Teorija konačnih grupa

Bilić, Martina

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Martina Bilić

TEORIJA KONAČNIH GRUPA

Diplomski rad

Voditelj rada:
prof. dr. sc.
Dražen Adamović

Zagreb, lipanj, 2022.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Obitelji za bezuvjetnu ljubav, pomoć, potporu i najbolji poklon koji su mi mogli dati, a to je vjera u mene.

Hvala mentoru prof. dr. sc. Draženu Adamoviću na strpljenju i pomoći u pisanju ovog rada te svim kolegama i prijateljima na zajedničkim uspomenama, dobrom društvu i međusobnoj motivaciji tijekom ove nezaboravne avanture.

Posebno hvala kolegi Gudelju na zajedničkom analiziranju i dijeljenju znanja te Ani, mojoj nesebičnoj "privremenoj mami" na svakom obroku nakon kolokvija (i češće). Zna se da ljubav ide kroz želudac, ali tvoja ljubav ima puno više putanja.

I jedno veliko hvala predivnim curama sa Šare za život ispunjen smijehom, optimizmom i neizmjernom podrškom jer bez njih studentski život ne bi imao smisao.

Sadržaj

Uvod

Grupe su zastupljene u skoro svim matematičkim teorijama, ali je njihova primjena važna u fizici i ostalim prirodnim znanostima. Teorija grupa prestavlja temeljni i jedan od najvažnijih dijelova algebre čija rana povijest datira iz 19. stoljeća. Temeljni problemi teorije grupa ne ovise o prirodi elemenata grupe što omogućava njezinu široku primjenu na gotovo sve druge matematičke discipline i mnoge druge znanosti (kristalografiju, spektroskopiju, kvantnu mehaniku, kvantnu teoriju polja). Različiti fizički sustavi te poznate sile u svemiru mogu se modelirati simetričnim grupama.

Posebno su značajne konačne grupe koje su bile jedno od najvažnijih matematičkih dostignuća 20. stoljeća. U teoriji konačnih grupa proučava se strukturna, apstraktna teorija koja se može primjeniti na sve grupe. Proučavaju se i neke klase konačnih grupa kao što su komutativne grupe i p-grupe. Sljedeći važni koraci u teoriji su konstrukcija i klasifikacija konačnih prostih grupa i konačnih Abelovih grupa. Glavni cilj ovog diplomskog rada je dati pregled o teoriji konačnih grupa, u kojem ćemo proučiti Sylowljeve teoreme. Osim toga, promatrat ćemo i Abelove grupe te neke primjere konačnih grupa.

U prvom poglavlju definirat ćemo monoide te homomorfizam i izmomorfizam monoida. Pomoću te definicije kasnije definiramo konačne grupe na kojima se temelji ovaj rad.

Na početku drugog poglavlja navest ćemo osnovne pojmove vezane uz grupe. Definirat ćemo grupu, podgrupu, generator grupe te homomorfizam grupa. Uvest ćemo pojmove za skup lijevih klasa te indeks podgrupe. Nakon osnovnih pojmova vezanih za grupe, definiramo normalne podgrupe. Kažemo da je podgrupa H normalna ako je $xH = Hx$, za svaki $x \in G$. Tu ćemo definiciju potkrijepiti primjerima. Definirat ćemo normalizator i centralizator grupe te kvocijentnu grupu.
Proučavat ćemo normalan i Abelov niz podgrupa, kojeg ćemo po potrebi popunjavati, a zatim ćemo definirati rješivu grupu i komutatorsku podgrupu. Navodimo i sljedeće teoreme:

Teorem 2.3.10 (Schreier). *Neka je G grupa. Dva normalna niza podgrupa koja završavaju sa trivijalnom grupom imaju ekvivalentna popunjenja.*

Teorem 2.3.11 (Jordan Hölder). *Neka je G grupa sa normalnim nizom podgrupa*

$$G = G_1 \supset G_2 \supset \cdots \supset G_r = \{e\}, \tag{1}$$

koji je takav da je svaka grupa G_i/G_{i+1} prosta te je $G_i \neq G_{i+1},\ i = 1, \ldots, r-1$. Tada je svaki drugi normalni niz podgrupa od G sa istim svojstvima ekvivalentan normalnom nizu (1).

Također, u ovom poglavlju definirat ćemo cikličke grupe te se kroz niz propozicija upoznati sa njihovim svojstvima.
Nadalje, kroz proučavanje djelovanja grupe na skupu saznajemo više o algebarskoj strukturi grupe. Tu definiramo djelovanje grupe na skup, centar grupe te bijekciju $c_x \colon G \to G$ sa $c_x(y) = xyx^{-1}$. Dodatno, uvodimo i pojam stabilizatora te orbite točke $s \in S$, gdje je S neki podskup grupe G na koji ona djeluje. Dio sa djelovanjem grupe na skupu zaključujemo teoremom:

Teorem 2.5.6. *Neka je G konačna grupa koja djeluje na samu sebe konjugiranjem. Tada je jednadžba klasa dana sa:*

$$[G : 1] = \sum_{x \in C} [G : G_x],$$

gdje je C skup predstavnika klasa konjugiranih elemenata.

Za kraj ovog poglavlja proučavat ćemo Sylowljeve podgrupe. Za prost broj p definirat ćemo $p-$grupu i $p-$podgrupu te Sylowljevu $p-$podgrupu:

Definicija 2.6.1. *Neka je G konačna grupa i p prost broj.*

(i) Kažemo da je G p-grupa, ako je $|G| = p^n,\ n \geq 0$.

(ii) Podgrupa H grupe G je p-podgrupa od G ako je H p-grupa.

(iii) H zovemo Sylowljevom p-podgrupom ako je $|H| = p^n$ i ako je p^n najveća potencija od p koja dijeli $|G|$.

Iskazali smo i dokazali Sylowljeve teoreme:

Teorem 2.6.3. *Neka je G konačna grupa i p prost broj, koji dijeli njen red. Tada postoji Sylowljeva $p-$podgrupa od G.*

Teorem 2.6.5. *Neka je G konačna grupa.*

(i) Svaka p-podgrupa je sadržana u nekoj Sylowljevoj p-podgrupi.

(ii) Sve Sylowljeve p-podgrupe su konjugirane.

(iii) Broj Sylowljevih p-podgrupa od G je oblika $kp + 1,\ k \in \mathbb{Z}_{\geq 0}$.

U trećem poglavlju proučavat ćemo Abelove grupe. Definiramo direktnu sumu Abelovih grupa te uvodimo pojam baze Abelove grupe. Abelova grupa naziva se slobodna, ako ona ima bazu. Sve baze slobodne Abelove grupe imaju isti broj elemenata, a taj kardinalni broj naziva se rang od A. Kroz teoreme i leme, uočit ćemo neka svojstva Abelovih podgrupa.
Nakon toga promatrat ćemo konačno generirane Abelove grupe. Posebnu pažnju posvetili smo torzionoj podgrupi.

Definicija 3.2.1. *Neka je A Abelova grupa.*

(i) $a \in A$ *zovemo torzionim elementom ako ima konačan period (red).*

(ii) Definiramo torzionu podgrupu od A kao skup:

$$A_{tor} = \{a \in A : a \text{ je torzioni element od } A\}.$$

(iii) A *je torziona grupa ako je* $A = A_{tor}$.

Za torzionu Abelovu grupu A, iskazali smo:

Teorem 3.2.2. *Neka je A torziona Abelova grupa. Tada je A direktna suma svojih podgrupa* $A(p) \neq 0$*, za sve proste p:*

$$A = \bigoplus_{p \text{ prost}} A(p).$$

Iskazali smo i dokazali sljedeći teorem:

Teorem 3.2.5. *Svaka konačna Abelova p-grupa je izomorfna produktu cikličkih p−grupa, redova* $p^{r_1}, \ldots p^{r_s}$*, gdje je* $r_1 \geq r_2 \geq \ldots \geq r_s \geq 1$*. Niz prirodnih brojeva* $(r_1, \ldots, r_s)$ *je jedinstveno određen.*

U četvrtom poglavlju navodimo neke primjere konačnih grupa malog reda i dokazujemo neke strukturne teoreme. Definirali smo diedralnu grupu te poludirektan produkt. Osnovna svojstva grupa reda p^2 iskazana su u propoziciji:

Propozicija 4.1.3. *Neka je G reda* p^2*, gdje je p prost broj. Tada je* $G \cong \mathbb{Z}_{p^2}$ *ili* $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Uz to, osnovna svojstva grupa reda pq iskazana su u propoziciji:

Propozicija 4.1.6. *Neka su p i q prosti brojevi,* $p > q$ *i neka je G grupa reda pq.*

(1) Ako $q \nmid p-1$, *tada je* $G \cong \mathbb{Z}_{pq}$.

(2) Neka $q \mid p-1$ *i neka je* $\phi\colon \mathbb{Z}_q \to Aut\left(\mathbb{Z}_p\right) \cong \mathbb{Z}_p^*$ *netrivijalan homomorfizam. Tada je* $G \cong \mathbb{Z}_{pq}$ *ili* $G \cong \mathbb{Z}_p \rtimes_\phi \mathbb{Z}_q$.

Za kraj klasificiramo sve konačne grupe reda 8 i 12.
Diplomski je većinom rađen prema knjigama [1] i [2]. Dijelovi ove teorije mogu se naći i u skriptama [3] i [4].

Poglavlje 1

Monoidi

U ovom poglavlju navest ćemo definiciju monoida, da bismo pomoću nje mogli definirati grupe u nastavku rada.

1.1 Monoidi

Definicija 1.1.1. *Monoid je uređen par* $(G, \cdot)$ *nepraznog skupa* G *i binarne operacije* $\cdot : G \times G \to G$ *koji zadovoljava*

(1) ASOCIJATIVNOST:

$$a\,(bc) = (ab)\,c, \ \textit{za svaki } a, b, c \in G$$

(2) Postoji jedinični element $e \in G$*:*

$$ae = ea = a, \ \textit{za svaki } a \in G.$$

Neka je G monoid te $x_1, x_2, ..., x_n$ elementi od G. Tada njihov produkt definiramo induktivno:

$$\prod_{\nu=1}^{n} x_\nu = x_1 \cdot \cdots x_n = (\, x_1 \cdot \cdots x_{n-1})\, x_n.$$

Tada vrijedi jednakost:

$$\prod_{\mu=1}^{m} x_\mu \cdot \prod_{\nu=1}^{n} x_{m+\nu} = \prod_{\nu=1}^{m+n} x_\nu.$$

Uz to vrijedi jednakost:

$$\prod_{m+1}^{m+n} x_\nu = \prod_{\nu=1}^{n} x_{m+\nu}$$

te definiramo

$$\prod_{\nu=1}^{0} x_\nu = e.$$

Teorem 1.1.2. *Neka je G komutativan monoid te $x_1, x_2, ..., x_n$ njegovi elementi. Neka je ψ bijekcija skupa cijelih brojeva $(1, ..., n)$ na samog sebe. Tada je $\prod_{\nu=1}^{n} x_{\psi(\nu)} = \prod_{\nu=1}^{n} x_\nu$.*

Dokaz. Dokaz provodimo indukcijom.
Tvrdnja je očita za n=1. Pretpostavimo da vrijedi i za n-1.
Neka je k takav da $\psi(k) = n$. Tada je

$$\begin{aligned}
\prod_{\nu=1}^{n} x_{\psi(\nu)} &= \prod_{\nu=1}^{k-1} x_{\psi(\nu)} \cdot x_{\psi(k)} \cdot \prod_{\nu=k+1}^{n} x_{\psi(\nu)} \\
&= \prod_{\nu=1}^{k-1} x_{\psi(\nu)} \cdot x_{\psi(k)} \cdot \prod_{\nu=1}^{n-k} x_{\psi(\nu)} \\
&= \prod_{\nu=1}^{k-1} x_{\varphi(\nu)} \cdot x_n \cdot \prod_{\nu=1}^{n-k} x_{\varphi(k-1+\nu)} \\
&= \prod_{\nu=1}^{k-1} x_{\varphi(\nu)} \cdot x_n \cdot \prod_{\nu=k}^{n-1} x_{\varphi(\nu)} \\
&= \prod_{\nu=1}^{n-1} x_{\varphi(\nu)} \cdot x_n \\
&= \prod_{\nu=1}^{n-1} x_{\psi(\nu)} \cdot x_n \\
&= \prod_{\nu=1}^{n-1} x_\nu \cdot x_n
\end{aligned}$$

□

Napomena 1.1.3. *Neka je G komutativan monoid, I skup, a $f: I \to G$ preslikavanje takvo da je $f(i) = e$, za skoro svaki $i \in I$. Neka je I_0 podskup od I koji se sastoji od svih i takvih da je $f(i) \neq e$. Tada sa $\prod_{i \in I} f(i)$ podrazumijevamo $\prod_{i \in I_0} f(i)$. Jasno je da je prazan produkt jednak e.*

Neka je H podskup od G koji sadrži jedinični element e i koji je takav da ako su $x, y \in H$ onda je i $xy \in H$. Takav skup H zove se podmonoid od G jer je monoid zatvoren unutar binarnog preslikavanja skupa G.

Definicija 1.1.4. *Neka su G i G′ monoidi. Homomorfizam monoida, odnosno homomorfizam sa G u G′ je preslikavanje $f : G \to G'$, takvo da je*

$$f(xy) = f(x) f(y), \quad \text{za svaki } x, y \in G,$$

dok se jedinični element od G preslika u jedinični element od G′.

Definicija 1.1.5. *Neka su G, G' monoidi. Homomorfizam $f : G \to G'$ naziva se izomorfizam i označava se sa $G \approx G'$, ako postoji homomorfizam $g : G' \to G$, takav da je $f \circ g = id_{G'}$ i $g \circ f = id_G$.*

Kada je $G = G'$ kažemo da je taj izmorfizam automorfizam, dok slučaj homomorfizma sa G u samoga sebe zovemo endomorfizam.

Primjer 1.1.6. *Neka je G monoid, $x \in G$ te $\mathbb{N}$ skup prirodnih brojava s nulom. Tada je preslikavanje $f : \mathbb{N} \to G$, takvo da je $f(n) = x^n$ homomorfizam.*

Poglavlje 2

Grupe

U ovom poglavlju proučavat ćemo grupe. Prvo ćemo navesti osnovne definicije i konstrukcije iz teorije grupa. Zatim ćemo navesti osnovne rezultate o normalnim podgrupama, rješivim grupama i Abelovim grupama. Proučavat ćemo i djelovanje grupe na skup, Sylowljeve pogdrupe, te dokazati Sylowljeve teoreme. Navedene pojmove i definicije može se pronaći u prvim poglavljima knjige [1].

2.1 Grupe

Definicija 2.1.1. *Monoid takav da za svaki $x \in G$ postoji jedinstven y iz G, takav da je $xy = yx = e$ zovemo grupa.*

Napomena 2.1.2. *Inverz y označavamo sa x^{-1}, odnosno $-x$, ako je zakon kompozicije napisan aditivno.*
On je jedinstven. Pretpostavimo da je i y' inverz od x. Tada je

$$y' = y'e = y'(xy) = (y'x)y = ey = y.$$

Primjer 2.1.3. *Neka je S neprazan skup, a G skup svih bijekcija skupa S. Tada je G grupa uz kompoziciju kao binarnu operaciju, dok je jedinični element od G identiteta od S.*

Elemente od G nazivamo permutacijama skupa S i označavamo ih sa $Perm(S)$.

Definicija 2.1.4. *Neka je G grupa. Podskup H od G koji je podmonoid zatvoren s obzirom na inverz, odnosno ako je $x \in H$, onda je i $x^{-1} \in H$, zovemo podgrupom od G.*

Podgrupa je trivijalna ako sarži samo jedinični element.

Definicija 2.1.5. *Neka je G grupa i $S \subset G$. Kažemo da skup S generira G ili da je skup S generator od G, u oznaci $G = \langle S \rangle$, ako je*

$$G = \{x_1 \cdots x_n : x_i \in S \text{ ili } x_i^{-1} \in S\}.$$

Definicija 2.1.6. *Neka su G i G' grupe. Preslikavanje $f : G \to G'$, takvo da je*

$$f(xy) = f(x) f(y), \quad \text{za svaki } x, y \in G,$$

naziva se homomorfizam grupa.

Definicija 2.1.7. *Neka su G, G' grupe. Homomorfizam $f : G \to G'$ naziva se izomorfizam grupa i označava se sa $G \approx G'$, ako postoji homomorfizam $g : G' \to G$, takav da je $f \circ g = id_{G'}$ i $g \circ f = id_G$.*

Definicija 2.1.8. *Neka su G i G' grupe. Izomorfizam $f : G \to G'$, takav da je $G = G'$ nazivamo automorfizam.*

Iz definicije automorfizma, direktno slijedi sljedeći rezultat:

Propozicija 2.1.9. *Označimo s $Aut(G)$ skup svih automorfizama grupe G. Tada je $Aut(G)$ grupa uz kompoziciju kao binarnu operaciju.*

Propozicija 2.1.10. *Neka je G grupa i H, K dvije podgrupe takve da je $H \cap K = e$, $HK = G$ i neka je $xy = yx$, za svaki $x \in H$ i za svaki $y \in K$. Tada je preslikavanje $H \times K \to G$ dano sa $(x, y) \mapsto xy$ izomorfizam.*

Za dokaz vidi [1], str. 11.

Definicija 2.1.11. *Neka je H podgrupa grupe G i $a \in G$. Skup*

$$aH = \{ah : h \in H\}$$

naziva se lijeva klasa podgrupe H određena elementom a.

Analogno definiramo desnu klasu podgrupe H.
Skup svih lijevih klasa podgrupe H označavamo sa G/H, dok skup svih desnih klasa podgrupe H označavamo sa $H\backslash G$.

Definicija 2.1.12. *Neka je H podgrupa grupe G i $a \in G$. Kardinalni broj skupa G/H, odnosno skupa $H\backslash G$, nazivamo indeks podgrupe H u G i označavamo sa $[G : H]$.*

Propozicija 2.1.13. *Neka je G grupa i H podgrupa. Tada je*

$$[G : H][H : 1] = [G : 1],$$

gdje vrijedi da ako su neka dva od navedenih indeksa konačna, onda je i treći pa jednakost vrijedi. Ako je $[G : 1]$ konačan, tada red od H dijeli red od G.

Promotrimo općenitiju situaciju. Neka su H, K podgrupe od G, takve da je $K \subset H$. Neka je lijeva klasa podgrupe K u H određena elementima $\{x_i\}$, a lijeva klasa podgrupe H u G sa $\{y_j\}$. Tvrdimo da je tada $\{y_j x_i\}$ skup reprezentativnih elemenata lijeve klase podgrupe K u G.
Dokažimo sada prethodnu propoziciju.

Dokaz. Iz iskaza Propozicije 2.1.13 imamo da je

$$H = \bigcup_i x_i K \tag{2.1}$$

$$G = \bigcup_j y_j H, \tag{2.2}$$

gdje su navedene unije disjunktne. Tada iz (2.1), (2.2) slijedi

$$G = \bigcup_{i,j} y_j x_i K. \tag{2.3}$$

Preostaje nam pokazati da je i ta unija disjunktna.
Pretpostavimo suprotno. Tada postoji par indeksa (j, i) te (j', i') takav da vrijedi

$$y_j x_i K = y_{j'} x_{i'} K. \tag{2.4}$$

Budući da su $x_i, x_{i'}$ iz H, množenjem sa H sa desne strane dobijemo

$$y_j H = y_{j'} H\ ,$$

odakle slijedi da je $y_j = y_{j'}$. Vratimo li se sada na jednakost (2.4) slijedi da je $x_i K = x_{i'} K$, odnosno $x_i = x_{i'}$.
Dakle, unija navedena pod (2.3) je disjunktna. □

Definicija 2.1.14. *Neka je $J_n = \{1, \ldots, n\}$ te S_n grupa permutacija skupa J_n. Kažemo da je τ transpozicija, odnosno ciklička permutacija sa 2 elementa, ako postoji $r \neq s$ iz J_n, za koje je*

$$\tau(r) = s,\ \tau(s) = r \text{ te } \tau(k) = k,\ \text{za svaki } k \neq r,\ s.$$

Propozicija 2.1.15. *Grupa S_n je generirana transpozicijama.*

Za dokaz vidi [2], str. 30.

Definicija 2.1.16. *Kažemo da je permutacija $\sigma \in S_n$ parna (neparna) ako se može napisati kao umnožak parnog (neparnog) broja transpozicija.*

Predznak permutacije σ definiran je sa

$$sgn(\sigma) = \begin{cases} 1, & \text{ako je } \sigma \text{ parna permutacija} \\ -1, & \text{ako je } \sigma \text{ neparna permutacija} \end{cases}$$

Pokazuje se da je $sgn\colon S_n \to \{\pm 1\}$ homomorfizam grupa. Označimo s A_n skup svih parnih permutacija. Budući da je A_n jezgra homomorfizma sgn, vidimo da je A_n grupa. Grupu A_n nazivamo alternirajuća grupa.

Definicija 2.1.17. *Neka je H podgrupa od G. Kažemo da je H normalna podgrupa ako je*

$$xHx^{-1} = H, \ \text{za svaki } x \in G \ (\text{ekvivalento sa } xH = Hx, \ \text{za svaki } x \in G).$$

Sljedeći rezultat je dobro poznat. Za dokaz vidi [1], str. 14.

Teorem 2.1.18. *Neka je H normalna podgrupa. Tada je G/H grupa u odnosu na množenje definirano sa:*

$$(xH)(yH) = xyHH = xyH$$

Definicija 2.1.19. *Neka je H normalna podgrupa. Tada grupu G/H zovemo kvocijentna grupa.*

Neka je $S \subset G$. Skup

$$N = N(S) = \{x \in G : xSx^{-1} = S\}$$

zovemo normalizatorom od S.
Ako skup S ima samo jedan element a, onda se skup N naziva centralizatorom od a.
Neka je S skup. Tada skup

$$Z(S) = \{x \in G : xyx^{-1} = y, \ \text{za svaki } y \in S\}$$

nazivamo centralizatorom od S.
Promotrimo li centralizator skupa G dobijemo podgrupu koja se sastoji od svih elemenata od G koji komutiraju sa svim drugim elementima. Takav centralizator naziva se centrom od G i označava se sa $Z(G)$. Direktno vidimo da je

$$xZ(G)x^{-1} = Z(G)$$

pa je zato $Z(G)$ normalna podgrupa od G.

Primjer 2.1.20. *Neka je*

$$SL(n,\mathbb{R}) = \{A \in GL(n,\mathbb{R}) : detA = 1\}.$$

Tada je $SL(n,\mathbb{R})$ *normalna podgrupa opće linearne grupe* $GL(n,\mathbb{R})$.

Niz homomorfizama i grupa

$$G' \xrightarrow{f} G \xrightarrow{g} G''$$

zovemo egzaktnim ako je $\mathrm{Im}(f) = \mathrm{Ker}(g)$.
Promotrimo li 0 kao trivijalnu grupu, niz

$$0 \to G' \xrightarrow{f} G \xrightarrow{g} G'' \to 0$$

je egzaktan ako je f injekcija, g surjekcija te $\mathrm{Im}(f) = \mathrm{Ker}(g)$.
Ako je $H = \mathrm{Ker}(g)$, tada imamo egzaktan niz

$$0 \to H \to G \to G/H \to 0.$$

2.2 Nizovi podgrupa i rješive grupe

Definicija 2.2.1. *Neka je G grupa. Kažemo da je niz podgrupa*

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_m$$

normalan ako je svaka G_{i+1} *normalna u* G_i, $i = 0, 1, \ldots, m-1$, *a Abelov ako je normalan i ako je svaka kvocijentna grupa* G_i/G_{i+1} *Abelova.*

Neka je $f\colon G \to G'$ homomorfizam grupa te

$$G' = G'_0 \supset G'_1 \supset \ldots \supset G'_m \tag{2.5}$$

normalan niz grupa. Tada je

$$G = G_0 \supset G_1 \supset \ldots \supset G_m, \quad G_i = f^{-1}(G'_i) \tag{2.6}$$

normalan niz grupa i za svaki k imamo injektivni homomorfizam

$$G_k/G_{k+1} \to G'_k/G'_{k+1}.$$

Nadalje, ako je niz (2.5) Abelov, onda je i niz (2.6) Abelov te ako je niz (2.5) ciklički, onda je i niz (2.6) ciklički.

Popunjenje niza je onaj niz kojega dobijemo umetanjem konačnog broja podgrupa.

Definicija 2.2.2. *Kažemo da je grupa G rješiva ako se može prikazati kao niz*

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_m = \{e\}$$

koji je Abelov.

Propozicija 2.2.3. *Neka je G konačna grupa. Abelov niz od G ima cikličko popunjenje. U slučaju kada je G rješiva, može se postići da to cikličko popunjenje završava trivijalnom podgrupom.*

Dokaz. Druga tvrdnja je direktna posljedica prve. Dovoljno je pokazati da svaka konačna Abelova grupa ima ciklički niz podgrupa. Dokaz provodimo induktivno po redu grupe G. Neka je

$$G = G_0 \supset \cdots \supset G_i \supset G_{i+1} \supset \cdots \supset G_m$$

Abelov niz. Uzmimo

$$x \in G,\ x \neq e,\ X = \langle x \rangle \text{ te } G' = G/X.$$

Po pretpostavci indukcije G' ima ciklički niz podgrupa. Imamo sljedeći dijagram:

$$\begin{array}{ccccc} G = G_0 & \supset \cdots \supset & & X & \supset \quad \{e\} \\ \downarrow & & & \downarrow & \\ G' = G'_0 & \supset \cdots \supset & G'_m = \{e\} & & \end{array}$$

Uzimanjem inverznih slika dobivamo ciklički niz podgrupa koja završava s X. Profinimo ga dodavanjem $\{e\}$ na kraju. Na ovaj način dobili smo traženi niz podgrupa. □

Teorem 2.2.4. *Neka je G grupa i H normalna podgrupa. G je rješiva ako i samo ako su H i G/H rješive.*

Dokaz. Pretpostavimo da je G rješiva i neka je $G = G_0 \supset G_1 \supset \cdots \supset G_r = \{e\}$ niz podgrupa. Budući da je G rješiva, G_{i+1} je normalna u $G_i,\ i = 0, 1, \ldots, r-1$ te je G_i/G_{i+1} Abelova.
Uzmimo da je $H_i = H \cap G_i$. Tada je H_{i+1} normalna u H_i i $H_i/H_{i+1} \to G_i/G_{i+1}$, zbog čega je H_i/H_{i+1} Abelova pa je H rješiva. Analogno se pokaže i za G/H.
Obrat tvrdnje dobijemo tako da uzmemo odgovarajuće popunjenje niza podgrupa od H dok ne dobijemo grupu G. □

Definicija 2.2.5. *Neka je G grupa. Podgrupu*

$$G^C = \langle xyx^{-1}y^{-1} :\ x, y \in G \rangle$$

zovemo komutatorska podgrupa od G.

Za $x, y \in G$ element oblika $xyx^{-1}y^{-1}$ zove se komutator elemenata x i y.

Teorem 2.2.6. *Za sve $n \geq 5$, simetrična grupa S_n nije rješiva.*

Dokaz. Neka je $N \subset H \subset S_n, N$ normalna podgrupa od H te H/N Abelova. Pokažimo da ako H sadrži sve 3−cikluse da tada N sadrži sve 3−cikluse.
Uzmimo $\{i, j, k, r, s\} \subset \{1, \ldots, n\}$ i neka je $\sigma = [i\ j\ k]$, $\tau = [k\ r\ s]$. Tada je

$$\sigma\tau\sigma^{-1}\tau^{-1} = [r\ k\ i] \ \in N.$$

Pretpostavimo sada da imamo normalan niz podgrupa

$$S_n = H_0 \supset H_1 \supset \cdots \supset H_m = \{e\}, \quad H_{i+1}/H_i \text{ Abelova.}$$

Budući da S_n sadrži sve 3−cikluse, onda H_1 sadrži sve 3−cikluse. Indukcijom slijedi da H_m sadrži sve 3−cikluse, što je kontradikcija. □

Definicija 2.2.7. *Kažemo da je netrivijalna grupa G prosta, odnosno jednostavna, ako su njene jedine normalne podgrupe $\{e\}$ i G.*

Definicija 2.2.8. *Neka je G grupa, gdje su njeni normalni nizovi dani sa*

$$G = G_1 \supset G_2 \supset \cdots \supset G_r = \{e\}$$

$$H = H_1 \supset H_2 \supset \cdots \supset H_s = \{e\}.$$

Kažemo da su ekvivalentni ako je $r = s$ i ako postoji permutacija indeksa $i = 1, \ldots, r-1$, $i \mapsto i'$, takva da je $G_i/G_{i+1} \approx H_{i'}/H_{i'+1}$.

Lema 2.2.9 (**Butterfly Lema**). *Neka su U, V, u, v podgrupe grupe G, gdje je u normalna podgrupa od U, a v normalna podgrupa od V. Tada je $u(U \cap v)$ normalna u $u(U \cap V)$, $(u \cap V)\, v$ normalna u $(U \cap V)\, v$ i postoji izomorfizam:*

$$\frac{u(U \cap V)}{u(U \cap v)} \approx \frac{(U \cap V)\, v}{(u \cap V)\, v}.$$

Za dokaz vidi [1], str. 20.

Teorem 2.2.10 (**Schreier**). *Neka je G grupa. Dva normalna niza podgrupa koja završavaju sa trivijalnom grupom imaju ekvivalentna popunjenja.*

Dokaz. Neka je G grupa i

$$G = G_1 \supset G_2 \supset \cdots \supset G_r = \{e\},$$

$$G = H_1 \supset H_2 \supset \cdots \supset H_s = \{e\}$$

dva silazna normalna niza od G. Definiramo

$$G_{ij} = G_{i+1}\left(H_j \cap G_i\right),\ i = 1, \ldots, r-1,\ j = 1, \ldots, s.$$

Tada je $G_{is} = G_{i+1}$ pa je popunjenje prvog silaznog niza dano sa:

$$G = G_{12} \supset G_{12} \supset \cdots \supset G_{1,s-1} \supset G_2$$

$$= G_{21} \supset G_{22} \supset \cdots \supset G_{r-1,1} \supset \cdots \supset G_{r-1,s-1} \supset \{e\}.$$

Na isti način za $j = 1, \ldots, s-1,\ i = 1, \ldots, r$ definiramo

$$H_{ji} = H_{j+1}\left(G_i \cap H_j\right)$$

pa dobijemo popunjenje drugog silaznog niza podgrupa od G. Oba popunjenja imaju $(r-1)(s-1)+1$ elemenata te završavaju trivijalnim elementom. Budući da po Butterfly lemi za $i = 1, \ldots, r-1,\ j = 1, \ldots, s-1$ imamo izomorfizam:

$$\frac{G_{ij}}{G_{i,j+1}} \approx \frac{H_{ji}}{H_{j,i+1}},$$

tvrdnja je dokazana jer su navedena popunjenja ekvivalentna za svaki par indeksa (i, j). □

Teorem 2.2.11 (**Jordan Hölder**). *Neka je G grupa sa normalnim nizom podgrupa*

$$G = G_1 \supset G_2 \supset \cdots \supset G_r = \{e\}, \tag{2.7}$$

koji je takav da je svaka grupa G_i/G_{i+1} prosta te je $G_i \neq G_{i+1},\ i = 1, \ldots, r-1$. Tada je svaki drugi normalni niz podgrupa od G sa istim svojstvima ekvivalentan normalnom nizu (2.7).

Za dokaz vidi [1], str. 22.

2.3 Cikličke grupe

Neka je $H \subset \mathbb{Z}$ podgrupa. Tada postoji $a \in H$ takav da je

$$H = a\mathbb{Z} = \{an : n \in \mathbb{Z}\}.$$

Definicija 2.3.1. *Kažemo da je grupa G ciklička ako postoji $a \in G$ takav da je*

$$G = \{a^n : n \in \mathbb{Z}\}.$$

U tom slučaju koristimo oznaku $G = \langle a \rangle$ i kažemo da je a generator od G.

Definicija 2.3.2. *Najmanji $m > 0$ takav da je $a^m = e$ zovemo eksponentom od a.*

Definicija 2.3.3. *Najmanji $m > 0$ takav da je $x^m = e$, za svaki $x \in G$ zovemo eksponentom od G.*

Definicija 2.3.4. *Neka je G grupa i $f : \mathbb{Z} \to G$ homomorfizam dan sa $f(n) = a^n$, za koji je $Ker(f) = d\mathbb{Z}$, $d > 0$. Taj d je jedinstven i zovemo ga periodom, odnosno redom od a. Ako je $d = 0$ kažemo da je a beskonačnog reda.*

Propozicija 2.3.5. *Neka je G konačna grupa reda $n > 1$. Red njenog elementa $a \neq e$ dijeli n. Ako je red od G prost broj p, tada je G ciklička i svaki generator je reda p.*

Dokaz. Neka je H ciklička grupa generirana s a. Tada je H reda $|a|$ i tvrdnja slijedi direktno iz Propozicije 2.1.13. □

Propozicija 2.3.6. *Neka je G ciklička grupa. Tada je svaka podgrupa od G ciklička. Neka je $f : G \to G'$ homomorfizam grupa. Tada je* $\mathrm{Im}(f)$ *ciklička podgrupa od G'.*

Dokaz. Ako je G beskonačna ciklička grupa, tada je ona izomorfna sa $\mathbb{Z}$. Svaka podgrupa od $\mathbb{Z}$ je oblika $m\mathbb{Z}$, za neki $m \in Z_{\geq 0}$, koja je jasno ciklička. Neka je $f : G \to G'$ homomorfizam, gdje je $G = \langle a \rangle$. Tada je $f(G) = \langle f(a) \rangle$ pa je zato $f(G)$ ciklička.
Neka je sada H podgrupa cikličke grupe G. Promotrimo surjektivan homomorfizam $f : \mathbb{Z} \to G$, $f(n) = a^n$. Tada je $f^{-1}(H)$ podgrupa od $\mathbb{Z}$ pa je ona ciklička i nužno oblika $m\mathbb{Z}$, $m \in \mathbb{Z}_{\geq 0}$. Dakle, postoji surjektivan homomorfizam $m\mathbb{Z} \to H$ pa je zato i H ciklička grupa. □

Propozicija 2.3.7. *Dvije cikličke grupe istog reda m su izomorfne.*

Dokaz. Neka je $G = \langle a \rangle$, $|G| = m$. Tada postoji surjektivan homomorfizam $f : \mathbb{Z} \to G$, $f(n) = a^n$. Jezgra tog homomorfizma je ciklička podgrupa $k\mathbb{Z}$, $k \in \mathbb{Z}_{\geq 0}$. Tada je $\mathbb{Z}/k\mathbb{Z} \approx G$ pa je zato $k = m$. □

Propozicija 2.3.8. *(i) Neka je G ciklička grupa sa dva generatora a, b. Tada postoji automorfizam grupe G koji šalje a u b. Vrijedi i obrat. Svaki automorfizam od G preslika a na neki generator grupe G.*

(ii) Neka je G ciklička grupa reda n te $d > 0$, takav da $d \mid n$. Tada postoji jedinstvena podgrupa od G reda $d > 0$.

(iii) Neka su G_1, G_2 cikličke grupe reda m, odnosno n. Ako su m i n relativno prosti tada je i grupa $G_1 \times G_2$ ciklička.

(iv) Neka je G konačna Abelova grupa. Ako G nije ciklička tada postoji prost broj p i podgrupa od G izomorfna sa $C \times C$, gdje je C ciklička grupa reda p.

Dokaz. (i) Neka je $G = \langle a \rangle = \langle b \rangle$. Tada vidimo da je sa $f\left(a^k\right) = b^k$ dobro definiran automorfizam koji šalje a u b. Dokažimo sada drugu tvrdnju.
Neka je $G = \langle a \rangle$ i f automorfizam od G. Pokažimo da je $G = \langle b \rangle$, gdje je $b = f(a)$. Uzmimo proizvoljan element $y \in G$. Budući da je f automorfizam od G, to postoji $x \in G$, takav da je $y = f(x)$. No, $x \in G$ pa postoji $k \in \mathbb{Z}_{\geq 0}$, takav da je $x = a^k$. Tada je $y = f(a)^k = b^k$. Ovim smo pokazali da je G ciklička grupa generirana s b.

(ii) Pretpostavimo da $d \mid n$, odnosno $md = n$, $m \in \mathbb{Z}_{\geq 0}$. Neka je $f\colon \mathbb{Z} \to G$ surjektivan homomorfizam. Tada je $f(m\mathbb{Z})$ podgrupa od G, a zbog izomorfizma $\mathbb{Z}/m\mathbb{Z} \approx G/f(m\mathbb{Z})$ je indeks $[G : f(m\mathbb{Z})] = m$, odnosno $f(m\mathbb{Z})$ je reda d.
Promotrimo i obrat tvrdnje. Neka je H podgrupa od G reda d. Tada je $f^{-1}(H) = m\mathbb{Z}$, odnosno $H = f(m\mathbb{Z})$, $m \in \mathbb{Z}_{\geq 0}$. $\mathbb{Z}/m\mathbb{Z} \approx G/H$ pa je $n = md$ i H je jedinstveno određena.

(iii) Neka su $G_1 = \langle a \rangle$ i $G_2 = \langle b \rangle$ cikličke grupe, takve da je $|G_1| = m$, $|G_2| = n$, gdje su m, n relativno prosti. Promotrimo li homomorfizam

$$f\colon \mathbb{Z} \to G_1 \times G_2, \text{ dan sa } f(k) = \left(a^k, b^k\right), \text{ za svaki } k \in \mathbb{Z},$$

možemo uočiti da element u jezgri mora biti djeljiv i sa m i sa n. Budući da su m i n relativno prosti, element iz jezgre mora biti djeljiv i sa njihovim produktom mn. S druge strane, jasno je da je $mn\mathbb{Z}$ sadržana u jezgri pa je $\operatorname{Ker}(f) = mn\mathbb{Z}$. Osim toga, f je surjektivan homomorfizam po kineskom teoremu o ostacima. Dobili smo da je $\operatorname{Im}(f) \approx G_1 \times G_2 \approx \mathbb{Z}/(mn\mathbb{Z})$, prema tome $G_1 \times G_2$ je izomorfna cikličkoj grupi reda mn.

(iv) Slijedit će direktno iz osnovnog strukturnog teorema o Abelovim grupama, odnosno Teorema 3.2.5.

□

2.4 Djelovanje grupe na skupu

Definicija 2.4.1. *Neka je S skup. Kažemo da grupa G djeluje na S ako je zadano preslikavanje*

$$G \times S \to S, \quad (x, s) \mapsto x.s$$

takvo da vrijedi:

(1) $(xy).s = x.(y.s)$, *za svaki* $x, y \in G$, $s \in S$,

(2) $e.s = s$, *za svaki* $s \in S$, *gdje je* e *jedinica u* G.

Promotrimo djelovanje grupe G na samu sebe. Za $x \in G$ definiramo preslikavanje

$$c_x \colon G \to G,\ c_x(y) = xyx^{-1}.$$

Vidimo da je $x \mapsto c_x$ homomorfizam sa $G \to Aut(G)$ i prema tome na taj način je definirano djelovanje grupe G na samu sebe. To djelovanje zove se konjugiranje.
Jezgra $x \mapsto c_x$ jednaka je

$$Z(G) = \{x \in G : xy = yx\},$$

tj. jezgra je centar grupe G.
Konjugiranje možemo promatrati i na skupu podskupova S grupe G. Tada je za

$$A \in S,\ c_x(A) = xAx^{-1}.$$

Neka su A, B dva podskupa. Kažemo da su oni konjugirani ako postoji $x \in G$ takav da je $B = xAx^{-1}$.
Osim toga možemo promatrati i translaciju koja je definirana kao preslikavanje

$$T_x \colon G \to G,\ T_x(y) = xy.$$

Definicija 2.4.2. *Neka* G *djeluje na* S *i neka je* $s \in S$. *Kažemo da je*

$$G_s = \{x \in G :\ x.s = s\}$$

stabilizator točke $s \in S$, *a*

$$Gs = \{x.s :\ x \in G\}$$

zovemo orbitom točke $s \in S$.

Lema 2.4.3. *Neka* G *djeluje na skup* S *i neka je* $s \in S$. *Tada je*

$$|Gs| = [G : G_s].$$

Dokaz. Lako se vidi da je preslikavanje

$$f \colon Gs \to G/G_s,\ \text{dano sa } f(xs) = xG_s$$

dobro definirano i bijekcija. Odatle slijedi tvrdnja. □

Teorem 2.4.4. *Pretpostavimo da grupa* G *djeluje na konačan skup* S. *Tada je*

$$card(S) = \sum_{i \in I} [G : G_{s_i}].$$

Dokaz. Prvo uočimo da djelovanje grupe G na skup S definira na S jednu particiju skupa, a članovi te particije su orbite. Dakle, S je disjunktna unija orbita:

$$S = \bigcup_{i \in I} Gs_i.$$

Tada iz Leme 2.4.3 slijedi:

$$card\,(S) = \sum_{i \in I} [G : G_{s_i}].$$

□

Teorem 2.4.5. *Neka je G konačna grupa koja djeluje na samu sebe konjugiranjem. Tada je jednadžba klasa dana sa:*

$$[G : 1] = \sum_{x \in C} [G : G_x],$$

gdje je C skup predstavnika klasa konjugiranih elemenata.

Dokaz. Primjenimo prethodni teorem za slučaj $S = G$ i konjugacijskog djelovanja. □

2.5 Sylowljeve podgrupe

Definicija 2.5.1. *Neka je G konačna grupa i p prost broj.*

(i) Kažemo da je G p-grupa, ako je $|G| = p^n,\ n \geq 0$.

(ii) Podgrupa H grupe G je p-podgrupa od G ako je H p-grupa.

(iii) H zovemo Sylowljevom p-podgrupom ako je $|H| = p^n$ i ako je p^n najveća potencija od p koja dijeli $|G|$.

Lema 2.5.2. *Neka je G konačna Abelova grupa reda m i p prost broj, $p \mid m$. Tada G sadrži podgrupu reda p.*

Dokaz. Dokažimo prvo da ako je n eksponent od G, onda $|G|$ dijeli neku potenciju od n. Dokaz te tvrdnje provodimo indukcijom po n.
Za $n = 1$ tvrdnja vrijedi. Pretpostavimo da vrijedi i za sve grupe eksponenta manjeg od n. Neka je sada G grupa eksponenta n. Odaberimo $b \in G, b \neq 1$. Tada je $H = \langle b \rangle$ ciklička, $|H|$ dijeli n i n je eksponent od G/H. Iz induktivne pretpostavke slijedi da $|G/H|$ dijeli n^s, za neki s. Tvrdnja slijedi iz

$$[G : 1] = |G| = [G : H] \cdot |H|.$$

Dakle, $|G|$ dijeli neku potenciju od n. Neka sada $p \mid |G| = m$.
Tada postoji x takav da $p \mid r(x)$ = red od x. (U suprotnom za svaki x,

$$p \nmid n \text{ pa } p \neq n = \prod_x r(x) \text{ i n je eksponent.}$$

To je kontradikcija zbog $p \mid m$ i $m \mid n^s$). Znači da je $x^{p^\ell} = e$, za neki ℓ pa prema tome $x^\ell \neq e$ generira cikličku grupu reda p. □

Teorem 2.5.3. *Neka je G konačna grupa i p prost broj, koji dijeli njen red. Tada postoji Sylowljeva p-podgrupa od G.*

Dokaz. Tvrdnju teorema dokazujemo indukcijom po redu grupe. Ako je red grupe prost broj, tada je tvrdnja jasna. Pretpostavimo da tvrdnja vrijedi za sve grupe G takve da je $|G| < N \in \mathbb{Z}_{>0}$. Neka je sada G grupa reda $N = p^n r$ i n je najveća potencija od p koja dijeli N.

(1) Pretpostavimo da postoji podgrupa $H \subsetneq G$, takva da je $[G : H]$ relativno prost s p. Tada je $|H| = p^n s$, za neki $s < r$. Po pretpostavci indukcije postoji Sylowljeva $p-$podgrupa P od H, no tada je P Sylowljeva podgrupa od G.

(2) Pretpostavimo da $p \mid [G : H]$ za svaku podgrupu $H \subsetneq G$. Primjenimo jednadžbu klasa za konjugirano djelovanje i dobijemo

$$|G| = |Z(G)| + \sum_{\text{orbite od bar 2 elementa}} [G : G_x],$$

gdje je $Z(G)$ centar grupe G. No $[G : G_x] > 1$ je djeljivo s p. Odatle slijedi da $p \mid |Z(G)|$. Lema 2.5.2 povlači da postoji podgrupa $H \subset Z(G)$, koja je ciklička podgrupa reda p. Uočimo da je H normalna jer je u centru.
Promatramo kanonski epimorfizam $f : G \to G/H$.
Budući da je $|G/H| = p^{n-1} r$, iz pretpostavke indukcije slijedi da postoji Sylowljeva p-podgrupa K' u G/H.
Neka je $K = f^{-1}(K')$. Tada je

$$K \supset H,\ f|_K : K \to K' \text{ i } K/H \cong K'.$$

Odatle slijedi da je $|K| = p^n$. Dakle, K je Sylowljeva $p-$podgrupa.

□

Lema 2.5.4. *Neka je H p-grupa koja djeluje na konačan skup S te fiksna točka $s \in S$ takva da je $xs = s$, za svaki $x \in H$. Tada je:*

(i) Broj fiksnih točaka od H je oblika $kp + card\,(S)\,,\ k \in \mathbb{Z}_{\geq 0}$.

(ii) Ako H ima točno jednu fiksnu točku $card\,(S)$ *je dan sa* $kp + 1,\ k \in \mathbb{Z}_{\geq 0}$.

(iii) Ako $p \mid card\,(S)$*, tada je broj fiknih točaka od H oblika* $kp,\ k \in \mathbb{Z}_{\geq 0}$.

Dokaz. Budući da su (ii) i (iii) posebni slučajevi od (i), dokazat ćemo samo slučaj (i). Koristit ćemo formulu za jednadžbu klasa:

$$card\,(S) = \sum_{s_i \in S} [H : H_{s_i}]$$

$$= \sum_{s_i \text{ fiksna točka}} [H : H_{s_i}] + \sum_{s_i \text{ nije fiksna točka}} [H : H_{s_i}].$$

Promotrimo ta dva slučaja.

Kada je s_i fiksna točka slijedi da je $[H : H_{s_i}] = [H : H] = 1$.

Kada s_i nije fiksna točka slijedi da je $[H : H_{s_i}] = kp,\ k \in \mathbb{Z}_{\geq 0}$.

Dakle, broj fiksnih točaka od H je oblika $kp + card\,(S)\,,\ k \in \mathbb{Z}_{\geq 0}$. □

Teorem 2.5.5. *Neka je G konačna grupa.*

(i) Svaka p-podgrupa je sadržana u nekoj Sylowljevoj p-podgrupi.

(ii) Sve Sylowljeve p-podgrupe su konjugirane.

(iii) Broj Sylowljevih p-podgrupa od G je oblika $kp + 1,\ k \in \mathbb{Z}_{\geq 0}$.

Dokaz. (i) Neka je S skup svih Sylowljevih p-podgrupa u G. Grupa G djeluje na S konjugacijom:

$$P \mapsto xPx^{-1}.$$

Jasno je da je $P \subset G_P$, gdje je G_P stabilizator grupe P. Broj elemenata orbite

$$S_0 = G.P = [G : G_P]$$

je relativno prost s p.

Neka je H $p-$podgrupa reda > 1. Promotrimo djelovanje od H na orbiti S_0.

S_0 je unija orbita od H s brojem elemenata $[H : H_{P'}]$.

Ako je $[H : H_{P'}] > 1$, tada $p \mid [H : H_{P'}]$ pa zbog toga postoji barem jedna jednočlana orbita $\{P'\}$. Iz toga slijedi da H normalizira P', odnosno

$$hP'h^{-1} = P',\ \text{za svaki } h \in H$$

pa je i HP' podgrupa:

$$hph_1p_1 = hh_1h_1^{-1}ph_1p_1 \in HP'.$$

Nadalje imamo da je $P' \subset HP'$ normalna podgrupa te da je

$$HP'/P' \cong H/(H \cap P').$$

To povlači da je red od HP' potencija od p. Zbog maksimalnosti je $HP' = P'$ pa je $H \subset P'$.

(ii) Neka je H Sylowljeva p-podgrupa. Iz (i) imamo da je $H \subseteq P'$, gdje je P' Sylowljeva. Iz toga slijedi da je $H = P'$. Budući da je P' konjugirana zadanoj P, slijedi da je $H = xPx^{-1}$.

(iii) Uzmimo da je $H = P$, $S_0 = G.P$. Tada H djeluje na S_0 konjugiranjem. Točno jedna orbita od H ima jedan element: $\{P\}$. Ostale orbite u S_0 imaju $[H : H_x]$ elemenata i taj broj je djeljiv s p. Zbog (ii) su sve Sylowljeve p-podgrupe konjugirane pa su u S_0. Odatle slijedi tvrdnja.

□

Teorem 2.5.6. *Neka je G konačna p-grupa. Tada je G rješiva grupa. Nadalje, ako je $|G| > 1$, tada je centar $Z(G)$ netrivijalan.*

Dokaz. Uočimo da je $G/Z(G)$ Abelova grupa, zato $G/Z(G)$ ima Abelov niz podgrupa. Ako je $Z(G)$ netrivijalan, tada Abelov niz podgrupa za $G/Z(G)$ možemo nadopuniti do Abelovog niza podgrupa od G. To pokazuje da je G rješiva uz uvjet netrivijalnosti centra. Pokažimo sada da je $Z(G)$ netrivijalan. Stoga prva tvrdnja slijedi iz druge. Promotrimo:

$$|G| = |Z(G)| + \sum_{\text{orbite s barem dva elementa}} [G : G_x].$$

Budući da p dijeli red grupe G i p dijeli svaki $[G : G_x]$, zaključujemo da p dijeli red centra $Z(G)$. Dakle, centar $Z(G)$ je netrivijalan. □

Korolar 2.5.7. *Neka je G p-grupa, $|G| \neq 1$. Tada postoji niz podgrupa*

$$G = G_n \supset \cdots \supset G_2 \supset G_1 \supset G_0 = \{e\},$$

takav da je G_i normalna podgrupa od G te su G_{i+1}/G_i cikličke reda p.

Dokaz. Po Teoremu 2.5.6 G ima netrivijalan centar pa u njemu postoji $a \neq e$, takav da je on reda p. Neka je $H = \langle a \rangle$. Pretpostavimo da je $G \neq H$ pa induktivno možemo naći niz podgrupa u G/H. Upravo je inverz tog niza traženi niz u G. □

Lema 2.5.8. *Neka je G konačna grupa i H podgrupa takva da je $[G : H] = p$, gdje je najmanji prost broj, takav da $p \mid |G|$. Tada je H normalna.*

Dokaz. Neka je $N(H)$ normalizator od H. Kada bi bilo $N(H) = G$, H bi bila normalna podgrupa i bili bismo gotovi.
Pretpostavimo da je $N(H) = H$. Tada orbita od H ima $p = [G : H]$ elemenata. Djelovanje od G na toj orbiti daje homomorfizam

$$\phi \colon G \to S_p, \text{ gdje je } |S_p| = p!.$$

Neka je $K = \mathrm{Ker}(\phi)$. Tada je

$$[G : K] = [G : H][H : K] = p[H : K].$$

Budući da samo p dijeli $p!$, treba postojati još neki prosti broj koji će dijeliti $(p-1)!$ i $[H : K]$. Međutim, kada bi takav postojao to bi bila kontradikcija s tvrdnjom da je p najmanji takav prost broj. □

Propozicija 2.5.9. *Neka je G grupa reda pg, gdje su p, q, $p \neq q$ prosti brojevi. Tada je G rješiva.*

Dokaz. Pretpostavimo da je $p < q$. Neka je Q Sylowljeva grupa, $|Q| = q$. Tada je $[G : Q] = p$ pa je Q po prethodnoj lemi normalna, a po Propozicji 2.3.5 znamo da je grupa prostog reda ciklička pa slijedi tvrdnja. □

Više riječi o grupama reda pq će biti kasnije u Propoziciji 4.1.6.

Poglavlje 3

Abelove grupe

U ovom poglavlju definirat ćemo direktne sume i slobodne Abelove grupe. Nakon toga proučit ćemo konačno generirane Abelove grupe. Posebnu pažnju posvetit ćemo torzionoj grupi koju smo definirali kao skup koji se sastoji od elemenata konačnog reda. Osim toga definirat ćemo i grupu bez torzije. Ti iskazi i definicije mogu se pronaći u knjizi [1].

3.1 Direktne sume i slobodne Abelove grupe

Definicija 3.1.1. *Neka su $(G, \cdot_G)$ i $(H, \cdot_H)$ grupe. Grupu sa binarnom operacijom na $G \times H$ definiranom sa*

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2)$$

nazivamo direktan produkt grupa i označavamo sa $G \oplus H$.

Definicija 3.1.2. *Neka je $(A_i)_{i \in I}$ familija Abelovih grupa. Definiramo direktnu sumu kao skup:*

$$A = \bigoplus_{i \in I} A_i = \{(x_i) : x_i = 0 \text{ za sve osim konačno indeksa } i \in I\} \subset \prod A_i,$$

gdje $\prod A_i$ označava direktan produkt grupa.

Primjer 3.1.3. *Neka su B, C podgrupe Abelove grupe A, takve da je $B+C = A$ i $B \cap C = \{0\}$. Preslikavanje $B \times C \to A$ dano sa $(x, y) \mapsto x + y$ je izomorfizam. Tada pišemo $A = B \oplus C$.*

Propozicija 3.1.4. *Neka je $A = \bigoplus_{i \in I} A_i$, B Abelova grupa te $\{f_i : A_i \to B\}$ familija homomorfizama. Tada postoji jedinstveno preslikavanje $f : A \to B$, $f \circ \lambda_j = f_j$, za svaki j, gdje je $\lambda_j : A_j \to A$ takva da su za $\lambda_j(x)$ sve komponente 0, osim j-te koja je x.*

Dokaz. Imamo :

$$\lambda_j \colon A_i \to \bigoplus_{i\in I} A_i, \qquad f \colon \bigoplus_{i\in I} A_i \to B, \qquad f_i \colon A_i \to B.$$

Uočimo da je $f \circ \lambda_j(x) = f_j(x)$, za svaki j i za svaki $x \in A_j$. Definiramo $f \colon A \to B$ sa

$$f((x)_{i\in I}) = \sum_{i\in I} f_i(x_i).$$

Sada je f definirana na jedinstven način i suma na desnoj strani je konačna jer su svi sumandi 0, osim konačno mnogo njih. □

Definicija 3.1.5. *Neka je A Abelova grupa.*

(i) Kažemo da je $\{e_i\}$ baza za A, ako se svaki $x \in A$ može zapisati kao $x = \sum e_i x_i$, gdje je skoro svaki $x_i \in \mathbb{Z}$ jednak 0.

(ii) Broj elemenata baze zove se rang od A.

Definicija 3.1.6. *Kažemo da je Abelova grupa G slobodna ako ona ima bazu.*

Slobodnu Abelovu grupu prikazujemo kao skup

$$\mathbb{Z}\langle S\rangle = F_{ab}(S) = \{\rho \colon S \to \mathbb{Z} \mid \rho(x) = 0 \text{ za skoro svaki } x \in S\},$$

gdje skup S nazivamo njezinim generatorom.

Neka je ρ preslikavanje takvo da je $\rho(x) = k,\ k \in \mathbb{Z},\ x \in S$. Tada se $\rho \in \mathbb{Z}\langle S\rangle$ može zapisati kao:

$$\rho = k_1 x_1 + \ldots + k_n x_n,\ k_i \in \mathbb{Z},\ x_i \in S.$$

Lema 3.1.7. *Neka je $A \xrightarrow{f} A'$ surjektivan homomorfizam Abelovih grupa, od kojih je A' slobodna Abelova grupa. Tada postoji podgrupa C od A, takva da je $f|_C \colon C \to A'$ izmorfizam za kojega je $A = B \oplus C$, gdje je $B = \operatorname{Ker}(f)$.*

Dokaz. Budući da je A' slobodna Abelova grupa po definiciji ima bazu. Neka je to $\{x'_i\}_{i\in I}$. Neka je $f(x_i) = x'_i$, za svaki $i \in I,\ x_i \in A$. Po iskazu leme postoji podgrupa C, takva da je $C \xrightarrow{f|_C} A'$ izomorfizam. Uzmimo onda da je generirana sa $x_i,\ i \in I$. Promotrimo jednakost

$$\sum_{i\in I} n_i x_i = 0,\ n \in \mathbb{Z}_{\geq 0},$$

u kojoj su skoro svi sumandi 0. Ako na nju djelujemo sa f slijedi:

$$0 = \sum_{i\in I} n_i f(x_i) = \sum_{i\in I} n_i x'_i. \tag{3.1}$$

Odatle slijedi da je za svaki i $n_i = 0$, odnosno da je $\{x_i\}_{i\in I}$ baza za C. Tada $x \in A$ možemo zapisati kao $x = \sum_{i\in I} n_i x_i$. Djelujemo li na tu jednakost sa f imamo:

$$f(x) = \sum_{i\in I} n_i f(x_i) = \sum_{i\in I} n_i x_i' \overset{(3.1)}{=} 0. \tag{3.2}$$

Dakle,

$$x - \sum_{i\in I} n_i x_i = b \in B,$$

odnosno nalazi se u jezgri od f, što povlači da je $x \in B + C$.
Za $y \in C$ takav da je $f(y) = 0$, vrijedi da je i $y = 0$ pa je $B \cap C = 0$.
Slijedi da je $A = B \oplus C$.

□

Teorem 3.1.8. *Neka je B podgrupa slobodne Abelove grupe A. Tada je i B slobodna Abelova grupa, sa rangom manjim od ranga grupe A.*
Bilo koje dvije baze slobodne Abelove grupe imaju isti kardinalni broj.

Dokaz. Neka je A slobodna Abelova grupa. Tada je možemo zapisati kao:

$$A = \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_n,$$

gdje je $\{x_1, \ldots, x_n\}$ njena baza. Definiramo

$$f\colon A \to \mathbb{Z}x_1,\ f(m_1x_1 + \ldots + m_nx_n) = m_1x_1,\ m_i \in \mathbb{Z}.$$

Budući da je B podgrupa od A, jezgra od $f|_B$ je slobodna podgrupa sadržana u $\langle x_2, \ldots, x_n\rangle$ pa njezina baza ima $\leq n-1$ element. Po Lemi 3.1.7 postoji podgrupa izomorfna podgrupi od $\mathbb{Z}x_1$. Uzmimo da je to $Im(f|_B)$. Ona zadovoljava jednakost:

$$B = Ker(f|_B) \oplus Im(f|_B).$$

Budući da je $f(B)$ ili 0 ili ciklička, slijedi da je B slobodna.
Dokažimo sada drugu tvrdnju teorema. Neka je S baza za B sa m elemenata, a T baza sa barem r elemenata. Dovoljno je pokazati da je $r \leq m$. Neka je p prost broj te P_i cikličke grupe reda p. Tada je :

$$B/pB = \bigoplus_{i=1,\ldots,m} P_i.$$

To povlači da je $|B/pB| = p^m$. Promotrimo li sada bazu T od B, uočavamo da B/pB sadrži $r-$člani produkt cikličkih grupa reda p. Dakle, $p^r \leq p^m$ pa je $r \leq m$. □

3.2 Konačno generirane Abelove grupe

Definicija 3.2.1. *Neka je A Abelova grupa.*

(i) $a \in A$ *zovemo torzionim elementom ako ima konačan period (red).*

(ii) Definiramo torzionu podgrupu od A kao skup:

$$A_{tor} = \{a \in A : a \text{ je torzioni element od } A\}.$$

(iii) A *je torziona grupa ako je* $A = A_{tor}$.

Teorem 3.2.2. *Neka je A torziona Abelova grupa. Tada je A direktna suma svojih podgrupa* $A(p) \neq 0$*, za sve proste p:*

$$A = \bigoplus_{p \text{ prost}} A(p).$$

Dokaz. Pokazat ćemo da je homomorfizam

$$\bigoplus_{\text{p prost}} A(p) \to A, \text{ dan sa } \left(x_p\right) \mapsto \sum x_p$$

injektivan i surjektivan. Da bismo dokazali injektivnost, uzmimo x iz jezgre. Tada je $\sum x_p = 0$. Neka je q prost broj, takav da je

$$x_q = \sum_{p \neq q} \left(-x_p\right).$$

Neka je m najmanji zajednički višekratnik perioda elemenata $x_p,\ p \neq q$. Tada je $mx_q = 0$, za $x_q \neq 0$, ali i $q^r x_q = 0$, za neki $r > 0$. Neka je d najveći zajednički djelitelj od m i q^r. Tada je $dx_q = 0$, a budući da je $d = 1$, slijedi da je $x_q = 0$. Dakle, jezgra homomorfizma je trivijalna.
Pokažimo sada surjektivnost. Neka je za $m \in \mathbb{Z}_{\geq 0}$

$$A_m = \{x \in A : mx = 0\}.$$

Tada je

$$A = \bigcup_{m \in \mathbb{Z}_{\geq 0}} A_m.$$

Uzmemo li da je $m = rs$, gdje su $r,\ s$ relativno prosti, vrijedi da je $A_m = A_r + A_s$. Budući da su $r,\ s$ relativno prosti postoje $a,\ b \in \mathbb{Z}$, takvi da je $ra + sb = 1$. Tada je i $x = arx + bsx$

pa je $arx \in A_s$ te $bsx \in A_r$ pa je tvrdnja dokazana. Ponavljanjem tog postupka, slijedi da ako je

$$m = \prod_{p|m} p^{e(p)}, \text{ tada je } A_m = \sum_{p|m} A_{p^{e(p)}}.$$

Dakle, $\bigoplus_{\text{p prost}} A(p) \to A$ je surjektivan homomorfizam pa je teorem dokazan. □

Primjer 3.2.3. *Neka je $A = \mathbb{Q}/\mathbb{Z}$. Tada je A torziona Abelova grupa.*

$$A \cong \bigoplus_{p} (\mathbb{Q}/\mathbb{Z})(p),$$

$(\mathbb{Q}/\mathbb{Z})(p) = \{a/p^k \mid a \in \mathbb{Z},\ k \in \mathbb{Z}_{\geq 0}\}$.

Neka je A konačna Abelova p-grupa, $b \in A,\ b \neq 0,\ k \geq 0$, takav da $p^k b \neq 0$ ima period p^m. Tada b ima period p^{k+m}.

Lema 3.2.4. *Neka je $\overline{b} \in A/A_1,\ |\overline{b}| = p^r$. Tada postoji predstavnik a od $\overline{b}$ u A, takav da je $|a| = p^r$.*

Dokaz. Neka je b predstavnik od $\overline{b}$ u A. Tada je $p^r b \in A_1 = \langle a_1 \rangle$ pa ga možemo zapisati kao $p^r b = na_1,\ n \geq 0$. Tvrdimo da je $|\overline{b}| \leq |b|$. Kada bi bilo $n = 0$, bili bismo gotovi, stoga pretpostavimo da je $n = p^k \mu$, takav da je μa_1 generator od A_1. Odatle je $|\mu a_1| = p^{r_1}$. Pretpostavimo da je $k \leq r_1$. Tada je

$$|p^k \mu a_1| = p^{r_1 - k}, \text{ što povlači } |b| = p^{r + r_1 - k}.$$

Iz toga slijedi da je $r + r_1 - k \leq r_1$ odnosno $r \leq k$. Tada postoji $c \in A_1$, takav da je $p^r b = p^r c$. Uzmimo da je $a = b - c$. Tada je a predstavnik od $\overline{b}$ u A i $p^r a = 0$ pa je $|a| \leq p^r$, odnosno $|a| = p^r$. □

Teorem 3.2.5. *Svaka konačna Abelova $p-$grupa je izomorfna produktu cikličkih $p-$grupa, redova $p^{r_1}, \ldots p^{r_s}$, gdje je $r_1 \geq r_2 \geq \ldots \geq r_s \geq 1$. Niz prirodnih brojeva $(r_1, \ldots, r_s)$ je jedinstveno određen.*

Dokaz. Bez smanjenja općenitosti možemo pretpostaviti da grupa A nije ciklička. Dokaz provodimo indukcijom po redu grupe. Uzmimo $a_1 \in A$ koji ima najveći period. Neka je $A_1 = \langle a_1 \rangle$ te $|a_1| = p^{r_1}$. Tada je po pretpostavci indukcije A/A_1 izomorfan:

$$A/A_1 = \overline{A_2} \times \cdots \times \overline{A_s},$$

gdje su $\overline{A_i}$ cikličke grupe reda $p^{r_i},\ i = 2, \ldots, s$ i smijemo pretpostaviti da je $r_2 \geq \cdots \geq r_s$. Uzmimo generator $\overline{a_i}$ grupe $\overline{A_i},\ i = 2, \ldots, s$. Po Lemi 3.2.4 postoji predstavnik od $\overline{a_i}$ u A,

koji je istog reda kao i $\overline{a_i}$. Neka je to a_i.
Tvrdimo da je A direktna suma od $A_1, \ldots, A_s$. Za $x \in A$, neka je $\overline{x} \in A/A_1$. Tada postoje $m_i \geq 0,\ i = 2, \ldots, s$, takvi da je

$$\overline{x} = m_2\overline{a_2} + \cdots + m_s\overline{a_s}.$$

Iz toga slijedi da je $x - m_2a_2 - \ldots - m_sa_s \in A_1$ pa postoji $m_1 \geq 0$, takav da je

$$x = m_1a_1 + m_2a_2 + \cdots + m_sa_s.$$

Zbog toga je $A_1 + \cdots + A_s = A$.
Obratno, pretpostavimo da su $m_i \geq 0,\ i = 1, \ldots, s$, takvi da vrijedi:

$$0 = m_1a_1 + \cdots + m_sa_s. \tag{3.3}$$

Budući da smo uzeli da je $|a_i| = p^{r_i},\ i = 1, \ldots, s$, možemo pretpostaviti da je $m_i < p^{r_i}$. Promotrimo li u gornjoj jednadžbi umjesto a_i−ova generatore $\overline{a_i}$ od $\overline{A_i},\ i = 2, \ldots, n$ imamo:

$$0 = m_2\overline{a_2} + \cdots + m_s\overline{a_s}.$$

Odatle slijedi da su $m_i = 0,\ i = 2, \ldots, s$, jer je A/A_1 direktan produkt grupa $\overline{A_2}, \ldots, \overline{A_s}$, ali tada je iz (3.3) i $m_1 = 0$, odnosno $m_i = 0$, za svaki $i = 1, \ldots, s$. To povlači da je

$$(A_1 + \cdots A_i) \cap A_{i+1} = 0, \text{ za svaki } i \geq 1,$$

stoga je A direktan produkt grupa $A_1, \ldots, A_s$. Pokažimo sada jedinstvenost koristeći indukciju. Pretpostavimo da grupu A možemo prikazati na dva načina, kao direktnu sumu cikličkih p−grupa redova

$$p^{r_1}, \ldots, p^{r_s},\ r_1 \geq \cdots \geq r_s \geq 1$$

te kao direktnu sumu cikličkih p−grupa redova

$$p^{m_1}, \ldots, p^{m_k},\ m_1 \geq \cdots \geq m_k \geq 1.$$

Tada je pA također p−grupa, takva da je $|pA| < |A|$ i direktna je suma cikličkih p−grupa redova

$$p^{r_1-1}, \ldots, p^{r_s-1}, \text{ odnosno redova } p^{m_1-1}, \ldots, p^{m_k-1}.$$

Iz pretpostavke indukcije slijedi da je niz prirodnih brojeva $(r_1 - 1, \ldots, r_s - 1)$ jedinstven i jednak nizu $(m_1 - 1, \ldots, m_k - 1)$. Dakle, $r_i - 1 = m_i - 1$, za svaki $i \geq 1$. Kada bi bilo $r_i = 1$, za neki i, tada bi cikličke p−podgrupe reda p^{r_i-1} i reda p^{m_i-1} bile jednake trivijalnoj grupi 0. Zbog toga se cikličke p−grupe, redova

$$p^{r_1}, \ldots, p^{r_s} \text{ te redova } p^{m_1}, \ldots, p^{m_k},$$

mogu razlikovati samo u redu zadnje podgrupe. Tada za neki $n \geq 1$ imamo cikličke $p-$grupe redova:

$$p^{r_1}, \ldots, p^{r_n}, \underbrace{p, \ldots, p}_{\nu \text{ puta}} \text{ i } p^{m_1}, \ldots, p^{m_n}, \underbrace{p, \ldots, p}_{\mu \text{ puta}}.$$

Iz toga slijedi da je red grupe A jednak

$$p^{r_1+\cdots+r_n} p^{\nu} = p^{r_1+\cdots+r_n} p^{\mu}$$

pa je $\nu = \mu$, čime je dokazana jedinstvenost. □

Definicija 3.2.6. *Neka je G grupa. Kažemo da je grupa G grupa bez torzije, ako je svaki $x \in G_{tor}$ jednak jediničnom elementu.*

Teorem 3.2.7. *Neka je A konačna Abelova grupa bez torzije. Tada je A slobodna Abelova grupa.*

Dokaz. Neka je $A \neq 0$ i S konačan skup generatora. Neka je $\{x_1, \ldots, x_n\} \subset S$ najveći podskup od S, takav da ako je

$$v_1 x_1 + v_2 x_2 + \ldots + v_n x_n = 0 \text{ slijedi da je } v_j = 0, \text{ za svaki } j = 1, \ldots, n. \tag{3.4}$$

Neka je B grupa s generatorima $x_1, \ldots, x_n$. Tada je B slobodna Abelova grupa. Za $y \in A$ postoje $m, m_1, \ldots, m_n \geq 0$, od kojih je m različit od 0 ili je barem jedan m_i različit od 0, takvi da

$$my + m_1 x_1 + \ldots + m_n x_n = 0.$$

Zbog (3.4), slijedi da je $m \neq 0$ pa je $my \in B$. Dakle, postoji $m \neq 0$, takav da je $mA \subset B$. Preslikavanje

$$x \mapsto mx$$

na A je homomorfizam sa trivijalnom jezgrom, budući je A grupa bez torzije. Stoga je to preslikavanje i izomorfizam sa A na podgrupu od B. Po Teoremu 3.1.8 slijedi da je mA slobodna Abelova grupa pa je i A slobodna Abelova grupa. □

Teorem 3.2.8. *Neka je A konačno generirana Abelova grupa te A_{tor} njena torziona podgrupa. U tom slučaju je A_{tor} konačna podgrupa, a A/A_{tor} slobodna Abelova grupa. Tada postoji slobodna podgrupa B od A, takva da je $A = B \oplus A_{tor}$.*

Za dokaz vidi [1], str. 46.

Poglavlje 4

Neki primjeri konačnih grupa

U ovom poglavlju slijedimo izlaganje iz poglavlja o grupama maloga reda knjige [2]. Definirat ćemo diedralnu grupu i poludirektan produkt. Kroz propozicije ćemo iskazati rezultate o grupama reda pq i p^2. Za kraj poglavlja klasificirat ćemo sve konačne grupe reda 8 i 12.

4.1 Neki primjeri konačnih grupa

Definicija 4.1.1. *Grupa simetrija pravilnog poligona naziva se diedralna grupa i označava sa D_{2n}.*

Navedimo sada bez dokaza sljedeći rezultat o diedralnim grupama. Za dokaz vidi [2].

Teorem 4.1.2. *Diedralna grupa reda $2n$ generirana je sa dva generatora x i y koji zadovoljavaju sljedeće relacije:*

$$x^n = e, \quad y^2 = e, \quad yxy^{-1} = x^{-1}.$$

Kao skup D_{2n} ima $2n$ elemenata:

$$D_{2n} = \{e,\ x,\ x^2, \ldots,\ x^{n-1},\ y,\ yx,\ yx^2, \ldots,\ yx^{n-1}\}.$$

Propozicija 4.1.3. *Neka je G reda p^2, gdje je p prost broj. Tada je $G \cong \mathbb{Z}_{p^2}$ ili $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.*

Dokaz. Kada bi G imala element reda p^2 pa je tvrdnja očita jer bi vrijedilo $G \cong \mathbb{Z}_{p^2}$.
Pretpostavimo da je $a \in G,\ a \neq e$ reda p.
Neka je $N = \langle a \rangle,\ b \in G,\ b \neq N$ te $H = \langle b \rangle$. Tada je $N \cong \mathbb{Z}_p$ i $H \cong \mathbb{Z}_p$. Budući da je p najmanji prost broj koji dijeli $|G|$, po Lemi 2.5.8 svaka podgrupa od G je normalna, a samim time i N i H. Iz toga slijedi

$$G \cong N \times H \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

□

Definicija 4.1.4. *Neka su N, H podgrupe od G, takve da je*

$$N \cap H = \{e\} \text{ i } NH = G.$$

Kažemo da je G poludirektan produkt od N i H, ako je barem jedna od podgrupa normalna.

Neka su N, H grupe te $\phi\colon H \to Aut(N)$ homomorfizam grupa. Zapišimo $\phi(h) \in Aut(N)$ kao ϕ_h. Definiramo $G = N \rtimes_\phi H = N \rtimes H$ kao skup $N \times H$ na kojem je operacija množenja dana sa:

$$(n_1, h_1)(n_2, h_2) = (n_1 \phi_{h_1}(n_2), h_1 h_2).$$

Uočimo da ćemo N i H promatrati kao podskupove $N \times \{e\}$, odnosno $\{e\} \times H$.

Teorem 4.1.5. *Koristeći gornju notaciju,*

(1) $G = N \rtimes_\phi H$ je grupa.

(2) H je podgrupa od G te je N normalna podgrupa od G.

Dokaz. (1) (e, e) je identiteta od G. Pokažimo da vrijedi asocijativnost:

$$\begin{aligned}((n_1, h_1)(n_2, h_2))(n_3, h_3) &= (n_1 \phi_{h_1}(n_2), h_1 h_2)(n_3, h_3) \\ &= (n_1 \phi_{h_1}(n_2)\, \phi_{h_1 h_2}(n_3), h_1 h_2 h_3) \\ &= (n_1 \phi_{h_1}(n_2)\, \phi_{h_1}(\phi_{h_2}(n_3)), h_1 h_2 h_3) \\ &= (n_1 \phi_{h_1}(n_2 \phi_{h_2}(n_3)), h_1 h_2 h_3) \\ &= (n_1, h_1)(n_2 \phi_{h_2}(n_3), h_2 h_3) \\ &= (n_1, h_1)((n_2, h_2)(n_3, h_3)).\end{aligned}$$

Da bismo dokazali da postoji inverz promotrimo:

$$\left(\phi_{h^{-1}}\left(n^{-1}\right), h^{-1}\right)(n, h) = \left(\phi_{h^{-1}}\left(n^{-1}\right) \cdot \phi_{h^{-1}}(n), h^{-1} h\right) = (\phi_{h^{-1}}(e), e) = (e, e),$$

$$(n, h)\left(\phi_{h^{-1}}\left(n^{-1}\right), h^{-1}\right) = \left(n \phi_h\left(\phi_{h^{-1}}\left(n^{-1}\right)\right), h h^{-1}\right) = \left(n \phi_e\left(n^{-1}\right), e\right) = \left(n n^{-1}, e\right) = (e, e).$$

Dakle, $(n, h)^{-1} = \left(\phi_{h^{-1}}\left(n^{-1}\right), h^{-1}\right)$.

(2) Iz definicije poludirektnog produkta slijedi da su N i H podgrupe od G. Neka je $\pi\colon N \rtimes_\phi H \to H$, dan sa $\phi(n,h) = h$. Vrijedi:

$$\pi((n_1,h_1)(n_2,h_2)) = \pi(n_1\phi_{n_2}(n_2), h_1h_2) = h_1h_2 = \pi(n_1,h_1)\pi(n_2,h_2)$$

pa je π homomorfizam grupa i $N = Ker(\pi)$ pa je N normalna podgrupa od G.

□

Propozicija 4.1.6. *Neka su p i q prosti brojevi, $p > q$ i neka je G grupa reda pq.*

(1) Ako $q \nmid p-1$, tada je $G \cong \mathbb{Z}_{pq}$.

(2) Neka $q \mid p-1$ i neka je $\phi\colon \mathbb{Z}_q \to Aut\left(\mathbb{Z}_p\right) \cong \mathbb{Z}_p^*$ netrivijalan homomorfizam. Tada je $G \cong \mathbb{Z}_{pq}$ ili $G \cong \mathbb{Z}_p \rtimes_\phi \mathbb{Z}_q$.

Za dokaz vidi [2], str. 40.

Korolar 4.1.7. *Neka je $|G| = 2p$ i $p = 2k+1$, $k \in \mathbb{Z}_{\geq 0}$. Tada je $G \cong \mathbb{Z}_{2p}$ ili $G \cong D_{2p}$.*

Dokaz. Jedini netrivijalan homomorfizam $\phi\colon \mathbb{Z}_2 \to Aut\left(\mathbb{Z}_p\right) = \mathbb{Z}_p^*$, gdje je $\mathbb{Z}_2 = \{0,1\}$, je homomorfizam

$$1 \mapsto \phi_1, \quad \phi_1(a) = -a.$$

Tada je $\mathbb{Z}_p \rtimes_\phi \mathbb{Z}_2 \cong D_{2p}$. □

Grupe reda 8

Propozicija 4.1.8. *Neka je G Abelova grupa reda 8. Tada je ona izomorfna točno jednoj od grupa:*

(1) $\mathbb{Z}_8$,

(2) $\mathbb{Z}_4 \times \mathbb{Z}_2$,

(3) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Dokaz. (1) Pretpostavimo da u G postoji element a reda 8. Tada je ona ciklička i izomorfna sa $\mathbb{Z}_8$.

(2) Pretpostavimo da G ima element a reda 4. Tada postoji $b \notin \langle a\rangle$ takav da je $b^2 = e$. Da bi to pokazali uzmimo $c \notin \langle a\rangle$. Tada su moguća sljedeća dva slučaja:

1°) $c^2 = e$.
Budući da je i b element iz $G/\langle a\rangle$ reda dva, koji je jednak jediničnom elementu, to povlači da je $b = c$.

2°) Red od c je 4 pa zbog $|G/\langle a\rangle| = 2$ slijedi $c^2 \in \langle a\rangle$. Jedini element iz $\langle a\rangle$ reda 2 je a^2 pa mora biti $a^2 = c^2$.

Neka je $b = ac$. Tada je $b^2 = a^2c^2 = a^4 = e$ pa je

$$G \cong \langle a\rangle \times \langle b\rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2.$$

(3) Pretpostavimo da su svi elementi iz G reda 2. Neka je $N = \langle a, b\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, gdje su $e \neq a, b \in G$ te $H = \langle c\rangle$, $e \neq c \in G$.
Budući da je tada $N \cap H = \langle e\rangle$ i $NH = G$ slijedi

$$G \cong N \times H \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

□

Teorem 4.1.9. *Označimo sa Q grupu s generatorima a, b za koje vrijede relacije:*

$$a^4 = e, \quad b^2 = a^2, \quad b^{-1}ab = a^{-1}.$$

Tada Q ima točno 8 elemenata i

$$Q = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

Grupa Q naziva se grupa kvateriona.

Dokaz se može naći u [2].

Propozicija 4.1.10. *Neka je G nekomutativna grupa reda 8. Tada je ona izomorfna ili sa grupom kvateriona Q ili sa D_8.*

Dokaz. G je ne-Abelova grupa pa nije ciklička te ne sadrži element reda 8. Kada bi postojao element a takav da je $a^2 = e$, za svaki $a \in G$, G bi bila Abelova. Uzmimo onda $a \in G$ reda 4 i neka je $b \in G$ takav da $b \notin \langle a\rangle$.

$$|G/\langle a\rangle| = 2, \text{ što povlači da je } b^2 \in \langle a\rangle.$$

$b^{-1}ab \in \langle a\rangle$ jer je $\langle a\rangle$ normalna podgrupa od G. Budući da G nije Abelova vrijedi $b^{-1}ab = a^3$.

1°) Ako je b reda 2, onda je $b^2 = e$. Tada su zadovoljene jednakosti:

$$a^4 = e, \quad b^2 = e, \quad b^{-1}ab = a^3$$

pa je $G \cong D_8$.

2°) Ako je b reda 4, onda je $b^2 = a^2$ i vrijede jednakosti:

$$a^4 = e, \quad b^2 = a^2, \quad b^{-1}ab = a^3$$

pa je $G \cong Q$.

□

Grupe reda 12

Propozicija 4.1.11. *Neka je G grupa reda p^2q, gdje su p, q prosti brojevi, $p \neq q$. Tada je G poludirektan produkt Sylowljeve p-podgrupe H i Sylowljeve q-podgrupe K.*

Dokaz. Promotrimo dva slučaja:

1°) $p > q$. Po Lemi 2.5.8 slijedi da je H normalna u G.

2°) $q > p$. Prema Teoremu 2.5.5 broj Sylowljevih $q-$podgrupa je $1 + kq, k \geq 0$. Tada imamo da je $1 + kq \mid p^2,\ k \geq 0$. Iz toga slijedi da je $k = 0$ ili $1 + kq = p^2$. Ako je $k = 0$ tada je Sylowljeva $q-$podgrupa normalna. Ako je

$$kq = p^2 - 1 \text{ to povlači da } q \mid (p-1)(p+1), \text{ odnosno } q = p + 1 \text{ jer je } q > p.$$

To je ekvivalentno tome da je $p = 2,\ q = 3$. Zaključujemo da je u slučaju $q > p$, Sylowljeva $q-$podgrupa normalna ili je $p = 2$ i $q = 3$.
Dakle, $|G| = 12$ i neka je K Sylowljeva $3-$podgrupa od G, koja nije normalna u G. Tada G ima 4 Sylowljeve $3-$podgrupe, čija unija ima 9 elemenata. Preostali elementi grupe G, zajedno sa jediničnim elementom, čine Sylowljevu $2-$podgrupu H od G pa je H normalna podgrupa od G.
Tada su u G 4 Sylowljeve 3-podgrupe čija unija ima 9 elemenata. Preostali elementi, uz jedinični element, tvore Sylowljeve 2-podgrupe H od G pa je H normalna u G.

Budući da je $H \cap K = \{e\},\ HK = G$ te je u oba navedena slučaja barem jedna od podgrupa normalna, G je poludirektan produkt od H i K. □

Propozicija 4.1.12. *Ne-Abelova grupa G reda 12 izomorfna je točno jednoj od idućih grupa:*

(1) A_4,

(2) D_{12},

(3) $T = \mathbb{Z}_3 \rtimes_\phi \mathbb{Z}_4$, *gdje je* $\phi \colon \mathbb{Z}_4 \to Aut(\mathbb{Z}_3) \cong \mathbb{Z}_2$ *netrivijalan homomorfizam.*

Za dokaz vidi [2], str. 43.

Propozicija 4.1.13. *Neka je G Abelova grupa reda 12. Tada je ona izomorfna ili sa $\mathbb{Z}_{12}$ ili sa $Z_2 \times \mathbb{Z}_6$.*

Dokaz se provodi korištenjem Propozicije 4.1.11.

Bibliografija

[1] Serge Lang, *Algebra*, Addison-Wesley, Reading, MA 1993.

[2] William A. Adkins, Steven H. Weintraub, *Algebra, An Approach via Module Theory*, Springer-Verlag, New York, 1992.

[3] Saša Krešić-Jurić, *Algebarske strukture*, Odjel za matematiku, Split, 2013.

[4] Neven Grbac, Vedrana Mikulić Crnković, *Algebarske strukture*, Odjel za matematiku, 2010./11.

Sažetak

Glavni cilj ovog rada bio je dati sažeti prikaz teorije grupa. U prvom poglavlju smo iznijeli osnovne pojmove i rezultate vezane za monoide, da bismo pomoću njih u drugom poglavlju definirali grupe. Kroz poglavlje o grupama, osim proučavanja njihovih osnovnih svojstava, definirali smo i normalne podgrupe te nizove podgrupa i rješive grupe. Iskazali smo Schreierov te Jordan Hölderov teorem. Nadalje, definirali smo cikličke grupe te kroz iskaze propozicija proučili njihova svojstva. Definirali smo i djelovanje grupe na skupu gdje smo saznali više o algebarskoj strukturi grupe. Taj dio smo zaključili teoremom o jednadžbi klasa. Promotrili smo Sylowljeve grupe te smo nakon definiranja osnovnih pojmova vezanih uz njih, iskazali i Sylowljeve teoreme. U trećem poglavlju prezentirali smo Abelove grupe. Definirali smo pojam direktne sume, baze te slobodne Abelove grupe. Kod proučavanja konačno generiranih Abelovih grupa, posebnu pažnju posvetili smo torzionoj podgrupi koju smo definirali kao skup svih elemenata grupe konačnog reda. U četvrtom poglavlju naveli smo neke primjere konačnih grupa i neke strukturne teoreme. Definirali smo diedralnu grupu i poludirektan produkt, a kroz propozicije smo dobili uvid u osnovna svojstva grupa reda p^2, odnosno reda pq. Za kraj smo klasificirali grupe reda 8 i 12.

Summary

The aim of this master's thesis was to provide a systematic review of theory of finite groups. The first chapter begined with basic notions and results of monoids, which introduced the term of groups in the second chapter. Through the chapter about groups, besides study of their basic properties, we defined normal subgroups, tower of subgroups and solvable groups. We presented Schreier and Jordan Hölder theorem. Furthermore, we presented operation of a group on a set where we found out more about algebraic structure of group. We concluded that part with the class formula. We considered Sylow subgroups and after defining basic notions regarding them, we presented Sylow theorems. In the third chapter, we analized Abelian groups. We defined direct sum, basis and free Abelian group. When studying finitely generated Abelian groups, we paid special attention to torsion subgroup which we defined as set of all elements of group with finite period. In the fourth chapter, we stated some examples of finite groups and some structural theorems. We defined dihedral group and semidirect product and through propositions we gave an insight in basic properties of groups of order p^2 and groups od oreder pq. In the end we classified groups of order 8 and 12.

Životopis

Martina Bilić rođena je 11. studenog 1997. godine u Splitu, gdje upisuje Osnovnu školu Lučac 2003. godine, a 2012. godine Treću gimnaziju, odnosno MIOC. Nakon završetka srednjoškolskog obrazovanja odlazi u Zagreb na studij matematike na Prirodoslovno-matematičkom fakultetu Sveučilišta u Zagrebu, koji upisuje 2016. godine. Po završetku preddiplomskog studija, 2019. godine stječe titulu sveučilišnog prvostupnika matematike, te upisuje diplomski studij Financijske i poslovne matematike na istome fakultetu.