UNIVERZITET U BEOGRADU
MATEMATIČKI FAKULTET

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Radoš V. Bakić

PRIMENA ARITMETIČKE FUNKCIJE Ψ U TEORIJI GRUPA

Magistarski rad

Beograd
1998.

Mentor: Prof. Dr. **Žarko Mijajlović**
Matematički fakultet Beograd

Članovi komisije: Prof. Dr. **Slaviša Prešić**
Matematički fakultet Beograd

Prof. Dr. **Aleksandar Lipkovski**
Matematički fakultet Beograd

Dr. **Aleksandar Krapež**
Matematički institut Beograd

06.05.98

1. Teorema klasifikacije kon. grupa
2. S_X - S obzirom da je X besk. sup
da li u neka svojstva ne zavisi od
pojedine aks. teorije skupova, na pr. AC.
3° F-ja Ψ i Ojlerova f-ja

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Zahvaljujem se svom mentoru Prof.Dr. Žarku Mijajloviću na pomoći u izradi ovog rada, kao i svim članovima komisije na njihovom trudu.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

SADRŽAJ

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

1. KRATAK PREGLED RADA I UVOD

Ovaj rad je sačinjen od više manjih rezultata do kojih sam došao za vreme studiranja na poslediplomskim studijama. Na početku je dat opis grupe automorfizama simetrične grupe na beskonačnom skupu, dakle jedan klasičan zadatak o isto takvom objektu. Pokazano je da su svi automorfizmi tačno konjugacije tj. da su svi automirfizmi unutrašnji. To je očekivani rezultat, koji je prirodna dopuna Hölder-ove teoreme, koja tvrdi isto ali za (skoro sve) konačne skupove. Zatim je uvedena standardna konstrukcija semi-direktnog proizvoda, i unakrsnog proizvoda, kao specijalnog slučaja semi-direktnog proizvoda. Tom je prilikom dat jedan originalan primer unakrsnog proizvoda, pa je pokazano da je grupa automorfizama karakteristično proste grupe po svojoj prirodi unakrsni proizvod. I u narednom poglavlju razmatrana je grupa automorfizama, u ovom slučaju, proizvoljne konačne Abel-ove grupe. Tom prilikom izvedena je formula za $|\mathrm{Aut}(G)|$ za proizvoljnu konačnu Abel-ovu grupu. Data je i teorema koja predstavlja uopštenje jedne teoreme Frobeniusa za rešive grupe. Na kraju su razmatrani tzv. grupni brojevi i pri tom je dat novi dokaz opisa nilpotentnih brojeva, koji je prvi dao Pazderski.

1.1. OSNOVNE ČINJENICE I OZNAKE

Pojam grupe uveo je u matematiku Galois, koji je u stvari i osnivač algebre. Može se smatrati, međutim da su prvi pravi algebarski problemi bili zadati još u staroj Grčkoj, pri čemu imamo u vidu probleme trisekcije ugla, kvadrature kruga i

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

duplikacije kocke. Rešavanje klasičnog problema rešivosti algebarske jednačine opšteg oblika od strane Galois-a, značilo je otvaranje nove oblasti matematike, koja će, kako se ispostavilo, naći svoju ulogu u raznim oblastima kako matematike tako i fizike, ali i zaživeti sopstvenim životom u obliku samostalne teorije.

Naveščemo sada neke osnovne teoreme i primere grupa koje ćemo koristiti u radu.

Teorema Lagrange-a: Ako je G konačna grupa i $H < G$, tada |H| deli |G|.

Cauchy-jeva Teorema: Ako je G konačna grupa i p prost broj, pri čemu p deli |G|, tada u G postoji element reda p.

Teorema o kosetima: Ako je G grupa i H<G a G/H skup koseta podgrupe H u G, tada postoji homomorfizam $\theta : G \to S(G/H)$, gde je $S(G/H)$ grupa permutacija skupa G/H. Pri tome je jezgro tog homomorfizma sadržano u H.

Osnovni primer grupe je grupa permutacija na nekom skupu X. To kazuje teorema Caley-ja:

Teorema Caley-a: Svaka grupa G izomorfna je podgrupi grupe permutacija na nekom skupu.

Grupu permutacija na nekom skupu X označićemo, standardno sa, S_X. Za $f \in S_X$ definišimo skup (f), suport od f, kao skup tačaka iz X koje nisu fiksne. Takođe, ako $f(a) \neq a$, kažemo da f pokreće a. Pod ciklusom $(x_1, x_2 \ldots\ldots, x_n)$ pri čemu $x_i \in X$, podrazumevamo permutaciju $\pi \in S_X$ takvu da $\pi(x_i)=x_{i+1}$ i $\pi(x_n)=x_1$ a

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

ako $x \neq x_i$ tada $\pi(x)=x$. Broj n zove se dužina ciklusa. Ciklus dužine 2 zove se transpozicija. Očigledno je red ciklusa dužine n, opet n. Dva ciklusa su disjuktna ako su im disjunktni suporti.

Teorema: Svaka permutacija na nekom skupu X, koja pokreće konačno mnogo elemenata, može se na jedinstven način prikazati kao proizvod disjuktnih ciklusa, do na njihovu permutaciju.

Grupa $H<S_X$ se naziva tranzitivnom ako $(\forall a,b \in X)\ (\exists f \in S_X) f(a)=b$.

Za netrivijalnu particiju $\{X_i | i \in I\}$ skupa X kažemo da čini sistem blokova za H, $H < S_X$ akko $f(X_i) = X_j$ za svako $i \in I$, gde je $f \in S_X$.

Ako je P prsten sa $GL_n(P)$ se označava grupa svih $n \times n$ matrica nad P koje su invertibilne.

Ako je T_n pravilni n-trougao, sa D_n označićemo grupu svih izometrijskih transformacija u ravni koje T_n slikaju na samog sebe (diedarska grupa n-tougla T_n).

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

2. AUTOMORFIZMI GRUPE S_X

Alternirajuća grupa na proizvoljnom skupu X, u oznaci A_X, definiše se kao podgrupa grupe permutacija S_X, generisana svim ciklusima dužine 3 tj. $A_X = \langle (x_1, x_2, x_3) \mid x_i \neq x_j, i \neq j, x_i \in X, 1 \leq i, j \leq 3 \rangle$. Dakle, A_X je uopštenje poznate definicije alternirajuće grupe na konačnom skupu, a sada X može biti i bilo koji beskonačni skup. Vidimo da elementi grupe A_X fiksiraju sve tačke skupa X osim njih konačno mnogo. Na skupu tačaka koje nisu fiksne, elementi iz A_X definišu parnu permutaciju u uobičajenom smislu. Pošto je generatorni skup grupe A_X invarijantan za sve unutrašnje automorfizme grupe S_X, odatle sledi da je i sama grupa A_X invarijantna tj. $A_X \lhd S_X$. Primetimo da uslov normalnosti podgrupe u grupi S_X tj. uslov $H \lhd S_X \Leftrightarrow (\forall g \in S_X) gHg^{-1} = H$ znači u stvari da je grupa H simetrična u odnosu na sve elemente skupa X, odnosno da su sve tačke iz X ravnopravne u grupi H. Vidimo da se taj princip ravnopravnosti poštuje u definiciji grupe A_X jer ni jednom elementu iz X nije dat poseban značaj. Tako na primer možemo definisati grupu S_X^k, za beskonačni kardinal k, $k \leq |X|$, koja je podgrupa grupe S_X. Grupu S_X^k činiće sve permutacije skupa X kod kojih je kardinalnost skupa pokretnih tačaka manja ili jednaka k. Prema ranije istaknutom principu, pošto definicija podgrupe S_X^k ne favorizuje ni jedan simbol iz X, važiće $S_X^k \lhd S_X$. Ono što je zanimljivo je da se sa do sada navedenim primerima normalnih podgrupa u S_X iscrpljuju svi mogući slučajevi tj. A_X i S_X^k $k \leq |X|$, k -

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

beskonačan su sve moguće netrivijalne normalne podgrupe u grupi S_X što je pokazao Baer Š1Ć.

Vratimo se sada na grupu A_X. Njena osnovna osobina je da je grupa A_X prosta. Dokaz ovog tvrđenja je potpuno isti kao za konačan slučaj tj. dokaz prostote za $A_n, |n| \geq 5$ ne zavisi od toga da li je n konačan ili ne. Kako $|A_X| = |X|$, u slučaju da je X beskonačan skup, vidimo da za svaki beskonačni kardinal k postoji prosta grupa kardinalnosti k.

Ciklus dužine 3 zvaćemo tercet. Skup svih mogućih terceta na X, prema definiciji definiše A_X. Međutim, ovaj skup generatora nije optimalan. Umesto njega se može uvesti novi skup generatora koji će biti minimalan. Uzmimo skup terceta $T(a, b) = \{(x, a, b) \mid a \neq b,\ a, b \neq x, x \in X\}$, gde su a i b dva fiksna elementa skupa X.

Jednostavno se pokazuje da je skup $T(a, b)$ takođe skup generatora za A_X koji je takođe i minimalan. Naime grupa A_X je tranzitivna, a svaki element iz skupa X, različit od a i b, pokrenut je u samo jednom tercetu iz T(a,b) pa ako bi proizvoljni tercet $(x, a, b) \in T(a, b)$ bio izostavljen, ne bismo mogli da generišemo ni jednu permutaciju iz A_X u kojoj je x pokrenut. Grupa A_X i njen generatorni skup $T(a, b)$ igraju ključnu ulogu u dokazu sledećeg tvrđenja:

Teorema 2.1. Za svaki skup X takav da je $|X| > 6$ važi $\mathrm{Aut}(S_X) \cong S_X$ gde je izomorfizam dat sa $f(\pi) = \sigma_\pi, \pi \in S_X$, a $\sigma_\pi(\beta) = \pi\beta\pi^{-1}$.

Ovakve grupe koje su izomorfne sa svojom grupom automorfizama preko preslikavanja koje element slika u unutrašnji automorfizam definisan tim elementom, zovu se savršene (ponegde "kompletne"). Jedna lepa osobina koje one imaju je da ako su normalna podgrupa onda su i direktni faktor. Dakle, Teorema 2.1. tvrdi da su skoro sve simetrične grupe savršene. U stvari jedini izuzeci su $|X| = 2$ i $|X| = 6$. U slučaju S_2 biće $\mathrm{Aut}(S_2)$ trivijalna a za S_6 imaćemo da je

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

öö $\mathrm{Inn}(S_6) \lhd \mathrm{Aut}(S_6)$ i $|\mathrm{Aut}(S_6) : \mathrm{Inn}(S_6)| = 2$. Primetimo da se savršena grupa mogla definisati kao grupa u kojoj je centar trivijalan a svaki automorfizam unutrašnji.

Teorema 2.1. je u stvari uopštenje teoreme Hölder-a koja tvrdi isto ali samo za $|X|$ konačan. Ovde ćemo dati dokaz za $|X|$ beskonačan. Od sada pa nadalje, X će biti beskonačan skup.

Sama grupa S_X je vrlo bogata jer sadrži kopije svih mogućih grupa, pa otuda potiču problemi u radu sa njom. Tako je i Hölder-ov dokaz konačne verzije Teoreme 2.1. kombinatornog karaktera sa puno detalja. Glavna lema u dokazu Teoreme 2.1. je sledeće poznato tvrđenje koje daje jedan dovoljan uslov za savršenost čime se eliminiše znatan deo poteškoća u radu sa S_X. Dakle [10]:

Lema 2.1. Grupa automorfizama proste grupe je savršena.

Primetimo da je u konačnom slučaju ispunjen uslov $\mathrm{Aut}(A_n) = S_n$, $n \neq 2, 6$ što je poznato. Odatle dobijamo ideju za dokaz savršenosti grupe S_X: grupa S_X će biti savršena ako je reprezentujemo (verno) kao grupu automorfizama neke proste grupe. Prirodan kandidat za tu prostu grupu je grupa A_X sa obzirom da je prema ranije rečenom, A_X prosta za $|X| \geq 5$ a i relacija $\mathrm{Aut}(A_n) = S_n$ je tačna za $n<\infty$ i $n\neq 2, 6$. Dakle, ideja je da se pokaže da relacija $\mathrm{Aut}(A_X) = S_X$ važi za svaki beskonačni skup X. Na ovaj način smo rad sa čitavom grupom S_X preneli skoro sasvim na rad sa A_X. Kako je $A_X \lhd S_X$ tada je restrikcija σ_π na A_X automorfizam grupe A_X za svako $\pi \in S_X$. Pri tome će restrikcije različitih unutrašnjih automorfizama biti različiti automorfizmi na A_X ako je $C(A_X)$, centralizator A_X u S_X, trivijalan. Pokažimo da je to ispunjeno. Neka je $\beta \in S_X$ tako da $\beta\pi\beta^{-1} = \pi$ za svako $\pi \in A_X$. Neka je $\beta(x_1) = x_2$ gde je $x_1 \neq x_2$, $x_1, x_2 \in X$. Tada je $\beta\pi\beta^{-1}(x_2) \neq \pi(x_2)$ pa je $\beta = i_X$ tj. $C(A_X)$ je trivijalan. Dakle restrikcije unutrašnjih automorfizama grupe S_X na A_X definišu grupu automorfizama u A_X izomorfnu sa S_X. Treba još pokazati da drugih automorfizama nema tj. $f \in \mathrm{Aut}(A_X) \Rightarrow f = \sigma_\pi$, $\pi \in S_X$. Ideja da to

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

pokažemo je da dokažemo da se dejstvo f na T(a,b), dakle na generatornom skupu za A_X, poklapa sa dejstvom nekog σ_π, tj $f(t)=\sigma_\pi(t)$ za sve $t\in T(a,b)$. Primetimo u vezi sa tim da važi $\pi T(a,b)\pi^{-1}=T(\pi(a),\pi(b))$. Važi i obratno, ako je za neki $f\in Aut(A_X)$ ispunjeno $f(T(a,b))=T(c,d)$, tada je f restrikcija nekog σ_π na A_X, $\pi\in S_X$. Permutacija π se tada može definisati na sledeći način: $\pi(a)=c$ i $\pi(b)=d$. Ako je $x\neq a,b$ tada postoji jedinstven $t\in T(a,b)$ takav da $t=(x,a,b)$ i $f(t)=(x',c,d)\in T(c,d)$. Definišimo $\pi(x)=x'$. Tada će se, kao što je to rečeno, f i σ_π poklapati na T(a,b) pa samim tim i na celoj A_X to jest biće $f=\sigma_\pi$. Dakle došli smo do zadatka da pokažemo da je $f(T(a,b))=T(c,d)$, za neke $c,d\in X$. Do ovoga zaključka doći ćemo postepeno. Za početak primetimo sledeće: ako je $t\in T(a,b)$ tada je red od t, u oznaci r(t), jednak 3, pa je i $r(f(t))=3$. Odatle sledi na osnovu faktorizacije permutacije ciklusima da se f(t) može prikazati kao proizvod terceta tj. $f(t)=t_1t_2.....t_n$, t_i su terceti. Takođe, ako $t, t'\in T(a,b)$ i $t=(a,b,e)$, $t'=(a,b,f)$ tada je $t\cdot t'=(a,f)(e,b)$ za $t\neq t'$. Dakle za $t\neq t'$, imamo da je $r(t\cdot t')=2$ pa je i $r(f(t\cdot t'))=2$. Uslov $r(\pi)=2$, za $\pi\in S_X$, znači da se π faktoriše isključivo transpozicijama, ili što je ekvivalentno, za svaka dva $a,b\in X$ važi $\pi(a)=b\Leftrightarrow\pi(b)=a$. U daljem radu to čemo koristiti dosta često. Primetimo da je za $t\in T(a,b)$, f(t) proizvod konačno mnogo terceta (jer pripada A_X), pa pokreće samo konačno mnogo simbola iz X.

Pokažimo sada sledeću jednostavnu lemu:

Lema 2.2. Neka su $t,t'\in T(a,b)$, $t\neq t'$, i $f\in Aut(A_X)$. Tada je $|sup(f(t))|=|sup(f(t'))|$ i $sup(f(t))\neq sup(f(t'))$.

Dokaz: neka je $f(t)=t_1.....t_m$ i $f(t')=t_1'.....t_n'$. Neka je još $a\in X\cap sup(f(t))$ i $a\notin sup(f(t'))$. recimo da je $t_1=(a,b,c)$. Tada neki od simbola $b,c\in X$ pada u $sup(f(t'))$. Neposredno se proverava i koristeći uslov $r(f(t\cdot t'))=2$, da neki t_i' mora tada imati oblik $t_i'=(d_a,b,c)$ gde $d_a\notin sup(f(t))$. Na ovaj način uspostavljena je bijekcija između skupova $sup(f(t))\setminus sup(f(t'))$ i $sup(f(t'))\setminus sup(f(t))$ gde se svakom a iz prvog skupa dodeljuje d_a iz drugog skupa. Odatle sledi $|sup(f(t))|=|sup(f(t'))|$. Pretpostavimo da

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

je sup(f(t)) =sup(f(t')). Kako je A_X tranzitivna grupa bez blokova, i kako je f(t)(sup(f(t)))=f(t')(sup(f(t')))=sup(f(t)), mora postojati neka $\pi \in f(T(a,b))$ takva da je $\pi=k_1 \ldots\ldots k_p$ (kanonski) i gde je $k_1=(e,h,g)$ gde su $e,h,g \in X$ takvi da $h \notin \sup(f(t))$ a $e \in \sup(f(t))$. Po pretpostavkama imamo da je $t_i=(e,x,n)$ za neko i, i $t_j'=(e,x',n')$ za neko j. Koristeći uslove $r(\pi f(t))=r(\pi f(t'))=2$, kao i to da f(t) i f(t') fiksiraju h, neposredno se proverava da mora biti x=x' i n=n'. Tada međutim dobijamo da $3|r(f(t\cdot t'))$ jer je $t_i \cdot t_j=t_i^2$ i $t_i \cdot t_j$ je kanonski faktor u $f(t\cdot t')$ reda 3. Ovim je dokaz kompletiran.

Iz dokaza gornje leme vidi se sledeća činjenica: ako $a \in \sup(f(t))$ i $a \notin \sup(f(t'))$, tada je $t_i=(a,b,c)$ i $t_j'=(d,b,c)$ za neke i, j gde $d \notin \sup(f(t))$. Lako se vidi da važi i obrnuto (koristeći uslov $r(f(t\cdot t'))=2$): ako je $t_i(a,b,c)$ i $t_j'=(d,b,c)$ tada su a i d fiksne tačke u f(t') i f(t) repektivno.

Razmotrimo na trenutak ponovo permutaciju $f(t)=t_1 \ldots\ldots t_m$. Kako je skup T(a,b) beskonačan i f izomorfizam, skup f(T(a,b)) je takođe beskonačan.

Prema Lemi 2.1. svaka $\pi \in (T(a,b))$ fiksira neki simbol iz sup(f(t)). Kako je sup(f(t)) konačan skup mora postojati neki $e \in \sup(f(t))$ takav da je fiksiran u beskonačno mnogo permutacija iz f(T(a,b)). Neka je recimo $t_1=(e,x,c)$. Prema prethodnim napomenama ako je $e \notin \sup(\pi)$, $\pi \in f(T(a,b))$, tada π ima faktor oblika (d,x,c), $d \notin \sup(f(t))$, i takvih π ima beskonačno mnogo. Takođe, za dve takve π i π_1, i odgovarajuće faktore (d,x,c) i (d_1,x,c) mora biti $d \neq d_1$ i $d \notin \sup(\pi_1)$, $d_1 \notin \sup(\pi)$. Pokazaćemo sada da faktor oblika (d,x,c) mora postojati u svakoj $\pi \in f(T(a,b))$.
Dakle:

Lema 2.3. Ako je e gore uvedeni element, tada svaka $\pi \in f(T(a,b))$ ima faktor (kanonski) oblika (d,x,c).

Dokaz: Neka je $\pi \in f(T(a,b))$. Prema ranije rečenom postoji beskonačno mnogo β, $\beta \in f(T(a,b))$, koje sadrže faktor oblika (d_β,x,c). Kako π pokreće samo konačno mnogo simbola iz X, imamo da je za neko od prethodnih β, d_β fiksna tačka u π.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Kako je (d_β,x,c) faktor u β, prema ranije dokazanom π ima faktor oblika (d,x,c), čime je Lema 2.3. dokazana.

Dakle svaka $\pi\in f(T(a,b))$ sadrži kanonski faktor oblika (d_π,x,c) za fiksne $x,c\in X$. Vidimo da $f(T(a,b))$ liči, za sada, na $T(x,c)$, a dokazaćemo da su jednaki. Podsetimo se da za $\pi,\beta\in f(T(a,b))$ važi $d_\pi\notin sup(\beta)$, dakle π je jedina permutacija iz $f(T(a,b))$ koja pokreće d_π. Sledeća lema odnosi se na grupe generalno, i s obzirom da je elementarna, verovatno je negde i formulisana.

Lema 2.4. Neka je G grupa sa skupom generatora K, $K\subseteq G$ i $H<G$, pri čemu je L skup generatora za H ($L\subseteq H$). Ako za sve $k\in K$ i sve $l\in L$ važi $\sigma_k(l)\in H$ tada (i samo tada) je $H\lhd G$.

Dokaz je očigledan, pa ga izostavljamo.

Da bismo pokazali da je $f(T(a,b))=T(x,c)$ treba da pokažemo da se svaka $\pi\in f(T(a,b))$ faktoriše tačno jednim tercetom tj $\pi=(d_\pi,x,c)$. To ćemo pokazati na osnovu osnovne osobine grupe A_X - da je prosta.

Lema 2.5. Važi $f(T(a,b))=T(x,c)$.

Dokaz: Neka je $H=\langle (d_\pi,xc)|\ \pi\in f(T(a,b))\rangle$. Ako bi važilo $f(T(a,b))\neq T(x,c)$ tada bi H bila prava podgrupa u A_X. Međutim važi i $H\lhd A_X$. Zaista, kako je T(a,b) generatorni skup za A_X, i f izomorfizam tada je i $f(T(a,b))$ generatorni skup za A_X. Takođe važi za $\alpha,\beta\in f(T(a,b))$: $\sigma_\alpha((d_\beta,x,c))=\alpha(d_\beta,x,c)\alpha^{-1}=(d_\alpha,x,c)(d_\beta,x,c)$ $(d_\alpha,x,c)^{-1}\in H$. Prema Lemi 2.5. bila bi H normalna u A_X, što je kontradikcija, čime je dokaz kompletiran.

Sada nam ostaje da ponovimo, već ranije skiciran dokaz Teoreme 1.2. za X beskonačan.

(Dokaz Teoreme 2.1.) Kako je za $f\in Aut(A_X)$ ispunjeno $f(T(a,b))=T(x,c)$ to se dejstvo f na T(a,b) poklapa sa dejstvom unutrašnjeg (za S_X) automorfizma σ_π, gde

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

je $\pi(a)=x$, $\pi(b)=c$ i ako $e \notin a,b$ i $(e,a,b) \in T(a,b)$, tada $\pi(e)=k$ gde je k određen sa $f(e,a,b)=(k,x,c)$. Dakle, S_X je grupa automorfizama od A_X, pa je po Lemi 2.2. savršena tj. nema drugih automorfizama osim unutrašnjih.

Razmotrimo sada jedan elementaran problem koji je srodan prethodnom, a to je da se opišu automorfizmi semi-grupe svih funkcija na nekom skupu X. Pokazaćemo da je za tu semigrupu, označimo je sa X^X, grupa automorfizama sastavljena od konjugacija permutacijama nad X tj. $f \in Aut(X^X) \Leftrightarrow f(g)=hgh^{-1}$ gde je $h \in S_X$, i h zavisi samo od f.

Lema 2.6. Ako je $h \in X^X$, h je konstanta funkcija akko $h \circ g=h$ za sve $g \in X^X$.

Dokaz: Smer ($\Rightarrow$) je očigledan, pa dokažimo smer ($\Leftarrow$). Ako h nije konstanta tada postoje $a,b \in X$, $a \neq b$, i $c,d \in X$ takvi da $h(c)=a$ i $h(d)=b$. Ako je g proizvoljna funkcija na X za koju je $g(d)=c$, neće važiti $h \circ g=h$, što je u suprotnosti sa pretpostavkom.

Ako je h konstantna funkcija na X, i $h(b)=a$ za sve $b \in X$, tada označimo h sa h_a.

Lema 2.7. Ako je $h=h_a$ konstantna funkcija tada je $f(h_a)$ takođe konstantna funkcija.

Dokaz: Kako je $h_a \circ f(g)=f(h_a)$ za sve $g \in X^X$, tada je $f(h_a) \circ f(g)=f(h_a)$. Pošto je f automorfizam važiće $f(h_a) \circ p=f(h_a)$ za sve $p \in X^X$, pa je po Lemi 2.6., funkcija $f(h_a)$ konstanta.

Ako je $f \in Aut(X^X)$, Lema 2.7. nam govori da f permutacije konstantne funkcije. Za dato $f \in Aut(X^X)$ možemo definisati $\bar{f} \in S_X$. uslovom $f(h_a)=h_{\bar{f}(a)}$, odakle je $h_{(f(g) \circ \bar{f})(a)}=h_{\bar{f}(g(a))}$ što je ekvivalento $(f(g) \circ \bar{f})(a)=(\bar{f} \circ g)(a)$. Kako prethodna jednakost važi za sve $a \in X$, ona povlači jednakost funkcija, pa sledi $f(g) \circ \bar{f} = \bar{f} \circ g$ tj. $f(g)=\bar{f} \circ g \circ \bar{f}^{-1}$. Takođe iz $\bar{f} \circ g \circ \bar{f}^{-1}=h_a$ tj. $\bar{f} \circ h_a=h_a \circ \bar{f}$ sledi $h_{\bar{f}(a)}=h_a$ tj. $\bar{f}(a)=a$ za sve $a \in X$, pa je $\bar{f}$ identično preslikavanje na X. To pokazuje

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

da je preslikavanje tj. automorfizam, iz $Aut(X^X)$ u S_X, koji $f \in Aut(X^X)$ slika u $\bar{f}$, takođe i 1-1 jer mu je jezgro trivijalno. Ako je $g \in S_X$ tada $f_g \in Aut(X^X)$, gde $f_g(h)=gh^{-1}g$, i još $\bar{f}_g=g$, dakle gore pomenuti homomorfizam je "na". iz svega dokazanog vidimo da je $Aut(X^X) \cong S_X$ i da su svi elementi $Aut(X^X)$ konjugacije permutacijama.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

3. REŠIVE I NILPOTENTNE GRUPE

U ovom odeljku daćemo osnovne osobine dve važne klase grupa, a to su rešive i nilpotentne grupe, koje su uopštenje klase Abel-ovih grupa, dok rešivost grupe takođe uopštava pojam nilpotentnosti.

3.1. NILPOTENTNE GRUPE

Ako je G grupa i $x,y \in G$ tada se komutator elemenata x i y, u oznaci [x,y], definiše kao $[x,y]=xyx^{-1}y^{-1}$. Ako su A i B podgrupe grupe G, tada se komutator grupe A i B u oznaci [A,B], definiše se $[A,B]=\langle [a,b] a \in A, b \in B \rangle$. Definisaćemo sada niži centralni red grupe G, na sledeći način: neka je po definiciji $\gamma_o G=G$ i $\gamma_{n+1}G=[G_n,G]$. Gornjom definicijom uveli smo jedan niz podgrupa grupe G, označen sa $\gamma_n G \lhd \gamma_m G$ za $n \geq m$. Dakle, γ_n od G je jedan nerastući niz, podgrupa u G. Element $\gamma_1 G=[G,G]$ zove se komutator grupe G. Primetimo da važi i više od relacije $\gamma_n G \lhd G$. Naime, lako se vidi da je $\gamma_n G$ invarijantna u G ne samo u odnosu na sve unutrašnje automorfizme, već i u odnosu na sve endomorfizme grupe tj. $\gamma_n G$ je potpuno invarijantna u G. Niz $\gamma_n G$ naziva se niži centralni niz grupe G. Za niži centralni niz neke grupe G, moguće su generalno tri mogućnosti:

a) Niz $\gamma_n G$ je beskonačan niz različitih podgrupa. Takav slučaj imamo na primer ako se za G uzme proizvoljna slobodna grupa. Tada će $\gamma_n G$ biti strogo opadajući niz podgrupa, koji se ipak u perspektivi završava u jediničnoj podgrupi, tj. imaćemo $\bigcap_{n=1}^{\infty} \gamma_n G = \{1\}$, kao što je to pokazao Magnus.

b) Niz $\gamma_n G$ se stabilizuje počevši od nekog n tj. za neko n i svako $m \geq n$, važi $\gamma_n G = \gamma_m G$. Taj slučaj imamo na primer za sve S_n $(n>4)$ gde je $\gamma_1 S_n = A_n = \gamma_m S_n$, za sve $m \geq 1$.

c) za neko n važi $\gamma_n G = \{1\}$.

Ako je za grupu G ispunjen uslov c) tada se kaže da je grupa G nilpotentna. Najmanje n za koje je ispunjen uslov $\gamma_n G = \{1\}$ zove se klasa nilpotentnosti grupe G.

Uopšteni komutator elemenata $x_1, \ldots\ldots x_n \in G$ u oznaci $[x_1, \ldots\ldots x_n]$ definiše se sa $[x_1, \ldots\ldots x_n] = [[x_1, \ldots\ldots x_{n-1}], x_n]$. Na osnovu gornje induktivne definicije uopštenog komutatora može se uslov $\gamma_n G = \{1\}$ zapisati u ekvivalentnom obliku: $(\forall x_1, \ldots\ldots, x_{n+1} \in G)$ $[x_1, \ldots\ldots, x_{n+1}] = 1$. Primetimo da prethodni uslov ima formu algebarskog zakona u strogom smislu pojma "zakon". Odatle vidimo da ako je G nilpotentna grupa klase n, tada su podgrupe i homomorfne slike grupe G, takođe nilpotentne, klase ne veće od n. Takođe je direktan proizvod nilpotentnih grupa klase ne veće od n, ista takva grupa. Sve je ovo, dakle, posledica činjenice da nilpotentne grupe klase ne veće od nekog n, čine varijetet. Sama klasa nilpotentnih grupa međutim ne čini varijet. Prema teoremi Birkhoff-a, klasa algebri čini varijet akko je zatvorena za podalgebre, homomorfne slike i direktne proizvode. Klasa nilpotentnih grupa je zatvorena, kao što smo videli, za prve dve konstrukcije ali nije za direktne proizvode. Na primer grupa D_{2^n} je, kako se pokazuje, nilpotentna grupa klase n, za $n \geq 2$. Ako uzmemo direktan proizvod $\prod_{n=2}^{\infty} D_{2^n}$, on neće biti nilpotentan. Osim pojma nižeg centralnog reda, postoji i pojam višeg centralnog reda, pomoću kojeg se takođe može definisati pojam nilpotentnosti.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Ako sa Z(G) obeležimo centar grupe G, viši centralni niz se definiše sa $Z_o(G)=\{1\}$, a $Z_{n+1}(G)$ uslovom $Z(G/Z_n(G))=Z_{n+1}(G)/Z_n(G)$. Niz $Z_n(G)$ je neopadajući niz normalnih podgrupa grupe G. Grupa G će biti nilpotentna klase n akko $Z_n(G)=\{1\}$ i $Z_{n-1}(G)\neq\{1\}$.

Osnovni primer nilpotentne grupe je konačna p-grupa (p prost broj). Ispostavlja se takođe da se konačne nilpotentne grupe skoro ne razlikuju od konačnih p-grupa, jer je svaka konačna nilpotentna grupa direktan proizvod p-grupa. Još jedan interesantan primer nilpotentne grupe povezan je sa konceptom tzv. Frattini-jeve podgrupe, koju ćemo sad definisati.

Ako je G (proizvoljna) grupa tada za $x\in G$ kažemo da je negenerator ako za svaki $A\subseteq G$, takav da $\langle\{x\}\cup A\rangle = G$, važi $\langle A\rangle = G$. Skup svih negeneratora grupe G čini pogrupu koja se zove Frattini-jeva podgrupa grupe G. Frattini-jeva podgrupa može se definisati i kao presek svih maksimalnih pravih podgrupa, ako one postoje. Ako nema maksimalnih podgrupa onda je Frattini-jeva podgrupa jednaka G. Pojam negeneratora može se na istovetan način definisati ne samo za grupe, već i za proizvoljne algebre na nekom jeziku, pa se samim tim, može definisati i Frattini-jeva podalgebra, opet potpuno analogno. I u ovom opštem slučaju, ostaje da važi i definicija preko maksimalnih podalgebri. Frattini-jevu podgrupu grupe G obeležićemo sa $\Phi(G)$. Ono što je zanimljivo je , da ako je G konačna grupa, tada je $\Phi(G)$ nilpotentna. U opštem slučaju, $\Phi(G)$ je karakteristična podgrupa grupe G.

Za konačne grupe, može se dati više interesantnih karakterizacija nilpotentnosti. Naime, za konačnu grupu G sledeći uslovi su ekvivalentni:

a) G je nilpotentna
b) svaka prava podgrupa grupe G je subnormalna tj. različita je od svog normalizatora
c) G je konačan direktan proizvod p-grupa (za ne obavezno iste proste brojeve p)
d) svaka dva elementa grupe G, uzajamno prostih redova, međusobno komutiraju.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

e) $G/Z(G)$ je nilpotentna

f) $\gamma_1 G = [G,G] < \Phi(G)$

3.2. REŠIVE GRUPE

Rešive grupe su uopštenja pojma nilpotentnosti mada su, istorijski gledano, definisane pre nilpotentih grupa. Rešive grupe su se pojavile praktično sa samim konceptom grupe u klasičnim radovima Galois-a. U njima je Galois pokazao da je polinomska jednačina rešiva u radikalima tačno tada kada je Galois-ova grupa tog polinoma rešiva. Daćemo sada definiciju rešive grupe.

Definicija: Ako je G grupa, pod n-tim izvodom podrazumeva se podgrupa grupe G definisana induktivno: $G^o = G, G^n = \left[G^{n-1}, G^{n-1}\right]$ gde G^n-označava n-ti izvod. Za grupu G kažemo da je rešiva ukoliko je $G^n = \{1\}$ za neko $n \in \mathbb{N}$.

Slično kao kod nilpotentnih grupa, može se definisati klasa (ili stepen) rešivosti kao najmanje n za koje je uslov $G^n = \{1\}$ ispunjen. Takođe za, fiksno n, uslov $G^n = \{1\}$ se može ekvivalentno izraziti u formi algebarskog zakona na sledeći način: ako definišemo

$$t_o(x_1, x_2, \ldots\ldots, x_{2^n}) = \left[t_{n-1}(x_1, \ldots\ldots, x_{2^{n-1}}), t_{n-1}(x_{2^{n-1}+1}, x_{2^{n-1}+2}, \ldots\ldots, x_{2^n})\right]$$

Uslov $G^n = \{1\}$ je tada ekvivalentan uslovu $t_n(x_1, \ldots\ldots\ldots x_{2^n}) = 1$.

Vidimo da rešive grupe i klase rešivosti ne veće od nekog n, čine varijetet. kao kod nilpotentnih grupa, cela klasa rešivih grupa ne čini varijetet, jer neće biti zatvorena za beskonačne direktne proizvode. Zatvorenost za osnovne konstrukcije omogućava (u konačnom slučaju) izvođenje dokaza indukcijom. Pomenimo ovde i čuvenu teoremu Feit-a i Thompson-a [2] koja kaže da su sve grupe neparnog reda rešive. Takođe, poznata teorema Burnside-a [3] tvrdi da su sve konačne grupe G, čiji je red oblika $|G| = p^n q^m$, ($p \neq q$, p i q su prosti) rešiva. Rešivost se može

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

okarakterisati i pomoću podgrupa. To je rezultat P.Hall-a [4]: grupa G reda $n = p_1^{a_1} \ldots\ldots p_m^{a_m}$ (kanonska faktorizacija) je rešiva akko za sve i, $1 \le i \le m$, postoji podgrupa indeksa $p_i^{a_i}$. Sa ovom teoremom, u njenoj potpunoj verziji, srešćemo se i u sledećem poglavlju. Još jedan važan potreban i dovoljan uslov da grupa G bude rešiva, a koji ne važi za nilpotentnost, je da postoji $H \lhd G$, takva da su H i G/H rešive.

Kao što smo rekli, rešive grupe su se pojavile pri rešavanju opšte algebarske jednačine n-tog stepena. Galois-ova grupa polinoma p(x), n-tog stepena, izomorfna je podgrupi S_n. Kako su sve podgrupe grupe S_n, $n \le 4$, rešive to su i sve jednačine stepena ne većeg od 4 rešive u radikalima. Ako je $n \ge 5$, tada je $S_n^1 = S_n^k = A_n$, za sve $k \ge 1$, pa vidimo da grupe S_n nisu rešive ($n \ge 5$). Prema tome svaka jednačina p(x)=0, gde je p(x) polinom čija je Galois-ova grupa jednaka S_n ne može biti rešiva u radikalima.

Pomenimo ovde još dve poznate teoreme koje predstavljaju vezu između nilpotentnosti i rešivosti. Prva teorema je rezultat Schmidt-a [7] i ona tvrdi da je konačna grupa rešiva ukoliko su joj sve prave podgrupe nilpotentne. Druga teorema je rezultat Wielandt-a [4]: konačna grupa G je rešiva akko je $G = B_1 B_2 \ldots\ldots B_n$, $B_n < G$, $B_i B_j = B_j B_i$ i B_i su nilpotentne.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

4. TEOREME SILOW-A

Teoreme Silow-a su, kako to autori ističu, ugaoni kamen teorije konačnih grupa. Prvi put su dokazane 1872 od strane norveškog matematičara V. Silow-a. Od tada su uopštavane i razrađivane od strane više matematičara: P.Hall-a, Čunihin-a, Wielandt-a itd. Posebno su interesantne teoreme P.Hall-a i teorema Schur-Zassenaus-a, koje iako nisu direktna uopštenja, teorema Silow-a, predstavljaju tvrđenja istog tipa. Naš cilj je da pojačamo njihovu sličnost dodavanjem nove tačke na Schur-Zassenhaus teoremu. U tom cilju, izložićemo pomenute tri teoreme na nama najzgodniji način.

Neka je G konačna grupa, $|G| = ab$ gde $(a,b)=1$. Tada:

Teorema Silow-a: Ako je $a = p^n$, p je prost broj, onda postoji podgrupa reda a, svake dve podgrupe reda a su konjugovane u G_i svaka podgrupa H takva da $|H|\,|\,a$ je sadržana u nekoj podgrupi reda a.

Podgrupe grupe G takve su da su reda $a = p^n$, gde $|G| = a \cdot b, (a,b) = 1$, zovu se Silow-ljeve podgrupe grupe G.

Teorema P.Hall [6]: Ako je G rešiva grupa, tada postoji podgrupa grupe G reda a, svake dve podgrupe reda a su konjugovane, i svaka podgrupa H takva da $|H|\,|\,a$ je sadržana u nekoj podgrupi reda a.

Podgrupa grupe G takva da su joj red i indeks uzajamno prosti zove se Hall-ova podgrupa grupe G.

Teorema Schur-Zassenhausa [6]: Ako u G postoji normalna podgrupa reda b, tada postoji podgrupa reda a i svake dve podgrupe reda a su konjugovane.

Naveli smo ove tri teoreme na način koji podcrtava njihovu srodnost. Dodajmo da Silow-ljeva teorema tvrdi i više: pod uvedenim pretpostavkama, broj podgrupa reda a je delilac od $|G|$ i jednak je 1 (mod p). Teorema P. Hall-a je u stvari, kako smo to ranije naveli, karakterizacija rešivosti konačne grupe, što je rezultat koji su gotovo istovremeno dobili P. Hall i Čunihin. Dokaz teoreme Schur-Zassenhaus-a je najteži od sva tri, i on čak koristi teoremu Feit-a Thompson-a o rešivosti grupa neparnog reda.

Ako pogledamo iskaze sve tri teoreme uočavamo njihovu sličnost tj. da u svim slučajevima imamo iste zaključke pod različitim predpostavkama. Jedino u slučaju Schur-Zassenhazus teoreme ne postoji tačka koja bi tvrdila da je svaka podgrupa čiji red deli a, sadržana u podgrupi reda a. Ovde ćemo dokazati da je to tačno. Dakle:

Teorema: Pod pretpostavkom Schur-Zassenhaus teoreme, svaka podgrupa grupe G, čiji red deli a, sadržana je u nekoj podgrupi reda a.

Dokaz: Neka je $H<G$ i $|H|\,|a$. Prema teoremi Schur-Zassenhaus-a postoji $H_1, H_1<G$ i $|H_1|=a$. Po pretpostavci, postoji $H_2, H_2 \lhd G$ i $|H_2|=b$. Uočimo sada proizvod $H\cdot H_2$. Kako je $H_2 \lhd G$, biće $H\cdot H_2 < G$ i pošto je $H_2 \cap H=\{1\}$, jer su H i H_2 uzajamno prostih redova, biće $|H\cdot H_2|=|H|\cdot b$. Uočimo sada proizvod $H_1HH_2 = H_1(HH_2)$. Ovaj skup

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

biće jednak celoj grupi G jer je već $H_1H_2 = G$. Prema formuli za red proizvoda imamo $|G| = |H_1(HH_2)| = |H_1| \cdot |HH_2| / |H_1 \cap HH_2| =$ $= a|H| \cdot b / |H_1 \cap HH_2| = |G| \cdot |H| / |H_1 \cap HH_2|$ odatle sledi $|H_1 \cap HH_2| = |H|$. Kako je $H_2 \lhd G$ to je i $H_2 \lhd HH_2$. Sada je u grupi HH_2 podgrupa H_2, normalna grupa čiji su red i indeks uzajamno prosti, a H i $HH_2 \cap H_1$ su dve podgrupe čiji je red jednak indeksu podgrupe H_2.

Prema Schur-Zassenhaus-ovoj teoremi, H i $HH_2 \cap H_1$ su konjugovane u HH_2 tj. $H = \sigma_x(HH_2 \cap H_1)$ za neko $x \in HH_2$. Ali tada pošto $HH_2 \cap H_1 < H_1$ važi $\sigma_x(HH_2 \cap H_1) = H < \sigma_x(H_1)$ i $\sigma_x(H_1)$ je grupa koju smo tražili.

Ostaje pitanje mogu li se različite pretpostavke ove tri teoreme izraziti na jedinstven način tj. da li su ove tri teoreme različiti aspekti jedne teoreme.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

5. SEMIDIREKTAN PROIZVOD GRUPA

Konstrukcija semidirektnog (ili poludirektnog) proizvoda predstavlja jedan važan način konstrukcije novih, od već poznatih grupa i predstavlja uopštenje direktnog proizvoda dve grupe.

Ako su A i B grupe i $\theta: B \to Aut(A)$ homomorfizam tada se na skupu $A \times B$ može definisati binarna operacija $\circ$, na sledeći način: $(a,b) \circ (a_1, b_1) = (a\theta_b(a_1), bb_1)$. U odnosu na ovu operaciju, skup $A \times B$ čini grupu, koju ćemo zvati semidirektan proizvod grupa A i B i obeležavati $A \times_\theta B$.

Vidimo da se grupa $A \times B$ može shvatiti kao poludirektan proizvod $A \times_\theta B$, gde $\theta: B \to Aut(A)$ i $\theta(b) = i_A$.

Takođe se može dati alternativna definicija semidirektnog proizvoda na sledeći način: grupa G je semidirektan proizvod svojih podgrupa A i B akko $G = AB, A \lhd G$ i $A \cap B = \{1\}$. Vidimo, recimo, u Schur-Zassenhaus-ovoj teoremi da je G semidirektan proizvod jedne podgrupe reda a i normalne podgrupe reda b. Semidirektan proizvod nije do na izomorfizam određen svojim faktorima A i B kao što je to slučaj sa direktnim proizvodom. Jedan interesantan primer ove konstrukcije može se dobiti ako se za proizvoljnu grupu A, za faktor B uzme baš Aut(A) i $\theta: Aut(A) \to Aut(A)$ se definiše kao identično preslikavanje. Tada se grupa

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

$A \times_\theta B$ tj $A \times_\theta Aut(A)$ naziva holomorf grupe A, u oznaci Hol A. S obzirom da se grupa A može indentifikovati sa grupom $\{(a, i_A) | a \in A\}$ možemo smatrati da je $A < Hol A$. Značaj grupe Hol A je u sledećem:

Svaki automorfizam grupe A može se dobiti kao restrikcija nekog unutrašnjeg automorfizma σ_b grupe Hol A.

Jedan specijalan slučaj semidirektnog proizvoda je tzv. unakrsni (ili spleteni) proizvod. Neka su A i B proizvoljne grupe i $\theta : B \to S_n$, homomorfizam. Tada postoji homomorfizam $\theta : B \to Aut(\prod_{i=1}^{n} A)$ koji je definisan na sledeći način:

$$\theta[b](a_1, \ldots\ldots a_n) = (a_{\theta^{-1}[b](1)}, \ldots\ldots, a_{\theta^{-1}[b](n)}) \text{ za } b \in B, \; a_1 \in A$$

Dakle, θ [b] permutuje koordinate u skladu sa permutacijom θ [b]. Grupa $\prod_{i=1}^{n} A \times_\theta B$ zove se unakrsni proizvod grupa A i B. A sada ćemo dati jedan originalan primer vezan za karakteristično proste grupe. Za grupu G kažemo da je karakteristično prosta ako ne postoji netrivijalna podgrupa invarijantna za sve automorfizme grupe G. Primer karakteristično proste grupe je $C_p \times \ldots\ldots \times C_p = (C_p)^n$ za p prost broj. Pokazuje se da su grupe oblika $(C_p)^n$ jedine konačne, Abel-ove karakteristične proste grupe. Od sada ćemo pod "karakteristično prosta grupa", podrazumevati samo takve grupe koje nisu Abel-ove. Karakteristično proste konačne grupe se lako opisuju do na klasu prostih grupa. Važi naime, da je konačna grupa karakteristično prosta akko je direktni stepen neke proste grupe. Trenutno se smatra da su poznate sve konačne proste grupe pa to znači da su poznate i sve konačne karakteristično proste grupe. Neka je konačna grupa G karakteristično prosta i unutrašnji direktan proizvod svojih prostih podgrupa $A_1, \ldots\ldots, A_n$ gde $A_i \cong A_j$. Dakle $G = \prod_{i=1}^{n} A_i$. Važi sledeći poznati stav:

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Lema 5.1. Neka je G prethodno uvedena grupa. Tada:

$H \lhd G \Rightarrow H = A_{\pi(1)} \times A_{\pi(2)} \times \ldots\ldots \times A_{\pi(k)}$ za neku permutaciju π skupa $\{1,2,\ldots\ldots,n\}$.

Kao neposrednu posledicu Leme 5.1. imamo:

Lema 5.2. Ako je G grupa kao u Lemi 5.1. i $G = \prod_{i=1}^{k} B_i$, unutrašnji direktan proizvod podgrupa B_i, gde su sve B_i proste, $1 \le i \le k$, tada je za svako i, $B_i = A_j$ (strogo jednako, a ne samo izomorfno) za neko j.

Dokaz: Kako je $B_i \lhd G$, po Lemi 4.2., $B_i = A_{\pi(1)} \times \ldots\ldots \times A_{\pi(k)}$, za $\pi \in S_n$, ali pošto je B_i prosta može postojati samo jedan faktor, tj. k=1 i $B_i = A_j$.

Naš cilj je da povežemo konstrukciju unakrsnog proizvoda sa grupom automorfizama karakteristično proste grupe, tj. da pokažemo da ako je G karakteristično prosta, Aut(G) je po svojoj prirodi unakrsni proizvod.

Neka je G karakteristično prosta konačna grupa i $G = \prod_{i=1}^{n} A_i$ njeno, kako iz dosadašnjeg razmatranja sledi, jedinstveno razlaganje u unutrašnji direktan proizvod svojih prostih izomorfnih podgrupa. Tada će s obzirom na svojstva direktnog proizvoda, osobine grupe G biti u potpunosti određene osobinama grupe $A_1 (\cong A_i, 1 \le i \le n)$, pa je prirodno očekivati da bi se i grupa Aut(G) mogla opisati kao funkcija grupe $Aut(A_i)$. Dokazaćemo da važi sledeće:

Teorema 5.1. Neka je G grupa definisana kao u prethodnom tekstu. Tada je Aut(G) jednak unakrsnom proizvodu grupe $Aut(A_1) \cong Aut(A_k)$ sa grupom S_n.

Dokaz: Primetimo da važi $A_1 \neq A_i \Rightarrow \prod_{i=1}^{n} A_i \cong A_1^n$, pa možemo umesto grupe G razmatrati grupu A_1^n i njenu grupu automorfizama. Definisaćemo unakrsni proizvod grupa $Aut(A_1)$ i S_n, u odnosu na $i: S_n \to S_n$, gde je i identično preslikavanje. Dakle $A = (Aut(A_1))^n \times_i S_n$ i pokažimo da je $A \cong Aut(A_1^n)$.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Definišimo sada $\Psi: A \to \mathrm{Aut}(A_1^n)$ ovako: za $b = ((b_1, \ldots\ldots, b_n), \pi)$ neka je $\Psi(b) = \Psi_b(a_1, \ldots\ldots, a_n) = (b_1(a_{\pi^{-1}(1)}), \ldots\ldots, b_n(a_{\pi^{-1}(n)}))$. Pokažimo da je zaista $\Psi_b \in \mathrm{Aut}(A_1^n)$. Imamo $\Psi_b((a_1, \ldots, a_n)(e_1, \ldots\ldots, e_n)) = \Psi_b(a_1e_1, \ldots\ldots, a_ne_n) =$

$= (b_1(a_{\pi^{-1}(1)}e_{\pi^{-1}(1)}), \ldots\ldots, b_n(a_{\pi^{-1}(n)}e_{\pi^{-1}(n)}) = (b_1(a_{\pi^{-1}(1)})b_1(e_{\pi^{-1}(1)}), \ldots\ldots$

$\ldots\ldots, b_n(a_{\pi^{-1}(n)})b_n(e_{\pi^{-1}(n)}).) = (b_1(a_{\pi^{-1}(1)}), \ldots\ldots, b_n(a_{\pi^{-1}(n)})(b_1(e_{\pi^{-1}(1)}), \ldots$

$., b_n(e_{\pi^{-1}(n)})) = \Psi_b(a_1, \ldots\ldots, a_n)\Psi_b(e_1, \ldots\ldots, e_n).$

Ako je $\Psi_b(a_1, \ldots\ldots, a_n) = \Psi_b(e_1, \ldots\ldots, e_n) \Rightarrow b_i(a_{\pi^{-1}(i)}) = b_i(e_{\pi^{-1}(i)}) \Rightarrow$

$\Rightarrow a_{\pi^{-1}(i)} = e_{\pi^{-1}(i)}$ za sve i, jer je $b_i \in \mathrm{Aut}(A_1) \Rightarrow (a_1, \ldots\ldots, a_n) = (e_1, \ldots., e_n)$. Kako je A_1^n konačna iz injektivnosti sledi da je Ψ i "na" tj. da je izomorfizam. Dokažimo da je $b \to \Psi_b$ izomorfizam. Za $b = ((b_1, \ldots\ldots, b_n), \pi)$ i $c = ((c_1, \ldots c_n), \gamma)$ elemente iz A, imamo prvo da je $b \cdot c = ((b_1c_{\pi^{-1}(1)}, \ldots, b_nc_{\pi^{-1}(n)}), \pi\gamma)$. Tada je

$$\Psi_{bc}(a_1, \ldots., a_n) = ((b_1c_{\pi^{-1}(1)})(a_{(\pi\gamma)^{-1}(1)}), \ldots\ldots, (b_nc_{\pi^{-1}(n)})(a_{(\pi\gamma)^{-1}(n)})) =$$

$= (b_1(c_{\pi^{-1}(1)}(a_{\gamma^{-1}(\pi^{-1}(1))}), \ldots., b_1(c_{\pi^{-1}(1)}(a_{\gamma^{-1}(\pi^{-1}(1))})) = \Psi_b(c_1(a_{\gamma^{-1}(1)}), \ldots, c_n(a_{\gamma^{-1}(n)})) =$

$= \Psi_b(\Psi_c(a_1, \ldots., a_n)) = (\Psi_b\Psi_c)(a_1, \ldots., a_n)$, za sve $(a_1, \ldots\ldots, a_n) \in A_1^n$. Ako je $\Psi_b(a_1, \ldots\ldots, a_n) = \Psi_c(a_1, \ldots\ldots, a_n)$ za sve $(a_1, \ldots\ldots, a_n) \in A_1^n$., uzmimo $a_1 = a_2 = \ldots$

$\ldots. = a_n \in A_1$. Tada ćemo dobiti da ja $b_i(a) = c_i(a)$, za svako $a \in A_1$ i svako i, pa će biti $b_i = c_i$ za sve i. Ako uzmemo $a_i \neq 1$, $a_k = 1$ za $k \neq i$ gde je i fiksan indeks iz $\Psi_b(a_1, \ldots., a_n) = \Psi_c(a_1, \ldots., a_n)$ sledi $b_{\pi(i)}(a_i) = c_{\pi(i)}(a_{(\gamma^{-1}\pi)(i)}) \neq 1$. Odatle $a_i = a_{(\gamma^{-1}\pi)(i)}$ tj. $i = (\gamma^{-1}\pi)(i)$ za sve i, pa $\gamma = \pi$ i konačno $b = c$. Pokažimo još da je $b \to \Psi_b$ "na" korespodencija. Neka je $f \in \mathrm{Aut}(A_1^n)$. Tada možemo smatrati da je A_1^n unutrašnji direktni proizvod svojih podgrupa $B_i \cong A_1$, gde se B_i dobija na prirodan način tj. B_i čine oni elementi kod kojih je svaka koordinata 1 sem eventualno i-te. Tada iz $A_1^n = \prod_{i=1}^{n} B_i$ sledi $f(A_1^n) = \prod_{1}^{n} f(B_i)$. Zbog jedinstvenosti razlaganja karakteristično proste grupe, imamo $f(B_i) = B_j = B_{\pi(i)} \cong A_1$ gde je

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

$\pi \in S_n$. Neka je $h_i : B_1 \to B_i$ izomorfizam koji prenosi prvu koordinatu na i-to mesto. Tada su i $h_j \cdot h_i^{-1} = \theta_{j,i} : B_i \to B_j$ izomorfizmi sa analognim dejstvom. Definišimo $f_{\pi(i)} = f \circ \theta_{i,\pi(i)} \in \mathrm{Aut}(B_{\pi(i)})$ a sa obzirom da je $B_{\pi(i)}$ prirodno indetifikovan sa A_1, možemo uzeti da je $f_{\pi(i)} \in \mathrm{Aut}(A_1)$. Uočimo sada $h = ((f_1, \ldots, f_n), \pi) \in A$. Ako je $b \in B_i$ i $b = (b_1, \ldots, b_n)$ tada je $\Psi_h(b) = (f_1(b_{\pi^{-1}(1)}), \ldots, f_n(b_{\pi^{-1}(n)}) = (1, 1, \ldots, 1, f_i(b_{\pi^{-1}(i)}), 1, \ldots, 1) = f(b)$. Kako se f i Ψ_h poklapaju na B_i za sve i, imamo $f = \Psi_h$.

Posledica: Neka je $G = \prod_{i=1}^{n} A_i$ razlaganje karakteristično proste grupe G na proste podgrupe. Tada $|\mathrm{Aut}(G)| = |(\mathrm{Aut}(A_1))^n \times_i S_n| = n! |(\mathrm{Aut}(A_1)|^n$

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

6. ARITMETIČKA FUNKCIJA Ψ

Ako je p prost broj, tada ćemo definisati $\Psi(p^n) = (p^n - 1)(p^{n-1} - 1)...(p - 1)$. Ako je $n = p_1^{a_1}....p_k^{a_k}$ kanonska faktorizacija proizvoljnog prirodnog broja u prostim brojevima p_i, tada funkciju Ψ definišemo pomoću $\Psi(n) = \Psi(p_1^{a_1}).....\Psi(p_k^{a_k})$. Dakle, funkcija Ψ je multiplikativna, što znači da je $\Psi(mn) = \Psi(m)\Psi(n)$, ukoliko su m i n uzajamno prosti. Ona je multiplikativna zahvaljujući odgovarajućoj definiciji, premda to nije njena bitna osobina.

Neka je G grupa i $G \cong (C_p)^n$. Tada je Aut(G) izomorfno, kako se pokazuje, grupi svih $n \times n$ matrica na poljem Z_p, koje su invertibilne ili koje, što je ekvivalentno, imaju determinantu različitu od 0 (mod p). Iz tog opisa grupe Aut(G) dobija se veza: $|\mathrm{Aut}(G)| = \prod_{k=0}^{n-1}(p^n - p^k) = p^{n(n-1)/2}\Psi(p^n)$. Ova formula predstavlja, da tako kažemo, "vrata" na koja funkcija Ψ ulazi u teoriju grupa i sva dalja njena pojavljivanja imaju osnovu u gornjoj vezi.

Neka je G sada proizvoljna konačna Abel-ova grupa. Naš cilj je da preko funkcije Ψ izrazimo red grupe automorfizama proizvoljne konačne Abel-ove grupe.

Za Abel-ovu grupu A i $n \in N$ možemo definisati $A_n = \left\{x \in A \middle| x^n = 1\right\}$, pri čemu $A_n < A$. Podgrupa A_n je očigledno potpuno invarijantna, tj. $h \in \mathrm{End}(A)$ povlači $h(A_n) \subseteq A_n$.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Lema 6.1. Neka je A konačna Abel-ova p grupa (p prost broj) i $h \in End(A)$. Tada $h \in Aut(A)$ akko $h(A_p) = A_p$.

Dokaz: Smer ($\Rightarrow$) je očigledan. Obrnuto uočimo A=ker(h). tada mora postojati $x \in \ker(h) \cap A_p$. Ako je $\ker(h) \neq \{0\}$ tada možemo uzeti x≠0, ali tada $h(x) \neq 0$ što je u suprotnosti sa $x \in \ker(h)$.

Kao što smo napomenuli, naš cilj je da odredimo red grupe automorfizama konačne Abel-ove grupe. U teoriji grupa poznat je stav, da ako je $G = A \times B$ gde su A i B karakteristične podgrupe grupe G, tada je $Aut(G) \cong Aut(A) \times Aut(B)$, pa i $|Aut(G)| = |Aut(A)||Aut(B)|$. Ako je G konačna Abel-ova grupa tada je ona direktan proizvod svojih Silow-ljevih podgrupa koje su njene karakteristične Abel-ove p-podgrupe. Sa obzirom na prethodno naveden stav, to znači da se problem određivanja $|Aut(G)|$ svodi na slučaj kada je G konačna Abel-ova p-grupa. Jedan slučaj, kada je $G = (C_p)^n$ već smo pomenuli. Opštiji slučaj, kada je $G = (C_{p^m})^n$, takođe je poznat. U tom slučaju je $Aut(G) \cong GL_n(Z_{p^m})$, gde je $GL_n(Z_{p^m})$ grupa matrica dimenzije n nad prstenom Z_{p^m} koje su invertibilne. Primetimo da je matrica $n \times n$ nad prstenom P invertibilna akko je njena determinanta invertibilna u P. U slučaju prstena Z_{p^m} to znači da je $M \in GL_n(Z_{p^m})$ invertibilna akko p ne deli $\det(M)$.

Takođe je poznato da je $\left|Aut((C_{p^m})^n)\right| = \left|GL_n(Z_{p^m})\right| = p^{n(n(2m-1)-1)/2}\Psi(p^n)$. Ostaje nam opšti slučaj.

Označimo sa r(x) red elementa x, a za $a \in Z, b \in N$, neka je $(a)_b$ ostatak od a pri deljenju sa b.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Neka je G konačna Abel-ova p-grupa. Ona se prema poznatom stavu razlaže na proizvod cikličnih grupa i kako razmatramo opšti slučaj neka je $G \cong (C_{p^{n_1}})^{k_1} \times (C_{p^{n_2}})^{k_2} \times ..... \times (C_{p^{n_m}})^{k_m}$ ili, što je isto, $G \cong (Z_{p^{n_1}})^{k_1} \oplus (Z_{p^{n_2}})^{k_2} \oplus ..... \oplus (Z_{p^{n_m}})^{k_m}$, gde $n_1 > n_2 > ..... > n_m$. Ako je $e_i = (0,0,....,1,.....0)$, gde je 1 na i-tom mestu, tada $\left\{ e_i \middle| 1 \le i \le t = \sum_{j=1}^{m} k_j \right\}$, generiše grupu G. Svaki element iz G je jedinstvena linearna kombinacija $\sum_{i=1}^{t} a_i e_i$ gde $a_i \in Z_{p^k}$, p^k je red od e_i. Slično postupku koji se primenjuje za linearne operatore, možemo svakom $h, h \in End(G)$, pridružiti jednu matricu dimenzije $t = \sum_{j=1}^{m} k_j$, označenu sa M_h. Pri tome i-ta kolona matrice M_h, predstavlja koeficijente u razvoju za $h(e_i) = \sum_{j=1}^{t} a_{ji} e_j$. Ako je $x = \sum_{i=1}^{t} c_i e_i$ element iz G, tada je $h(x) = \sum_{i=1}^{t} b_i e_i$ gde je $b_i = (\sum_{j=1}^{t} a_{ij} c_j) p^k$ gde je $r(e_i) = p^k$.

Primetimo, ovde jednu bitnu stvar: ako je $h(e_i) = \sum_{j=1}^{t} a_{ji} e_j$ pri čemu je $r(e_i) = p^k$, tad ako je j<i i $r(e_j) = p^n > p^k$, mora biti a_{ji} deljivo sa p. To će biti zato jer $r(h(e_i))$ deli $r(e_i)$, pa iz toga da p ne deli a_{ji} sledi da je $r(a_{ji} e_j) = p^n$. Tada bi bilo $r(h(e_i)) \ge p^n$ a to je u kontradikcijji sa $p^n < p^k = r(e_i)$ i $r(h(e_i)) | r(e_i)$.

Iz ovog zaključivanja sledi da je $p^k a_{ji} e_j = 0$, pa sledi da je a_{ji} deljivo sa p^{n-k}.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Neka je M matrica $t\times t$ u kojoj je prvih k_1 vrsta iz $Z_{p^{n_1}}$, sledećih k_2 iz $Z_{p^{n_2}}$ itd. dakle M je matrica tipa M_h. Prethodno razmatranje pokazuje da nije svaka matrica tipa M_h reprezentant nekog endomorfizma. Matrica M će u svakom slučaju definisati jedno preslikavanje $\theta_M : G \to G$, na isti način kao što ga definiše M_h, tj.

$\theta_M(x_1,.....x_t) = M(x_1,....,x_t)^T = (y_1,.....,y_t)$, $\quad y_j = (\sum_{i=1}^{t} a_{ji}x_i)p^k$ gde $r(e_j) = p^k$.

Preslikavanje θ_M biće homomorfizam sa matricom M, kao reprezentantom u odnosu na bazu $\{e_i\}$ akko $r(\theta_M(e_i)) \mid r(e_i)$ ili, što je isto, akko $r(\theta_M(e_i)) \le r(e_i)$. Jasno je da ako je θ_M homomorfizam imamo $r(\theta_M(e_i)) \mid r(e_i)$. Obratno, neka $r(\theta_M(e_i)) \mid r(e_i)$, za sve $1 \le i \le t$. Tada kao što smo pokazali ranije, imamo: akko je a_{ji} neki element matrice M i $r(e_i) = p^k$, tada za sve m, $1 \le m \le i$ važi $p^{s-k} \mid a_{jm}$, gde je $r(e_m) = p^s$. Treba, dakle, pokazati da je θ_M homomorfizam. Jasno je da se θ_M može razložiti na zbir t^2 preslikavanja $\theta_{ij}, 1 \le ij \le t$, gde je θ_{ij} definisano matricom koja ima sve nule osim na poziciji (i,j), na kojoj se nalazi odgovarajući element matrice M. Kako je zbir endomorfizama u Abel-ovoj grupi opet endomorfizam dovoljno je pokazati da je θ_{ij} endomorfizam. Neka je a_{ij} element matrice M na poziciji (i,j), $x = \sum_{k=1}^{t} x_k e_k$, $y = \sum_{k=1}^{t} y_j e_k \in G$. Tada je $\theta_{ij}(x+y) = ((x_j + y_j)_{p^k} a_{ij})_{p^n} e_i$ gde $p^k r(e_j)$, $p^n = r(e_i)$.

Takođe imamo :

$$\theta_{ij}(x) + \theta_{ij}(y) = ((a_{ij}x_j)_{p^n} + (a_{ij}y_j)_{p^n})_{p^n} e_i = (a_{ij}x_j + a_{aj}y_j)_{p^n} e_i.$$

Analizirajmo koeficijent $((x_j + y_j)_{p^k} a_{ij})_{p^n}$. Ako je $p^n \ge p^k$, tada, kao što smo pretpostavili, $a_{ij} = cp^{n-k}$. Sada je:

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

$$((x_j + y_j)_{p^k} a_{ij})_{p^n} = ((x_j + y_j - dp^k)a_{ij})_{p^n} = (x_j a_{ij} + y_j a_{ij})_{p^n}$$

Ako je $p^n < p^k$ **imamo:**

$$((x_j + y_j)_{p^k} a_{ij})_{p^n} = (((x_j + y_j)_{p^k})_{p^n} a_{ij})_{p^n} = ((x_j + y_j)a_{ijj})_{p^n} = (x_j a_{ij} + y_j a_{ij})_{p^n}$$

Znači u svakom slučaju je $\theta_{ij}(x+y) = \theta_{ij}(x) + \theta_{ij}(y)$, **pa je i** θ_M **homorfizam.**

Dakle dali smo potreban i dovoljan uslov da matrica M reprezentuje neki endomorfizam grupe G.

Uočimo sada grupu G_p. **Ona je generisana sa skupom** $\{e_i' | 1 \le i \le t\}$, **gde** $e_i' = p^{k-1}e_i$, $r(e_i) = p^k$. **Biće** $\langle e_1' \rangle \oplus ..... \oplus \langle e_t' \rangle$. **Grupu** G_p **možemo shvatiti kao vektorski prostor nad poljem** Z_p **sa bazom** e_i'.

Neka je $h \in End(G)$.

Kao što smo rekli biće $h(G_p) \subseteq G_p$. **Dakle h možemo shvatiti kao linearni operator na** G_p **nad vektorskim** Z_p **prostoru. Odredimo sada matricu za h, kao linearnog operatora na** G_p, **u odnosu na bazu** e_i'. **Potražimo zato** $h(e_i')$ **kao linearnu konbinaciju od** e_k'. **Imamo za** $M_h = [a_{ij}]$

$$e_i' = p^{k-1}e_i$$

$$h(e_i') = p^{k-1}h(e_i) = \sum_{j=1}^{t}(p^{k-1}a_{ji})e_j$$

Ovde je, naravno, $r(e_i) = p^k$. **Analizirajmo jedan sabirak** $p^{k-1}a_{ji}e_j$. **Ako je** $r(e_j) = p^n > p^k$, **tada, kao što smo rekli,** $p^{n-k}c = a_{ji}$ **pa** $p^{k-1}a_{ji}e_j = p^{n-1}ce_j' = (c)_p e_j'$. **Za** $p^n = p^k$ **sledi:** $p^{k-1}a_{ji}e_j = p^{k-1}(a_{ji})_p e_j = (a_{ji})_p e_j'$. **I na kraju za** $p^n < p^k$ **imamo** $p^{k-1}a_{ji}e_j = 0 \cdot e_j'$. **Dakle imamo** $h(e_i') = \sum_{j=1}^{t} c_j e_j'$, **gde** $c_j = 0$ **ako je** $r(e_j) < r(e_i)$, **a za** $r(e_j) = r(e_i)$ **imamo** $c_j = (a_{ij})_p$.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

To znači da matrica za h, kao linearnog operatora na G_p, ima oblik:

$$\begin{bmatrix} M_1' & & & \\ & M_2' & & \\ & & \cdot & \\ & & & M_m' \end{bmatrix} = M_o$$

gde je M_i' matrica dimenzija $k_i \times k_i$ i nastaje tako što se u matrici M_h odgovarajuća polja zamene svojim ostacima po modulu p. Takođe, sva polja ispod glavne dijagonale koja nisu ni u jednoj M_i', su jednaka 0.

Prema Lemi 6.1. h će biti automorfizam na G akko M_o reprezentuje invertibilni linearni operator akko je M_o invertibilna u $GL_t(Z_p)$ akko $\det(M_o) \neq 0$. Sa obzirom na oblik matrice M_o imamo $\det(M_o) = \det(M_1')\det(M_2')....\det(M_m')$. Dakle $\det(M_o) \neq 0$ akko za sve $1 \leq i \leq m, \det(M_m') \neq 0$.

Neka je sada M_i podmatrica matrice M_h koja zauzima ista polja kao M_i'. Primetimo da je M_i matrica nad prstenom $Z_p n_i$. Sa obzirom da je det funkcija a_{ij} na jeziku +, -, •, a $()_p$ je u odnosu na prethodne operacije homorfizam imaćemo da važi $(\det(M_i))_p = (\det(M_i'))_p$. To dalje znači da je $M_i' \in GL_{k_i}(Z_p)$ akko $M_i \in GL_{k_i}(Z_{p^{n_i}})$.

Već smo istakli da je $\left|GL_{k_i}(Z_{p^{n_i}})\right| = p^{k_i(k_i(2n_i-1)-1)/2}\Psi(p^{k_i})$. Sada smo konačno definisali potreban i dovoljan uslov za M_h, da bi h bio automorfizam: ako je a_{ij} neko polje matrice M_h i $r(e_j) = p^k$, tada za $1 \leq s \leq j$, i $r(e_s) = p^n$, važi p^{n-k} deli a_{ij} (uslov homomorfnosti); za sve matrice $M_i, M_i \in GL_{k_i}(Z_{p^{n_i}})$ gde je $Z_{p^{n_i}}$ odgovarajući prsten (uslov bijektivnosti). Sledeći dva prethodna uslova za popunjavanje matrice M_h možemo naći $|\mathrm{Aut}(G)|$. Uslov bijektivnosti nam govori kako da popunimo polja koja se nalaze u M_i. Preostala polja iznad glavne

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

dijagonale popunjavamo u skladu sa uslovom homomorfnosti. Za preostala polja ispod glavne dijagonale nema nikakvih uslova. Na taj način, dobija se da je:

$$\left|\mathrm{Aut}(G)\right| = p^{S+S_1} \prod_{i=1}^{m} \Psi(p^{k_i})$$

gde

$$S = 2 \cdot \sum_{1 \le i < j \le m} k_i k_j n_j, \qquad S_1 = \frac{1}{2} \cdot \sum_{i=1}^{m} k_i (k_i (2n_i - 1) - 1)$$

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

7. PROSTI DELIOCI BROJA |Aut(G)|

Ako je G konačna Abel-ova grupa i $|G| = p_1^{a_1} \ldots p_k^{a_k}$ kanonska faktorizacija prostim brojevima p_i, iz prethodnog poglavlja sledi da ako je p prost broj i p deli $|\mathrm{Aut}(G)|$ tada $p = p_i$, za neki $1 \le i \le k$, ili $p \mid p_i^n - 1$, $1 \le n \le d_i$, za neki $1 \le i \le k$. U ovom poglavlju dokazaćemo da je to tačno za proizvoljnu, dakle ne obavezno Abel-ovu, grupu čiji je red jednak redu od G.

Ova činjenica poznata je za konačne rešive grupe i to je rezultat P.Hall-a [7]. U tom rezultatu tvrdi se i više:

Teorema 7.1. (P.Hall): Neka je G rešiva grupa i $|G| = p_1^{a_1} \ldots\ldots p_k^{a_k}$ (kanonski). Tada $|\mathrm{Aut}(G)|$ deli $|G| \prod_{i=1}^{k} |\Phi(S_i)|^{d_i} p_i^{d_i(d_i-1)/2} \Psi(p^{d_i})$.

Ovde je S_i proizvoljna Silow-ljeva podgrupa reda $p_i^{a_i}$, a $\Phi(S_i)$ njena Frattini-jeva podgrupa, dok je d_i definisan sa $|S_i : \Phi(S_i)| = p_i^{d_1}$. Sa obzirom da su sve S_i podgrupe konjugovane u G, dakle izomorfne, biće i njihove Frattini-jeve podgrupe izomorfne i istog indeksa u S_i. Dakle faktor $|\Phi(S_i)|^{d_i}$ zavisi samo od indeksa i, a ne i od izbora S_i.

Neka je G konačna p-grupa. Tada grupa G ima jednu osobinu koja podseća na vektorske prostore. Važi naime [7]:

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Teorema 7.2. (Burnside) Neka je G konačna p-grupa. Tada ako su $X,Y \subseteq G$ dva minimalna generatorna skupa grupe G, važi $|X| = |Y|$.

Ova teorema smatra se osnovnom u teoriji konačih p-grupa. Primetimo da ona ne važi za proizvoljnu (pa čak i ne potpuno proizvoljnu) grupu G. Ako, na primer, uzmemo grupu $(Z_6,+)$, biće šlć i [2,3] dva minimalna generatora skupa različite kardinalnosti.

Ako je G konačna p-grupa, prirodno je broj $|X|$, gde je X minimalni generatorni skup za G, nazvati dimenzijom grupe G i obeležiti sa d(G). Dakle, sa obzirom na teoremu Burnside-a d(G) je dobro definisan, tj. ne zavisi od X.

Pokazuje se da u konačnoj p-grupi G važi $\Phi(G)=G^p \cdot G'$, gde je $G^p = \{x^p | x \in G\}$ a G' je komutator grupe G. Odatle se izvodi da se za konačnu p-grupu G, $\Phi(G)$ može definisati kao minimalna normalna podgrupa grupe G, čija je faktor-grupa izomorfna sa $(C_p)^k$ za neko k. S obzirom da je $\Phi(G)$ skup negeneratora za G, pokazuje se da je baš $k = d(G)$. Imamo, dakle, da je $|G:\Phi(G)| = p^{d(G)}$. Ako se vratimo na Teoremu 6.1., vidimo da parametri d_i koji se javljaju u proizvodu predstavljaju dimenziju proizvoljne grupe S_i. Još jedna posledica koju možemo izvesti iz $|G:\Phi(G)| = p^{d(G)}$ je da ako $|G| = p^t$, tada $d(G) \le t$, a jednakost važi akko $G \cong (C_p)^t$. Pomenimo još da ako $H < G, |H| = p^s$, može biti $d(H) > d(G)$, ali ako $|G| = p^t$, mora biti $d(H) \le s < t$. Dakle t je gornja granica za dimenzije svih podgrupa grupe G.

Za konačnu p-grupu G može se dati preciznija verzija Teoreme 1. koja takođe pripada P.Hall-u.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Teorema 7.3.: Ako je G konačna p-grupa i d(G)=d tada $|\mathrm{Aut}(G)|$ deli $|\Phi(G)|^d p^{d(d-1)/2}\Psi(p^d)$.

Sada ćemo dati uopštenje Teoreme 7.3. za proizvoljnu konačnu grupu G. Pre toga pomenimo još jednu činjenicu na kojoj se taj dokaz bazira, a koja se koristi i pri dokazu Teoreme 7.3.. Ako je G konačna p-grupa, dimenzije d, tada skup $G_d = \{(x_1,\ldots,x_d) | \{x_1,\ldots,x_d\}$ generiše G, $x_i \in G\}$ $|\Phi(G)|^d p^{d(d-1)/2}\Psi(p^d)$. elemenata. Prelazimo sada na dokaz najavljene teoreme.

Teorema 7.4.: Neka je G konačna grupa i $|G| = p_1^{a_1}\ldots\ldots p_k^{a_k}$ (kanonski). Za $1 \le i \le k$, neka je s_i broj Silow-ljevih podgrupa reda $p_i^{d_i}$ a d_i dimenzija bilo koje od njih. Tada $|\mathrm{Aut}(G)| \left| \prod_{i=1}^{k} s_i \cdot |\Phi(G)|^{d_i} \cdot p_i^{\frac{d_i(d_i-1)}{2}} \cdot \psi\left(p_i^{d_i}\right) \right.$.

Dokaz: Neka je $G_i = \bigcup_{\substack{H<G \\ |H|=p_i^{a_i}}} H_{d_i}$. Kao što smo rekli H_{d_i} je skup svih uređenih minimalnih generatornih skupova za neku p_i - Silow-ljevu podgrupu H. Tada je G_i, po definiciji, skup svih $(x_1, x_2, \ldots\ldots, x_{d_i})$, takvih da $\{x_1,\ldots\ldots,x_{d_i}\}$ generiše neku p_i-Silow-ljevu podgrupu. Kako su sve p_i-Silow-ljeve podgrupe konjugovane, dakle izomorfne, biće $|H_{d_i}|$ nezavisan od izbora H i $|H_{d_i}| = |\Phi(H)|^{d_i} p_i^{d_i(d_i-1)/2}\Psi(p_i^{d_i}) = B_i$, i još $|G_i| = s_i f_i$. Neka je sada $G_o = G_1 \times \ldots\ldots \times G_k$, Decartes-ov proizvod skupova G_i. Očigledno $|G_o| = \prod_{i=1}^{k} |G_i| = \prod_{i=1}^{k} s_i\beta_i$. Dakle ako $X \in G_o$, tada $X = (x_1, x_2, \ldots\ldots, x_k)$ gde je X_i uređeni minimalni generatorni skup za neku p_i-Silow-ljevu podgrupu. Neka je $f \in \mathrm{Aut}(G)$ i $X \in G_i$. Ako je $X = (y_1, \ldots\ldots, y_{d_i})$ i ako definišemo $f_i(X) = (f(y_1), \ldots\ldots, f(y_{d_i}))$, jasno je da je f_i preslikavanje na G_i, jer $f_i(X)$ će biti

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

minimalni generatorni skup za f(H) ako je X_i bio isto to za H. Slično, ako je $t \in G_o$, $t = (t_1, t_2, ..., t_k)$, definišemo $f_o(t) = (f_1(t_1), ..., f_k(t_k))$ i kako $f_i : G_i \to G_i$ imaćemo $f_o : G_o \to G_o$.

Iz činjenice da je $f \in Aut(G)$, dakle bijekcija, sledi da je f_i permutacija na G_i a odatle i da je f_o permutacija na G_o. To znači da je preslikavanjem $\theta(f) = f_o, \theta : Aut(G) \to S_{G_o}$ zadato jedno dejstvo grupe Aut(G_o) na G_o. Pokažimo da je stabilizator F_t, proizvoljnog elementa $t \in G_o$, jedinična podgrupa grupe Aut(G).Neka je $t \in G_o$ i $f \in Aut(G)$, pri čemu $f_o(t) = t$. Ako je $t = (t_1, t_2, ..., t_k)$ imamo $f_i(t_i) = t_i = (x_1, ..., x_{d_i})$ tj. $f(x_j) = x_j$, za sve $1 \le i \le k$, $1 \le j \le d_i$. Dakle f fiksira za svako $1 \le i \le k$ generatorni skup neke p_i-Silow-ljeve podgrupe H_i (tačka po tačka) pa onda fiksira (tačka po tačka) i celu $H_i, |H_i| = p_i^{a_i}$. Kako skup fiksiranih tačaka nekog automorfizma čini podgrupu G, vidimo da podgrupa fiksnih tačaka G_f za naše f ima za svako $1 \le i \le m$, Silow-ljevu podgrupu reda $p_i^{a_i}$. Prema Lagrange-ovoj teoremi $p_i^{a_i} | G_f$ tj. $|G| = |G_f|$, što znači $G = G_f$. Dakle f je identički automorfizam što smo hteli da pokažemo. Sledi da orbita svakog $t \in G_o$ ima $|Aut(G)|$ elemenata pa odatle $|Aut(G)|$ deli $|G_o| = \prod_{i=1}^{k} s_i \beta_i$, čime je teorema dokazana.

Posledica 7.1. Neka je G grupa i $|G| = p_1^{a_1} ..... p_k^{a_k}$ (kanonski). Ako je p prost broj i $p | Aut(G)$, tada $p = p_i$ ili $p | p_i^n - 1$, $1 \le n \le a_i$.

Dokaz: Uz oznake iz prethodne teoreme imamo $p \Big| \prod_{i=1}^{k} s_i \beta_i$. Po teoremi Silow-a $s_i \big| |G|$, pa prema tome, ako $p \ne p_i$ za sve $1 \le i \le k$, tada $p \Big| \beta_j = \left|\Phi(H_j)\right|^{d_j} p^{d_j(d_j-1)/2} \Psi(p^{d_j})$ za neko $1 \le j \le k$. Odatle $p \Big| \Psi(p^{d_j})$ iz čega sledi tvrđenje.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Na primer, ako $|G| = 168 = 2^3 \cdot 7 \cdot 3$, na osnovu prethodne posledice imamo da $|\mathrm{Aut}(G)|$ može biti deljiv samo sa 2,3 i 7, kao prostim deliocima.

Primetimo da Teorema 7.4., iako se odnosi na proizvoljnu grupu G, može biti, za neke G, ne manje precizna od Teoreme 7.1. koja se odnosi na rešive grupe. Obe teoreme tvrde da $|\mathrm{Aut}(G)|$ deli neki brojevi. Taj broj se za Teoremu 7.4. dobija tako što se $|G|$ u broju iz Teoreme 7.1. zameni sa $\prod_{i=1}^{k} s_i$. Ako je $|G| = p_1^{a_1} p_2^{a_2}$, prema spomenutoj Burnside-ovoj teoremi, G rešiva i važiće $|G| \geq s_1 s_2$, pa ocena iz Teoreme 7.1. nije bolja nego ona iz Teoreme.7.4.

Ako imamo dodatne pretpostavke o grupi G, tada se može dati u nekim slučajevima, još preciznije tvrđenje za $|\mathrm{Aut}(G)|$ koje je tipa Teoreme 7.4. Za slučaj kad je G rešiva to je, na primer, Teorema 7.1..

Mi ćemo to uraditi za slučaj kad je G prosta.

Teorema 7.5.: Neka je G grupa kao u Teoremi 7.4. (oznake iste). Pretpostavimo da je G prosta. Tada $|\mathrm{Aut}(G)| \,|\, s_i ! \beta_i$, za sve $1 \leq i \leq k$.

Dokaz: Neka je $G(p_i) = \left\{ x \in G \,\middle|\, r(x) = p_i^m \right\}$, gde je r(x) red od x. Prema teoremi Silow-a, svaki $x \in G(p_i)$, sadržan je u nekoj p_i-Silow-ljevoj podgrupi. To znači da je $G(p_i) = \bigcup_{H \in L_i} H$ gde je L_i skup svih p_i- Silow-ljevih podgrupa. Primetimo da je $G(p_i)$ invarijantan za sve unutrašnje automorfizme grupe G. To znači da $G(p_i)$ generiše normalnu podgrupu grupe G, ali kako je G prosta, sledi, $\langle G(p_i) \rangle = G_0$. Odatle imamo da je automorfizam f, identičko preslikavanje akko f fiksira skup $G(p_i)$ tačka po tačka.

Neka je kao u Teoremi 7.4., $G_i = \bigcup_{\substack{H<G \\ |H| = p_i^{a_i}}} H_{d_i}$. Definišimo sada G_i' na sledeći način: $G_i' \subseteq \prod_{i=1}^{s_i} G_i$ (Descartes-ov) proizvod, pri čemu $X = (x_1, \ldots, x_{s_i}) \in G_i'$ akko

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

za svaki $H_{d_i} \subseteq G_i$, $|H| = p_i^{a_i}$, postoji x_j, $1 \le j \le s_i$, takav da $x_j \in H_{d_i}$. Drugim rečima, $X = (x_1, \ldots, x_{s_i}) \in G_i'$ akko su x_j uređeni minimalni generatorni skupovi koji svi pripadaju različitim p_i-Silow-ljevim podgrupama. Kada se prebroje elementi u G_i' dobija se da je $|G_i'| = s_i ! \beta_i$. Ako je $f \in \mathrm{Aut}(G)$ možemo, slično kao u Teoremi 7.4. definisati $f_o : G_i' \to G_i'$ na sledeći način: ako je $X = (x_1, \ldots, x_{s_i}) \in G_i'$ tada $f_o(x) = (f_i(x_1), \ldots, f_i(x_{s_i}))$. Podsećamo $f_o : G_i \to G_i$, i da je definisana sa $f_i(y_1, \ldots, y_{d_i}) = (f_i(y_1), \ldots, f_i(y_{d_i}))$ gde $(y_1, \ldots, y_{d_i}) \in G_i$. Preslikavanje f_i se javljalo i u Teoremi 7.4., i kao što je i tamo rečeno, ono je permutacija na G_i. Odatle neposredno sledi i da je f_o permutacija na G_i', što znači da $\theta : \mathrm{Aut}(G) \to S_{G_i'}$, zadato sa $\theta(f) = f_o$, predstavlja dejstvo. Odredimo opet centralizator H_X, za proizvoljni $X \in G_i'$, tj. pokažimo da se on sastoji samo od identičkog automorfizma. neka $f \in \mathrm{Aut}(G)$, $X = (x_1, \ldots, x_{s_i}) \in G_i'$ i $f(X) = X$ tj. $f_i(x_j) = x_j$ za $i \le j \le x_{s_i}$. To znači da ako $x_j = (y_1, \ldots, y_{d_i})$, tada $f(y_t) = y_t, 1 \le t \le d_i, 1 \le j \le x_{s_i}$. dakle, automorfizam f fiksira minimalni generatorni skup proizvoljne p_i-Silow-ljeve podgrupe i to tačka po tačka, pa onda tačka po tačka fiksira i svaku p_i-Silow-ljevu podgrupu, odnosno čitav G_i, što je, kako smo videli, potrebno i dovoljno da bi f bilo identičko preslikavanje. Odatle zaključujemo da je orbita svakog elementa G_i' kardinalnosti $|\mathrm{Aut}(G)|$, pa imamo $|\mathrm{Aut}(G)| \,|\, s_i ! \beta_i$ što je i trebalo dokazati.

Posledica 2. Neka je G konačna prosta grupa, uz sve oznake kao u teoremama 7.4. i 7.5.. Tada $|\mathrm{Aut}(G)|$ deli NZD.$(\prod s_i \beta_i, s_1 ! \beta_1, s_2 ! \beta_2, \ldots, s_k ! \beta_k)$.

Dokaz: Sledi neposredno iz Teorema 7.4 i 7.5..

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

8. FUNKCIJA Ψ I SEMI-DIREKTAN PROIZVOD

U ovom poglavlju daćemo jednu vezu između funkcije Ψ i semi-direktnog proizvoda konačnih rešivih grupa. Teorema koju ćemo dokazati davaće dovoljan uslov da konačna rešiva grupa bude semi-direktan proizvod svoje dve Hall-ove podgrupe.

Pre nego formulišemo i dokažemo najavljenu teoremu, navešćemo neke poznate činjenice koje ćemo koristiti u dokazu:

Lema 8.1.: Neka je G konačna rešiva grupa. Tada za neki prost broj p koji deli $|G|$, postoji $H, H \lhd G$ i $H \cong (C_p)^n$ za neko n.

Lema 8.2.: Ako je G rešiva grupa, onda je i njena faktor-grupa takođe rešiva.

Lema 8.3.: Neka su A i B konačne grupe takve da $(|A|,|B|) = 1, h : A \to B$ homomorfizam. Tada $h(x) = 1$, za sve $x \in A$ tj. $A = \ker(h)$.

Što se tiče Leme 8.2., nju smo već pomenuli kada smo govorili o rešivim grupama. U vezi Leme 8.3. recimo samo da je ona direktna posledica prve teoreme o izomorfizmu. Prelazimo sada na najavljenu teoremu.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Teorema 8.1.: Neka je G konačna rešiva grupa i $|G| = ab, (a,b) = 1$. Neka je takođe $(a, \Psi(b)) = 1$. Tada je G semidirektan proizvod svojih podgrupa A i B takvih da $|A| = a, |B| = b$ i $A \lhd G$.

Dokaz: Prema teoremi P.Hall-a za konačne grupe odmah imamo da postoji $B, B < G$ i $|B| = b$. Dokaz tvrđenja svodi se na to da pokažemo egzistenciju normalne podgrupe reda a. Dokaz ćemo izvesti indukcijom po redu grupe G, pri čemu je baza indukcije trivijalna pa je preskačemo. Neka je $|G| > 1$. Prema Lemi 8.1., postoji $H, H \lhd G$ i $H \cong (C_p)^n$, p je prost broj. Pretpostavimo kao prvi slučaj da p deli a. Tada je faktor grupa $G/H = K$ rešiva (po Lemi 8.2.) konačna grupa i $|G/H| < |G|$. Pošto je $|K| = |G/H| = |G|/|H|$ i p deli a, imamo $|K| = b \cdot \frac{a}{p^n}$, i $(b, \frac{a}{p^n}) = 1$, a takođe će biti i $(\Psi(b), \frac{a}{p^n}) = 1$. Dakle, možemo da na grupu G primenimo indukcijsku hipotezu, što znači da postoji $K_1, K_1 \lhd K$ i $|K_1| = \frac{a}{p^n}$. Ako je $h: G \to K$, prirodni homomorfizam, tada $K_1 \lhd K$ povlači $h^{-1}(K_1) \lhd G$. Međutim $|h^{-1}(K_1)| = a$, pa je $h^{-1}(K_1)$ tražena podgrupa A. Neka sada p deli b i neka je opet $K = G/H, |K| = \frac{b}{p^n}$. Opet će važiti da je K rešiva, $(a, \frac{b}{p^n}) = 1, (a, \Psi(\frac{b}{p^n})) = 1$, pa možemo na K primeniti indukcijsku hipotezu. Ona nam daje da postoji $K_1, K_1 \lhd K$ i $|K_1| = a$. Ako je $h: G \to K$, opet prirodni homomorfizam, imaćemo $h^{-1}(K_1) \lhd G$. i $|h^{-1}(K_1)| = a \cdot p^n$. Analizirajmo malo grupu $h^{-1}(K_1)$. Ona je rešiva (jer je podgrupa rešive grupe opet rešiva), pa po teoremi Hall-a postoji $A, A < h^{-1}(K_1)$ i $|A| = a$. Takođe imamo da $H < h^{-1}(K_1)$ jer je $H = h^{-1}(1)$. Kako je $H \lhd G$ biće i $H \lhd h^{-1}(K_1)$. Iz $H \lhd h^{-1}(K_1)$ zaključujemo da grupa A dejstvuje na H, dejstvom θ gde je $x \in A$, $\theta_x(y) = xyx^{-1}, y \in H$ (svakom $x \in A$, θ pridružuje restrikciju na H unutrašnjeg automorfizma σ_x grupe $h^{-1}(K_1)$). Preslikavanje θ je jedan homomorfizam iz A u

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Aut(H). Kako je $H \cong (C_p)^n$, kao što smo ranije rekli $|\mathrm{Aut}(H)| = p^{n(n-1)/2}\Psi(p^n)$. Iz $(\Psi(b),a)=1$ i $p|b$ sledi $(\Psi(p^n),a)=1$ pa $(|A|,|\mathrm{Aut}(H)|)=1$. Po Lemi 8.2. to znači da A=ker(θ), tj. da $xyx^{-1}=y$ ili $x=yxy^{-1}$ za sve $x \in A, y \in H$. Poslednja jednakost tvrdi da H<C gde je C normalizator od A u $h^{-1}(K_1)$. Kako je takođe A<C tada $A \cdot H < C$. Ali kako $|AH| = ap^n$ imamo $C = h^{-1}(K_1)$ tj. $A \lhd h^{-1}(K_1)$. Pokažimo da je $A \lhd G$. Ako je $x \in G$ tada je $\sigma_x(A) \subseteq \sigma_x(h^{-1}(K_1)) = h^{-1}(K_1)$. Kako je A normalna Hall-ova podgrupa u $h^{-1}(K_1)$, ona je i jedina podgrupa reda a, a kako je $|\sigma_x(A)| = a$, sledi $A = \sigma_x(A)$. Pošto je $x \in G$ bio proizvoljan, sledi $A \lhd G$, čime je dokaz kompletiran.

Posledica 8.1. Neka je G proizvoljna konačna grupa i $|G| = a \cdot b$, $(a,b)=1$. Ako $(a,\Psi(b))=1$ i $(\Psi(a),b)=1$, tada je $G \cong A \times B$; gde $A,B<G, |A| = a, |B| = b$.

Dokaz: Primetimo da uslovi $(a,\Psi(b))=1$ i $(\Psi(a),b)=1$ povlače u slučaju $a,b>1$ da je $|G|$ neparan. Ako a=1 ili b=1, tvrđenje sledi direktno. Kako je $|G|$ neparan, prema pomenutoj Feit-Thompson teoremi, G je rešiva. Prema Teoremi 8.1. to znači da postoje A i B, $A \lhd G$ i $B \lhd G$, $|A| = a$, $|B| = b$. Kako (a,b)=1, imamo $A \cap B = \{1\}$, i kako $AB = G$, sledi $G \cong A \times B$.

Na primer neka je G grupa reda $|G|=3^2 \cdot 7 \cdot 5$. Ako uzmemo $a = 3^2 \cdot 7$ i b=5 tada su uslovi Posledice 8.1. ispunjeni i postojaće grupe A, B podgrupe u G takve da je $G = A \times B$.

Pomenimo ovde jednu poznatu teoremu čiji je autor Frobenius [4]. Ona je nezavisna od prethodnih teorema ali je u prirodnoj vezi sa njima kako će se to videti iz njenog iskaza. Dajmo prvo jednu definiciju: neka je G grupa i $|G| = p^n a$, (a,p)=1, p je prost broj i neka postoji $H, H \lhd G, |H| = a$. Tada se kaže da je grupa G, p-nilpotentna. Može se tako pokazati da je konačna grupa G nilpotentna akko je p-nilpotentna za svaki prost broj p koji deli $|G|$, što uspostavlja vezu između obične nilpotentnosti i p-nilpotentnosti.

Navodimo sada najavljenu Frobenius-ovu teoremu:

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Teorema 8.2.(Frobenius): Neka je G proizvoljna konačna grupa i $|G| = ap^n$ gde je p prost broj i $(a, \Psi(p^n)) = 1$. Tada je G, p-nilpotentna.

Primetimo da je u gornjoj teoremi uslov da je $|G|/a$ stepen prostog broja neophodan tj. teorema ne mora da važi pod pretpostavkama da je $|G| = ab, (a,b) = 1\ (a, \Psi(b)) = 1$. Uzmimo, na primer, grupu A_5. Imamo $|A_5| = 5 \cdot 2^2 \cdot 3$. Ako stavimo a=5, $b = 2^2 \cdot 3$, vidimo da A_5 nema normalnu podgrupu reda 5 jer je prosta. Ovaj primer pokazuje takođe da je uslov rešivosti grupe G neophodan za važenje Teoreme 8.1. Inače Teorema 8.1. može se dokazati elegantnije uz pomoć Teoreme 8.2. Neka je, naime, G grupa iz pretpostavke i oznake iz Teoreme 8.1. Primetimo prvo da ako su dve podgrupe u G konjugovane, onda su konjugovani i njihovi normalizatori. Specijalno, ako su dve podgrupe u G konjugovan, onda su njihovi normalizatori jednakih redova. To važi za proizvoljnu grupu G, a za našu grupu G iz Teoreme 8.1. važi da postoji podgrupa reda a i da su sve one konjugovane (Hall-ova teorema). Dakle, sve podgrupe reda a imaju normalizatore jednakih redova, i označimo taj red sa n_a. Ako je $b = p_1^{a_1} \ldots . p_k^{a_k}$ (kanonski) tada za svaki $1 \le i \le k$, postoji podgrupa $H_i, |H_i| = a \cdot p_i^{a_i}$ opet po Hall-ovoj teoremi. Po Teoremi 8.2. postoji H_i normalna. Sa obzirom na ono što je rečeno o normalizatorima podgrupe od a elemenata, imaćemo da $p_i^{a_i}$ deli red normalizatora podgrupe od a elemenata i to za vaki $1 \le i \le k$. To znači da je taj red deljiv i sa b, pa onda i sa $ab = |G|$, odavde imamo da je podgrupa od a elemenata normalna u G što je ekvivalentno Teoremi 8.1.

Može se dati i preciznija verzija Teoreme 8.2. koja takođe pripada Frobenius-u.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Teorema 8.2': Neka je G konačna grupa i $|G| = ap^n$, $(a,p) = 1$, p je prost broj. Ako je $(a, \Psi(p^d)) = 1$, gde je $d = \max\{d(H) | H < H_p\}$, pri čemu je H_p jedna fiksirana p Silow-ljeva podgrupa.

Kao specijalni slučaj Teoreme 8.2'. imamo sledeću teoremu koja pripada Burnside-u.

Teorema 8.3.: Neka je G konačna grupa i p prost broj, $|G| = ap^n$, $(a,p) = 1$. Ako je p Silow-ljeva podgrupa ciklična i $(a, \Psi(p)) = (a, p-1) = 1$, tada je G p-nilpotentna.

Koristeći prethodnu teoremu možemo uopštiti jednu poznatu teoremu iz teorije grupa: (Poincare) Ako su H i G konačne grupe i H<G, pri čemu je $|G:H| = p$, gde je p najmanji prost broj koji deli red grupe G, tada je $H \lhd G$. Dokazaćemo sledeće uopštenje prethodne teoreme:

Teorema 8.4.: Neka je G konačna grupa i H<G takva da je $|G:H| = p$, p je prost broj. Ako je $(a, \Psi(p)) = (a, p-1) = 1$, tada je $H \lhd G$.

Dokaz: Izvodimo ga indukcijom po $|G|$ pri čemu je baza trivijalna. Neka je dakle H<G i $|G:H| = p$. Tada postoji homomorfizam $\theta: G \to S(G/H)$, gde je $S(G/H)$ grupa permutacija na kosetima podgrupe H (sa G/H smo označili taj skup koseta koji je za sada samo skup tj. ne znamo da li je i grupa). Kako je $|G:H| = p$ imamo da je $|S(G/H)| = p!$. Pretpostavimo prvi slučaj, da je $|G| = ap$, $(a,p) = 1$. Tada tvrđenje sledi na osnovu Teoreme 8.3.. Naime, p-Silow-ljeva podgrupa je u tom slučaju reda p, pa je ciklična. Na osnovu Teoreme 8.3. imamo da postoji normalna podgrupa reda a, koja je, sa obzirom da je normalna i Hall-ova, jedina podgrupa reda a u G, pa se poklapa sa H.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Pretpostavimo sada drugi slučaj da je $|G| = ap^n$, $(a,p) = 1$, $n > 1$. **Kao što smo rekli** θ **je homomorfizam,** $\theta = G \to S(G/H)$. **Kako** $|G| = ap^n$ **ne deli** $|S(G/H)| = p!$, **i kako** $|G/\ker(h)|$ **deli** $|S(G/H)|$, **jer je G/ker(h) izomorfno nekoj podgrupi u S(G/H), zaključujemo da je jezgro netrivijalno tj** $|\ker(h)| > 1$. **Odatle sledi da je** $|G/\ker(h)| < |G|$. **Ako je** $k:G \to G/\ker(h)$ **prirodni homomorfizam tada je** $K(H) \lhd G/\ker(h)$ **i** $|G/\ker(h):K(H)| = p$ **jer je po "n faktorijel teoremi",** $\ker(h) = \text{core}(H) = \bigcap_{x \in G} \sigma_x(H) < H$. **Sada možemo primeniti indukcijsku hipotezu na grupu G/ker(h), pa dobijamo da je** $K(H) \lhd G/\ker(h)$. **To je, međutim, prema Teoremi o korespodenciji [6] ekvivalentno sa** $H \lhd G$ **što je i trebalo dokazati.**

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

9. GRUPNI BROJEVI

Neka je K neka klasa konačnih grupa i n prirodni broj takav da sve grupe reda n, pripadaju K. Tada je prirodno n nazvati K-brojem. Na, primer prosti brojevi su ciklični, jer su sve grupe čiji je red prost broj, ciklične. Grupe čiji je red kvadrat prostog broja su Abel-ove, pa su brojevi p^2, p prost, Abel-ovi. Grupe čiji je red proizvoljni stepen nekog prostog broja su nilpotentne, dakle, brojevi p^n, p prost broj, $n \in N$ su nilpotentni. Grupe neparnog reda su rešive (Feit-Thompson-ova teorema), dakle neparni brojevi su rešivi. Može se sada postaviti problem sledećeg tipa: za datu klasu konačnih grupa K, odrediti sve K brojeve.

Sve ciklične brojeve odredio je Burnside:

Teoreme 9.1. Broj $n \in N$ je cikličan akko $n = p_1 \ldots\ldots p_k$ (kanonski) i za svaka dva i, j tako da $1 \le i,j \le k$ važi p_i ne deli $\Psi(p_j) = p_j - 1$.

Na primer, broj $1001 = 11 \cdot 7 \cdot 13$ je cikličan.

Sve Abel-ove brojeve opisao je L.E.Dickson [8]:

Teorema 9.2. Broj $n \in N$ je Abel-ov akko $n = p_1^{a_1} \ldots\ldots p_k^{a_k}$ (kanonski) gde $a_j \le 2, 1 \le j \le k$ sve $j, 1 \le j \le k$ važi p_j ne deli $\Psi(n)$.

Na primer, broj $3^2 \cdot 11 \cdot 17$ je Abel-ov.

Sve nilpotentne brojeve opisao je G. Pazderski [9], a mi ćemo ovde dati originalan dokaz tog opisa:

Teorema 9.3. Broj $n \in N$ je nilpotentan akko $n = p_1^{a_1} \ldots\ldots\ldots p_k^{a_k}$ (kanonski) i za sve j, $1 \leq j \leq k$ važi p_j ne deli $\psi(n)$ ili (što je isto) $(n, \Psi(n)) = 1$.

Dokaz: Neka je $n = p_1^{a_1} \ldots\ldots\ldots p_k^{a_k}$, i p_j ne deli $\psi(n)$, za sve $1 \leq j \leq k$. Primetimo da prethodni uslov implicira da je n oblika $p_1^{a_1}$ ili neparan. U prvom slučaju odmah sledi da je grupa reda n nilpotentna. Pretpostavimo zato da je G grupa reda n, koji je neparan. Prema Feit-Thompson-ovoj teoremi G je rešiva. Ako stavimo $a = p_i^{a_i}$, $b = n / p_i^{a_i}$ tada (a,b)=1 i $(a, \psi(b))=1$. Primenjujući Teoremu 9.1. dobijamo da će podgrupa reda a, tj. p_i Silow-ljeva podgrupa u G biti normalna, i to za svako $1 \leq j \leq k$.

Odatle sledi da je G direktan proizvod svojih Silow-ljevih podgrupa, a to je, sa obzirom da je G konačna, ekvivalentno činjenici da je G nilpotentna. Dokazaćemo da su prethodno opisani brojevi, jedini koji su nilpotentni. Neka je $n = p_1^{a_1} \ldots\ldots\ldots p_k^{a_k}$, i p_i deli $p_j^m - 1$ za neke $1 \leq i,j \leq k$ i $1 \leq m \leq a_j$. Dakle, pretpostavimo da za n nije ispunjen uslov $(n, \psi(n))=1$. Konstruisaćemo grupu reda n koja nije nilpotentna. Kao što smo već imali važi $\left|\mathrm{Aut}((C_{p_j})^m)\right| = p_j^{m(m-1)/2} \Psi(p_j^m)$. Sa obzirom da p_i deli $p_j^m - 1$ i kako je $\Psi(p_j^m) = (p_j^m - 1)\Psi(p_j^{m-1})$ imamo da p_i deli $\left|\mathrm{Aut}((C_{r_j})^m)\right|$. Prema Cauchy-jevoj lemi postoji u $\mathrm{Aut}((C_{r_j})^m)$ podgrupa K, takva da $|K| = p_i$. Sada možemo konstruisati semidirektan proizvod $(C_{p_j})^m \times_\theta K = A$ gde je $\theta: K \to \mathrm{Aut}(C_{p_j})^m$, inkluziono preslikavanje. Tad će biti $|A| = p_j^m p_i$. Pokazujemo

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

sada da grupa A ne može biti nilpotentna. Kako je $|K| = p_i > 1$ i preslikavanje θ monomorfizam na $(C_{p_j})^m$. To znači da postoji $x \in (C_{p_j})^m$ takav da $f(x) \neq X$. Uočomo sada dva elementa grupe A i to (x, i_A) i (1,f), gde je i_A identičko preslikavanje na A a 1 je neutral u grupi $(C_{p_j})^m$. Neposredno se proverava da je red elemenata (x, i_A) jednak p_j, a da je red elementa (1,f), jedak p_i. Ako bi grupa A bila nilpotentna ova dva elementa morala bi da međusobno komutiraju, s obzirom da su im redovi uzajamno prosti. Međutim imamo da je $(1,f)(x,i_A) = (f(x),f)$ dok je $(x,i_A(1,f) = (x,f)$ što, uz $f(x) \neq x$ znači da oni ne komutiraju. Dakle, A nije nilpotentna. Ako uzmemo sada grupu $G = A \times C_t$ gde je $t = n/|A|$, biće $|G| = n$, ali G nije nilpotentna. Ona sadrži podgrupu izomorfnu sa A, koja nije nilpotentna, dok u nilpotentnoj grupi svaka podgrupa mora biti nilpotentna. Sledi da n nije nilpotentna, čime je dokaz kompletiran.

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs

Literatura

[1] **Baer R.** "Die Kompositionsreihe der Gruppe aller einenindeutigen Abbildungen einer unendlicnen Menge ausf sich", *Studia Mathematica* **1935** (5), 15-17

[2] **Feit W., Thompson J.** "Solvability of groups of odd order", *Pacific J. Math.* **13** (1963), 775-129

[3] **Aschнbacher M.** "Finite group theory", *Cambridge University Press,* 1986

[4] **Huppert B.** "Endliche Gruppen I", *Springer-Verlag,* Berlin, Heidelberg, New York, 1967.

[5] **Bakić R.** "On a theorem of Frobenius", *Publ. Inst. Math.* **61** (75) 41-44

[6] **Grulović M. Z.** "Osnovi teorije grupa", *Institut za matematiku, Novi Sad* 1997.

[7] **Robinson D. J.** "A course in the theory of groups" *Springer-Verlag,* New York 1996.

[8] **Dickson L. E.** "Definition of a group and a field by independent postulates", *Trans. Amer. Math. Soc.* **6**, 198-204, (1905).

[9] **Pazderski G.** "Die Ordnungen, zu denen nur Gruppen mit gegebenen Eigenshaften gehoren" *Arch.Math.***10** (1959), 331-343

[10] **Rotman J.J.** "The theory of groups" *Allyn and Bacon,* Boston 1973.

[11] **Levi I.** "Automorphisms of normal transformation semigroups" *Proc. of Edinburgh Math. Soc.*

[12] **Bozović N., Mijajlović Z.** "Uvod u teoriju grupa" *Naučna knjiga,* Beograd

Virtual Library of Faculty of Mathematics - University of Belgrade
elibrary.matf.bg.ac.rs