 Leipzig 1927.

Lang Serge

[1] Algebra, Reading Mass. 1965 (r. Moskva, 1968, 564).

Lejeune — Dirichlet P. G.

Vorlesungen über Zahlentheorie (redigirao i dopunio R. Dedekind 1863_1, 1871_2, 1879_3, 1894_4, 17 + 657 str.). Isp. Dedekindova Djela (Gesammelte mathematische Werke, Braunschweig III, 508 str.).

Lichnerowicz A.

[1] Algèbre et Analyse linéaires, Paris 1947, 316 (njem. prevod. Berlin 1956,1 2 + 304).

Lomont J. S.

[1] Applications of finite groups, New York—London 1959, 10 + 346.

Lugowski H. — Weinert H. J.

[1] Grundzüge der Algebra, Leipzig. I - Allgemeine Gruppentheorio, 1957, 5 + 234; II - Allgemeine Ring- und Körper-Theorie 1958; III - Auflösungstheorie algebraischer Gleichungen, 1960, 274.

L'ubarskij G. Ja.

Teorija grupp i jijo primenjenije v fizike, Moskva 1958, 354 (na engl. preveo Dedijer).

Mac Duffee C. C.

[1] The theory of matrices (Ergebnisse d. Math. 2), Berlin 1933, 6 + 110.

[2] An introduction to abstract algebra, London 1940, 8 + 304.

Mal'cev A. I.

[1] Osnoví linejnoj algebri, Moskva, 1956_2, 340.

Marković Željko

[4] Uvod u višu analizu; I - 1947_2, 8 + 618; II - 1952, 12 + 640.

Matvijevskaja E. M.

[1] Učenije o čisle na sredn'evjekovom bližn'em i sredn'em vostoke Taškent, 1967, 344.

Miličić Pavle — Uščumlić Momčilo

[1] Zbirka zadataka iz Više matematike I, Građevinska knj., Beograd, 1969_3, 6 + 633; II 1971, 6 + 792.

Mitrinović D. S. sa saradnicima

[4] Zbornik matematičkih problema. I - Beograd 1958_2, 6 + 352; II - Beograd 1958_2, 16 + 408; III - Beograd 1960, 16 + 336.

Mitrinović D. S. — Mihailović D.

[1] Linearna algebra. Analitička geometrija. Polinomi. Beograd 1959, 16 + 414.

Mostowski Andrzej

[1] Logika matematyczna, Warszawa—Wroclaw 1948, VIII + 388.

Muir Thomas

[1] The theory of determinants in the historical order of development, Vol. 1, London 1906_2, 11 + 491; Vol. 2 (period 1841—1860), London 1911, 16 + 475.

Najmark M. A.

[1] Normirovanníje kol'ca, Moskva 1956, 488.

Nešić Dimitrije

[1] Algebarska analiza, 1 - Beograd 1883; 2 - Beograd (1883), 12 + 670.

Obreškov N.

[1] Visša algebra, Sofija 1947_2, 10 + 524.

[2] — — II, 1935, 12 + 480.

[3] Sbornik ot zadači i teoremi po visša algebra, Sofija 1932, 8 + 488.

[4] Verteilung und Berechnung der Nullstellen reeller Polynome, Berlin 1963, 8 + 298 (navedena je opsežna bibliografija).

Ostrowski A. M.

[1] Solution of equations and systems of equations. Acad. Press, New York—London, 1960 (ruski: Moskva, 1963, 219).

Perron O.

[1] Algebra. I - Die Grundlagen, Berlin—Leipzig 1932_2, 8 + 302; II - Theorie der algebraischen Gleichungen, 1933_2, 8 + 262.

Pickert G.

[1] Einführung in die höhere Algebra, Göttingen 1951, 298.

Plemelj J.

[1] Algebra in teorija števil, Ljubljana 1962, 16 + 280.

Postnikov M. M.
[1] Teorija Galua, Moskva 1963, 218.
Prachar Karl
[1] Primzahlverteilung, Berlin—Göttingen—Heidelberg, 1957 (ruski, Moskva 1967, 511).
Prijatelj Niko
[1] Uvod v matematično logiko, Ljubljana 1960, 150.
Proskurjakov I. V.
[1] Sbornik zadač po linejnoj algebri, Moskva 1957, 368.
Rašajski Borivoje
[1] Analitička geometrija, Beograd, Građevinska knjiga, 1968_2, 6 + 320.
Rudeanu Sergiŭ
[1] Axiomele laticilor şi ale algebeler booleene, Bucuresti 1963, 159.
Scholz A. — Schoeneberg B.
[1] Einführung in die Zahlentheorie (S. G. 1131), Berlin 1961, 128.
Scorza G.
[1] Gruppi astratti, Roma 1942, 8 + 242.
Sedmak V.
[1] Uvod u algebru, Zagreb 1961, 16 + 240.
Serre Jean Pierre
[1] Représentations linéaires des groupes finis, Paris 1967 (ruski: Moskva, 1970, 132).
Serret J. A.
[1] Cours d'algèbre supérieure. I - Paris 1928_7, 648; II - Paris 1928_7, 696 (njem. Leipzig 1868_2, 528, 574).
Sierpiński Waclaw
[1] Teoria liczb. I - Warszawa 1950, 8 + 544; II - Warszawa 1959, 488.
[2] Zasady algebry wyzszej z przypisem A. Mostowskiego Zarys teorii Galois, Warszawa—Wroclaw 1951_2, 8 + 436.
[3] Algèbre des ensembles, Warszawa—Wroclaw 1951, 205.
Sikorski Roman
[1] Boolean algebras (Ergebnisse der Math.), Berlin—Gottingen—Heidelberg 1960, 10 + 176.
Simonart F.
[1] Leçons d'algèbre supérieure, Louvain—Paris 1934, 11 + 327.
Smirnov V. I.
[1] Kurs višej matematiki III_1, Moskva—Leningrad, 1949_4, 335.
Smith D. E.
[1] History of mathematics. I - New York 1958, 22 + 596; II - New York 1958, 12 + 725.
Specht W.
[1] Gruppentheorie, Berlin—Göttingen—Heidelberg 1956, 4 + 458.
Speiser A.
[1] Theorie der Gruppen von endlicher Ordnung, Berlin 1937_3, 10 + 262.
Steinitz E.
[1] Algebraische Theorie der Körper: a) Journal für die reine und angew. Mathematik; b) kao knjigu izdali Baer R. — Hasse H, Berlin—Leipzig 1930.
Stojaković Mirko
Teorija jednačina, Naučna knjiga, Beograd 1966, 155.
Stone M. H.
[1] Linear transformations in Hilbert space, New York 1932, 8 + 622.
Struik, Dirk J.
[1] A concise history of Mathematics, Dover Publ. New York (na srpskohrvatski preveo Milenko Nikolić, Beograd, Zavod za izdavanje udžbenika SRS, 1969, 372).

Szász Gabor

[1] Introduction to Lattice Theory, Budapest, 1963, 229.

Šilov G. E.

[1] Vvedenije v teoriju linejnih prostranstv, Moskva 1956, 303.

Taton R. (sa saradnicima)

[1] Histoire générale des Sciences. I - La science antique et médiévale, Paris 1957, 8 + 628; II - La science moderne (1450—1800), Paris 1958, 8 + 800.

Tropfke J.

[1] Geschichte der Elementar-Mathematik, Berlin—Leipzig. 1. Rechnen, 1930_3, 7 + 222; 2. Allgemeine Aritmetik, 1933_3, 266; 3. Proportionen. Gleichungen, 1937_3.

Vajda S.

[1] The theory of games and linear programming, London.

[2] Théorie des jeux et programmation linéaire (traduit et adapté par J. Bouzitat), Paris 1959, 14 + 256.

Vígodski M. Ja.

[1] Arifmetika i algebra v drevnem mirje, Moskva—Leningrad 1941, 252; Moskva 1967_2 (pripremio B. A. Rozenfel'd) 368.

Vilenkín N. Ja.

[1] Specijal'níe funkciji i teorija predstavlenij grupp, Moskva, 1965, 588.

Vidav Ivan

[1] Višja matematika, Ljubljana, I (1949) 334, II (1951) 442.

Vinogradov I. M.

[1] Osnoví teoriji čisel, Moskva—Leningrad 1949, 180.

van der Waerden Z. L.

[1] Moderne Algebra. I - (1930); 1960_5 8 + 292; II - (1931) 8 + 216 1959_4, 10 + 275.

Weber H.

[1] Lehrbuch der Algebra. I - Braunschweig 1895_1, 1898_2, 16 + 704; II - Braunschweig 1899_1, 1899_2, 16 + 885; III - Braunschweig 1908_2, 16 + 733.

Wedderburn J. H. M.

[1] Lectures on matrices, Amer. Math. Soc., New York 1934, 10 + 205 (kopija od 1949). Tu se nalazi popis literature o matricama prikazan po svakoj godini za razdoblje 1853—1936 (svega 661 djelo).

Weyl H.

[1] Gruppentheorie und Quantenmechanik, Leipzig 1928, 8 + 288.

[2] The classical groups. Their invariants and representations. Princeton 1953, 14 + 320.

Whittaker Edmund — Robinson G.

[1] Tečaj numeričke matematike; prevela Vojna Radojčić, Beograd 1951, 12 + 362 (original London 1948_4).

Wieleitner H.

[1] Istorija matematiki ot Dekarta do serediní XIX stoletija (ruski prevod s njemačkoga pod uredništvom A. P. Juškeviča) Moskva, Nauka, 1966, 508.

Wintner A.

[1] Spektraltheorie der unendlichen Matrizen, Leipzig 1929, 12 + 280.

Zariski O. — Samuel P.

[1] Commutative algebra. I - Princeton 1958, 11 + 329; II - 1960, 10 + 414 (ruski, Moskva 1963, I - 374 str., II - 440 str.).

Zassenhaus H.

[1] Lehrbuch der Gruppentheorie I, Leipzig—Berlin 1937, 152.

Zurmühl R.

[1] Matrizen, Berlin—Heidelberg 1950, 16 + 428 (odn. 1964_4, 12 + 452).

ABECEDNI POPIS IMENA

(brojevi označavaju stranice; mastan broj znači da se nalazi i slika)

ABECEDNI SADRŽAJ

(brojevi redom označavaju: poglavlje, paragraf itd.)

PREGLED OZNAKA

(brojevi označavaju redom: poglavlje, paragraf itd.)

o, O, $\ll$	6 § 7.14.31
$\vartheta(x)$	6 § 7.14.32
$P(x)$	6 § 7.14.30
$\zeta(s)$	6 § 7.14.33
$M(a, b)$, $a M b$, $\mathrm{W}(a, b)$, $a \mathrm{W} b$	6 § 8.3
$\Phi(m)$, $\varphi(m)$	6 § 17.16.2
$d_o n$	6 § 19.4.6
σn	6 § 19.4.7. 1)
$d_r(n)$	6 § 19.4.8. 1)
Sp	7 § 8.2.1
σ_p	24 § 2.5 (nota)
	27 § 2.9
δ_{ij}, δ^i_j	10 § 3.6
$L(R, M)$	13 § 3.7.3
G/F	17 § 11.4
$G_1 \oplus G_2$	17 § 14.5.5
$[G, G]$	17 § 18.2
G'	17 § 18.3
$\Phi_n(x)$	18 § 5.1 (2)
$V_n(R)$	25 § 2
$x \ominus y$	25 § 3.1
$V\star$	26 § 2.4
ZG	17 § 9.5
S_n	17 § 7.4

Ako je R dvočlana relacija, tada R_1 znači *prvi* a R_2 *drugi* dio (član) od R; tako npr. ako (5) znači jednadžbu, tada $(5)_1$ znači *lijevu* a $(5)_2$ znači *desnu* stranu od (5).

Ako S označuje skup, tada se svaki član iz S označuje sa $\dot{S}$ (tačka iznad S) ili $S^{\cdot}$; neka određena tačka iz S označuje se sa $\underset{\cdot}{S}$ (tačka ispod oznake za skup).

$\dot{n}$ ili $n^{\cdot}$ označuje *svaki* redni broj $< n$; $n^{\cdot} = \underbrace{0, 1, 2, \ldots}_{n}$

NERIJEŠENI PROBLEMI

P_1	6 § 6.12.8	P_{16}	6 § 7.14.19	P_{29}	6 § 7.14.36
P_2	6 § 6.12.9	P_{17}	6 § 7.14.20	P_{30}	6 § 14.9.11
P_3	6 § 7.5	P_{18}	6 § 7.14.21	P_{31}	6 § 17.7.18
P_4—P_5	6 § 7.12 (2 probl.)	P_{19}	6 § 7.14.22	P_{32}	6 § 17.7.19
P_6—P_7	6 § 7.14.3 (2 probl.)	P_{20}	6 § 7.14.23	P_{33}	6 § 19.3.10
P_8	6 § 7.14.10	P_{21}	6 § 7.14.25	P_{34}	6 § 19.4.3. 3).
P_9	6 § 7.14.11	P_{22}	6 § 7.14.26	P_{35}	6 § 19.4.7. 4).
P_{10}	6 § 7.14.12	P_{23}	6 § 7.14.27	P_{36}	6 § 19.4.12. 3).
P_{11}	6 § 7.14. 13.7).	P_{24}	6 § 7.14.28	P_{37}	6 § 19.4.12. 4).
P_{12}	6 § 7.14.14	P_{25}	6 § 7.14.29	P_{38}	6 § 19.4.13. 2).
P_{13}	6 § 7.14.16	P_{26}	6 § 7.14.33. 3).	P_{39}	6 § 19.4.13. 3).
P_{14}	6 § 7.14.17	P_{27}	6 § 7.14.34	P_{40}	17 § 20.11 3.4)
P_{15}	6 § 7.14.18	P_{28}	6 § 7.14.35	P_{41}	32 § 8.7.3.

Dr ĐURO KUREPA

VIŠA ALGEBRA

Knjiga prva

IZDAVAČ

Zavod za izdavanje udžbenika
Socijalističke Republike Srbije
Beograd, Obilićev venac 5/I

Urednik

BRANISLAV MATIĆ

Tehnički urednik

MIODRAG VUKOTIĆ

Korektori

SELMA ČOLOVIĆ, VIŠESLAVA NIKOLIĆ
NADEŽDA PLANOJEVIĆ, JELENA DAVIDOVIĆ
MILKA STEFANOVIĆ

Rukopis predat u štampu maja 1970. godine;
štampanje završeno juna 1971. godine.

Obim: $51^3/_4$ štamparskih tabaka
Tiraž: 2.500 primeraka
Format: 17×24 cm

Štampa Beogradski izdavačko-grafički zavod,
Beograd, Bulevar vojvode Mišića 17