

# Algebarska struktura grupa

---

**Galiot, Nataša**

**Undergraduate thesis / Završni rad**

**2017**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

*Permanent link / Trajna poveznica:* <https://um.nsk.hr/um:nbn:hr:126:279155>

*Rights / Prava:* [In copyright](#)/[Zaštićeno autorskim pravom.](#)

*Download date / Datum preuzimanja:* **2024-07-23**



*Repository / Repozitorij:*

[Repository of School of Applied Mathematics and Computer Science](#)



Sveučilište J.J. Strossmayera u Osijeku  
Odjel za matematiku  
Sveučilišni preddiplomski studij matematike

**Nataša Galiot**  
**Algebarska struktura grupa**  
Završni rad

Osijek, 2017.

Sveučilište J. J. Strossmayera u Osijeku  
Odjel za matematiku  
Preddiplomski studij matematike

Nataša Galot

**Algebarska struktura grupa**

Završni rad

Voditelj: izv.prof.dr.sc. Ivan Matić

Osijek, 2017.

**Sažetak.** U ovom radu pisat ćemo o algebarskoj strukturi grupa. U uvodu ćemo navesti definiciju grupe, njezina osnovna svojstva te pojmove poput Abelova grupa, podgrupa, homomorfizam i izomorfizam grupa.

Nadalje, u drugom dijelu opisat ćemo nekoliko različitih vrsta grupa počevši s normalnim i kvocijentnim grupama u sklopu kojih ćemo iskazati i dokazati Lagrangeov teorem i prvi teorem o izomorfizmu. Sljedeće ćemo opisati cikličke i na kraju p-grupe uz koje vežemo i pojam Sylowljevih p-grupa, Cauchyjev teorem te tri Sylowljeva teorema.

**Ključne riječi:** grupa, Abelova grupa, podgrupa, homomorfizam, izomorfizam, normalne grupe, kvocijentne grupe, cikličke grupe, p-grupe, Lagrangeov teorem, prvi teorem o izomorfizmu, Cauchyjev teorem, Sylowljevi teoremi

**Abstract.** In this term paper we will write about algebraic structure group. In Introduction we will cite the definition of a group, its elementary characteristics and terms as Abelian group, subgroup, homomorphism and isomorphism of group.

Furthermore, in second part we'll describe few different type of groups starting with normal and quotient/factor groups within which we will state and prove Lagrange's theorem and first theorem of isomorphism. Next we will describe cyclic and at the end p-groups with which we associate the term of Sylow-s p-groups, Cauchy's theorem and three Sylow's theorems.

**Key words:** group, Abelian group, subgroup, homomorphism, isomorphism, normal groups, quotient / factor groups, cyclic groups, p-groups, Lagrange's theorem, first theorem of isomorphism, Cauchy's theorem, Sylow's theorems.

# Sadržaj

<b>1</b>	<b>Uvod</b>	<b>4</b>
<b>2</b>	<b>Posebni oblici grupa</b>	<b>8</b>
2.1	Normalne i kvocijentne podgrupe . . . . .	8
2.2	Cikličke grupe . . . . .	12
2.3	$p$ -grupe . . . . .	13
<b>3</b>	<b>Primjena</b>	<b>15</b>

# 1 Uvod

Promatrat ćemo parove koji se sastoje od skupa i binarne operacije definirane na tom skupu. Započnimo sa osnovnom definicijom grupe i njezinim svojstvima.

**Definicija 1.1.** *Neka je  $G$  neprazan skup na kojem je definirana binarna operacija  $*$  :  $G \rightarrow G$ . Kažemo da je  $G$  grupa ukoliko vrijede sljedeća svojstva:*

1. *Zatvorenost: Za svaki  $a, b \in G$  vrijedi*

$$ab \in G$$

2. *Asocijativnost: Za svaki  $a, b, c \in G$  vrijedi*

$$(ab)c = a(bc)$$

3. *Postojanje neutralnog elementa: Postoji element  $1 \in G$ , koji nazivamo neutralni element (jedinica grupe), takav da za svaki  $a \in G$  vrijedi*

$$1a = a \text{ (lijeva jedinica)}$$

$$a1 = a \text{ (desna jedinica)}$$

4. *Postojanje inverznog elementa: Za svaki  $a \in G$  postoji element  $a^{-1} \in G$  koji nazivamo inverz elementa  $a$  za koji vrijedi*

$$aa^{-1} = 1 \text{ (desni inverz)}$$

$$a^{-1}a = 1 \text{ (lijevi inverz)}$$

Za elemente  $a, b \in G$  kažemo da su komutativni, tj da komutiraju ukoliko je  $ab = ba$ .

Za pojam komutativnosti vezan je pojam Abelove grupe. Grupa je Abelova ako svaki par elemenata iz grupe komutira. Konačna je ukoliko je skup  $G$  konačan, a u suprotnom je beskonačna. Uobičajeno je govoriti „ $G$  je grupa“ iako je  $G$  skup, ali se podrazumijeva da je tada skupu  $G$  pridružena binarna operacija.

**Primjer 1.2.** (a) *Najjednostavniji primjer grupe je trivijalna grupa  $G = \{1\}$  koja sadrži neutralni element.*

(b) *Skup  $K_4 = \{1, -1, i, -i\}$  na kojem je definirano množenje je Abelova grupa.*

*Provjerimo vrijede li svojstva iz definicije grupe i da li elementi skupa  $K_4$  komutiraju.*

- *Zatvorenost:* Je li za svaka dva elementa  $a, b \in K_4$  i  $ab \in K_4$ ? Odgovor je potvrđan.

•	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

- *komutativnost:* Uočljivo je iz prethodne tablice kako je  $ab = ba$  za svaka dva elementa  $a, b \in K_4$
- *asocijativnost:* Vrijedi li  $(ab)c = a(bc)$  za svaka tri elementa  $a, b, c \in K_4$ ?

$$(1(-1))i = 1((-1)i)$$

$$(1(-1))(-i) = 1(-1(-i))$$

$$(1(-i))i = 1((-i)i)$$

$$((-1)1)(-i) = -1(1(-i))$$

$$(-1(-i))i = -1((-i)i)$$

$$((-1)1)i = -1(1i)$$

$$(i(-1))1 = i((-1)1)$$

$$(i(-1))(-i) = i(-1(-i))$$

$$(i1)(-i) = i(1(-i))$$

Pokazali smo kako  $K_4$  zadovoljava i ovaj aksiom grupe.

- *Postojanje neutralnog elementa:* Tražimo element  $e \in K_4$  takav da je za svaki  $a \in K_4$   $ae = a$ . Prema tome,  $e = 1$ ,  $1 \in K_4$ , je neutralni element.
- *Postojanje inverznog elementa:* Postoji desni inverz u skupu  $K_4$ , a kako su elementi u tom skupu komutativni, slijedi kako općenito postoji inverzni element u tom skupu.

$$ab = e$$

$$ab = 1$$

$$1 \cdot 1 = 1$$

$$-1(-1) = 1$$

$$i(-i) = 1$$

$$(-i)i = 1$$

Iz navedenoga slijedi kako je  $K_4$  Abelova grupa.

Nadalje, ako je  $a$  element grupe, tada se svaki cijeli broj  $n$  sa svojstvom da je  $a^n = 1$  naziva se eksponent elementa  $a$ . Ukoliko  $a$  nema eksponenta, kažemo da je beskonačnog reda. Red grupe  $G$ , koji označavamo sa  $|G|$  ili  $o(G)$ , je broj elemenata u skupu  $G$ .

**Definicija 1.3.** Neka je  $G$  grupa i  $H$  podskup od  $G$ .  $H$  se naziva podgrupa grupe  $G$  ako je  $H$  grupa obzirom na istu operaciju kao i  $G$ . Pišemo  $H \leq G$ .

Svaka grupa ima najmanje dvije podgrupe:  $1$  i  $G$ . Činjenicu da je skup  $H$  podgrupa grupe  $G$  lako pokazujemo pomoću sljedećeg teorema.

**Teorem 1.4.** Neka je  $H$  podskup od  $G$  te  $H$  neprazan skup.  $H$  je podgrupa od  $G$  ako i samo ako za sve  $a, b \in H$  vrijedi  $ab^{-1} \in H$ .

**Dokaz.** Pretpostavimo prvo kako je  $H$  podgrupa od  $G$ . Prema tome postoje  $a, b^{-1} \in H$ , a kako vrijedi svojstvo zatvorenosti u odnosu na danu operaciju, slijedi da je  $ab^{-1} \in H$ . Pretpostavimo sada kako je  $ab^{-1} \in H$  za svaki  $a, b \in H$ . S obzirom da je  $H$  neprazan skup, u njemu postoji neki element  $a \in H$ . Tada je i  $aa^{-1} = 1 \in H$ . Dakle,  $H$  sadrži neutralni element. Također, za svaki  $b \in H$  vrijedi  $eb^{-1} = b^{-1} \in H$  pa zaključujemo kako postoji i inverzni element. Nadalje, za elemente  $a, b \in H$  je i  $b^{-1} \in H$  pa je isto tako i  $a(b^{-1})^{-1} = ab \in H$ , odnosno  $H$  je zatvoren u odnosu na danu operaciju. Svojstvo asocijativnosti je naslijeđeno iz  $G$ . Prema tome,  $H$  je grupa.  $\square$

**Primjer 1.5.** Ponekad kada želimo pokazati kako je neki skup grupa, može nam biti lakše pokazati kako je dani skup podgrupa neke grupe nego posebno provjeravati svaki od aksioma grupe.

Pogledajmo je li  $(S_1, \cdot)$  grupa, pri čemu je  $S_1 = \{z \in \mathbb{C} : |z| = 1\}$ . Umjesto da provjeravamo svaki od aksioma grupe, pokušat ćemo pokazati da je  $S_1$  podgrupa neke grupe. Uzmimo na primjer grupu  $\mathbb{C}^*$ . Kako je  $z$  kompleksan broj, možemo ga zapisati u sljedećem obliku:

$$\begin{aligned} z &= |z|(\cos t + i \sin t), t \in \mathbb{R} \\ &= |z|e^{it}, t \in \mathbb{R}. \end{aligned}$$

Prema tome,  $S_1$  ima oblik  $S_1 = \{e^{it} : t \in \mathbb{R}\}$ . Tvrdimo da je  $S_1 \leq \mathbb{C}^*$ .  $S_1$  je svakako podskup od  $\mathbb{C}^*$  jer su neki kompleksni brojevi podskup svih kompleksnih brojeva. Također je neprazan skup jer je barem  $1 \in S_1$ . Uzmimo sada dva elementa  $z_1, z_2$  iz  $S_1$  oblika  $z_1 = e^{it_1}$ ,  $z_2 = e^{it_2}$ , za realne brojeve  $t_1$  i  $t_2$ . Tada je:

$$z_1 z_2^{-1} = e^{it_1} e^{-it_2} = e^{i(t_1 - t_2)} \in S_1.$$

Iz toga prema prethodno dokazanom teoremu slijedi kako je  $S_1$  podgrupa od  $\mathbb{C}^*$ , a iz definicije podgrupe slijedi kako je  $S_1$  upravo grupa.

Sljedeća dva važna pojma u teoriji grupa su homomorfizam i izomorfizam grupa. Neka su  $G_1$  i  $G_2$  grupe. Preslikavanje  $\varphi : G_1 \rightarrow G_2$  naziva se homomorfizam grupa ako za svaki  $a, b \in G_1$  vrijedi

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Kažemo da je grupa  $G_1$  izomorfna grupi  $G_2$  ako postoji izomorfizam (bijektivno preslikavanje)  $\varphi : G_1 \rightarrow G_2$ .

**Primjer 1.6.** Pokažimo da je preslikavanje  $f(x) = i^x$  homomorfizam grupe  $(\mathbb{Z}, +)$  u grupu  $(K_4, \cdot)$ . Neka su  $x$  i  $y$  iz skupa cijelih brojeva. Trebamo provjeriti vrijedi li:

$$f(x + y) = f(x)f(y).$$



*Izračunom lijeve i desne strane dobijemo*

$$f(x + y) = i^{x+y}$$

$$f(x)f(y) = i^x i^y = i^{x+y}.$$

*Kako su desne strane obje jednakosti jednake, zaključujemo kako je  $f$  homomorfizam.*

Bitno je spomenuti i sliku i jezgru grupe. Pretpostavimo li kako je preslikavanje  $\varphi : G_1 \rightarrow G_2$  homomorfizam grupa, tada stavljamo:

$Im\varphi = \{\varphi(a) : a \in G_1\} \leq G_2$  je slika od  $\varphi$ ,

$Ker\varphi = \{a \in G_1 : \varphi(a) = e_{G_2}\} \leq G_1$  je jezgra od  $\varphi$ .

## 2 Posebni oblici grupa

Iako postoji više različitih oblika grupa, u ovom radu opisat ćemo normalne, kvocijentne, cikličke i  $p$ -grupe te navesti važnija svojstva, pojmove i teoreme vezane za njih.

### 2.1 Normalne i kvocijentne podgrupe

Neka je  $H$  podgrupa grupe  $G$  te neka su  $a, b \in G$ . Kažemo da je element  $a$  desno kongruentan  $b$  modulo  $H$  ukoliko je  $b^{-1}a \in H$ . Oznaka je  $a \sim^H b$ . Analogno se definira i relacija „biti lijevo kongruentan modulo  $H$ “ koju označavamo sa  $a^H \sim b$ . Promotrimo tu relaciju na sljedećem primjeru.

**Primjer 2.1.**  $n\mathbb{Z}$  je podgrupa grupe  $\mathbb{Z}$  uz zbrajanje za prirodan broj  $n$  pa stoga je i  $6\mathbb{Z}$  podgrupa grupe  $\mathbb{Z}$ . Neka su  $a, b \in \mathbb{Z}$ .  $a$  je desno kongruentno  $b$  modulo  $6\mathbb{Z}$  ako i samo ako je  $-b + a \in 6\mathbb{Z}$  a to pak vrijedi ako i samo ako je  $a = b \pmod{6}$ .

„Biti desno kongruentan modulo  $H$ “ je relacija ekvivalencije na  $G$  i to se jednostavno provjeri ispitivanjem svojstava ekvivalentnosti:

- Refleksivnost: Za  $a \in G$   $a \sim^H a$  jer je  $a^{-1}a = e \in H$
- Simetričnost: Za  $a, b \in G$  takve da je  $a \sim^H b$  vrijedi  $b^{-1}a \in H$  iz čega slijedi da je  $(b^{-1}a)^{-1} = a^{-1}(b^{-1})^{-1} = a^{-1}b \in H$  pa je prema tome  $b \sim^H a$ .
- Transitivnost: Neka su  $a, b, c \in G$  takvi daje  $a \sim^H b$  i  $b \sim^H c$ . Tada je  $b^{-1}a \in H$  i  $c^{-1}b \in H$ , odnosno  $(c^{-1}b)(b^{-1}a) = c^{-1}(bb^{-1})a = c^{-1}a \in H$ , a to znači da je  $a \sim^H c$ .

Ukoliko s  $[a]$  označimo klasu ekvivalencije elemenata  $a \in G$ , tada je

$$[a] = \{ah : h \in H\} = aH$$

te tu klasu nazivamo desna  $H$ -klasa u grupi  $G$ . Analogno se definira i lijeva  $H$ -klasa. Grupa  $G$  je disjunktna unija svih svojih desnih  $H$ -klasa. Uz ove pojmove vežemo Lagrangeov teorem koji nam govori o redu grupe  $G$  i njezine podgrupe  $H$ , ali prije iskaza i dokaza navedenog teorema, promotrimo lemu koja će nam koristiti u dokazu teorema.

**Lema 2.2.** . Neka je  $G$  grupa i  $H$  podgrupa od  $G$ . Tada je

$$|aH| = |Ha| = |H| \text{ za svaki } a \in G.$$

**Dokaz.** Trebamo pokazati kako su redovi od  $aH$ ,  $Ha$  i  $H$  jednaki. Promatrat ćemo preslikavanja  $f : Ha \rightarrow H$  i  $g : aH \rightarrow H$  dana sa  $f(ha) = h$  i  $g(ah) = h$  te pokazati da su bijektivna. Oba su očito surjektivna jer se za  $h$  iz  $H$  elementi  $ah$  i  $ha$  preslikaju u njega. Uzmimo sada elemente  $h_1a$  i  $h_2a$  iz  $Ha$  koji se preslikaju u isti element iz  $H$ .

$$f(h_1a) = h_1$$

$$f(h_2a) = h_2$$

Kako je po pretpostavci  $h_1 = h_2$ , slijedi da je i  $h_1a = h_2a$  pa je  $f$  injektivno preslikavanje, a analogno se pokaže kako je i  $g$  injektivno preslikavanje.  $\square$

**Teorem 2.3** (Lagrangeov teorem). *Neka je  $G$  konačna grupa i  $H$  njezina podgrupa. Tada je red od  $G$  djeljiv redom od  $H$ , tj  $|H|$  dijeli  $|G|$ . Točnije, ako označimo  $|G| = n$  i  $|H| = k$ , a sa  $p$  označimo broj desnih, odnosno lijevih  $H$ -klasa u  $G$ , tada je  $n = pk$ .*

**Dokaz.** Neka su  $a_1, a_2, \dots, a_p$  predstavnici svih desnih  $H$ -klasa u  $G$ . Kako znamo da je  $G$  disjunktna unija svojih desnih  $H$ -klasa, možemo pisati:

$$G = a_1H \cup a_2H \cup \dots \cup a_pH.$$

Prema tome vrijedi da je

$$|G| = |a_1H| + |a_2H| + \dots + |a_pH|.$$

Iskoristimo li prethodnu lemu, dobijemo kako je

$$|G| = |H| + |H| + \dots + |H| = p|H|.$$

Iz tog rezultata slijedi tvrdnja teorema. □

**Primjer 2.4.** (a) *Neka je  $G$  grupa prostog reda kojeg ćemo označiti za  $n$  i  $H$  podgrupa od  $G$ . Prema prethodnom teoremu  $|H|$  dijeli  $|G|$ , a kako su jedini djelitelji prostog broja  $n$  jedinica i on sam, to znači kako su mogući redovi podgrupe  $H$  iz skupa  $\{1, n\}$ , odnosno,  $H = \{e\}$  ili  $H = G$ . Iz ovog primjera zaključujemo kako grupa prostog reda ima samo trivijalne podgrupe.*

(b) *Neka je  $G$  grupa reda 8 i  $H$  podgrupa od  $G$ . Tada je  $|H| \in \{1, 2, 4, 8\}$ .*

Za podgrupu  $H$  grupe  $G$  kažemo da je podgrupa konačnog indeksa u grupi  $G$  ako ima samo konačno mnogo desnih  $H$ -klasa u  $G$ . Taj broj desnih  $H$ -klasa označavamo sa  $[G : H]$  i nazivamo indeks od  $H$  u  $G$ . U slučaju da je  $G$  konačna grupa, tada je red od  $G$  jednak umnošku indeksa od  $H$  u  $G$  i reda podgrupe  $H$ .

**Definicija 2.5.** . *Podgrupa  $H$  grupe  $G$  naziva se normalna podgrupa u oznaci  $H \trianglelefteq G$  ukoliko za svaki element  $c \in G$  vrijedi*

$$Hc = cH, \text{ to jest } \{hc : h \in H\} = \{ch : h \in H\}.$$

Navedimo sada dva primjera.

**Primjer 2.6.** *Svaka podgrupa Abelove grupe je normalna.*

**Primjer 2.7.** *Pokažimo da je  $SL_n(R)$  normalna podgrupa od  $GL_n(R)$ . Znamo kako je  $SL_n(R)$  podgrupa od  $GL_n(R)$ . Uzmimo sada  $A \in SL_n(R)$  i  $B \in GL_n(R)$ . Vrijedi sljedeće:*

$$\begin{aligned} \det(BAB^{-1}) &= \det(B) \det(A) \det(B^{-1}) \\ &= \det(B) \det(B^{-1}) \\ &= 1. \end{aligned}$$

Znači,  $BAB^{-1} \in SL_n(R)$  pa je  $SL_n(R)$  normalna podgrupa od  $GL_n(R)$ .

Kako bismo definirali kvocijentnu grupu grupu grupe  $G$  po normalnoj podgrupi  $H$ , promotrimo najprije sljedeće.

Neka je  $H$  normalna podgrupa grupe  $G$ . Označimo sa  $G/H$  skup svih  $H$ -klasa u grupi  $G$  te na tom skupu ćemo definirati binarnu operaciju zadanu na sljedeći način:

$$(aH)(bH) = abH, \text{ pri čemu su } a, b \in H.$$

Provjerimo je li navedena operacija dobro definirana, to jest da ne ovisi o izboru reprezentanata  $a$  i  $b$ . U tu svrhu izaberimo  $a', b' \in H$  takve da je

$$\begin{aligned} aH &= a'H & a &\sim^H a' \\ bH &= b'H & b &\sim^H b'. \end{aligned}$$

Trebamo pokazati da izrazi  $(aH)(bH) = abH$  i  $(a'H)(b'H) = a'b'H$  daju jednake rezultate, odnosno povlači li  $a \sim^H a'$  i  $b \sim^H b'$  da je također  $ab \sim^H a'b'$ . Prema pretpostavci je  $a \sim^H a'$ , to jest  $a^{-1}a' \in H$  pa možemo odabrati element  $h_1$  iz podgrupe  $H$  i označiti  $a^{-1}a' = h_1$ . Pomnožimo li jednakost s  $a$ , dobijemo kako je  $a' = ah_1$ . Analogno slijedi iz  $b \sim^H b'$  da je  $b' = bh_2$ , pri čemu je  $h_2 \in H$ . Nadalje, iskoristit ćemo činjenicu da je  $H$  normalna podgrupa od  $G$ . Tada je

$$\begin{aligned} b^{-1}Hb &= bH \\ b^{-1}Hb &= H \\ b^{-1}h_1b &\in H. \end{aligned}$$

Promotrimo sada umnožak  $a'b'$ .

$$\begin{aligned} a'b' &= ah_1bh_2 \\ &= ah_1bh_2 \\ &= abb^{-1}h_1bh_2 \\ &= ab(b^{-1}h_1b)h_2. \end{aligned}$$

Ovdje ćemo iskoristiti prethodni rezultat i označiti:

$$\begin{aligned} b^{-1}h_1b &= h_3 \\ &= ah_3h_2, h_3, h_2 \in H. \end{aligned}$$

Kako su  $h_3$  i  $h_2$  elementi podgrupe  $H$ , možemo njihov umnožak označiti sa  $h_4$  koji se također nalazi u  $H$  pa imamo  $a'b' = ah_4$ . Sada je preostalo pomnožiti izraz sa  $(ab)^{-1}$ .

$$(ab)^{-1}a'b' = h_4 \in H$$

Iz toga proizlazi kako je  $ab \sim^H a'b'$  i  $abH = a'b'H$  te je skup  $G/H$  grupa.

**Definicija 2.8.**  $G/H$  naziva se kvocijentna grupa grupe  $G$  po normalnoj podgrupi  $H$ .

**Teorem 2.9.** Neka je  $\varphi : G_1 \rightarrow G_2$  homomorfizam grupa.

(i)  $\text{Ker}\varphi$  je normalna podgrupa od  $G_1$ .

(ii) (Prvi teorem o izomorfizmu)

Preslikavanje  $\Phi : G_1/\text{Ker}\varphi \rightarrow \text{Im}\varphi$  definirano izrazom

$$\Phi(a\text{Ker}\varphi) = \varphi(a), a \in G_1$$

je izomorfizam kvocijentne grupe  $G_1/\text{Ker}\varphi$  na grupu  $\text{Im}\varphi$ .

**Dokaz.** Dokaz prvog dijela ovog teorema se svodi na korištenje činjenice kako je preslikavanje  $\varphi$  homomorfizam i promatranje djelovanja navedenog preslikavanja na element  $a^{-1}ha$ , pri čemu je  $a \in G_1$ ,  $h \in Ker\varphi$ .

Dokaz prvog teorema o izomorfizmu je također veoma jednostavan. Prvo je potrebno pokazati kako je preslikavanje  $\Phi(aKer\varphi) = \varphi(a)$  dobro definirano što ćemo pokazati odabirom nekog drugog reprezentanta i pokazivanjem da to ne utječe na rezultat.

Neka je

$$aKer\varphi = a'Ker\varphi.$$

Iz  $a \sim^{Ker\varphi} a'$  slijedi da je  $a^{-1}a' \in Ker\varphi$ , tj.  $a^{-1}a' = h, h \in Ker\varphi$ . Neka je

$$\Phi(aKer\varphi) = \varphi(a),$$

$$\Phi(a'Ker\varphi) = \varphi(a'),$$

$$a' = ah \text{ za neki } h \in Ker\varphi.$$

Prema tome vrijedi

$$\Phi(a'Ker\varphi) = \varphi(a') = \varphi(ah) = \varphi(a)\varphi(h) = \varphi(a) = \Phi(aKer\varphi)$$

pa je to preslikavanje dobro definirano. Nadalje, kako bismo pokazali da je izomorfizam, moramo pokazati da je homomorfizam i bijekcija.

- Homomorfizam:

$$\Phi((aKer\varphi)(bKer\varphi)) = \Phi(abKer\varphi) = \varphi(ab) = \varphi(a)\varphi(b) = \Phi(aKer\varphi)\Phi(bKer\varphi)$$

- Surjektivnost: Budući da je kodomena preslikavanja jednaka slici od  $\varphi$ , iz same definicije preslikavanja  $\Phi$  slijedi da je ono surjektivnost.
- Injektivnost:

$$\Phi(aKer\varphi) = \Phi(bKer\varphi)$$

$$\varphi(a) = \varphi(b)/\varphi(b)^{-1}$$

$$\varphi(a)\varphi(b)^{-1} = e_{G_2}$$

$$\varphi(a)\varphi(b^{-1}) = e_{G_2}$$

$$\varphi(ab^{-1}) = e_{G_2}$$

$$ab^{-1} \in Ker\varphi$$

$$Ker\varphi \trianglelefteq G_1$$

$$\Rightarrow a \sim^{Ker\varphi} b$$

$$\Rightarrow aKer\varphi = bKer\varphi.$$

Prema tome, tvrdnja teorema vrijedi. □

Podskup grupe  $G$  u oznaci  $Z(G) = \{x \in G : ax = xa, \text{ za svaki } a \in G\}$  naziva se centar grupe. On je normalna komutativna podgrupa od  $G$ , a ako je  $H$  podgrupa od  $G$  takva da je ujedno i podskup centra grupe, tada je  $H$  normalna podgrupa od  $G$  i takva podgrupa se naziva centralna.

## 2.2 Cikličke grupe

Kako bismo definirali cikličke grupe, najprije moramo reći što je grupa generirana skupom  $S$ . Promotrimo grupu  $G$  za koju ćemo označiti:

$$a^0 = e$$

$$a^1 = a$$

$$a^2 = aa$$

pri čemu je  $a \in G$ . Za  $n \geq 3$  stavimo da je

$$a^n = aa^{n-1},$$

a za  $n < 0$ ,  $n \in \mathbb{Z}$  stavimo

$$a^n = (a^{-1})^{-n}.$$

Na taj smo način definirali sve potencije  $a^n$  elementa  $a$  za cjelobrojne  $n$ . Nadalje, neka je preslikavanje  $\Phi_a : \mathbb{Z} \rightarrow G$  određeno izrazom

$$\Phi_a(n) = a^n.$$

Kako za cjelobrojne  $m$  i  $n$  vrijedi da je

$$\Phi_a(m+n) = a^{m+n} = a^n a^m = \Phi_a(n)\Phi_a(m),$$

slijedi da je  $\Phi_a$  homomorfizam grupa. Sada definiramo  $\langle a \rangle$  kao sliku preslikavanja  $\Phi_a$ , odnosno skup svih  $a^n$  za cjelobrojne brojeve  $n$ . Taj skup je najmanja podgrupa od  $G$  koja sadrži element  $a$ . Općenito, neka je  $S$  neprazan podskup grupe  $G$ . Za najmanju podgrupu od  $G$  koja sadrži  $S$  kažemo da je generirana sa  $S$  i pišemo  $\langle S \rangle$ .

**Definicija 2.10.** *Grupa generirana jednim elementom naziva se ciklička grupa.*

U kontekstu cikličkih grupa, red  $|\langle a \rangle| = m$  naziva se period ili red elementa  $a$  te ukoliko  $\langle a \rangle$  nije konačna, element  $a$  nije konačnog reda. Neutralni element (jedinica) jedini je element reda 1. Ukoliko je  $a$  element reda  $m$  u konačnoj grupi  $G$ , tada red elementa  $a$  dijeli red od  $G$ . Prema tome, ako je  $G$  prostog reda i  $a$  njezin element različit od neutralnog elementa tada je  $\langle a \rangle = G$  iz čega možemo zaključiti kako je grupa prostog reda ciklička. U ovom dijelu ćemo još samo pokazati kako je svaka podgrupa cikličke grupe  $G$  također ciklička i kako je za svaku podgrupu  $H$  od  $G$  kvocijentna grupa  $G/H$  ciklička.

**Dokaz.** U slučaju da je  $G$  beskonačna grupa, ona je izomorfna skupu cijelih brojeva, a to znači da je svaka podgrupa od  $G$  izomorfna ili  $\{0\} = \langle 0 \rangle$  ili  $m\mathbb{Z} = \langle m \rangle$  pa je stoga ciklička.

Slično tome, svaka kvocijentna grupa grupe  $G$  je izomorfna ili  $\mathbb{Z}/\{0\} = \mathbb{Z} = \langle 1 \rangle$  ili  $\mathbb{Z}/m\mathbb{Z}$  (koja je izomorfna  $\mathbb{Z}m = \langle 1 \rangle$ ) pa je ciklička.

S druge pak strane, neka je  $G$  konačna grupa reda  $n$  i  $G = \langle a \rangle$  te označimo sa  $H$  podgrupu od  $G$  koja ne sadrži samo neutralni element. Tada postoji element  $a^m \in H$  za prirodni broj  $m$ . Neka je  $m$  najmanji takav za koji to vrijedi, to jest  $m = \min\{k \in \mathbb{N} : a^k \in H\}$ . Ono što tvrdimo jest da je  $H = \langle a^m \rangle$  za  $a^m \in H$ . Tada je  $\langle a^m \rangle$  podskup od  $H$ . Uzmimo neki element  $b$  iz podgrupe  $H$ . Taj element se nalazi i u grupi  $G$ , odnosno vrijedi sljedeće:

$$b \in G = \{e, a, a^2, \dots, a^{n-1}\} \text{ te je } b = a^k \text{ za } 0 \leq k \leq n-1.$$

Nadalje, označimo li s  $k = sm + j$ , pri čemu je  $0 \leq j \leq m$  dobijemo sljedeće:

$$b = a^{sm+j} = a^{sm} a^j / a^{-(sm)}$$

$$ba^{-sm} = a^j$$

$$b(a^m)^{-s} = a^j.$$

Promotrimo li posljednji izraz uočavamo kako iz činjenice da su  $b$  i  $a^m$  elementi podgrupe  $H$  možemo zaključiti kako je i  $a^j$  element iz  $H$ . Zbog činjenice da je  $j$  strogo manji od  $m$  slijedi da je  $j = 0$  te

$$b = a^{sm} = (a^s)^m \in \langle a^m \rangle$$

. U konačnici to znači da je  $H$  podskup od  $\langle a^m \rangle$  pa je  $H = \langle a^m \rangle$ , čime je dokazan prvi dio tvrdnje.

Pretpostavimo li kako je  $H$  podgrupa od  $G$ , a znamo kako element  $a$  generira grupu  $G$ , tada klasa  $aH$  generira kvocijentnu grupu  $G/H$ , to jest  $G/H$  je ciklička grupa.  $\square$

**Primjer 2.11.** *Dokažimo kako grupa  $(\mathbb{Q}, +)$  nije ciklička grupa.*

*Pretpostavimo suprotno, to jest da postoje relativno prosti brojevi  $m \in \mathbb{Z}$ ,  $n \in \mathbb{N}$  takvi da je*

$$q = \langle \frac{m}{n} \rangle.$$

*Tada za svaki  $q \in \mathbb{Q}$  postoji  $k \in \mathbb{Z}$  takav da vrijedi*

$$q = \frac{km}{n}.$$

*Uzmimo na primjer*

$$q = \frac{1}{2n}.$$

*Iz toga slijedi da je*

$$\frac{1}{2n} = k \frac{m}{n},$$

*odnosno da je*

$$km = \frac{1}{2},$$

*a to nije moguće jer su  $k$  i  $m$  cijeli brojevi.*

## 2.3 $p$ -grupe

Konačnu grupu reda  $p^n$ , pri čemu je  $p$  prost broj i  $n$  prirodan, nazivamo  $p$ -grupom. Podgrupa  $H$  konačne grupe  $G$  je  $p$ -podgrupa ukoliko je  $H$   $p$ -grupa. Primjerice, grupa reda 60 nije  $p$ -grupa, dok grupa reda  $9 = 3^2$  jest. Jedna pak posebna vrsta  $p$ -grupa su Sylowljeve  $p$ -podgrupe čiju ćemo definiciju sljedeću iskazati.

**Definicija 2.12.** *Podgrupa  $H$  konačne grupe  $G$  zove se Sylowljeva  $p$ -podgrupa ako je  $H$   $p$ -podgrupa i ako indeks  $[G : H]$  nije djeljiv s  $p$ .*

Prije iskaza samih Sylowljevih teorema, spomenimo i Cauchyjev teorem. On kaže kako kad imamo konačnu grupu  $G$  i  $p$  prost broj koji dijeli red grupe  $G$ , tada grupa  $G$  sadrži podgrupu reda  $p$ . Drugim riječima, grupa  $G$  tada sadrži element reda  $p$ .

**Teorem 2.13** (Prvi Sylowljev teorem). *Neka je  $G$  grupa reda  $p^n m$ , gdje su  $n \geq 1$  i  $p$  prost broj takav da je  $(p, n) = 1$ . Tada  $G$  sadrži podgrupu reda  $p^i$  za svaki  $1 \leq i \leq n$  i svaka podgrupa od  $G$  reda  $p^i$  za  $i < n$  je normalna u nekoj podgrupi reda  $p^{i+1}$ .*

**Teorem 2.14** (Drugi Sylowljev teorem). *Neka je  $G$  konačna grupa i  $p$  prost broj koji dijeli red od  $G$ .*

(i) *Svaka  $p$ -podgrupa grupe  $G$  sadržana je u nekoj Sylowljevoj  $p$ -podgrupi grupe  $G$ .*

(ii) *Sve Sylowljeve  $p$ -podgrupe grupe  $G$  su međusobno konjugiranje. Drugim riječima, ako su  $H$  i  $K$  dvije Sylowljeve  $p$ -podgrupe grupe  $G$ , tada postoji  $a \in G$  takav da je  $K = aHa^{-1}$ .*

**Teorem 2.15** (Treći Sylowljev teorem). *Neka je  $G$  konačna grupa i neka je  $p$  prost broj koji dijeli red od  $G$ . Broj Sylowljevih  $p$ -podgrupa grupe  $G$  dijeli red od  $G$ . Broj Sylowljevih  $p$ -podgrupa grupe  $G$  dijeli  $|G| = n$ . Također, broj Sylowljevih  $p$ -podgrupa grupe  $G$  oblika je  $kp + 1$  za neki nenegativan cijeli broj  $k$ .*

**Primjer 2.16.** *Ukoliko je red grupe  $G$  jednak  $15 = 3 \cdot 5$ , tada postoji Sylowljeva 3-podgrupa i Sylowljeva 5-podgrupa.*

**Primjer 2.17.** *Pokažimo kako je konačna grupa  $G$   $p$ -grupa ako i samo ako je red svakog elementa grupe  $G$  potencija broja  $p$ .*

*Pretpostavimo najprije kako je  $G$   $p$ -grupa, to jest neka postoji prirodan broj  $k$  takav da je  $|G| = p^k$ . Prema Lagrangeovom teoremu  $|a| = |\langle a \rangle|$  i on dijeli red od  $G$ , odnosno  $p^k$ . Dakle, red od  $a$  je oblika  $p^l$  pri čemu je  $l$  manje ili jednako od  $k$  za svaki  $a$  iz grupe  $G$ , a to upravo znači kako je red svakog elementa od  $G$  potencija broja  $p$ .*

*S druge pak strane, pretpostavimo kako je red svakog elementa grupe  $G$  potencija broja  $p$ . Također, pretpostavimo da  $G$  nije  $p$ -grupa, to jest kako ne postoji prost broj  $q$  različit od  $p$  takav da  $q$  dijeli red od  $G$ . Cauchyjev teorem kaže kako  $G$  sadrži element reda  $q$ , a to nije moguće pa je  $G$   $p$ -grupa.*

U ovom poglavlju spomenimo još samo pojam proste grupe. Grupa  $G$  zove se prosta ako su jedine njezine normalne podgrupe  $\{e\}$  i  $G$ , to jest ako nema netrivialnih normalnih podgrupa.

**Primjer 2.18.** *Grupa reda 12 nije prosta. Broj 12 možemo zapisati kao umnožak  $2^2 \cdot 3$ . Prema trećem Sylowljevom teoremu broj Sylowljevih 3-podgrupa je oblika  $3k + 1$  i  $3k + 1$  dijeli 12. Uzmimo sada različite brojeve  $k$  i pogledajmo što dobijemo.*

$$k = 0 \rightarrow 3k + 1 = 1, 1 \text{ dijeli } 12$$

$$k = 1 \rightarrow 3k + 1 = 4, 4 \text{ dijeli } 12$$

$$k = 2 \rightarrow 3k + 1 = 7, 7 \text{ ne dijeli } 12$$

$$k = 3 \rightarrow 3k + 1 = 10, 10 \text{ ne dijeli } 12$$

$$k = 4 \rightarrow 3k + 1 = 13, 13 \text{ ne dijeli } 12$$

*Stat ćemo kod  $k = 4$  jer smo dobili broj veći od 12 pa nema smisla nastavljati postupak. Uočavamo kako je  $k = 0$  ili  $k = 1$ . Ako je  $k = 0$ , postoji jedinstvena Sylowljeva 3 - podgrupa pa je ona normalna. Pretpostavimo da je  $k \neq 0$ , odnosno da je  $k = 1$ . Tada postoje četiri Sylowljeve 3-podgrupe reda 3, to jest imamo 8 elemenata reda 3. Preostala četiri elementa tvore grupu reda 4 i to je jedinstvena Sylowljeva 2-podgrupa pa je normalna. Dakle, grupa reda 12 nije prosta.*



### 3 Primjena

Teorija grupa ima široku primjenu ne samo u matematici, već i u drugim znanostima poput fizike, kemije i računarstva, ali i u umjetnosti. Primjerice, u glazbenoj umjetnosti grupu  $\mathbb{Z}_{12}$  možemo povezati s činjenicom kako od srednjeg tona C do idućeg tona C na klaviru postoji 12 tipki. Kako ljudsko uho prirodno čuje frekvencije s 12 intervala među njima, možemo slikovito reći da ljudi čuju u aritmetici modulo 12. Kako bismo primijenili matematiku na ovu činjenicu potrebno je samo definirati preslikavanje između kompletiranog niza od 12 nota (kromatske ljestvice) i elemenata grupe  $\mathbb{Z}_{12}$ . „To činimo na sljedeći način:

$$\begin{aligned} C \mapsto 0, C\sharp \mapsto 1, D \mapsto 2, D\sharp \mapsto 3, E \mapsto 4, \\ F\sharp \mapsto 5, F \mapsto 6, G \mapsto 7, G\sharp \mapsto 8, A \mapsto 9, \\ A\sharp \mapsto 10, B \mapsto 11 \end{aligned}$$

Sada je lako zapisati na primjer C-dur ljestvicu:  $\{C, D, E, F, G, A, B\} = \{0, 2, 4, 5, 7, 9, 11\}$  [2]."

Drugi zanimljiv primjer uporabe teorije grupa odnosi se na veoma popularnu trodimenzionalnu mehaničku igračku koju je 1974. godine izumio kipar i profesor arhitekture Ernő Rubik te ju nazvao „Čarobna kocka“, a koju danas poznajemo pod imenom Rubikova kocka. Označimo sa  $G$  skup svih mogućih poteza koje možemo napraviti na Rubikovoj kocki, a  $*$  preslikavanje koje ćemo nazvati „uzastopno izvođenje poteza“ pri čemu potezom smatramo zaokret jedne od njezinih strana u smjeru kazaljke na satu za 90 stupnjeva. Promotrimo ima li ova struktura svojstva grupe. Operacija  $*$  je asocijativna, neutralni potez pri kojem nije promijenjen izgled kocke nazivamo neutralnim elementom. Nadalje, svaki potez je invertibilan (jednostavnim okretanjem kocke u položaj iz kojeg smo je pomaknuli). Dakle,  $(G, *)$  je grupa koju nazivamo grupom Rubikove kocke, ali uočimo kako ta grupa nije Abelova. Njezin red je jednak broju svih mogućih poteza koje je moguće na njoj napraviti i iznosi  $43 \cdot 10^{18}$ , a red elementa pak govori koliko je puta potrebno izvršiti neki potez kako bi se izgled kocke vratio u prvobitni položaj. Uz pomoć teorije grupa moguće je odrediti algoritam za njezino slaganje.

Govoreći u širom spektru, teorija grupa je studija simetrije i pomaže nam u analizi simetričnih objekata – što se može odnositi na geometrijsku strukturu, fizikalne zakonitosti, kemijske strukture, ali i apstraktnije pojmove poput trigonometrijskih funkcija.

## Literatura

- [1] M. Benko, Grupa Rubikove kocke, Diplomski rad, Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet, Zagreb, 2015.
- [2] M. Karaga, A. Petrovečki, Primjena teorije grupa u teoriji glazbe ili kako smjestiti Beethovena na torus, *math.e*, 25 (2014), 18-35, ([http://e.math.hr/broj\\_25/Karaga](http://e.math.hr/broj_25/Karaga))
- [3] S. Roman, *Fundamentals of Group Theory, An Advanced Approach*, New York, 2012.