Osječki matematički list 24 (2024), 49–74

Uvod u konačne p-grupe

Marijana Greblički*

Sažetak

U ovom radu dan je uvod u teoriju konačnih p-grupa za prost broj p.

Ključne riječi: *grupa, konačna p-grupa, podgrupa, maksimalna podgrupa, abelova grupa, centar grupe, ciklička grupa, normalna grupa*

Introduction to finite p-groups

Abstract

In this paper, an introduction to the theory of finite p-groups is given for a prime number p.

Keywords: *group, finite p-group, subgroup, maximal subgroup, Abelian group, group's center, cyclic group, normal group*

1 O teoriji konačnih grupa

U godinama od 2000. do 2003. profesor Zvonimir Janko s njemačkog Sveučilišta u Heidelbergu držao je predavanja Konačne p-grupe 1, 2, 3 na poslijediplomskom studiju matematike Matematičkog odsjeka Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu. Na način nadasve jasan, precizan i pun humora, profesor Janko uveo je buduće doktore matematike u teoriju p-grupa i to krenuvši od samih osnova i početaka teorije pa

*Fakultet prometnih znanosti, Sveučilište u Zagrebu, email: mgreblicki@fpz.unizg.hr

do aktualnih problema u istraživanju. Prisustvovati ovim predavanjima i oduprijeti se želji da postanete aktivni član obitelji istraživača konačnih p-grupa vođeni besprijekornim savjetima i smjernicama profesora Janka za mnoge od slušatelja bilo je nemoguće. Dapače! Brojni članci i disertacije izniknuli su kao posljedica pomenutih predavanja i Profesorovog jedinstvenog pogleda u svijet konačnih p-grupa. Na veliku žalost sviju koji su ga poznavali i bili dotaknuti njegovim životom i djelom, 12.4.2022. neposredno prije svog 90. rođendana preminuo je profesor Zvonimir Janko ostavivši iza sebe nevjerojatnu matematičku baštinu koja ga je svrstala u redove najvećih matematičara naše ere. Sve do zadnjeg dana nije prestao s istraživanjem i radom na zajedničkom šestom svesku u nizu jednog od najopsežnijih pregleda ikoje matematičke grane u svijetu, Groups of Prime Power Order Vol. 6. Sve sveske, Groups of Prime Power Order Vol. 1-5, sem prvog na kojem je bio recenzent, napisao je u koautorstvu s profesorom Yakovom Berkovichem s izraelskog Sveučilišta u Haifi.

Pogledajmo kroz samo par prekretnica kratki povijesni tijek razvoja teorije grupa. Nakon gotovo 100 godina od otkrića pet Mathieuovih sporadičnih jednostavnih grupa M_{11}, M_{12} iz 1861., M_{22}, M_{23} i M_{24} iz 1873. godine, smatralo se da ne postoje druge sporadične jednostavne grupe (grupe koje nisu članice neke beskonačne serije) i da će se uskoro dokazati da uopće nema drugih konačnih jednostavnih grupa osim onih koje su već poznate. Godine 1964. Janko dolazi do svojeg epohalnoga otkrića - prve Jankove sporadične jednostavne grupe J_1. Tim otkrićem u svijetu grupa kreće dvadesetogodišnji lov na preostale sporadične jednostavne grupe. Lov je završen brojem 26 - naime otkriveno je ukupno 26 sporadičnih jednostavnih grupa i dokazano je da ne postoje nikoje druge sporadične jednostavne grupe. Teorija konačnih rješivih grupa (grupa je rješiva ako postoji prirodan broj $n \in \mathbb{N}$ takav da je n-ta kvocijentna podgrupa grupe G trivijalna, tj. $C^n(G) = \{1\}$) time je 1983. godine dovedena do zadovoljavajućeg stupnja kada je nadasve simbolično baš profesor Janko došao do otkrića posljednje sporadične jednostavne grupe J_4 (posljednje od četiri Jankove grupe J_1, J_2, J_3, J_4), te je tako zgotovljen teorem čiji se dokaz proteže u preko više od 500 članaka raznih matematičkih časopisa svijeta i na više od 10000 stranica, a on glasi ovako:

Svaka neabelova konačna jednostavna grupa je ili grupa Lieovog tipa ili alternirana grupa ili neka od sljedećih 26 sporadičnih grupa:

$M_{11}, M_{12}, M_{23}, M_{24}, J_1, J_2, J_3, J_4, HS, Co_1, Co_2, Co_3, He, Mc, Suz, Fi_{22}, Fi_{23}, Fi_{24}, F_1 = M(\text{"the Monster"- čudovište}), F_2, F_3, F_5, Ly, Ru, O'N.$

Kako smo naveli, završetkom klasifikacije jednostavnih sporadičnih grupa u teoriji grupa preostalo je za klasificirati konačne p-grupe. No ta klasifikacija, u klasičnom smislu nabrajanja svih mogućih konačnih p-grupa, nije uistinu niti moguća. Naime, konačna p-grupa ima previše normalnih podgrupa, što za posljedicu ima postojanje izuzetno velikog broja neizomorfnih p-grupa nekog određenog reda (npr. postoji 267 neizomorfnih 2-grupa reda 2^6, dok je grupa reda 2^{10} već 49487653422). Stoga se pristupilo drugačijim načinima klasifikacije p-grupa. Grupe se klasificiraju s obzirom na njihova različita svojstva koja su ispunjena za dovoljno velike skupove/klase grupa. Štoviše, ta svojstva pokušavaju se zadati tako da pokrivaju čak i sve konačne p-grupe (npr. proučavaju se regularne i iregularne grupe, modularne i nemodularne grupe, p-grupe s "malom" abelovom podgrupom i p-grupe s "velikom" abelovom podgrupom...). Svojstva, odnosno probleme vezane uz dotična svojstva, dijelimo u 4 glavne skupine: $\mathcal{A}$-problemi vezani uz abelovost grupa, Ω-problemi vezani uz Ω_n podgrupe, M-problemi vezani uz metacikličnost grupa i tzv. specijalni problemi. Važno je napomenuti da su od velikog značaja konačne 2-grupe koje su nerijetko i puno kompleksnije za proučavanje. Naime, ako je G neabelova konačna prosta grupa i struktura njezine Sylowljeve 2-podgrupe P je poznata, onda je određena gotovo čitava struktura grupe G.

Da bismo razumjeli ove posljednje rečenice krenimo s osnovama teorije konačnih p-grupa sljedeći primjer predavanja profesora Janka.

2 Uvod u konačne p-grupe

2.1 Grupe

Definicija 2.1. *Grupa je uređeni par* $(G, \cdot)$*, gdje je* G *neprazan skup, a* $" \cdot "$ *binarna operacija za koju vrijedi:*
$(G1)$ *za svaki par elemenata* $x, y \in G$ *je* $x \cdot y \in G$ *(zatvorenost);*
$(G2)$ *za sve elemente* $x, y, z \in G$ *vrijedi* $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ *(asocijativnost);*
$(G3)$ *postoji element* $1 \in G$ *takav da je za sve* $g \in G$

$$1 \cdot g = g \cdot 1 = g \ (1 - \textit{neutralni element grupe } G);$$

$(G4)$ *za svaki element* $g \in G$ *postoji element* $g^{-1} \in G$ *takav da je*

$$g \cdot g^{-1} = g^{-1} \cdot g = 1 \ (g^{-1} - \textit{inverzni element elementa } g).$$

Grupa G *je abelova ili komutativna ako za sve* $x, y \in G$ *vrijedi još i*

$$x \cdot y = y \cdot x \ (\textit{komutativnost}).$$

Napomena 2.1. *Lako se pokazuje da je* $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.

Dokaz. Iz tvrdnje $(x \cdot y)^{-1} \cdot (x \cdot y) = 1$, množenjem zdesna prvo elementom y^{-1} pa zatim elementom x^{-1} slijedi tvrdnja. □

Definicija 2.2. *Kažemo da je grupa G konačna ako ima konačan broj elemenata. Broj elemenata grupe G nazivamo red grupe i označavamo s $|G|$.*

Kažemo da je grupa G p-grupa ako je njezin red potencija prostog broja p, tj. $|G| = p^n, n \in \mathbb{N}$.

U daljnjem tekstu pretpostavljamo da su sve promatrane grupe konačne.

Definicija 2.3. *Umnožak podskupova $A, B \subseteq G$ grupe G je skup*

$$A \cdot B = \{a \cdot b \mid a \in A, b \in B\}.$$

Za jednočlan skup $B = \{b\}$ pišemo $A \cdot B = A \cdot \{b\} = \{a \cdot b \mid a \in A\} = Ab$. Inverzni skup podskupa $A \subseteq G$ je $A^{-1} = \{a^{-1} \mid a \in A\}$.

Napomena 2.2. *Za umnožak skupova $A, B, C \subseteq G$ očigledno vrijedi:*

1. $(A \cdot B) \cdot C = A \cdot (B \cdot C)$,
2. $A \cdot 1 = 1 \cdot A = A$,
3. $|Ab| = |bA| = |A|$, *gdje s $|A|$ označavamo kardinalni broj skupa A.*

Definicija 2.4. *Za neprazan podskup H grupe G kažemo da je podgrupa grupe G ukoliko je i H grupa s obzirom na operaciju iz G.*
Podgrupu označavamo s $H \leq G$. Ako je $H \neq G$, onda pišemo $H < G$ i kažemo da je H prava podgrupa grupe G. Ako je $H = \{1\}$, kažemo da je H trivijalna podgrupa od G.
Kažemo da je M maksimalna podgrupa grupe G ako iz $M \leq H < G$ slijedi $H = M$.

Teorem 2.1. *Podskup $H \subseteq G$ grupe G je podgrupa grupe G onda i samo onda ako je $HH \subseteq H$, tj.*

$$H \leq G \Leftrightarrow HH \subseteq H.$$

Dokaz. Ako je $H \leq G$, očigledno je $HH \subseteq H$. Obratno, iz $HH \subseteq H$ za bilo koji $a \in H$ vrijedi $aH \subseteq H$. Zbog $|aH| = |H|$ je $aH = H$, pa postoji $x \in H$ takav da je $ax = a$, dakle $x = 1 \in H$. Onda opet postoji $y \in H$ za koji je $ay = 1$, dakle $y = a^{-1} \in H$. Stoga je H podgrupa grupe G. □

Teorem 2.2. *Za podgrupu $H \leq G$ i podskup $A \subseteq G$ vrijedi*

$$A \subseteq H \Leftrightarrow AH = H \Leftrightarrow HA = H.$$

Dokaz. Po teoremu 2.1 iz $A \subseteq H$ slijedi $AH = H, HA = H$. Obratno, iz $AH = H$ i $a \in A$ slijedi $aH \subseteq H$, pa je i $a \cdot 1 \in H$, tj. $A \subseteq H$. $\square$

Teorem 2.3. *Neka je G grupa i $H, K \leq G$. Onda je $H \cap K$ također podgrupa grupe G.*

Definicija 2.5. *Neka je G grupa, $X \neq \emptyset$, $X \subseteq G$. Najmanju podgrupu grupe G koja sadrži X označavamo s $\langle X \rangle$, dakle je*

$$\langle X \rangle = \bigcap_{X \subseteq H \leq G} H,$$

a sastoji se od svih mogućih umnožaka elemenata iz X i njihovih inverznih elemenata. Elemente iz X zovemo izvodnicama (generatorima) podgrupe $\langle X \rangle$.

Ako je $Y \subseteq G$ takav da vrijedi $\langle Y \rangle = G$, onda kažemo da je grupa G izvedena (generirana) podskupom Y.

Neka je $a \in G$. Grupa $\langle \{a\} \rangle = \langle a \rangle$ izvedena (generirana) elementom a zove se ciklička grupa elementa a. Red elementa a definira se kao red grupe $\langle a \rangle$. Označava se s

$$|\langle a \rangle| = |a| = o(a).$$

Skup svih elemenata reda k, pri čemu k dijeli $|G|$, iz grupe G označavamo s

$$O_k(G) = \{g \in G \mid o(g) = k\}.$$

Definicija 2.6. *Za podgrupu H grupe G i za svaki element $g \in G$, podskup $Hg = \{hg \mid h \in H\}$ zovemo desna klasa. Analogno definiramo i lijevu klasu gH. Pritom je $|Hg| = |gH| = |H|$.*

Teorem 2.4. *Ako je $H \leq G$, onda je skup svih različitih desnih klasa $\{Hg_1, ..., Hg_s\}$ grupe G s obzirom na podgrupu H particija grupe G, tj.*

$$G = \bigsqcup_{i=1}^{s} Hg_i,$$

pri čemu s $\bigsqcup$ označavamo disjunktnu uniju skupova. Stoga je

$$|G| = \sum_{i=1}^{s} |Hg_i| = s|H|.$$

Broj s jednak je kvocijentu $\dfrac{|G|}{|H|}$ i označavamo ga $s = |G : H|$, te zovemo indeks podgrupe H u grupi G.

Korolar 2.1. (a) *Red podgrupe je djelitelj reda grupe.*

(b) *Svaka grupa prostog reda p je ciklička, jer grupa reda p nema netrivijalnih pravih podgrupa, pa svaki element grupe osim neutralnog izvodi (generira) cijelu grupu.*

Teorem 2.5. *Neka je $H \leq G$ i neka su $g, k \in G$. Tad je $Hg = Hk$ onda i samo onda ako je $gk^{-1} \in H$.*

Dokaz. Ako je $Hg = Hk$, onda je $Hgk^{-1} = H$. Dakle, prema teoremu 2.2 $gk^{-1} \in H$. Obratno, ako je $gk^{-1} \in H$, onda je $Hgk^{-1} = H$. Množenjem elementom k zdesna slijedi $Hg = Hk$. $\square$

Teorem 2.6. **(*O indeksima*)**
Neka je $H \leq K \leq G$. Onda vrijedi

$$|G : H| = |G : K| \cdot |K : H|.$$

Teorem 2.7. *Neka su H i K podgrupe grupe G. Onda su $H, K \subseteq K \cdot H$ i vrijedi*

$$|K \cdot H| = \frac{|K| \cdot |H|}{|K \cap H|} \quad i \quad |H \cdot K| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

Dokaz. Prema teoremu 2.1 vrijedi $H \cap K \leq K$. Onda imamo particiju $K = \bigsqcup_i (H \cap K)k_i$ grupe K nad podgrupom $H \cap K$. Tvrdimo da je $H \cdot K = \bigsqcup_i Hk_i$ particija podskupa $H \cdot K$. Naime, neka je $Hk_i = Hk_j$. Onda je prema teoremu 2.5 $k_i{k_j}^{-1} \in H$. Dakle, $k_i{k_j}^{-1} \in H \cap K$. Onda mora biti $(H \cap K)k_i = (H \cap K)k_j$. Zaključci vrijede i u obratnom smjeru. Slijedi da skup $H \cdot K$ ima $|H \cdot K| = |H| \cdot |K : (H \cap K)|$ elemenata. Dakle, $|H \cdot K| = \frac{|H| \cdot |K|}{|K \cap H|}$. Analogno slijedi i druga jednakost. $\square$

Teorem 2.8. *Neka su $H, K \leq G$. Podskup $H \cdot K$ je podgrupa od G onda i samo onda ako je $H \cdot K = K \cdot H$. Onda kažemo da su podgrupe H i K permutabilne.*

Teorem 2.9. *Ako grupa G nema pravih podgrupa, onda je $G = \{1\}$ ili je G ciklička grupa prostog reda.*

Dokaz. Jedine podgrupe od G su G i $\{1\}$. Ako je $G = \{1\}$ dokaz je gotov. Stoga, pretpostavimo $G \neq \{1\}$. Neka je $x \in G$, $x \neq 1$ bilo koji element. Sada je podgrupa $\langle x \rangle \neq \{1\}$, pa je $\langle x \rangle = G$ i $|\langle x \rangle| = |x| = |G|$.
Ako je $|G| = n_1 \cdot n_2$, $n_1, n_2 > 1$, onda je $|\langle x^{n_1} \rangle| = |x^{n_1}| = n_2$, pa bi bilo $\{1\} < \langle x^{n_1} \rangle < G$, što je u protuslovlju s pretpostavkom. Dakle je $|G| = p$, za neki prosti broj p. $\square$

2.2 Normalizatori i centralizatori podgrupa

Definicija 2.7. *Neka su $g \in G$ i $x \in G$. Onda preslikavanje $\varphi : G \to G$, $\varphi : x \mapsto \varphi_x(g) := g^{-1}xg$, zovemo konjugiranje elementom g, a $\varphi_x(g) := g^{-1}xg$ zovemo g-konjugat elementa x. Za podskup $S \subseteq G$ je g-konjugat skupa S skup*

$$\varphi_S(g) = \{\varphi_s(g) \mid s \in S,\ g \in G\}.$$

Definicija 2.8. *Neka je G grupa. Za $x, y \in G$ označavamo $x \sim y$ ako je x konjugiran s y, tj. onda i samo onda ako postoji $g \in G$ takav da je $\varphi_x(g) = y$.*

Teorem 2.10. *Preslikavanje $\varphi : G \to G$, $x \mapsto \varphi_x(g)$, $\forall x \in G$, je bijekcija. Vrijedi $\varphi_x(gh) = \varphi_x(\varphi_x(g))(h)$, $\forall x, g, h \in G$.*
Relacija $\sim$ je relacija ekvivalencije. Klase ove relacije ekvivalencije zovu se konjugirane klase i one tvore particiju grupe G, tj.

$$G = \bigsqcup_{i=1}^{s} K_i = K_1 \cup K_2 \cup ... \cup K_s,$$

pri čemu uzimamo da je $K_1 = \{1\}$. Klasu K_i, za neki $i \in \{1, ..., s\}$, tvore svi elementi dobiveni konjugiranjem bilo kojeg elementa $x_i \in K_i$, tj.

$$K_i = \{\varphi_{x_i}(g) \mid g \in G\}.$$

Broj s zove se klasni broj. Vrijedi klasna jednakost

$$|G| = n = k_1 + k_2 + ... + k_s,$$

gdje je $|K_i| = k_i$, te $k_1 = 1$.

Dokaz. Za svaki $x \in G$ je $x = g^{-1}(gxg^{-1})g = \varphi_{gxg^{-1}}(g)$, pa je φ surjekcija. Ako je $\varphi_x(g) = \varphi_y(g)$, tj. $g^{-1}xg = g^{-1}yg$ množeći s g i s g^{-1} slijeva, odnosno s desna dobivamo $x = y$, pa je φ injekcija. Također je $\varphi_x(gh) = (gh)^{-1}x(gh) = h^{-1}(g^{-1}xg)h = \varphi_{\varphi_x(g)}(h)$. Ostale tvrdnje se lako provjeravaju na temelju definicija. $\square$

Definicija 2.9. *Kažemo da je podgrupa H grupe G normalna podgrupa u G, te pišemo $H \trianglelefteq G$, ako vrijedi*

$$\varphi_H(g) = H,\ \forall g \in G,$$

tj. ako vrijedi

$$Hg = gH,$$

dakle ako su lijeve klase podgrupe H jednake desnim.

Definicija 2.10. *Normalizator podskupa S u grupi G je skup*

$$N_G(S) = \{g \in G \mid \varphi_S(g) = S\}.$$

Centralizator podskupa S u grupi G je skup

$$C_G(S) = \{g \in G \mid \varphi_s(g) = s, \forall s \in S\}.$$

Lako se vidi da su $N_G(S)$ i $C_G(S)$ podgrupe grupe G i da je $C_G(S) \trianglelefteq N_G(S)$ (v. teorem 2.19 za slučaj kad je S podgrupa).

Teorem 2.11. (*O normalizatoru*)
Broj elemenata skupa $\varphi_S(g) = \{\varphi_S(g) \mid g \in G\}$ svih različitih g-konjugata $\varphi_S(g)$ podskupa S u grupi G jednaka je indeksu normalizatora $N_G(S)$ od S u G, tj.

$$|\varphi_S(g)| = |G : N_G(S)|.$$

Dokaz. $\varphi_S(g_1) = \varphi_S(g_2) \Leftrightarrow \varphi_S(g_1 g_2^{-1}) = \varphi_S(g_2 g_2^{-1}) \Leftrightarrow \varphi_S(g_1 g_2^{-1}) = \varphi_S(1) = S \Leftrightarrow g_1 g_2^{-1} \in N_G(S) \Leftrightarrow N_G(S)g_1 = N_G(S)g_2$, pa različitih g-konjugata $\varphi_S(g)$ ima toliko koliko i različitih konjugiranih klasa podgrupe $N_G(S)$ u G, tj. $|\varphi_S(G)| = |G : N_G(S)|$. □

Definicija 2.11. *Neka je $N \trianglelefteq G$ i $G/N = \{gN \mid g \in G\}$. Onda je G/N grupa za binarnu operaciju*

$$g_1 N \cdot g_2 N = g_1 g_2 NN = g_1 g_2 N.$$

Grupa G/N zove se kvocijentna grupa grupe G obzirom na N i njezin je red

$$|G/N| = |G : N|.$$

Označimo li $gN = \overline{g}$, pišemo $G/N = \overline{G} = \{\overline{g} \mid g \in G\}$.

Teorem 2.12. (*Zakon korespodencije*)
Neka je $N \trianglelefteq G$. Onda između skupa svih podgrupa H grupe G koje sadrže N i svih podgrupa $\overline{H} = H/N$ kvocijentne grupe $\overline{G} = G/N$ postoji bijekcija,

$$\overline{H} \longleftrightarrow H = \bigcup_{hN \in \overline{H}} hN.$$

Naime, ako je $H \leq G$ onda je i $\overline{H} \leq \overline{G}$ i obratno.

Dokaz. Za $N \leq H \leq G$ je $H/N = \overline{H} = \{hN \mid h \in H\}$, pa je $h_1N \cdot h_2N = h_1h_2N \in \overline{H}$, te je $\overline{H} \leq \overline{G}$ po teoremu 2.1.
Obratno, ako je $\overline{H} \leq \overline{G}$ onda je $H = \bigcup_{hN \in \overline{H}} hN \leq G$, jer iz $h_1, h_2 \in H$ slijedi da postoje $h'N, h''N \in \overline{H}$ takvi da je $h_1 \in h'N$, $h_2 \in h''N$, pa je $h_1h_2 \in h'Nh''N = h'h''N \subseteq H$, tj. $H \leq G$ također po teoremu 2.1. $\square$

Napomena 2.3. *Također, uz uvjete teorema 2.12, vrijedi* $H \trianglelefteq G \Leftrightarrow \overline{H} \trianglelefteq \overline{G}$.

Definicija 2.12. *Neka su G i H grupe. Homomorfizam iz G u H je preslikavanje $\varphi : G \to H$ takvo da $\forall x, y \in G$ vrijedi*

$$\varphi(xy) = \varphi(x)\varphi(y).$$

Slika od φ je skup $Im\varphi = \varphi(G) = \{\varphi(x) \mid x \in G\}$.
Jezgra od φ je skup $Ker\varphi = \{x \in G \mid \varphi(x) = 1_H\}$.

Lako se provjeri da je $\varphi(1_G) = 1_H$, $\varphi(x^{-1}) = (\varphi(x))^{-1}$.
Također vrijedi: $Im\varphi \leq H$ i $Ker\varphi \trianglelefteq G$.

Definicija 2.13. *Ako je homomorfizam $\varphi : G \to H$ bijekcija kažemo da je φ izomorfizam i da je grupa G izomorfna grupi H, što označavamo s $G \cong H$.*

Izomorfizam $\alpha : G \to G$ zove se automorfizam grupe G.
S $Aut(G)$ označavamo grupu svih automorfizama grupe G.

Teorem 2.13. (***Prvi teorem o homomorfizmu***)
Ako je $\varphi : G \to H$ homomorfizam grupa G i H, onda je

$$G/Ker\varphi \cong Im\varphi.$$

Dokaz. Za svaki $g \in Ker\varphi$ vrijedi $\varphi(g) = 1$. Označimo s $Ker\varphi = N$. Imamo: $\varphi(xn) = \varphi(x)\varphi(n) = \varphi(x)$, $\forall n \in N, \forall x \in G$. Dakle svi elementi iz klase xN preslikani su na $\varphi(x)$. Vrijedi $\forall x, y \in G$:

$$\varphi(x)(\varphi(y))^{-1} = 1 \Rightarrow \varphi(x)\varphi(y^{-1}) = 1 \Rightarrow \varphi(xy^{-1}) = 1 \Rightarrow xy^{-1} \in \mathbb{N},$$

tj. po teoremu 2.5 slijedi $xN = yN$. Dakle, x i y leže u istoj klasi. To je ekvivalentno tvrdnji da elementi iz različitih klasa imaju različite slike, tj. preslikavanje $f : G/N \to Im\varphi$, $f : xN \mapsto \varphi(x)$, je injekcija. Također, f je očigledno i surjekcija. Budući da je

$$f(xN \cdot yN) = f(xyN) = \varphi(xy) = \varphi(x) \cdot \varphi(y) = f(xN) \cdot f(yN),$$

stoga je f homomorfizam, tj. izomorfizam. $\square$

Teorem 2.14. (***Drugi teorem o izomorfizmu***)
Neka je $N \trianglelefteq G$ i $H \leq G$. Onda je $HN = \langle H, N \rangle$ očigledno podgrupa grupe G, $N \trianglelefteq HN$, $H \cap N \trianglelefteq H$ i vrijedi

$$H/(H \cap N) \cong HN/N.$$

Dokaz. Promatrajmo preslikavanje $\varphi : H \to HN/N$ takvo da je $\varphi(x) = xnN = xN$, $\forall x \in H$, $\forall n \in \mathbb{N}$. Kako je $\varphi(xy) = xyN = (xN)(yN) = \varphi(x)\varphi(y)$, $\forall x, y \in H$, očigledno je φ homomorfizam. Vrijedi $Ker\varphi = H \cap N$. Naime,

$$\begin{aligned} Ker\varphi &= \{x \in H \mid \varphi(x) = 1_{HN/N}\} \\ &= \{x \in H \mid xN = N\} \\ &= \{x \in H \mid x \in N\} \\ &= H \cap N. \end{aligned}$$

Surjektivnost od φ slijedi iz $xnN = xN = \varphi(x)$. Sada prema teoremu 2.13 slijedi $H \cap N \trianglelefteq H$ i $H/(H \cap N) \cong HN/N$. □

Teorem 2.15. (***Treći teorem o izomorfizmu***)
Neka je $K \trianglelefteq G$, $N \trianglelefteq G$ i $N \trianglelefteq K$. Onda je $K/N \trianglelefteq G/N$ i vrijedi

$$(G/N)/(K/N) \cong G/K.$$

Dokaz. Definiramo preslikavanje $\varphi : G/N \to G/K$ s $\varphi(gN) = gK$. Pretpostavimo da je $xN = yN$. Slijedi po teoremu 2.5 $y^{-1}x \in N$. Kako je $N \leq K$, slijedi $y^{-1}x \in K$, pa je opet po teoremu 2.5 $xK = yK$, tj. $\varphi(xN) = \varphi(yN)$. Dakle, φ je dobro definirano preslikavanje.
Tvrdimo da je φ homomorfizam. Naime,

$$\varphi(xN)\varphi(yN) = (xK)(yK) = xyK = \varphi(xyN).$$

Očigledno je φ surjekcija i

$$\begin{aligned} Ker\varphi &= \{gN \in G/N \mid \varphi(gN) = 1_{G/K}\} \\ &= \{gN \in G/N \mid gK = K\} \\ &= \{gN \in G/N \mid g \in K\} \\ &= K/N. \end{aligned}$$

Sada prema teoremu 2.13 slijedi tvrdnja. □

Definicija 2.14. *Podgrupa $Z(G) = \{g \in G \mid gx = xg, \forall x \in G\}$ zove se centar grupe G.*
Za abelovu grupu G vrijedi $Z(G) = G$, inače $Z(G) < G$.
Vrijedi općenito $Z(G) \trianglelefteq G$ i $Z(G) = C_G(G)$.

Teorem 2.16. *Neka je $x \in G$. Definiramo preslikavanje $\varphi_x : G \to G$ s $\varphi_x(g) = x^{-1}gx$, $\forall g \in G$. Preslikavanje φ_x je automorfizam grupe G, koji zovemo unutarnji automorfizam određen elementom x. S $Int(G)$ označavamo skup svih unutarnjih automorfizama grupe G. Vrijedi: $Int(G) \trianglelefteq Aut(G)$ i*

$$G/Z(G) \cong Int(G).$$

Dokaz. Tvrdimo da je φ_x automorfizam.

(a) Za sve $g, h \in G$ slijedi

$$\varphi_x(g)\varphi_x(h) = (x^{-1}gx)(x^{-1}hx) = x^{-1}(gh)x = \varphi_x(gh).$$

Dakle, φ_x je homomorfizam.

(b) Ako je $\varphi_x(g) = \varphi_x(h)$, onda je $x^{-1}gx = x^{-1}hx \;\Rightarrow\; g = h$. Dakle, φ_x je injekcija.

(c) Za dani $h \in G$ vrijedi $\varphi_x(xhx^{-1}) = x^{-1}(xhx^{-1})x = h$, pa slijedi da je φ_x surjekcija.

(d) Pokazali smo da je φ_x automorfizam. Sada definiramo preslikavanje:
$\Phi : G \to Aut(G)$ sa $\Phi(x) = \varphi_x$.
Za svaki $g \in G$ vrijedi

$$(\varphi_x \circ \varphi_y)(g) = \varphi_y(\varphi_x(g)) = \varphi_y((x^{-1}gx)) = y^{-1}x^{-1}gxy = \varphi_{xy}(g),$$

pa slijedi $\varphi_x \circ \varphi_y = \varphi_{xy}$. Poradi $\Phi(x)\Phi(y) = \varphi_x \circ \varphi_y = \varphi_{xy} = \Phi(xy)$ slijedi da je Φ homomorfizam.

Očigledno je $Im\Phi = Int(G)$ i

$$\begin{aligned} Ker\phi &= \{x \in G \mid \Phi(x)(:= \varphi_x) = id_G\} \\ &= \{x \in G \mid \varphi_x(g) = id_G(g),\ \forall g \in G\} \\ &= \{x \in G \mid x^{-1}gx = g,\ \forall g \in G\} \\ &= \{x \in G \mid xg = gx,\ \forall g \in G\} \\ &= Z(G). \end{aligned}$$

Nadalje, ako je $\psi \in Aut(G)$, $\varphi_x \in Int(G)$, onda je
$(\psi^{-1}\varphi_x\psi)(g) = \psi(x^{-1}(\psi^{-1}(g)x) = (\psi(x))^{-1}g\psi(x) = \varphi_{\psi(x)}(g)$,
tj. $\psi^{-1}\varphi_x\psi = \varphi_{\psi(x)} \in Int(G)$, pa je $\psi^{-1}Int(G)\psi \subseteq Int(G)$. Dakle, $\psi^{-1}Int(G)\psi = Int(G)$, te je $Int(G) \trianglelefteq Aut(G)$.
Sada prema teoremu 2.13 slijedi, uz $Z(G) \trianglelefteq G$, da je $G/Z(G) \cong Int(G)$.□

Definicija 2.15. *Podgrupa M je karakteristična u G ako je $\varphi(M) = M$, za svaki $\varphi \in Aut(G)$. Pišemo M char G.*

Budući da je $Int(G) \leq Aut(G)$ očigledno vrijedi:

Teorem 2.17. *Neka je $M \leq G$ i M char G. Onda je $M \trianglelefteq G$.*

Teorem 2.18. (***O cikličkom proširenju centra***)
Ako je $G/Z(G)$ ciklička grupa, onda je G abelova grupa.

Dokaz. Kako je $G/Z(G)$ ciklička grupa, slijedi $G = \langle a, Z(G) \rangle$, za neki $a \in G \setminus Z(G)$, što je abelova grupa, jer sve izvodnice (generatori) međusobno komutiraju. □

Teorem 2.19. *Za svaku podgrupu H grupe G vrijedi $C_G(H) \trianglelefteq N_G(H)$ i kvocijentna grupa $N_G(H)/C_G(H)$ je izomorfna nekoj podgrupi grupe $Aut(H)$.*

Dokaz. Neka je $H \leq G$. Promatramo $N_G(H)$. Ako je $g \in N_G(H)$, onda je $\varphi_g(H) = H$. Dakle je $\varphi_g|_H : h \mapsto \varphi_g(h)$, $h \in H$, automorfizam od H. Sada je preslikavanje $\Phi : N_G(H) \longrightarrow Aut(H)$, $\Phi : g \mapsto \varphi_g|_H$ homomorfizam, jer je $\Phi(g'g'') = \varphi_{g'g''}(h) = (g'')^{-1}\varphi_{g'}(h)g'' = (g'')^{-1}(g')^{-1}hg'g'' = (g'g'')^{-1}hg'g''$, tj. na H je $\varphi_{g'g''} = \varphi_{g'} \circ \varphi_{g''}$, dakle

$$\Phi(g'g'') = \Phi(g') \cdot \Phi(g'').$$

Očigledno je $Ker\Phi = C_G(H)$. Sada, prema teoremu 2.13 slijedi $C_G(H) \trianglelefteq N_G(H)$ i kvocijentna grupa $N_G(H)/C_G(H)$ je izomorfna nekoj podgrupi od $Aut(H)$. □

Teorem 2.20. *Neka G p-grupa i $N \trianglelefteq G$, $N \neq \{1\}$. Onda je $N \cap Z(G) \neq \{1\}$. Posebice je uvijek $Z(G) \neq \{1\}$.*

Dokaz. Neka je $N \trianglelefteq G$ i $|G| = p^n$, gdje je p prosti broj i $n \in \mathbb{N}$. Imamo particiju $N = \bigsqcup_{i=0}^{s} N_i$ grupe N, gdje su N_i konjugirane klase od N s obzirom na G. Neka je $|N_i| = k_i$ broj elemenata klase N_i. Vrijedi klasna jednakost za N

$$|N| = k_0 + k_1 + ... + k_s.$$

Označimo li s $N_0 = \{1\}$ onda je $k_0 = 1$, te $|N| = p^r$, $r \leq n$. Ako je $x_i \in N_i$ onda je po teoremu 2.11 $k_i = |G : C_G(x_i)| = p^{r_i}$, tj. k_i je uvijek p-potencija za $1 \leq i \leq s$. Naime, za jednočlan skup $S = \{x\}$ je $C_G(\{x\}) = N_G(\{x\})$. Iz klasne jednakosti za N slijedi da među njima mora biti još konjugiranih klasa duljine 1, dakle takvih $x_i, i > 1$, za koje je $C_G(x_i) = G$, tj. $x_i \in Z(G)$. Stoga postoje netrivijalni elementi iz $Z(G)$ koji su sadržani u N. □

Korolar 2.2. *Ako je N minimalna normalna podgrupa p-grupe G, u oznaci* $N \in \mathcal{A}_1$*, tj. vrijedi da je* $N \trianglelefteq G$ *i* $\{1\}$ *je jedina normalna podgrupa grupe G sadržana u N, onda je* $N \leq Z(G)$ *i* $|N| = p$*. Nadalje vrijedi da je svaka grupa N reda* p^2 *abelova grupa pri čemu p dijeli* $|Aut(N)|$*, ali* p^2 *ne dijeli* $|Aut(N)|$*.*

Dokaz. Za dokaz vidjeti teorem 2.1.
Vrijedi $|Aut(N)| = |GL_2(p)| = (p^2 - 1) \cdot (p-1) \cdot p$, gdje je općenito skup svih $n \times n$ regularnih matrica s cijelim brojevima iz skupa $\{0, 1, ..., p-1\}$, za p prost broj, kao pripadajućim elementima, uz operaciju množenja matrica konačna grupa te ju označavamo s $(GL_n(p), \cdot)$ i nazivamo opća linearna grupa reda n. □

Teorem 2.21. *Neka je E elementarno abelova grupa reda* p^n*,* $E \cong E_{p^n}$*. Onda je*

$$|Aut(E)| = |GL_n(p)| = (p^n - 1) \cdot (p^{n-1} - 1) \cdot ... \cdot (p-1) \cdot p.$$

Dokaz. *([3], 194)* □

Definicija 2.16. *Neka je G p-grupa reda* p^n*, gdje je p prosti broj. Definiramo gornji centralni niz:*
$Z_0(G) = \{1\}$*,* $Z_1(G) = Z(G)$*, i općenito*

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)).$$

Po teoremu 2.20 je $Z(G/Z_i(G)) \neq \{1_{G/Z_i(G)}\}$*, za* $Z_i(G) < G$*.*
Najmanji prirodan broj c takav da je $Z_c(G) = G$ *zove se klasa nilpotentnosti p-grupe G i pišemo* $c = cl(G)$*.*
Nadalje, definiramo donji centralni niz:
$K_1(G) = G$, $K_2(G) = G' = [G, G] \trianglelefteq G$, $K_3(G) = [G, K_2(G)] \trianglelefteq G, ..., K_n(G) = [G, K_{n-1}(G)] \trianglelefteq G, itd.$
Za konačnu p-grupu G reda p^n *gdje je p prosti broj, vrijedi*

$$K_1(G) = G > K_2(G) > K_3(G) > ... > K_{r+1}(G) = \{1\},$$

i duljina donjeg centralnog niza jednaka je r*.*
Najmanji prirodan broj c takav da je $Z_c(G) = G$ *nazivamo klasa nilpotentnosti p-grupe G i označavamo s* $cl(G)$*.*

Teorem 2.22. *Neka je G konačna p-grupa klase nilpotentnosti c. Onda je* $r = c$*, tj. duljina donjeg centralnog niza jednaka je duljini gornjeg centralnog niza.*

2.3 Komutatori i komutatorske grupe

U teoriji konačnih p-grupa, pa tako i kod profesora Janka i profesora Berkovicha, uobičajena oznaka preslikavanja $\varphi_x(g)$, konjugiranja elementa x elementom g, je x^g te ćemo u nastavku rada upotrebljavati takvu notaciju.

Definicija 2.17. *Neka su $x, y \in G$. Komutator elemenata x i y je*

$$[x, y] := x^{-1}y^{-1}xy.$$

Očigledno je $xy = yx[x, y]$.
Ako su $A, B \leq G$ onda je njihova komutatorska podgrupa

$$[A, B] = \langle [a, b] \mid a \in A, b \in B \rangle.$$

Grupu $G' = [G, G]$ zovemo komutatorska podgrupa grupe G.

Teorem 2.23. *Za svaku grupu G vrijedi*

$$G' \text{ char } G, \text{ pa je } G' \trianglelefteq G.$$

Dokaz. Neka je $[a, b] \in G'$, za $a, b \in G$, i $\varphi \in Aut(G)$. Onda vrijedi $[a, b]^\varphi = [a^\varphi, b^\varphi] \in G'$. Dakle, G' je φ-stalna grupa, tj. $G'^\varphi = G'$, za sve automorfizme φ, tj. G' char G, a po teoremu 2.17 i $G' \trianglelefteq G$. □

Teorem 2.24.
(a) Grupa G je abelova onda i samo onda ako je $G' = \{1\}$, pa ponekad kraće pišemo $G' = 1$.

(b) Grupa G' je najmanja normalna podgrupa od G takva da je G/G' abelova grupa.

Dokaz. (a) Trivijalno.
(b) Neka je $N \trianglelefteq G$. Grupa G/N je abelova grupa onda i samo onda ako je $G' \leq N$. Naime, ako je G/N abelova grupa, onda $\forall a, b \in G$ vrijedi:

$$aN \cdot bN = bN \cdot aN \;\Rightarrow abN = baN.$$

Množenjem gornje jednakosti slijeva elementima b^{-1} i a^{-1} slijedi

$$a^{-1}b^{-1}abN = N \;\Rightarrow a^{-1}b^{-1}ab \in N,$$

tj. $[a, b] \in N$. Dakle, $[x, y] \in N$, $\forall x, y \in G \;\Rightarrow G' \leq N$. Obratno, iz $G' \leq N$ slijedi $aN \cdot bN = abN = ba[a, b]N = baN = bN \cdot aN$, jer je $[a, b] \in G' \leq N$. Dakle je G/N abelova grupa.
Ako sada uzmemo $N = G'$ slijedi tvrdnja. □

Lako se provjeri da vrijedi:

Teorem 2.25. *Neka su $x, y, z \in G$. Onda vrijedi:*

(a) $[xy, z] = [x, z]^y [y, z]$,
(b) $[x, yz] = [x, z][x, y]^z$,
(c) $[x, y]^{-1} = [y, x]$.

Teorem 2.26. *Neka je $A \leq G, B \subseteq G$. Ako je $[A, B] \leq A$ onda je $B \subseteq N_G(A)$.*

Dokaz. Za $a \in A, b \in B$ je po pretpostavci $[a, b] = a^{-1}b^{-1}ab = a^{-1}a^b \in A$, pa je $a^b \in A$. Dakle, $B \subseteq N_G(A)$. □

Teorem 2.27. **(*O normalizatoru u p-grupi G*)**
Neka je G p-grupa i neka je $H < G$. Onda je $N_G(H) > H$.

Dokaz. Promatrajmo gornji centralni niz grupe G:

$$\{1\} = Z_0(G) < Z_1(G) < Z_2(G) < ... < Z_c(G) = G.$$

Neka je $i \in \{0, 1, ..., c\}$ indeks takav da je

$$Z_i(G) \leq H, \text{ ali } Z_{i+1}(G) \nleq H.$$

Prema definiciji centra znamo

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)).$$

No onda je $[G, Z_{i+1}(G)] \leq Z_i(G)$, a $H < G$, pa je i

$$[H, Z_{i+1}(G)] \leq Z_i(G) \leq H.$$

Stoga je po teoremu 2.26 $Z_{i+1}(G) \leq N_G(H)$, tj. $N_G(H) > H$. □

Korolar 2.3. *Ako je H maksimalna podgrupa p-grupe G onda je $H \trianglelefteq G$ i $|G : H| = p$.*

Dokaz. Po teoremu 2.27 je $N_G(H) > H$, pa je po definiciji 2.4 $N_G(H) = G$.
Dakle je $H \trianglelefteq G$ i G/H nema netrivijalnih pravih podgrupa.
Stoga je $|G : H| = p$. □

Definicija 2.18. *Kompozicioni niz p-grupe G je niz*

$$G_0 = \{1\} \lhd G_1 \lhd G_2 \lhd .... \lhd G_n = G,$$

gdje je G_i maksimalna podgrupa od G_{i+1}, i za svaku kvocijentnu grupu vrijedi $|G_{i+1}/G_i| = p$.

Definicija 2.19. *Niz* $N_0 = \{1\} \leq N_1 \leq .... \leq N_n = G$ *je glavni niz grupe* G *ako je za svaki* $i \in \{0, 1, ..., n-1\}$ $N_i \trianglelefteq G$ *i* N_{i+1}/N_i *minimalna normalna podgrupa od* G/N_i.

Teorem 2.28. *Za svaku podgrupu postoji kompozicioni niz, za normalnu podgrupu postoji glavni niz.*

Teorem 2.29. (***N. Blackburn***)
Neka je G *p-grupa maksimalne klase nilpotentnosti i* $|G| = p^n$, $n \in \mathbb{N}$. *Onda za svaki* $k \in \mathbb{N}$, $0 \leq k \leq n-2$, *postoji jedinstvena normalna podgrupa* N *grupe* G *takva da je* $|N| = p^k$ *i* $N = Z_k(G) = K_{n-k}(G)$.

Dokaz. ([2], *8-10*) □

Korolar 2.4. *Ako je* H *podgrupa od* G *reda* p^k, *onda* H *ima za svaki* r, $0 < r < k$, *neku podgrupu reda* p^r. *Ako je* $H \trianglelefteq G$ *onda za svaki* r, $0 < r < k$, H *ima podgrupu reda* p^r *koja je normalna u* G.

Dokaz. ([4], *301-302*) □

2.4 Eksponent grupe. Frattinijeva podgrupa

Definicija 2.20. *Neka je* G *grupa. Ako je* $G = M \cdot N$, *gdje su* $M, N \leq G$, *onda kažemo da je* G *produkt svojih podgrupa* M *i* N. *Ako su* $M, N \neq \{1\}$ *kažemo da grupa* G *ima faktorizaciju.*

Ako je dodatno $M \cap N = \{1\}$ *i* $M \trianglelefteq G$, *onda kažemo da je* G *semidirektni produkt od* M *i* N.

Ako je dodatno $M \cap N = \{1\}$ *i* $M, N \trianglelefteq G$, *onda kažemo da je* G *direktni produkt od* M *i* N, *oznakom* $G = M \times N$.

Grupa G *je centralni produkt dviju podgrupa* $M, N \leq G$ *s amalgamiranom podgrupom* $D = M \cap N$, *tj. takvom grupom* D *koja je netrivijalna podgrupa i od* M *i od* N, *ako vrijedi*

$$G = M \cdot N,\ M, N \trianglelefteq G, \text{ te ako je } [x, y] = 1,\ \forall x \in M,\ \forall y \in N.$$

Pišemo $G = M * N$.

Neka je G *p-grupa. Ako je* $G = M \cdot N$, *gdje su* $M, N \trianglelefteq G$ *takve da je* $M \cap N = [M, N] \cong Z_p$, *onda kažemo da je* G *drugo-direktni produkt grupa* M *i* N. *Pišemo* $G = M \times_2 N$.

Teorem 2.30. *Neka je G abelova p-grupa, $|G| = p^n$. Onda je*

$$G \cong Z_{p^{n_1}} \times Z_{p^{n_2}} \times ... \times Z_{p^{n_k}},$$

gdje je $\sum_{i=1}^{k} n_i = n$. Ne smanjujući općenitost, možemo pretpostaviti da je $n_1 \geq n_2 \geq ... \geq n_k$ i pri tome je uređeni k-terac $(n_1, n_2, ..., n_k)$ jednoznačno određen.

Korolar 2.5. *Ako abelova p-grupa G sadrži samo jednu podgrupu reda p, onda je G ciklička grupa.*

Definicija 2.21. *Neka je G grupa. Najmanji mogući $e \in \mathbb{N}$ takav da je $x^e = 1$, $\forall x \in G$, zove se eksponent grupe G, oznakom $exp(G) \equiv e$.*

Teorem 2.31. *Neka je G 2-grupa i $exp(G) = 2$. Onda je G abelova grupa.*

Dokaz. Iz $(ab)^2 = abab = 1 = a^2b^2$ slijedi $ba = ab$, za sve $a, b \in G$. □

Definicija 2.22. *Abelovu p-grupu G izomorfnu direktnom produktu $\mathbb{Z}_p \times ... \times \mathbb{Z}_p$, gdje se $\mathbb{Z}_p$ pojavljuje n puta, nazivamo elementarno abelova p-grupa reda p^n, te označavamo s E_{p^n}.*

Definicija 2.23. *Neka je G p-grupa. Frattinijeva podgrupa grupe G je presjek svih maksimalnih podgrupa od G, tj,*

$$\Phi(G) = \bigcap_{\substack{M < G \\ max}} M.$$

Definicija 2.24. *Element $x \in G$ je neizvodnica (antigenerator) grupe G ako za svaki podskup $S \subseteq G$ vrijedi*

$$\langle S, x \rangle = G \Rightarrow \langle S \rangle = G.$$

Teorem 2.32. *Za svaku konačnu grupu G i $S \subseteq G$ vrijedi*

$$\langle S, \Phi(G) \rangle = G \Rightarrow \langle S \rangle = G.$$

Frattinijevu podgrupu $\Phi(G)$ tvore sve neizvodnice grupe G.

Dokaz. Neka je $x \in \Phi(G)$ i pokažimo da je x neizvodnica grupe G. Pretpostavimo da je $\langle S, x \rangle = G$ i $\langle S \rangle < G$. Neka je M maksimalna podgrupa od G takva da je $\langle S \rangle \subseteq M$. Kako je $x \in \Phi(G)$, onda je $x \in M$. Dakle je $\langle S, x \rangle \leq M \neq G$, što je protuslovlje.
Obratno, pretpostavimo da je $y \in G$ neizvodnica grupe G. Tada iz $\langle S, y \rangle = G$ slijedi $\langle S \rangle = G$. Pretpostavimo $y \notin \Phi(G)$. Dakle postoji barem jedna maksimalna podgrupa M grupe G takva da $y \notin M$. Slijedi $\langle M, y \rangle = G$. No y nije izvodnica grupe G, pa je $M = G$, što je protuslovlje. □

Definicija 2.25. *Neka je G p-grupa. Grupa $\Omega_i(G)$ je grupa*

$$\Omega_i(G) = \langle x \in G \mid x^{p^i} = 1 \rangle,\ i \in \mathbb{N}.$$

Grupa izvedena svim p^i-tim potencijama elemenata grupe G je

$$\mho_i(G) = \langle x^{p^i} \mid x \in G \rangle,\ i \in \mathbb{N}.$$

Očigledno je $\Omega_i(G)$ char G i $\mho_i(G)$ char G.

Teorem 2.33. *Neka je E normalna elementarno abelova podgrupa 2-grupe G i neka je $g \in G$ i $g^2 \in E$. Onda vrijedi*

$$|C_E(g)|^2 \geq |E|.$$

Dokaz. Zbog $g^2 \in E$ vrijedi $x^{g^2} = x$, za svaki $x \in E$. Stoga je

$$(xx^g)^g = x^g x^{g^2} = x^g x = xx^g,\ \forall x \in E,$$

tj. $xx^g \in C_E(g)$. Sada, za $x, y \in E$, imamo

$$xx^g = yy^g \Leftrightarrow xy = x^g y^g = (xy)^g \Leftrightarrow xy \in C_E(g)$$

$$\Leftrightarrow xy^{-1} \in C_E(g) \Leftrightarrow_{Tm.2.5} C_E(g)x = C_E(g)y.$$

Dakle, $xx^g \neq yy^g \Leftrightarrow C_E(g)x \neq C_E(g)y$, pa je stoga po teoremu 2.11

$$|C_E(g)| \geq |E : C_E(g)| \Rightarrow |C_E(g)|^2 \geq |E|.$$

□

Definicija 2.26. *Za konačnu p-grupu G kažemo da je regularna ako za sve $x, y \in G$ postoji $z \in \langle x, y \rangle'$ takav da vrijedi*

$$x^p y^p = (xy)^p z^p.$$

Za konačnu p-grupu G koja nije regularna kažemo da je iregularna.

Teorem 2.34. *Neka je G regularna p-grupa eksponenta p^e i $k \leq e$. Onda je*

$$exp(\Omega_k(G)) = p^k.$$

Sve p-grupe klase nilpotentnosti manje od p su regularne.
Sve grupe eksponenta p su regularne.
Regularne 2-grupe su abelove.

Dokaz. ([1], 179-181) □

Teorem 2.35. *Za svaku p-grupu G vrijedi $\Phi(G) = G' \cdot \mho_1(G)$.*

Posebice, ako je G 2-grupa onda je $\Phi(G) = \mho_1(G)$.

Dokaz. Neka je M bilo koja maksimalna podgrupa od G. Onda je po korolaru 2.2 $M \trianglelefteq G$ i $|G/M| = p$, te je G/M abelova grupa, pa je stoga po teoremu 2.24 $G' \leq M$. Neka je $x \in G$. Slijedi da je $x^p \in M$. Dakle, $\mho_1(G) \leq M$. Prema tome, $G' \cdot \mho_1(G) \leq M$. Kako to vrijedi za svaku maksimalnu podgrupu $M \leq G$, prema definiciji 2.23 slijedi $G' \cdot \mho_1(G) \leq \Phi(G)$.

Obratno, neka je $L = G' \cdot \mho_1(G)$. Kako su G', $\mho_1(G)$ char G slijedi

$$L \text{ char } G \Rightarrow L \trianglelefteq G.$$

Poradi $G' \leq L$ je G/L abelova grupa. Za $x \in G$ je $x^p \in \mho_1(G)$, dakle $x^p \in L$. Za $xL \in G/L$ vrijedi $(xL)^p = x^p L^p = L$. Dakle G/L je elementarno abelova grupa, $G/L \cong E_{p^s}$, $s \leq n$. Presjek svih maksimalnih podgrupa od G koje sadrže L jednak je L, pa iznova prema definiciji 2.23 slijedi $\Phi(G) \leq L = G' \cdot \mho_1(G)$.
Dakle, $\Phi(G) = G' \cdot \mho_1(G)$.

Za 2-grupe je $exp(G/\mho_1(G)) = 2$, pa je po teoremu 2.31 $G/\mho_1(G)$ abelova grupa. Stoga je $G' \leq \mho_1(G)$ i $\Phi(G) = \mho_1(G)$. □

Teorem 2.36. *Za svaku p-grupu G i podgrupu $H \leq G$ vrijedi $\Phi(H) \leq \Phi(G)$.*

Dokaz. Neka je $H \leq G$. Onda je prema teoremu 2.35 $\Phi(H) = H' \cdot \mho_1(H)$. No vrijedi $H' \leq G'$ i $\mho_1(H) \leq \mho_1(G)$. Dakle,

$$\Phi(H) = H' \cdot \mho_1(H) \leq G' \cdot \mho_1(G) = \Phi(G).$$

Teorem 2.37. (***Burnside; O bazama***)

(a) Ako je G p-grupa i $G/\Phi(G)$ reda p^d, onda broj d označavamo s $d(G)$ i nazivamo dimenzija grupe G, i vrijedi $G/\Phi(G) \cong E_{p^d}$.

(b) $\Phi(G)$ je najmanja normalna podgrupa od G takva da je $G/\Phi(G)$ elementarno abelova grupa.

(c) Neka je $G = \langle x_1, ..., x_r \rangle$ grupa izvedena s r elemenata. Tada vrijedi $r \geq d$.

(d) Ako je $|G/\Phi(G)| = p^d$, onda postoji d elemenata iz G koji izvode G.

Dokaz. (a) U teoremu 2.35 pokazano je: $G/\Phi(G) \cong E_{p^d}$.

(b) Ako je $N \trianglelefteq G$ i G/N elementarno abelova grupa onda je $G' \leq N$ i $\mho_1(G) \leq N$, pa je $\Phi(G) = G' \cdot \mho_1(G) \leq N$.

(c) Neka je $N \trianglelefteq G$ i $G = \langle x_1, ..., x_r \rangle$. Prema definiciji množenja klasa slijedi da je i G/N izvedena s r elemenata: $G/N = \langle Nx_1, ..., Nx_r \rangle$. Dakle, $G/\Phi(G) \cong E_{p^d}$ je izvedena elementima $\Phi(G)x_1, ..., \Phi(G)x_r$, pa slijedi $r \geq d$.

(d) Neka su $y_1, ..., y_d \in G$ pogodno odabrani elementi i

$$G/\Phi(G) \cong E_{p^d} = \langle \Phi(G)y_1, ..., \Phi(G)y_d \rangle.$$

Sada je

$$\langle y_1, ..., y_d, \Phi(G) \rangle = G \ \Rightarrow \ \langle y_1, ..., y_d \rangle = G,$$

jer po teoremu 2.32 elementi iz $\Phi(G)$ nisu izvodnice. □

Korolar 2.6. *Ako je G p-grupa i G/G' ciklička grupa, onda je i G ciklička grupa.*

Dokaz. Znamo $G', \Phi(G) \trianglelefteq G$ i prema teoremu 2.35 slijedi $G' \trianglelefteq \Phi(G)$. Po pretpostavci je G/G' ciklička grupa, a znamo da je kvocijentna grupa cikličke grupe ciklička. Sada iz teorema 2.15 slijedi da je

$$(G/G')/(\Phi(G)/G') = G/\Phi(G)$$

ciklička grupa i $exp(G/\Phi(G)) = p$, tj. $d(G) = 1$. Dakle, G je ciklička grupa. □

Definicija 2.27. *Neka je G p-grupa i $A \subseteq G$. Normalno zatvorenje A^G definiramo kao:*

$$A^G = \bigcap_{A \subseteq B_i \trianglelefteq G} B_i \trianglelefteq G.$$

A^G je najmanja normalna podgrupa od G koja sadrži A.
Ponekad normalno zatvorenje skupa $A \subseteq G$ označavamo s $\langle\langle A \rangle\rangle$.
Za $G = \langle a_1, a_2, ..., a_t \rangle$ je $G' = \langle\langle [a_i, a_j] \mid 1 \leq i, j \leq t \rangle\rangle$.

Teorem 2.38. **(*O dvjema normalnim podgrupama*)**
Neka je G p-grupa. Ako su M, $N \trianglelefteq G$, onda je $G/(M \cap N)$ izomorfna nekoj podgrupi direktnog produkta $(G/M) \times (G/N)$.

Dokaz. Neka je $\alpha : G \to (G/M) \times (G/N)$ preslikavanje definirano sa:

$$\text{za } x \in G \ \Rightarrow \ x^\alpha = (Mx, Nx).$$

Za $x, y \in G$ vrijedi

$$(xy)^\alpha = (Mxy, Nxy) = (Mx, Nx)(My, Ny) = x^\alpha y^\alpha.$$

Dakle, α je homomorfizam. Nadalje, za $x \in jz\alpha$ vrijedi

$$(Mx, Nx) = (M, N) \Rightarrow Mx = M, \ Nx = N \Rightarrow x \in M \cap N.$$

Dakle, $jz\alpha = M \cap N$. Sada, prema teoremu 2.14 slijedi da je $G/(M \cap N)$ izomorfna nekoj podgrupi od $(G/M) \times (G/N)$. □

2.5 O p-grupama klase nilpotentnosti 2 i abelovim maksimalnim podgrupama

Definicija 2.28. *Grupa G, $|G| = p^n$, je grupa maksimalne klase nilpotentnost ako je $cl(G) = n - 1$.*

Napomena 2.4. *Neka je G p-grupa, $|G| = p^n$. Grupa G je klase 2, $cl(G) = 2$ onda i samo onda ako je G neabelova grupa i $Z_2(G) = G$, tj.*
$\{1\} < G' \leq Z(G)$.

Dokaz. Po definiciji 2.16 je $Z_2(G) = G$, dakle $Z_2(G)/Z(G) = G/Z(G) = Z(G/Z(G))$, tj. $G/Z(G)$ je abelova grupa, pa je $G' \leq Z(G)$. I obratno iz $G' \leq Z(G)$ slijedi da je $G/Z(G)$ abelova grupa. Stoga je $Z(G/Z(G)) = G/Z(G)$, pa je $Z_2(G) = G$. □

Napomena 2.5. *Neka je G p-grupa. Ako postoji podgrupa $H < G$ takva da je $N_G(H)$ maksimalne klase nilpotentnosti onda je i G maksimalne klase nilpotentnosti.*

Teorem 2.39. **(*O p-grupama razreda* 2)**
U p-grupi G razreda 2 vrijede sljedeće jednakosti:

(a) $[xy, uv] = [x, u][x, v][y, u][y, v]$ - *"distributivnost " komutatora umnožaka,*

(b) $[x^n, y] = [x, y^n] = [x, y]^n$,

(c) $(x \cdot y)^n = x^n \cdot y^n \cdot [y, x]^{\binom{n}{2}}$.

Dokaz. Za $x, y, u, v \in G$ vrijedi:

(a) $[xy, uv] = [x, uv]^y[y, uv] = [x, v][x, u]^v[y, v][y, u]^v = [x, u][x, v][y, u][y, v]$.

(b) Tvrdnju dokazujemo matematičkom indukcijom po n.

Baza: Očigledno tvrdnja vrijedi za $n = 1$.

Korak: Neka je $n > 1$. Pretpostavimo da tvrdnja vrijedi za $n-1$, te dokažimo da vrijedi i za n. Imamo:

$$[x, y^n] =_{(a)}= [x, y^{n-1}y] = [x, y^{n-1}][x, y] = [x, y]^{n-1}[x, y] = [x, y]^n.$$

Sada:

$$[x^n, y] = ([y, x^n])^{-1} = ([y, x]^n)^{-1} = ([y, x]^{-1})^n = [x, y]^n.$$

Dakle prema načelu matematičke indukcije tvrdnja vrijedi za svaki n.

(c) Tvrdnju dokazujemo matematičkom indukcijom po n.

Baza: Za $n = 1$ tvrdnja očigledno vrijedi.

Korak: Neka je $n > 1$. Pretpostavimo da tvrdnja vrijedi za $n-1$, te dokažimo da vrijedi i za n. Imamo:

$$\begin{aligned}
(xy)^n &= (xy)^{n-1}(xy) \\
&= (\textit{pretpostavka indukcije}) = x^{n-1}y^{n-1}[y, x]^{\binom{n-1}{2}}(xy) \\
&= (\textit{jer je } [y, x]^{\binom{n-1}{2}} \in G' \leq Z(G)) = x^{n-1}(y^{n-1}x)y[y, x]^{\binom{n-1}{2}} \\
&= x^{n-1}xy^{n-1}[y^{n-1}, x]y[y, x]^{\binom{n-1}{2}} \\
&= (\textit{slučaj } (b)) = x^n y^n [y, x]^{n-1}[y, x]^{\binom{n-1}{2}} \\
&= x^n y^n [y, x]^{\binom{n}{2}}.
\end{aligned}$$

Prema načelu matematičke indukcije tvrdnja vrijedi za svaki n. $\square$

Teorem 2.40. *Neka je $G = \langle a_1, ..., a_n \rangle$. Onda je*

$$G' = \langle \{[a_i, a_j]^g \mid g \in G\}, i, j \in \{1, ..., n\} \rangle.$$

Dokaz. Označimo $H = \langle \{[a_i, a_j]^g \mid g \in G\}, i, j \in \{1, ..., n\} \rangle$ i dokažimo $H = G'$. Očito je $H \leq G'$. S druge strane vrijedi, za $[a_i, a_j] \in H$, $[a_i, a_j a_k] =$ (*teorem 2.39*)$= [a_i, a_k][a_i, a_j]^{a_k} \in H$. Sada pretpostavimo da je, za svaki $x \in G$, $[a_i, x] \in H$. Vrijedi $[a_i, xa_j] = [a_i, a_j][a_i, x]^{a_j} \in HH^{a_j} = H$, što povlači $[a_i, xa_j] \in H$. Analogno, uz $[a_i, x] \in H$, pretpostavimo da je $[y, x] \in H$. Promatramo $[ya_i, x] = [y, x]^{a_i}[a_i, x] \in H^{a_i}H = H$, pa slijedi da za svaki $x, y \in G$ vrijedi $[x, y] \in H$, tj. $G' \leq H$. Dakle pokazali smo $H = G' = \langle \{[a_i, a_j]^g \mid g \in G\}, i, j \in \{1, ..., n\} \rangle$. $\square$

Iz prethodnog teorema slijedi:

Korolar 2.7. *Neka je* $G' \leq Z(G)$ *i* $G = \langle a_1, ..., a_n \rangle$. *Onda je*

$$G' = \langle [a_i, a_j], i, j \in \{1, ..., n\} \rangle.$$

Teorem 2.41. (***O abelovoj maksimalnoj podgrupi***)
Neka je A maksimalna podgrupa p-grupe G, te neka je A abelova, a G nije abelova grupa. Onda vrijedi

$$|G| = p \cdot |G'| \cdot |Z(G)|.$$

Dokaz. Prema korolaru 2.2 je $|G/A| = p$, te je po korolaru 2.1 i teoremu 2.24 G/A abelova grupa, odnosno $G' \leq A$. Vrijedi $|G| = p \cdot |A|$, te $Z(G) \leq A$, jer G nije abelova grupa. Neka je $g \in G \setminus A$. Definiramo preslikavanje $\varphi : A \to A$, uz

$$a^{\varphi} = [a, g], \ \forall a \in A.$$

Kako je $G' \leq A$, φ je dobro definirano preslikavanje. Za $a, b \in A$ vrijedi

$$\begin{aligned} (ab)^{\varphi} &= [ab, g] \\ &= (\textit{teorem 2.25}) = [a, g]^b [b, g] \\ &= ([a, g]^b = [a, g], \textit{ jer je } Z(A){=}A) = [a, g][b, g] \\ &= a^{\varphi} b^{\varphi}. \end{aligned}$$

Dakle, φ je homomorfizam. Vrijedi

$$jz\varphi = \{a \in A \mid [a, g] = 1\} = C_A(g) = Z(G).$$

Naime, elementi iz $C_A(g)$ komutiraju s g i s elementima iz A, pa slijedi da komutiraju s cijelim G. Dakle, $C_A(g) \subseteq Z(G) \leq A$. Obratna inkluzija je očigledna.
U grupi $sl\varphi = \{[a, g] \mid a \in A\} \leq G'$ vrijedi za svaki $a \in A$:

1) $[a, g]^g = [a^g, g^g] = [a^g, g] \in sl\varphi$, pa je $sl\varphi \trianglelefteq G$

2) $[a, g^{\alpha}] = [a, gg^{\alpha-1}] = [a, g^{\alpha-1}][a, g]^{g^{\alpha-1}} \in sl\varphi$, jer je $[a, g^{\alpha-1}] \in sl\varphi$ po indukciji, a $[a, g]^{g^{\alpha-1}} \in sl\varphi$ po 1).

Također, $G/sl\varphi$ je abelova grupa. Naime, neka su $g_1, g_2 \in G$ bilo koja dva elementa i $g_1 = a_1 g^{\alpha}, g_2 = a_2 g^{\beta}$, za $g \in G, a_1, a_2 \in A$. Tada vrijedi

$$\begin{aligned} [a_1 g^{\alpha}, a_2 g^{\beta}] &= [a_1, a_2 g^{\beta}]^{g^{\alpha}} [g^{\alpha}, a_2 g^{\beta}] \\ &= \{[a_1, g^{\beta}][a_1, a_2]^{g^{\beta}}\}^{g^{\alpha}} [g^{\alpha}, g^{\beta}][g^{\alpha}, a_2]^{g^{\beta}} \in sl\varphi \cdot sl\varphi = sl\varphi, \\ & \quad \textit{prema 1), 2) i teoremu 2.25 c).} \end{aligned}$$

□

Stoga je po teoremu 2.24 $G' \leq sl\varphi$. Dakle, $sl\varphi = G'$. Sada prema teoremu 2.13 slijedi

$$A/Z(G) \cong G' \Rightarrow |A| = |G'| \cdot |Z(G)| \Rightarrow |G| = p \cdot |G'| \cdot |Z(G)|.$$

2.6 O minimalno-neabelovim p-grupama i grupama s cikličkom maksimalnom podgrupom

Definicija 2.29. *Kažemo da je p-grupa G minimalno-neabelova, što označavamo s $G \in \mathcal{A}_1$, ako je neabelova, ali su sve prave podgrupe grupe G abelove.*

Teorem 2.42. (***O minimalno-neabelovoj p-grupi***)
Neka je G minimalno-neabelova p-grupa reda p^n. Onda je

$$G = \langle x, y \rangle, \ \ |G'| = p \ \ i \ \ \Phi(G) = Z(G) \text{ je indeksa } p^2 \text{ u } G.$$

Dokaz. Neka su $x, y \in G$ bilo koja dva elementa takva da je $[x, y] \neq 1$. Naime, takvi elementi opstoje u G, jer je G neabelova grupa. Neka je $U = \langle x, y \rangle$. Kako je G minimalno-neabelova grupa slijedi $U = G$, jer U nije abelova grupa. Dakle, G ima dvije izvodnice, pa je po teoremu 2.37 $|G/\Phi(G)| = p^2$.

Neka su A i B dvije različite maksimalne podgrupe iz G. Po korolaru 2.1 je $|G : A| = |G : B| = p$. Sada je $D = A \cap B = \Phi(G)$, jer je $|G/D| = |G/\Phi(G)| = p^2$. Kako su A i B abelove grupe, vrijedi $C_G(D) \geq \langle A, B \rangle = A \cdot B = G$. Dakle, $D \leq Z(G)$. Još više, vrijedi $D = Z(G)$. Naime, kada bi bilo $D < Z(G)$, onda bi $G/Z(G)$ bila ciklička grupa, tj. G abelova grupa, što je protuslovlje. Dakle je $\Phi(G) = Z(G)$.
Sada prema teoremu 2.41 slijedi

$$\frac{|G|}{|Z(G)|} = p \cdot |G'| \Rightarrow p^2 = p \cdot |G'| \Rightarrow |G'| = p.$$

Teorem 2.43. (***O p-grupama s cikličkom maksimalnom podgrupom***)
Neka je G neabelova grupa reda p^{n+1}, koja ima cikličku maksimalnu podgrupu $\langle a \rangle$ reda p^n. Onda je G izomorfna jednoj od sljedeće četiri grupe:

(a) *M-grupi $M_{p^{n+1}}$ reda p^{n+1}, gdje je $n \geq 2$, odnosno $n \geq 3$, za $p = 2$.*
$M_{p^{n+1}} = \langle a, b \mid a^{p^n} = b^p = 1, a^b = a^{1+p^{n-1}} \rangle$

(b) *diedralnoj grupi $D_{2^{n+1}}$ reda 2^{n+1}, $n \geq 2$*
$D_{2^{n+1}} = \langle a, b \mid a^{2^n} = b^2 = 1, a^b = a^{-1} \rangle$

(c) *generiranoj kvaternionskoj grupi* $Q_{2^{n+1}}$ *reda* 2^{n+1}, $n \geq 2$
$Q_{2^{n+1}} = \langle a, b \mid a^{2^n} = b^4 = 1, b^2 = a^{2^{n-1}}, a^b = a^{-1} \rangle$
Ako je $n = 2$, *dobivamo* Q_8.

(d) *semidiedralnoj grupi* $SD_{2^{n+1}}$ *reda* 2^{n+1}, $n \geq 3$
$SD_{2^{n+1}} = \langle a, b \mid a^{2^n} = b^2 = 1, a^b = a^{-1+2^{n-1}} \rangle$.

Dokaz. ([4], *90-93*) □

Teorem 2.44. (***Olga Taussky***)
Neka je G *neabelova* 2*-grupa takva da je* $|G : G'| = 4$. *Onda je*

$$G \cong D_{2^n} \text{ ili } Q_{2^n} \text{ ili } SD_{2^n}.$$

Dokaz. ([4], *339-340*) □

Propozicija 2.1. (***Roquette***)
Neka je G *konačna* p*-grupa i neka je* N *normalna podgrupa grupe* G. *Pretpostavimo da je svaka* G*-invarijantva podgrupa reda* p^2 *od* N *ciklička. Onda je* N *ciklička ili* 2*-grupa maksimalne klase nilpotentnosti. Ako još vrijedi i* $N \leq \Phi(G)$, *onda je* N *ciklička grupa.*

Dokaz. ([5]) □

Propozicija 2.2. (***Burnside***)
Neka je G p*-grupa i* N *normalna podgrupa grupe* G *takva da je* $N \leq \Phi(G)$. *Ako je* $Z(N)$ *ciklička grupa, onda je i* N *ciklička grupa.*

Dokaz. ([5]) □

Teorem 2.45. *Ako je* G *neabelova* p*-grupa,* $d(G) = 2$ *i* $|G'| = p$, *onda je* G *minimalno-neabelova grupa.*

Dokaz. Ovaj teorem je obrat teorema 2.42.
Kako je $|G'| = p$, slijedi $G' \leq Z(G)$, pa je prema napomeni 2.4 grupa G klase 2. Onda prema teoremu 2.39 $\forall x, y \in G$ vrijedi

$$[x, y]^n = [x, y^n], \ \ n \in \mathbb{Z}.$$

Posebice, za $n = p$ imamo $[x, y]^p = [x, y^p]$. No, $[x, y] \in G'$, pa je $[x, y]^p = [x, y^p] = 1$, $\forall x, y \in G$. Dakle,

$$\mho_1(G) = \langle y^p \mid y \in G \rangle \leq Z(G).$$

Sada imamo $G' \leq Z(G)$ i $\mho_1(G) \leq Z(G)$, te prema teoremu 2.35 slijedi

$$G' \cdot \mho_1(G) = \Phi(G) \leq Z(G).$$

Po pretpostavci je $d(G) = 2$, tj. $|G/\Phi(G)| = p^2$. Stoga je $Z(G) = \Phi(G)$, jer bi inače G bila abelova grupa.
Neka je $M \leq G$ maksimalna podgrupa, pa je po korolaru 2.2 $|G : M| = p$. Znamo $\Phi(G) < M$, tj. $Z(G) < M$, a onda i $Z(G) \leq Z(M)$, pa je $|M : Z(M)| \leq p$. Sada prema teoremu 2.18 slijedi da je M abelova grupa, tj. G je minimalno-neabelova grupa. $\square$

Ovim pregledom osnovnih definicija i tvrdnji o konačnim p-grupama ponuđen je temelj svakome tko ima želju upustiti se u istraživanje istih. Velika zahvala jednom od glavnih kreatora teorije konačnih p-grupa posljednjih četrdesetak godina, profesoru Zvonimiru Janku, njegovim predavanjima i nadasve "zaraznom" istraživačkom entuzijazmu.
Hvala Vam Profesore!

Literatura

[1] Y. Berkovich - Z. Janko, *Groups of Prime Power Order, Vol. II*, Walter de Gruyter, Berlin New York, 2008.

[2] N. Blackburn, *Generalizations of Certain Elementary Theorems on p-Groups*, Proc. London Math. Soc.(3)11, 1961, 1–22.

[3] J. F. Humphreys, *A Course in Group Theory*, Oxford University Press, Oxford, 1985.

[4] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin Heidelberg New York, 1971.

[5] Z. Janko, *Konačne p-grupe II*, skripta, predavanja održao prof. dr. sc. Z. Janko (Mathematisches Institut, Universität Heidelberg) na Poslijediplomskom studiju matematike, Matematičkog odsjeka Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu, ak. god. 2001./2002.