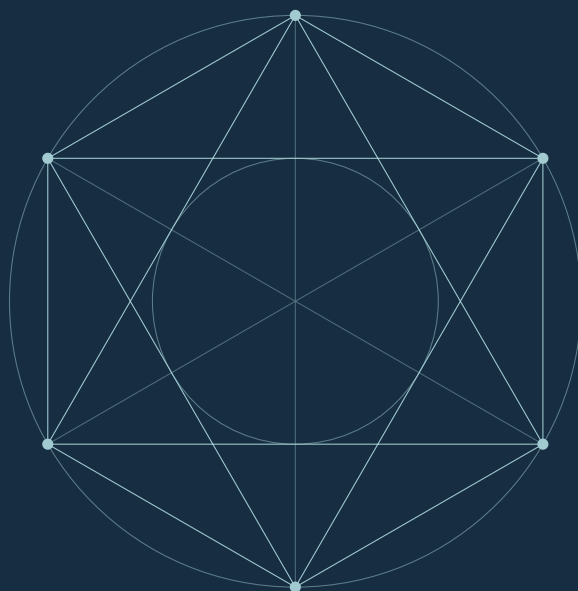


PRIRODOSLOVNO-MATEMATIČKI FAKULTET
ODJEL ZA MATEMATIKU · SPLIT

Saša Krešić-Jurić

Algebarske strukture

Grupe · Prsteni · Moduli · Algebre



Sadržaj

1	Grupe	4
1.1	Polugrupe i grupe	4
1.2	Homomorfizmi grupa	12
1.3	Podgrupe i susjedne klase	15
1.4	Normalne podgrupe i kvocijentne grupe	20
1.5	Teoremi o izomorfizmima	24
1.6	Cikličke grupe	28
1.7	Grupe permutacija	32
1.8	Diedralne grupe	38
1.9	Djelovanje grupe	42
1.10	Direktni i poludirektni umnožak grupa	49
1.10.1	Direktni umnožak	49
1.10.2	Poludirektni umnožak	54
1.11	Konačno generirane Abelove grupe	58
1.12	Sylowljevi teoremi	62
2	Prsteni	66
2.1	Osnovna svojstva prstena	66
2.2	Vrste prstena	70
2.3	Podprsten i karakteristika prstena	72
2.4	Prsten kvaterniona	74
2.5	Prsten matrica	77
2.6	Prsten grupe	79
2.7	Ideali i kvocijentni prsten	80
2.8	Homomorfizmi prstena	85
2.9	Euklidska domena i domena glavnih ideala	90
2.10	Prsten polinoma	93
2.10.1	Ireducibilni polinomi	96
2.11	Maksimalni ideali	99
3	Moduli	103
3.1	Definicija i primjeri modula	103
3.2	Podmoduli i direktne sume	105
3.3	Homomorfizmi modula i kvocijentni moduli	110
3.4	Kvocijentni modul	111

4	Pregled ostalih algebarskih struktura	114
4.1	Asocijativne algebre	114
4.2	Liejeve algebre	117
4.3	Klasične Liejeve algebre	122
4.3.1	Opća i specijalna linearna Liejeva algebra	123
4.3.2	Ortogonalne Liejeve algebre	123
4.3.3	Simplektička Liejeva algebra	123
4.3.4	Unitarne Liejeve algebre	123
4.4	Weylove algebre	124

Predgovor

Ova skripta namijenjena je studentima Prirodoslovno-matematičkog fakulteta u Splitu koji pohađaju kolegij Algebarske strukture. Skripta je podijeljena u četiri cjeline – *Grupe*, *Prsteni*, *Moduli* i *Ostale algebarske strukture*. Svojim sadržajem potpuno obuhvaća gradivo predviđeno nastavnim planom za ovaj kolegij. Naglasak je dan na proučavanju grupa i prstena, dok se moduli i ostale algebarske strukture razmatraju samo na uvodnom nivou i kroz različite primjere.

Prvi dio posvećen je osnovama teorije grupa, uključujući teoreme o izomorfizmima, djelovanje grupe na skup i teoreme o strukturi grupa. Posebno se razmatraju različiti primjeri grupa kao što su cikličke grupe, grupe permutacija i diedarske grupe.

U drugom dijelu razmatraju se osnove teorije prstena koja uključuje domene glavnih ideala, euklidske domene i maksimalne ideale. Poseban naglasak dan je na različitim primjerima prstena, a naročito prstenu polinoma i njegovim svojstvima.

U trećem dijelu izloženi su osnovni koncepti vezani za teoriju modula, dok je u četvrtom dijelu dan kratak pregled nekih algebarskih struktura kao što su asocijativne algebre, Weylove algebre i Liejeve algebre. Ove strukture ilustrirane su primjerima iz geometrije, linearne algebre i fizike.

01

Grupe

1.1 Polugrupe i grupe

Grupe su važne matematičke strukture koje imaju svoje podrijetlo u teoriji algebarskih jednažbi, teoriji brojeva i geometriji. Prva formalna definicija apstraktne grupe u modernom smislu pojavila se 1882. godine. Danas teorija grupa igra važnu ulogu u matematici i fizici gdje se najčešće javlja kao alat pri proučavanju simetrija određenih sustava, kako diskretnih tako i kontinuiranih. U ovom poglavlju upoznat ćemo različite primjere grupa i proučavati njihova osnovna svojstva.

Definicija 1.1. *Binarna operacija na skupu G je preslikavanje s kartezijevog umnoška $G \times G$ u skup G .*

Rezultat binarne operacije $\cdot : G \times G \rightarrow G$ na elementu $(a, b) \in G \times G$ označavamo s $a \cdot b$ i nazivamo umnožak elemenata a i b . Radi jednostavnosti, rezultat binarne operacije kraće zapisujemo kao ab . Primjeri binarnih operacija su standardno zbrajanje i množenje na skupovima $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ili $\mathbb{C}$, i vektorski umnožak na skupu $\mathbb{R}^3$,

$$u \times v = (u_2v_3 - u_3v_2, u_3v_1 - u_1v_3, u_1v_2 - u_2v_1)$$

gdje su $u = (u_1, u_2, u_3)$ i $v = (v_1, v_2, v_3)$ vektori u $\mathbb{R}^3$. Za binarnu operaciju kažemo da je asocijativna ako vrijedi

$$(ab)c = a(bc) \quad \text{za sve } a, b, c \in G.$$

Ako je

$$ab = ba \quad \text{za sve } a, b \in G,$$

onda kažemo da je binarna operacija komutativna. Zbrajanje i množenje na $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ili $\mathbb{C}$ su očigledno komutativne i asocijativne operacije, dok vektorski umnožak nije ni komutativan niti asocijativan.

Najjednostavnija algebarska struktura je polugrupa koju definiramo kao neprazan skup G s asocijativnom binarnom operacijom. Primjeri polugrupa su

- (i) skupovi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ili $\mathbb{C}$ s operacijama zbrajanja ili množenja,
- (ii) skup svih preslikavanja $f: S \rightarrow S$ s nepraznog skupa S na samog sebe.

Zanimljivija algebarska struktura je grupa koju definiramo kao polugrupu u kojoj postoji neutralni element i u kojoj svaki element ima inverz.

Definicija 1.2. *Neprazan skup G s binarnom operacijom $\cdot: G \times G \rightarrow G$ naziva se grupa ako zadovoljava sljedeća svojstva:*

- (i) $a(bc) = (ab)c$ za sve $a, b, c \in G$,
- (ii) postoji element $e \in G$, kojeg nazivamo neutralni element ili jedinica, takav da je $ae = ea = a$ za svaki $a \in G$,
- (iii) za svaki $a \in G$ postoji element $b \in G$, kojeg nazivamo inverzni element od a , takav da je $ab = ba = e$.

Grupu s pripadnom binarnom operacijom zapisujemo kao uređeni par $(G, \cdot)$ ili samo G kada je binarna operacija poznata iz konteksta. Kardinalni broj skupa G naziva se red grupe G i označava s $|G|$. Ako je $|G|$ konačan, onda kažemo da je G konačna grupa, a u protivnom da je G beskonačna grupa. Najjednostavnija grupa je grupa koja sadrži samo jedinicu, $G = \{e\}$. Primjeri grupa koje svakodnevno susrećemo su skupovi brojeva $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ sa standardnim zbrajanjem te skupovi $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ i $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ sa standardnim množenjem.

Promotrimo neka elementarna svojstva grupa.

Propozicija 1.1. *Neka je G grupa.*

- (i) *Neutralni element $e \in G$ je jedinstven.*
- (ii) *Svaki element iz G ima jedinstveni inverzni element.*

Dokaz (i) Pretpostavimo da su e_1 i e_2 jedinice u grupi G . Tada prema svojstvu (ii) definicije 1.2 vrijedi $e_1e_2 = e_2$ i $e_1e_2 = e_1$ jer su e_1 i e_2 jedinice u G . Stoga je $e_1 = e_2$.

(ii) Neka je $a \in G$, i neka su b_1 i b_2 inverzi elementa a . Tada za b_1 i b_2 vrijedi

$$ab_1 = b_1a = e \quad \text{i} \quad ab_2 = b_2a = e.$$

Oдавde slijedi

$$b_1 = b_1e = b_1(ab_2) = (b_1a)b_2 = eb_2 = b_2.$$

■

Lako se provjeri da je inverz umnoška dvaju elemenata jednak

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Doista, zbog asocijativnosti množenja imamo

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e,$$

i

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = e.$$

Asocijativnost množenja u grupi G implicira da za sve $a_1, a_2, \dots, a_n \in G$ rezultat množenja ovih elemenata ne ovisi o tome kako ih grupiramo, stoga umnožak pišemo bez zagrada $a_1a_2 \dots a_n$. Indukcijom se lako pokazuje da je inverz elementa $a_1a_2 \dots a_n$ dan sa

$$(a_1a_2 \dots a_n)^{-1} = a_n^{-1}a_{n-1}^{-1} \dots a_1^{-1}.$$

Potencije elementa se definiraju na prirodni način sa

$$a^n = a \, a \, \dots \, a \quad (n \text{ puta}), \quad (1.1)$$

$$a^{-n} = a^{-1} a^{-1} \dots a^{-1} \quad (n \text{ puta}). \quad (1.2)$$

Sljedeća propozicija slijedi izravno iz svojstava grupe pa dokaz izostavljamo.

Propozicija 1.2. *Neka je G grupa i neka su $a, x, y \in G$. Tada*

(i) $ax = ay$ implicira $x = y$,

(ii) $xa = ya$ implicira $x = y$.

Svojstva (i) i (ii) nazivamo pravilo kraćenja jer se element $a \in G$ može pokratiti na obje strane jednadžbe. Ako su $a, b \in G$, onda svojstva grupe također impliciraju da jednadžbe $ax = b$ i $ya = b$ imaju jedinstvena rješenja $x = a^{-1}b$ i $y = ba^{-1}$.

Definicija 1.3. *Kažemo da je G Abelova ili komutativna grupa ako vrijedi*

$$ab = ba \quad \text{za sve } a, b \in G.$$

Binarnu operaciju u Abelovoj grupi označavamo s $+$, dok za neutralni i inverzni element uvodimo oznake 0 i $-a$. Dakle, u Abelovoj grupi vrijedi

$$a + b = b + a, \quad a + 0 = 0 + a = a, \quad a + (-a) = (-a) + a = 0,$$

za sve $a, b \in G$.

Za potencije elementa u Abelovoj grupi koristimo oznake

$$\begin{aligned} na &= a + a + \dots + a \quad (n \text{ puta}), \\ (-n)a &= -a - a \dots - a \quad (n \text{ puta}). \end{aligned}$$

Binarnu operaciju u grupi možemo predložiti pomoću Cayleyeve tablice u kojoj se nalaze umnošci elemenata grupe.



Slika 1.1. Niels Henrik Abel, 1802-1829. Norveški matematičar Niels Abel je dokazao da nije moguće algebarskim metodama riješiti opću polinomijalnu jednadžbu petog stupnja.

Definicija 1.4. Neka je $G = \{g_1, g_2, \dots, g_n\}$ konačna grupa. Tablica množenja ili Cayleyeva tablica grupe G je $n \times n$ matrica čiji element na mjestu (i, j) je umnožak $g_i g_j$.

Mnoga svojstva grupe se mogu vidjeti iz njezine Cayleyeve tablice. Na primjer, ako je grupa komutativna, tj. $g_i g_j = g_j g_i$ za sve i, j , onda je Cayleyeva tablica simetrična u odnosu na dijagonalu (i, i) . Mjesta gdje se u tablici nalaze jedinice odgovaraju elementima koji su međusobno inverzni. Kako je množenje fiksnim elementom injektivno preslikavanje na G , svaki redak ili stupac sadrži točno po jedan element iz G . Drugim riječima, svaki redak ili stupac predstavlja permutaciju elemenata grupe G .

Primjer 1.1. Neka je $G = \{e, a, b\}$ grupa od tri elementa. Odredimo Cayleyevu tablicu grupe G . Ako je $ab = a$ onda je $b = a^{-1}a = e$, kontradikcija. Ako je $ab = b$, onda je $a = bb^{-1}$, kontradikcija. Budući da je G zatvorena na množenje, zaključujemo da je $ab = e$ što implicira $a = b^{-1}$ i $ba = e$. Dakle, parcijalna Cayleyeva tablica grupe G je

$\cdot$	e	a	b
e	e	a	b
a	a	$?$	e
b	b	e	$?$

Tablica 1.1. Parcijalna Cayleyeva tablica grupe $G = \{e, a, b\}$.

Kako se u svakom retku (stupcu) Cayleyeve tablice nalaze svi elementi grupe G jer je množenje fiksnim elementom bijekcija na G , zaključujemo da je Cayleyeva tablica dana sa

$+(mod 4)$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Tablica 1.3. Cayleyeva tablica grupe $\mathbb{Z}_4$.

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Tablica 1.2. Cayleyeva tablica grupe $G = \{e, a, b\}$.

□

Primjer 1.2. *Zbrajanje modulo n .* Neka je $n \in \mathbb{N}$. Definirajmo relaciju ekvivalencije na skupu $\mathbb{Z}$ s

$$x \equiv y \pmod{n} \text{ ako je } x - y = qn \text{ za neki } q \in \mathbb{Z}.$$

Neka je $\bar{x}$ klasa ekvivalencije elementa $x \in \mathbb{Z}$, $\bar{x} = \{x + pn \mid p \in \mathbb{Z}\}$. Tada je $\bar{x} = \bar{y}$ ako i samo ako je $x - y = qn$ za neki $q \in \mathbb{Z}$. Označimo skup svih klasa ekvivalencije s

$$\mathbb{Z}_n = \{\bar{x} \mid x \in \mathbb{Z}\}.$$

Na skupu $\mathbb{Z}_n$ možemo definirati zbrajanje modulo n na prirodan način s

$$\bar{x} + \bar{y} = \overline{x + y}.$$

Pokažimo da je ova operacija dobro definirana, odnosno da ne ovisi o predstavniku klase ekvivalencije. Ako je $\bar{x} = \bar{x}_1$ i $\bar{y} = \bar{y}_1$, onda je $x - x_1 = pn$ i $y - y_1 = qn$ za neke $p, q \in \mathbb{Z}$. U tom slučaju vrijedi

$$x + y - (x_1 + y_1) = (p + q)n,$$

što povlači $\overline{x + y} = \overline{x_1 + y_1}$. Neutralni element je klasa ekvivalencije $\bar{0}$, a inverzni element je $-\bar{x} = \overline{-x}$. Kako je zbrajanje komutativno zaključujemo da je $(\mathbb{Z}_n, +)$ Abelova grupa. S obzirom da je $\bar{n} = \bar{0}$, $\mathbb{Z}_n$ ima točno n elemenata

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}.$$

Cayleyeva tablica grupe $\mathbb{Z}_4$ prikazana je u tablici 1.3. □

Primjer 1.3. *Množenje modulo n .* Neka je $\mathbb{Z}_n$ skup kao u prethodnom primjeru. Na skupu $\mathbb{Z}_n$ možemo definirati množenje modulo n pravilom $\bar{x}\bar{y} = \overline{xy}$. Lako se provjeri da je množenje dobro definirano. Neka je $\bar{x} = \bar{x}_1$ i $\bar{y} = \bar{y}_1$. Tada je $x - x_1 = pn$ i $y - y_1 = qn$ za neke $p, q \in \mathbb{Z}$ iz čega slijedi

$$xy = (x_1 + pn)(y_1 + qn) = x_1y_1 + (py_1 + qx_1)n + pqn^2. \quad (1.3)$$

$\cdot \pmod{6}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Tablica 1.4. Tablica množenja polugrupe $\mathbb{Z}_6$.

Dakle, $\overline{xy} = \overline{x_1y_1}$. Na taj način $(\mathbb{Z}_n, \cdot)$ postaje polugrupa s jedinicom $\bar{1}$. Neka je $(\mathbb{Z}_n)^\times$ skup svih invertibilnih elemenata u $\mathbb{Z}_n$. Tada je $(\mathbb{Z}_n)^\times$ Abelova grupa u odnosu na množenje modulo n . Očigledno je da $\bar{0}$ nema inverz jer je $\bar{0}\bar{x} = \bar{0}$ za svaki $x \in \mathbb{Z}$ pa se invertibilni elementi nalaze u skupu $\{\bar{1}, \bar{2}, \bar{3}, \dots, \overline{n-1}\}$. Kao konkretni primjer promotrimo polugrupu

$$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}.$$

Iz tablice množenja 1.4 zaključujemo da samo elementi $\bar{1}$ i $\bar{5}$ imaju inverz jer je $\bar{1}\bar{1} = \bar{1}$ i $\bar{5}\bar{5} = \bar{1}$, stoga je

$$(\mathbb{Z}_6)^\times = \{\bar{1}, \bar{5}\}.$$

□

Primjer 1.4. Lako se provjeri da je podskup od $\mathbb{Q}$ oblika

$$G = \{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\}$$

grupa obzirom na zbrajanje. Pokažimo da je $G^* = G \setminus \{0\}$ grupa obzirom na množenje. Neka su $a_1 + \sqrt{2}b_1, a_2 + \sqrt{2}b_2 \in G^*$. Tada a_i i b_i nisu oba nula. Pokažimo da je

$$(a_1 + \sqrt{2}b_1)(a_2 + \sqrt{2}b_2) = a_1a_2 + 2b_1b_2 + (a_1b_2 + b_1a_2)\sqrt{2} \in G^*. \quad (1.4)$$

Pretpostavimo da je

$$a_1a_2 + 2b_1b_2 = 0 \quad \text{i} \quad a_1b_2 + b_1a_2 = 0. \quad (1.5)$$

Množenjem prve jednadžbe s b_2 i korištenjem druge jednadžbe dobivamo

$$b_1(-a_2^2 + 2b_2^2) = 0. \quad (1.6)$$

Slično, ponavljanjem postupka gdje prvu jednadžbu množimo s a_2 dobivamo

$$a_1(a_2^2 - 2b_2^2) = 0. \quad (1.7)$$

Kako a_1 i b_1 nisu oba nula, iz jednadžbi (1.6) i (1.7) slijedi $a_2^2 - 2b_2^2 = 0$, što vodi na kontradikciju jer su a_2 i b_2 racionalni brojevi koji nisu oba nula. Zaključujemo da je $a_1a_2 + 2b_1b_2 \neq 0$ ili $a_1b_2 + b_1a_2 \neq 0$ čime je dokazana tvrdnja (1.4). Očigledno je $1 \in G^*$ za $a = 1$ i $b = 0$. Nadalje, iz uvjeta da su a i b racionalni brojevi koji nisu oba nula slijedi $a^2 - 2b^2 \neq 0$ pa je

$$\frac{1}{a + \sqrt{2}b} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in G^*. \quad (1.8)$$

Dakle, G^* je grupa obzirom na množenje. □

Primjer 1.5. *Opća linearna grupa* $GL(n, \mathbb{R})$. Neka je $M(n, \mathbb{R})$ skup svih matrica reda n nad poljem $\mathbb{R}$. $M(n, \mathbb{R})$ je polugrupa u odnosu na matrično množenje. Skup $GL(n, \mathbb{R})$ svih invertibilnih matrica reda n je grupa s jedinicom I gdje je I jedinična matrica reda n . Kako je matrica $A \in M(n, \mathbb{R})$ invertibilna ako i samo ako je $\det(A) \neq 0$, grupu $GL(n, \mathbb{R})$ možemo definirati kao

$$GL(n, \mathbb{R}) = \{A \in M(n, \mathbb{R}) \mid \det(A) \neq 0\}.$$

Ova grupa naziva se opća linearna grupa reda n . $\square$

Primjer 1.6. *Heisenbergova grupa*. Skup gornje trokutastih matrica oblika

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$$

je zatvoren na matrično množenje i inverziju jer je

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a & -b + ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}.$$

Stoga je H grupa koju nazivamo Heisenbergova grupa. $\square$

Primjer 1.7. *Unitarna grupa* $U(1)$. Skup kompleksnih brojeva $\{e^{i\theta} \mid \theta \in \mathbb{R}\}$ je očigledno grupa s obzirom na množenje jer je $e^{i\theta_1}e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$ i $(e^{i\theta})^{-1} = e^{-i\theta}$. Ovu grupu nazivamo unitarna grupa i označavamo sa $U(1)$. Elementi grupe tvore jediničnu kružnicu $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$. $\square$

Primjer 1.8. *Grupa rotacija* $SO(2)$. Skup matrica oblika

$$R_\theta = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}, \quad \theta \in \mathbb{R},$$

je zatvoren na matrično množenje i inverziju. Doista, za proizvoljne matrice R_θ i R_φ vrijedi

$$\begin{aligned} R_\theta R_\varphi &= \begin{pmatrix} \cos \theta \cos \varphi - \sin \theta \sin \varphi & -\cos \theta \sin \varphi - \sin \theta \cos \varphi \\ \sin \theta \cos \varphi + \cos \theta \sin \varphi & -\sin \theta \sin \varphi + \cos \theta \cos \varphi \end{pmatrix} \\ &= \begin{pmatrix} \cos(\theta + \varphi) & -\sin(\theta + \varphi) \\ \sin(\theta + \varphi) & \cos(\theta + \varphi) \end{pmatrix} = R_{\theta+\varphi} \in SO(2). \end{aligned}$$

Neutralni element je jedinična matrica I koja odgovara parametru $\theta = 0$,

$$R_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$$

Inverzna matrica R_θ^{-1} dana je s

$$R_\theta^{-1} = \frac{1}{\cos^2 \theta + \sin^2 \theta} \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix},$$

iz čega slijedi da je $R_\theta^{-1} = R_{-\theta}$. Ove matrice tvore grupu rotacija u ravni, u oznaci $SO(2)$, jer matrica R_θ predstavlja operator rotacije oko z osi koja djeluje na točke u xy -ravni. Ako točku (x, y) zarotiramo u pozitivnom smjeru za kut θ , onda nova točka ima koordinate

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \cos \theta - y \sin \theta \\ x \sin \theta + y \cos \theta \end{pmatrix} \quad (1.9)$$

(vidi sliku 1.2). $\square$

Primjer 1.9. *Lorentzova grupa $O(1, 3)$.* Lorentzova grupa je grupa matrica

$$O(1, 3) = \left\{ A \in GL(4, \mathbb{R}) \mid A^T \eta A = \eta \right\} \quad (1.10)$$

gdje je

$$\eta = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \quad (1.11)$$

Doista, ako su $A, B \in O(1, 3)$, onda je

$$(AB)^T \eta (AB) = B^T (A^T \eta A) B = B^T \eta B = \eta \quad (1.12)$$

što povlači $AB \in O(1, 3)$. Nadalje, iz relacije $AA^{-1} = I$ slijedi $(A^{-1})^T A^T = I$, odnosno

$$(A^{-1})^T A^T \eta = \eta. \quad (1.13)$$

S druge strane, iz uvjeta $A^T \eta A = \eta$ slijedi $A^T \eta = \eta A^{-1}$ što zajedno sa (1.13) daje

$$(A^{-1})^T \eta A^{-1} = \eta \quad (1.14)$$

pa je $A^{-1} \in O(1, 3)$. Zaključujemo da je $O(1, 3)$ grupa obzirom na matrično množenje. Lorentzova grupa, nazvana po nizozemskom fizičaru Hendriku Lorentzu, ima važnu ulogu u specijalnoj teoriji relativnosti i teorijskoj fizici uopće. Njezini elementi su izometrije prostora Minkowskog koje fiksiraju ishodište. $\square$

Primjer 1.10. *Grupe simetrija diferencijalnih jednadžbi.* Elementi neke grupe mogu ovisiti o jednom ili više realnih parametara. Takve grupe imaju primjenu u proučavanju simetrija diferencijalnih jednadžbi, odnosno u proučavanju transformacija nezavisnih i zavisnih varijabli koje čuvaju oblik diferencijalne jednadžbe. Promotrimo diferencijalnu jednadžbu za nepoznatu funkciju $u = u(x)$,

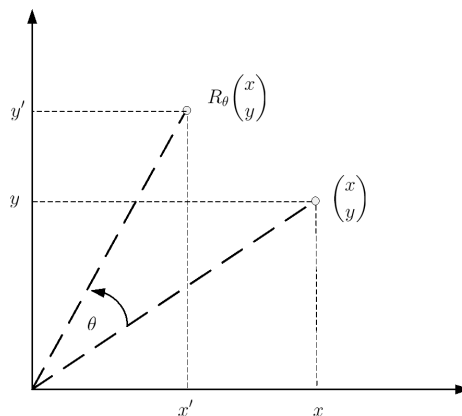
$$x^2 \frac{d^2 u}{dx^2} = F\left(x \frac{du}{dx} - u\right) \quad (1.15)$$

gdje je F zadana funkcija. Definirajmo transformaciju

$$T_{(\lambda, \epsilon)}(x, u) = (\lambda x, u + \epsilon x), \quad \epsilon \in \mathbb{R}, \lambda \in \mathbb{R}^+. \quad (1.16)$$

Skup svih transformacija (1.16) tvori grupu jer je

$$T_{(\lambda_2, \epsilon_2)} \circ T_{(\lambda_1, \epsilon_1)} = T_{(\lambda_1 \lambda_2, \epsilon_1 + \lambda_1 \epsilon_2)}. \quad (1.17)$$



Slika 1.2. Operator rotacije R_θ djeluje na točku $\begin{pmatrix} x \\ y \end{pmatrix}$.

Jedinica u grupi je transformacija $T_{(1,0)}$, a inverzni element je

$$T_{(\lambda, \epsilon)}^{-1} = T_{(1/\lambda, -\epsilon/\lambda)}. \quad (1.18)$$

Transformacija (1.16) ne mijenja oblik diferencijalne jednačbe (1.15). Definirajmo nove varijable

$$y = \lambda x, \quad v = u + \epsilon x. \quad (1.19)$$

Tada je

$$\frac{dv}{dy} = \frac{1}{\lambda} \frac{du}{dx} + \frac{\epsilon}{\lambda}, \quad \frac{d^2v}{dy^2} = \frac{1}{\lambda^2} \frac{d^2u}{dx^2}. \quad (1.20)$$

Odavde slijedi

$$y^2 \frac{d^2v}{dy^2} = (\lambda x)^2 \frac{1}{\lambda^2} \frac{d^2u}{dx^2} = x^2 \frac{d^2u}{dx^2}. \quad (1.21)$$

Nadalje, iz (1.20) dobivamo

$$y \frac{dv}{dy} - v = \lambda x \left(\frac{1}{\lambda} \frac{du}{dx} + \frac{\epsilon}{\lambda} \right) - (u + \epsilon x) = x \frac{du}{dx} - u. \quad (1.22)$$

Jednačbe (1.21) i (1.22) impliciraju da varijable (y, v) zadovoljavaju istu diferencijalnu jednačbu kao (x, u) što znači da je jednačba (1.15) invarijantna u odnosu na grupu transformacija (1.16). Poznavanje simetrija neke jednačbe nam omogućuje da od poznatog rješenja $u(x)$ tvorimo nova rješenja $v(y) = u(y/\lambda) + \epsilon y/\lambda$. $\square$

1.2 Homomorfizmi grupa

Promotrimo grupu $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ s operacijom zbrajanja modulo 4 (vidi tablicu 1.3) i grupu $G = \{1, i, -1, -i\}$ s operacijom množenja. Lako se uočava da $\mathbb{Z}_4$ i G imaju istu strukturu ako definiramo preslikavanje $\phi: \mathbb{Z}_4 \rightarrow G$ sa

$$\phi(\bar{0}) = 1, \quad \phi(\bar{1}) = i, \quad \phi(\bar{2}) = -1, \quad \phi(\bar{3}) = -i. \quad (1.23)$$

Primijetimo da je $\phi(\bar{a} + \bar{b}) = \phi(\bar{a})\phi(\bar{b})$ za sve $\bar{a}, \bar{b} \in \mathbb{Z}_4$ što povlači da se tablica množenja za $\mathbb{Z}_4$ preslikava u tablicu množenja za G . Ovakva preslikavanja imaju važnu ulogu u teoriji grupa.

Definicija 1.5. Neka su G i H grupe. Preslikavanje $\phi: G \rightarrow H$ naziva se *homomorfizam grupe* ako vrijedi

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

Ako je ϕ surjektivno preslikavanje, onda se ϕ naziva *epimorfizam*, a ako je ϕ injekcija, onda ϕ nazivamo *monomorfizam*.

Monomorfizmi su važni jer “čuvaju” strukturu grupe u smislu da se umnožak elemenata x i y preslikava u umnožak njihovih slika $\phi(x)$ i $\phi(y)$. Ako ϕ nije injekcija, onda ϕ ne čuva strukturu grupe. Na primjer, očigledno je da trivijalni homomorfizam $\phi(x) = e'$, gdje je e' jedinica u H , ne čuva strukturu grupe jer se čitava grupa G preslikava u jedan element.

Definicija 1.6. Ako je $\phi: G \rightarrow H$ bijekcija i homomorfizam, onda se ϕ naziva *izomorfizam*. U tom slučaju su G i H izomorfne grupe, i pišemo $G \simeq H$. Ako je $G = H$, onda ϕ nazivamo *automorfizam*.

Primjer 1.11. Skup $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ je grupa u odnosu na množenje kompleksnih brojeva. Konjugacija $\phi: \mathbb{C}^* \rightarrow \mathbb{C}^*$, $\phi(z) = \bar{z}$, je homomorfizam jer je

$$\phi(z_1 z_2) = \overline{z_1 z_2} = \bar{z}_1 \bar{z}_2 = \phi(z_1) \phi(z_2).$$

Kako je ϕ bijekcija na $\mathbb{C}^*$, ϕ je izomorfizam na $\mathbb{C}^*$. $\square$

Primjer 1.12. Neka su $(\mathbb{R}, +)$ i $(\mathbb{R}^+, \cdot)$ grupe s operacijama zbrajanja odnosno množenja, redom, gdje je $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$. Eksponencijalna funkcija $\phi: \mathbb{R} \rightarrow \mathbb{R}^+$, $\phi(x) = e^x$, je homomorfizam jer vrijedi

$$\phi(x_1 + x_2) = e^{x_1 + x_2} = e^{x_1} e^{x_2} = \phi(x_1) \phi(x_2).$$

Funkcija $\phi: \mathbb{R} \rightarrow \mathbb{R}^+$ je bijekcija gdje je $\phi^{-1}(x) = \ln(x)$ inverzno preslikavanje. Stoga je $\phi: \mathbb{R} \rightarrow \mathbb{R}^+$ izomorfizam. $\square$

Primjer 1.13. Preslikavanje $\phi: SO(2) \rightarrow U(1)$ koje matrici $R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$ pridružuje kompleksni broj $e^{i\theta} \in U(1)$ je homomorfizam jer je

$$\phi(R_\theta R_\varphi) = \phi(R_{\theta+\varphi}) = e^{i(\theta+\varphi)} = e^{i\theta} e^{i\varphi} = \phi(R_\theta) \phi(R_\varphi). \quad (1.24)$$

$\square$

Primjer 1.14. Preslikavanje $\phi: GL(n, \mathbb{R}) \rightarrow \mathbb{R}^*$ definirano s $\phi(A) = \det(A)$ je homomorfizam, jer iz Binet-Cauchyevog teorema slijedi

$$\phi(AB) = \det(AB) = \det(A)\det(B) = \phi(A)\phi(B).$$

$\square$

Primjer 1.15. Neka je G grupa i neka su $\varphi_1, \varphi_2: G \rightarrow G$ definirani sa $\varphi_1(g) = g^{-1}$ i $\varphi_2(g) = g^2$. Preslikavanja φ_1 i φ_2 su homomorfizmi ako i samo ako je G Abelova grupa. $\square$

Unutarnji automorfizam ili konjugacija

Neka je G grupa i odaberimo $a \in G$. Definirajmo preslikavanje $C_a: G \rightarrow G$ s $C_a(x) = axa^{-1}$. Pokažimo da je C_a automorfizam grupe G . Zbog asocijativnosti množenja imamo

$$C_a(xy) = axya^{-1} = (axa^{-1})(aya^{-1}) = C_a(x)C_a(y),$$

pa zaključujemo da je C_a homomorfizam. Pretpostavimo da je $C_a(x) = C_a(y)$, odnosno

$$axa^{-1} = aya^{-1}. \quad (1.25)$$

Množenjem jednačbe (1.25) slijeva s a^{-1} i zdesna s a dobivamo $x = y$, stoga je C_a injekcija. Neka je $y \in G$ proizvoljan element. Tada za $x = a^{-1}ya$ imamo

$$C_a(x) = a(a^{-1}ya)a^{-1} = y,$$

što pokazuje da je C_a surjekcija. Dakle, C_a je automorfizam grupe G koji nazivamo unutarnji automorfizam ili konjugacija elementom a .

Sljedeći teoremi daju neka osnovna svojstva homomorfizama.

Teorem 1.1. *Neka su G i H grupe s pripadnim jedinicama $e \in G$ i $e' \in H$ i neka je $\phi: G \rightarrow H$ homomorfizam. Tada je*

$$(i) \quad \phi(e) = e',$$

$$(ii) \quad \phi(x^{-1}) = \phi(x)^{-1} \text{ za svaki } x \in G.$$

Dokaz (i) Kako je $ee = e$, slijedi

$$\phi(e) = \phi(ee) = \phi(e)\phi(e). \quad (1.26)$$

Množenjem jednačbe (1.26) zdesna s $\phi(e)^{-1}$ dobivamo

$$\phi(e)\phi(e)^{-1} = \phi(e).$$

Međutim, $\phi(e)\phi(e)^{-1} = e'$ pa zaključujemo $\phi(e) = e'$.

(ii) Neka je $x \in G$. Djelovanjem homomorfizma ϕ na $xx^{-1} = x^{-1}x = e$ dobivamo

$$\phi(xx^{-1}) = \phi(x)\phi(x^{-1}) = e', \quad (1.27)$$

$$\phi(x^{-1}x) = \phi(x^{-1})\phi(x) = e'. \quad (1.28)$$

Prema definiciji inverznog elementa, relacije (1.27)-(1.28) povlače da je $\phi(x)^{-1} = \phi(x^{-1})$. ■

Teorem 1.1 pokazuje da homomorfizmi, osim što čuvaju množenje, čuvaju neutralni element i inverznu operaciju $x \mapsto x^{-1}$. Ako su dvije grupe G i H izomorfne, onda one imaju istu strukturu, pa su G i H samo različite realizacije iste algebarske strukture.

Definicija 1.7. Neka su G i H grupe. Jezgra homomorfizma $\phi: G \rightarrow H$ je skup

$$\ker(\phi) = \{x \in G \mid \phi(x) = e'\}.$$

Slika homomorfizma je skup

$$\text{Im}(\phi) = \{\phi(x) \mid x \in G\}.$$

Sljedeći teorem daje karakterizaciju injektivnog homomorfizma.

Teorem 1.2. Homomorfizam grupa $\phi: G \rightarrow H$ je injektivan ako i samo ako je $\ker(\phi) = \{e\}$.

Dokaz Pretpostavimo da je ϕ injektivan homomorfizam. Ako je $x \in \ker(\phi)$, onda po teoremu 1.1(i) vrijedi

$$\phi(x) = e' = \phi(e),$$

iz čega slijedi $x = e$ jer je ϕ injekcija. Dakle, $\ker(\phi) = \{e\}$. Pretpostavimo sada da je $\ker(\phi) = \{e\}$. Ako je $\phi(x) = \phi(y)$, onda je $\phi(x)\phi(y)^{-1} = e'$. Teorem 1.1 (ii) sada implicira

$$e' = \phi(x)\phi(y)^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1}),$$

iz čega dobivamo $xy^{-1} \in \ker(\phi) = \{e\}$. Dakle, $xy^{-1} = e$, pa zaključujemo $x = y$. Time je pokazano da je ϕ injekcija. ■

Navedimo još neka svojstva homomorfizama koja se lako dokazuju.

- (1) Ako su $\phi_1: G \rightarrow H$ i $\phi_2: H \rightarrow K$ homomorfizmi, onda je kompozicija $\phi_2 \circ \phi_1: G \rightarrow K$ homomorfizam.
- (2) Ako je $\phi: G \rightarrow H$ izomorfizam, onda je inverzno preslikavanje $\phi^{-1}: H \rightarrow G$ izomorfizam.

1.3 Podgrupe i susjedne klase

Definicija 1.8. Neka je G grupa. Neprazan podskup $H \subseteq G$ naziva se podgrupa od G , i zapisuje $H \leq G$, ako je H grupa u odnosu na množenje u G . Ako je $H \neq G$, onda koristimo oznaku $H < G$.

Iz definicije slijedi da je podgrupa H zatvorena u odnosu na operacije množenja i invertiranja, odnosno za sve $a, b \in H$ vrijedi $ab \in H$ i $a^{-1} \in H$. Primijetimo također da podgrupa H ima istu jedinicu kao i grupa G . Svaka grupa G ima trivijalne podgrupe $\{e\}$ i G . Da bismo ustanovili je li neki podskup $H \subset G$ podgrupa trebamo provjeriti da li je H zatvoren na množenje i invertiranje. Sljedeći teorem pokazuje da se ove dvije operacije mogu kombinirati u jednu što daje kriterij za egzistenciju podgrupe.

Teorem 1.3. *Neka je G grupa. Neprazan podskup $H \subseteq G$ je podgrupa od G ako i samo ako je*

$$ab^{-1} \in H \quad \text{za sve} \quad a, b \in H. \quad (1.29)$$

Dokaz Neka je H podgrupa od G . Odaberimo $a, b \in H$. Tada je $ab^{-1} \in H$ jer je H zatvorena na množenje i invertiranje. Pretpostavimo sada da vrijedi (1.29). Tada za $a = b \in H$ dobivamo $e = aa^{-1} \in H$. Neka su sada $a, b \in H$ proizvoljni elementi. Tada je $b^{-1} = eb^{-1} \in H$, pa je H zatvorena na invertiranje. Nadalje, (1.29) povlači $ab = a(b^{-1})^{-1} \in H$, stoga je H zatvorena na množenje. Time je dokazano da je H podgrupa od G . ■

Primjer 1.16. Specijalna linearna grupa $SL(n, \mathbb{R})$ je definirana sa

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

Ako su $A, B \in SL(n, \mathbb{R})$, onda je

$$\det(AB^{-1}) = \frac{\det(A)}{\det(B)} = 1,$$

stoga je $AB^{-1} \in SL(n, \mathbb{R})$. Dakle, $SL(n, \mathbb{R})$ je podgrupa opće linearne grupe $GL(n, \mathbb{R})$. □

Primjer 1.17. Unitarna grupa $U(1) = \{e^{i\theta} \mid \theta \in \mathbb{R}\}$ je podgrupa grupe kompleksnih brojeva $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ obzirom na množenje jer je $e^{i\theta_1}(e^{i\theta_2})^{-1} = e^{i(\theta_1 - \theta_2)} \in U(1)$. □

Ako su H_1 i H_2 podgrupe od G , lako se vidi da je $H_1 \cap H_2$ podgrupa od G . Doista, $H_1 \cap H_2$ je neprazan skup jer je $e \in H_1 \cap H_2$. Ako su $a, b \in H_1 \cap H_2$, onda je $a, b \in H_1$ i $a, b \in H_2$ što implicira $a^{-1}b \in H_1$ i $a^{-1}b \in H_2$. Dakle, $a^{-1}b \in H_1 \cap H_2$ pa je $H_1 \cap H_2$ podgrupa od G prema teoremu 1.3. Primijetimo da je $H_1 \cap H_2$ najveća podgrupa od G koja je sadržana u H_1 i u H_2 . Slično se pokazuje da je presjek bilo koje familije podgrupa $\bigcap_{i \in I} H_i$ također podgrupa od G .

Naglasimo, međutim, da unija $H_1 \cup H_2$ ne mora biti podgrupa od G . U tom smislu dokažimo sljedeću tvrdnju. Unija podgrupa $H_1 \cup H_2$ je podgrupa od G ako i samo ako je $H_1 \subseteq H_2$ ili $H_2 \subseteq H_1$. Ako je jedna podgrupa sadržana u drugoj, očigledno je $H_1 \cup H_2$ podgrupa od G . Pretpostavimo sada da je $H_1 \cup H_2$ podgrupa od G , ali H_1 nije podskup od H_2 niti je H_2 podskup od H_1 . Tada postoje elementi $a \in H_1 \setminus H_2$ i $b \in H_2 \setminus H_1$. Kako su $a, b \in H_1 \cup H_2$, to je $ab \in H_1 \cup H_2$ jer je $H_1 \cup H_2$ zatvorena na množenje. Ako je $ab \in H_1$, onda je $a^{-1}(ab) = b \in H_1$, kontradikcija jer je $b \in H_2 \setminus H_1$. Ako je $ab \in H_2$, onda je $(ab)b^{-1} = a \in H_2$, kontradikcija jer je $a \in H_1 \setminus H_2$. U svakom slučaju dobivamo kontradikciju s pretpostavkom da H_1 nije podskup od H_2 niti je H_2 podskup od H_1 . Zaključujemo da je $H_1 \subseteq H_2$ ili $H_2 \subseteq H_1$.

Svakom homomorfizmu grupa pridružene su dvije podgrupe: jezgra homomorfizma i slika homomorfizma.

Teorem 1.4. *Neka je $\phi: G \rightarrow H$ homomorfizam grupa. Jezgra homomorfizma $\ker(\phi)$ je podgrupa od G , a slika homomorfizma $\text{Im}(\phi)$ je podgrupa od H .*

Dokaz Neka su e i e' neutralni elementi u G i H , redom. Skupovi $\ker(\phi)$ i $\text{Im}(\phi)$ su neprazni jer je $e \in \ker(\phi)$ i $e' = \phi(e) \in \text{Im}(\phi)$. Neka su $a, b \in \ker(\phi)$. Tada je

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} = e'(e')^{-1} = e',$$

što pokazuje $ab^{-1} \in \ker(\phi)$. Prema teoremu 1.3, $\ker(\phi)$ je podgrupa od G .

Neka su $x, y \in \text{Im}(\phi)$. Tada postoje $a, b \in G$ takvi da je $\phi(a) = x$ i $\phi(b) = y$. Stoga je $xy^{-1} = \phi(a)\phi(b)^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1})$, što pokazuje da je $xy^{-1} \in \text{Im}(\phi)$. Dakle, $\text{Im}(\phi)$ je podgrupa od H . ■

U strukturi grupe G važnu ulogu ima centar grupe $Z(G)$ kojeg tvore svi elementi iz G koji komutiraju sa svim elementima iz G .

Definicija 1.9. *Centar grupe G je skup*

$$Z(G) = \{g \in G \mid ga = ag \text{ za svaki } a \in G\}.$$

Primijetimo da je G Abelova grupa ako i samo ako je $Z(G) = G$ pa veličina centra pokazuje koliko se G razlikuje od Abelove grupe na istom skupu G .

Teorem 1.5. *$Z(G)$ je podgrupa od G .*

Dokaz Neka su $a, b \in Z(G)$. Onda je $ag = ga$ i $bg = gb$ za svaki $g \in G$. Primijetimo da iz zadnje jednakosti proizlazi $gb^{-1} = b^{-1}g$ pa imamo

$$(ab^{-1})g = agb^{-1} = g(ab^{-1}) \quad \text{za svaki } g \in G$$

što povlači $ab^{-1} \in Z(G)$. ■

Pojam centra grupe se može poopćiti na centralizator proizvoljnog podskupa $A \subseteq G$ ako promatramo sve elemente u G koji komutiraju sa svim elementima skupa A .

Definicija 1.10. *Neka je A podskup grupe G . Centralizator skupa A u G je skup*

$$C_G(A) = \{g \in G \mid gag^{-1} = a \text{ za svaki } a \in A\}.$$

Primijetimo da je $gag^{-1} = a$ ako i samo ako je $ga = ag$, stoga je $C_G(A)$ skup svih elemenata u G koji komutiraju sa svim elementima iz A . Primijetimo da je $C_G(A) \neq \emptyset$ jer je $e \in C_G(A)$. Također, ako je $A = G$, onda je $C_G(G) = Z(G)$. Na isti način kao u teoremu 1.5 se pokazuje da je $C_G(A)$ podgrupa od G za svaki podskup $A \subseteq G$. Iz definicije 1.10 slijedi da je $g \in C_G(A)$ ako i samo ako je $gag^{-1} = a$ za svaki $a \in A$. Drugim riječima, svaki element $a \in A$ je invarijantan na konjugaciju elementima $g \in C_G(A)$. Ako je $A = \{a\}$ jednačlani skup, onda centralizator označavamo sa $C_G(a)$.

Sada ćemo uvesti pojam lijeve i desne susjedne klase pridružene podgrupi $H \subseteq G$. Promatrajući sljedeću relaciju na skupu G ,

$$a \sim b \Leftrightarrow a^{-1}b \in H.$$

Lako se pokazuje da je $\sim$ relacija ekvivalencije na grupi G :

- (1) $a \sim a$ jer je $a^{-1}a = e \in H$,
- (2) $a \sim b \Rightarrow b^{-1}a = (a^{-1}b)^{-1} \in H$ jer je $a^{-1}b \in H \Rightarrow b \sim a$,
- (3) $a \sim b$ i $b \sim c \Rightarrow a^{-1}b \in H$ i $b^{-1}c \in H \Rightarrow (a^{-1}b)(b^{-1}c) = a^{-1}c \in H \Rightarrow a \sim c$.

Klasa ekvivalencije elementa $a \in G$ je skup

$$\bar{a} = \{b \in G \mid a^{-1}b \in H\} = \{b \in G \mid b \in aH\} = aH.$$

Definicija 1.11. *Neka je H podgrupa grupe G i neka je $a \in G$. Skup*

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

naziva se lijeva susjedna klasa podgrupe H određena elementom a . Skup svih lijevih susjednih klasa podgrupe H označavamo sa G/H .

Slično, na grupi G možemo uvesti relaciju ekvivalencije sa

$$a \sim b \Leftrightarrow ab^{-1} \in H. \quad (1.30)$$

U ovom slučaju, klasa ekvivalencije elementa $a \in G$ je desna susjedna klasa $\bar{a} = Ha$ gdje je

$$Ha = \{ha \mid h \in H\}.$$

Skup svih desnih susjednih klasa pod grupe H označavamo sa $H \backslash G$. Susjedna klasa generirana elementom $e \in G$ je lijeva i desna susjedna klasa jer je $eH = He = H$. Uočimo da je $aH = bH$ ako i samo ako je $a \sim b$, odnosno ako i samo ako je $a^{-1}b \in H$. Slično, $Ha = Hb$ ako i samo ako je $ab^{-1} \in H$.

Lijevo množenje $L_a: H \rightarrow aH$, definirano sa $L_a(g) = ag$, je bijekcija sa H na aH pa skupovi H i aH imaju isti kardinalni broj. Slično, desno množenje $R_a: H \rightarrow Ha$, definirano sa

$R_a(g) = ga$, je bijekcija sa H na Ha . Stoga za kardinalne brojeve lijevih i desnih susjednih klasa vrijedi

$$|H| = |aH| = |Ha|. \quad (1.31)$$

Propozicija 1.3. *Skupovi lijevih i desnih susjednih klasa podgrupe H u grupi G imaju isti kardinalni broj,*

$$|G/H| = |H \backslash G|. \quad (1.32)$$

Dokaz Definirajmo preslikavanje $\psi: G/H \rightarrow H \backslash G$ sa $\psi(aH) = Ha^{-1}$. Ako je $\psi(aH) = \psi(bH)$, onda je $Ha^{-1} = Hb^{-1}$ što implicira $h_1(a^{-1}b) = h_2$ za neke $h_1, h_2 \in H$. Odavde slijedi da je $a^{-1}b = h_1^{-1}h_2 \in H$, odnosno $a \sim b$ pa je $aH = bH$ jer a i b pripadaju istoj klasi ekvivalencije. Dakle, ψ je injekcija. Nadalje, $\psi(a^{-1}H) = Ha$ implicira da je ψ surjekcija pa zaključujemo da je ψ bijekcija. Stoga skupovi G/H i $H \backslash G$ imaju isti kardinalni broj. ■

Definicija 1.12. *Neka je H podgrupa grupe G . Kardinalni broj skupa G/H , tj. skupa $H \backslash G$, naziva se indeks podgrupe H u G , i označava se sa $[G : H]$.*

Ako je $H = \{e\}$ trivijalna podgrupa, onda je $aH = \{a\}$ za svaki $a \in G$. Iz ovoga slijedi da je broj susjednih klasa podgrupe $H = \{e\}$ jednak broju elemenata grupe G , odnosno $[G : H] = |G|$. Ako je $H = G$, onda je $aH = H$ za svaki $a \in G$, pa je $[G : H] = 1$. Za proizvoljnu podgrupu očekujemo da se indeks nalazi između 1 i $|G|$.

Teorem 1.6 (Lagrangeov teorem). *Neka je G konačna grupa i neka je H podgrupa od G . Tada je*

$$|G| = [G : H] |H|.$$

Dokaz Odaberimo $a \in G$. Klase ekvivalencije aH tvore particiju skupa G pa se G može napisati kao disjunktna unija $G = \bigcup_{a \in C} aH$ gdje C sadrži točno jedan element iz svake susjedne klase aH . Kako je $|aH| = |H|$, odavde slijedi da je

$$|G| = \sum_{a \in C} |aH| = \sum_{a \in C} |H| = k |H| \quad (1.33)$$

gdje je k broj elemenata u skupu C što je broj različitih susjednih klasa aH . Dakle, $k = [G : H]$ što povlači $|G| = [G : H] |H|$. ■

Lagrangeov teorem ima važnu ulogu u proučavanju strukture grupa. Na primjer, teorem implicira da red podgrupe dijeli red grupe jer je

$$|H| = \frac{|G|}{[G : H]}.$$

Ova činjenica ima za posljedicu da red podgrupe ne može biti proizvoljan. Ako je $|G| = p$ gdje je p prosti broj, onda je $|H| = 1$ ili $|H| = p$ što povlači da G ima samo trivijalne podgrupe $H = \{e\}$ i $H = G$. ■

1.4 Normalne podgrupe i kvocijentne grupe

U ovom poglavlju ćemo proučavati podgrupe kod kojih su lijeve i desne susjedne klase jednake. Takve grupe nazivamo normalne podgrupe i dane su sljedećom definicijom.

Definicija 1.13. *Neka je G grupa. Kažemo da je podgrupa $N \subseteq G$ normalna podgrupa od G ako je $xNx^{-1} \subseteq N$ za svaki $x \in G$.*

Za normalnu podgrupu koristimo oznaku $N \triangleleft G$. Ako je G Abelova grupa, onda je svaka podgrupa od G normalna jer je $xyx^{-1} = y \in N$ za svaki $x \in G$ i $y \in N$. Trivijalna podgrupa $\{e\}$ je normalna podgrupa svake grupe G jer je $xex^{-1} = e$. Primijetimo da iz definicije 1.13 slijedi da je N normalna podgrupa svake podgrupe $H \subseteq G$ koja sadrži N . Sljedeći teorem daje karakterizaciju normalnih podgrupa.

Teorem 1.7. *Neka je N podgrupa grupe G . Tada su sljedeće tvrdnje ekvivalentne:*

- (i) $N \triangleleft G$,
- (ii) $xN = Nx$ za svaki $x \in G$,
- (iii) $xNx^{-1} = N$ za svaki $x \in G$.

Dokaz (i) $\Rightarrow$ (ii) Neka je $N \triangleleft G$ i neka je $x \in G$. Svaki $y \in xN$ je oblika $y = xh$ za neki $h \in N$ pa vrijedi $y = (xhx^{-1})x \in Nx$ jer je $xhx^{-1} \in N$. Dakle, $xN \subseteq Nx$. Slično se pokazuje druga inkluzija $Nx \subseteq xN$ pa zaključujemo da je $Nx = xN$.

(ii) $\Rightarrow$ (iii) Pretpostavimo da je $xN = Nx$ za svaki $x \in G$. Ako je $y \in xNx^{-1}$, onda je $y = xhx^{-1}$ za neki $h \in N$. Iz pretpostavke (ii) slijedi da je $xh = h'x$ za neki $h' \in N$ što povlači $y = xhx^{-1} = h'xx^{-1} = h' \in N$. Dakle, $xNx^{-1} \subseteq N$. Neka je sada $y \in N$. Pretpostavka (ii) povlači da je $yx = xy'$ za neki $y' \in N$ pa vrijedi $y = x(x^{-1}yx)x^{-1} = xy'x^{-1} \in xNx^{-1}$. Dakle, $N \subseteq xNx^{-1}$ čime je dokazano $xNx^{-1} = N$.

(iii) $\Rightarrow$ (i) Tvrdnja trivijalno vrijedi jer je $xNx^{-1} = N \subseteq N$ za svaki $x \in G$. ■

Primjer 1.18. Neka je $Z(G)$ centar grupe G i neka je $x \in G$. Tada za svaki $y \in Z(G)$ vrijedi $xyx^{-1} = xx^{-1}y = y$ što povlači

$$xZ(G)x^{-1} = \{xyx^{-1} \mid y \in Z(G)\} = Z(G).$$

Dakle, $Z(G)$ je normalna podgrupa od G . □

Primjer 1.19. Neka je $\varphi: G \rightarrow H$ homomorfizam s grupe G u grupu H . Ako je $g \in \ker(\varphi)$ i $x \in G$, onda je

$$\varphi(xgx^{-1}) = \varphi(x)\varphi(g)\varphi(x)^{-1} = \varphi(x)\varphi(x)^{-1} = e,$$

dakle $xgx^{-1} \in \ker(\varphi)$. Odavde slijedi da je $x\ker(\varphi)x^{-1} \subseteq \ker(\varphi)$ za svaki $x \in G$, pa je $\ker(\varphi)$ normalna podgrupa od G . $\square$

Primjer 1.20. Pokažimo da je $SL(n, \mathbb{R})$ normalna podgrupa opće linearne grupe $GL(n, \mathbb{R})$. Odaberimo $A \in SL(n, \mathbb{R})$ i $B \in GL(n, \mathbb{R})$. Prema Binet-Cauchyevom teoremu imamo

$$\det(BAB^{-1}) = \det(B)\det(A)\det(B^{-1}) = \det(B)\frac{1}{\det(B)} = 1,$$

jer je $\det(A) = 1$. Dakle, $BAB^{-1} \in SL(n, \mathbb{R})$ što pokazuje da je

$$BSL(n, \mathbb{R})B^{-1} \subseteq SL(n, \mathbb{R}).$$

$\square$

Propozicija 1.4. Ako je H podgrupa grupe G takva da je $[G: H] = 2$, onda je $H \triangleleft G$.

Dokaz Kako je $[G: H] = 2$, skup lijevih susjednih klasa sadrži dva elementa H i gH gdje je $g \in G \setminus H$. Skupovi H i gH tvore particiju skupa G što povlači da je $gH = G \setminus H$. Dvije desne susjedne klase H i Hg također tvore particiju skupa G i vrijedi $Hg = G \setminus H$. Stoga zaključujemo da je $gH = Hg$ za svaki $g \in G \setminus H$, odnosno $gH = Hg$ za svaki $g \in G$. Prema teoremu 1.7, H je normalna podgrupa od G . $\blacksquare$

Promotrimo sada sljedeći problem. Neka je H podgrupa od G . Očigledno je $xNx^{-1} \subseteq N$ za svaki $x \in N$ pa je N normalna podgrupa same sebe. Prirodno je zapitati se koja je najveća podgrupa od G koja sadrži N kao normalnu podgrupu. Ovo razmatranje vodi na pojam normalizatora skupa, odnosno grupe.

Definicija 1.14. Neka je A podskup grupe G . Definirajmo skup $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. Normalizator skupa A u G je definiran s

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}.$$

Ako je $g \in C_G(A)$, onda je $gag^{-1} = a$ za svaki $a \in A$ što implicira $gAg^{-1} = A$. Ovo povlači $g \in N_G(A)$, stoga je $C_G(A) \leq N_G(A)$. Skup A ne mora biti sadržan u $N_G(A)$. Međutim, ako je A podgrupa od G , onda je $gAg^{-1} = A$ za svaki $g \in A$ pa slijedi $A \subseteq N_G(A)$.

Prema teoremu 1.7, za normalnu podgrupu N od G vrijedi $xN = Nx$, $x \in G$, što je ekvivalentno sa

$$xNx^{-1} = N \quad \text{za svaki } x \in G.$$

Stoga se normalne podgrupe mogu karakterizirati kao one podgrupe čiji je normalizator cijela grupa G ,

$$N_G(N) = G.$$

Teorem 1.8. *Neka je G grupa.*

- (i) *Za svaki neprazni podskup $A \subseteq G$, $N_G(A)$ je podgrupa od G .*
- (ii) *Za svaku podgrupu H od G , $N_G(H)$ je najveća podgrupa od G takva da je $H \triangleleft N_G(H)$.*

Dokaz (i) Neka su $g, h \in N_G(A)$. Tada je $gAg^{-1} = A$ i $hAh^{-1} = A$. Primijetimo da $hAh^{-1} = A$ implicira $h^{-1}Ah = A$ iz čega slijedi

$$(gh^{-1})A(gh^{-1})^{-1} = g(h^{-1}Ah)g^{-1} = gAg^{-1} = A.$$

Ovo povlači $gh^{-1} \in N_G(A)$, pa zaključujemo da je $N_G(A)$ podgrupa od G .

(ii) Kako je $H \subseteq N_G(H)$, to je H podgrupa od $N_G(H)$. Nadalje, H je normalna podgrupa od $N_G(H)$ jer je $gHg^{-1} = H$ za svaki $g \in N_G(H)$ prema definiciji normalizatora. Neka je K podgrupa od G takva da je $H \triangleleft K$. Tada je $kHk^{-1} = H$ za svaki $k \in K$ što po definiciji normalizatora implicira $K \subseteq N_G(H)$. Dakle, $N_G(H)$ je najveća podgrupa od G takva da je $H \triangleleft N_G(H)$. ■

Ako je $N \triangleleft G$, onda su prema teoremu 1.7 skupovi lijevih i desnih susjednih klasa jednaki, pa ih možemo jednostavno označiti s G/N . Na skupu G/N se može definirati struktura grupe koju nazivamo kvocijentna grupa. Konstrukcijom kvocijentne grupe G/N dobivamo grupu koja je općenito “manja” od G . Struktura grupe G se odražava na strukturu grupe G/N , pa kvocijentne grupe imaju važnu ulogu u proučavanju strukture grupa.

Teorem 1.9. *Neka je N normalna podgrupa grupe G . Tada je G/N grupa u odnosu na množenje definirano s*

$$(xN)(yN) = (xy)N. \quad (1.34)$$

Preslikavanje $\pi: G \rightarrow G/N$, $\pi(x) = xN$, je epimorfizam i $\ker(\pi) = N$.

Dokaz Potrebno je pokazati da je množenje (1.34) dobro definirano u smislu da rezultat ne ovisi o predstavnicima susjednih klasa xN i yN . Pretpostavimo da je

$$xN = x'N \quad \text{i} \quad yN = y'N. \quad (1.35)$$

Kako je N normalna podgrupa, prema teoremu 1.7 vrijedi $gN = Ng$ za svaki $g \in G$. Oдавде i iz (1.35) slijedi

$$(xy)N = x(y'N) = x(Ny') = (x'N)y' = (x'y')N.$$

Dakle, rezultat množenja ne ovisi o predstavnicima klasa pa je operacija (1.34) dobro definirana. Asocijativnost množenja u G se prenosi na G/N , stoga je

$$(xN)(yN)(zN) = (xyz)N.$$

Jedinica u G/N je susjedna klasa $eN = N$ jer je

$$(xN)(eN) = (eN)(xN) = xN.$$

Inverz elementa xN je susjedna klasa $x^{-1}N$ jer je

$$(xN)(x^{-1}N) = (x^{-1}N)(xN) = eN.$$

Iz navedenog zaključujemo da je G/N grupa u odnosu na množenje (1.34). Preslikavanje $\pi: G \rightarrow G/N$, $\pi(x) = xN$, je očigledno surjekcija. Nadalje, iz definicije množenja u G/N slijedi

$$\pi(xy) = (xy)N = (xN)(yN) = \pi(x)\pi(y),$$

stoga je π homomorfizam. Jezgra homomorfizma je dana s

$$\ker(\pi) = \{x \in G \mid xN = N\} = N$$

jer je $xN = N$ ako i samo ako je $x \in N$. ■

Definicija 1.15. *Neka je N normalna podgrupa grupe G . Grupa G/N naziva se kvocijentna grupa, a homomorfizam $\pi: G \rightarrow G/N$, $\pi(x) = xN$, naziva se kanonski homomorfizam ili projekcija sa G na G/N .*

Pretpostavimo da je G konačna grupa. Prema definiciji indeksa red kvocijentne grupe G/N je $[G : N]$, pa iz Lagrangeovog teorema 1.6 dobivamo jednostavnu formulu za red kvocijentne grupe,

$$|G/N| = [G : N] = \frac{|G|}{|N|}.$$

Sljedeći rezultat pokazuje kako se od postojećih podgrupa mogu formirati nove podgrupe.

Teorem 1.10. *Neka je G grupa i neka su H i N podgrupe od G . Definirajmo skup*

$$HN = \{ab \mid a \in H, b \in N\}.$$

- (i) *Ako je $N \triangleleft G$, onda je $HN = NH$ i HN je podgrupa od G .*
- (ii) *Ako su $H \triangleleft G$ i $N \triangleleft G$, onda je $HN \triangleleft G$.*

Dokaz (i) Pokažimo da je $HN = NH$. Ako je $y \in HN$, onda je $y = ab$ za neke $a \in H$ i $b \in N$ pa vrijedi $y = (aba^{-1})a \in NH$ jer je $aba^{-1} \in N$. Stoga je $HN \subseteq NH$. Slično se pokazuje da je $NH \subseteq HN$ pa zaključujemo da je $HN = NH$.

Pokažimo sada da je HN podgrupa od G . Neka su $x, y \in HN$. Tada su $x = a_1b_1$ i $y = a_2b_2$ za neke $a_1, a_2 \in H$ i $b_1, b_2 \in N$. Stoga je

$$xy^{-1} = a_1(b_1b_2^{-1})a_2^{-1} = a_1ha_2^{-1} \quad (1.36)$$

gdje je $h = b_1b_2^{-1} \in N$. Prema teoremu 1.7 (ii) vrijedi $Na_2^{-1} = a_2^{-1}N$ pa je $ha_2^{-1} = a_2^{-1}h'$ za neki $h' \in N$. Iz jednadžbe (1.36) sada dobivamo

$$xy^{-1} = a_1a_2^{-1}h' \in HN$$

jer je $a_1a_2^{-1} \in H$. Time je pokazano da je HN podgrupa od G .

(ii) Prema prvoj tvrdnji teorema, HN je podgrupa od G . Nadalje, za svaki $x \in G$ vrijedi $xHx^{-1} \subseteq H$ i $xNx^{-1} \subseteq N$ jer su $H \triangleleft G$ i $N \triangleleft G$ što povlači

$$\begin{aligned} xHNx^{-1} &= \{xabbx^{-1} \mid a \in H, b \in N\} \\ &= \{(xax^{-1})(xbx^{-1}) \mid a \in H, b \in N\} = (xHx^{-1})(xNx^{-1}) \subseteq HN. \end{aligned}$$

Dakle, HN je normalna podgrupa od G . ■

1.5 Teoremi o izomorfizmima

U ovom poglavlju ćemo dokazati neke važne rezultate o kvocijentnim grupama i homomorfizmima. Prvi rezultat poznat je kao Fundamentalni teorem o homomorfizmu koji ponekad omogućuje lakše prepoznavanje strukture kvocijentne grupe.

Teorem 1.11 (Prvi teorem o izomorfizmu). *Neka je $\phi: G \rightarrow H$ homomorfizam grupa. Tada je*

$$G/\ker(\phi) \simeq \text{Im}(\phi).$$

Posebno, ako je ϕ surjekcija, onda je

$$G/\ker(\phi) \simeq H.$$

Dokaz Neka je $K = \ker(\phi)$. Definirajmo preslikavanje $\psi: G/K \rightarrow H$ s $\psi(xK) = \phi(x)$. Pokažimo da je ψ dobro definirano. Ako je $xK = yK$, onda je $x^{-1}y \in K$ što povlači $\phi(x^{-1}y) = e$. Iz teorema 1.1 slijedi da je $\phi(x) = \phi(y)$ što pokazuje da ψ ne ovisi o predstavniku susjedne klase xK . Preslikavanje ψ je homomorfizam jer vrijedi

$$\psi((xK)(yK)) = \psi((xy)K) = \phi(xy) = \phi(x)\phi(y) = \psi(xK)\psi(yK).$$

Nadalje, ako je $\psi(xK) = \psi(yK)$, onda je $\phi(x) = \phi(y)$ što implicira $\phi(x^{-1}y) = e$, odnosno $x^{-1}y \in K$. Odavde slijedi da je $xK = yK$ pa je preslikavanje ψ injektivno. Kako je očigledno $\text{Im}(\psi) = \text{Im}(\phi)$, zaključujemo da je $\psi: G/K \rightarrow \text{Im}(\phi)$ izomorfizam. Ako je ϕ surjekcija, tj. ako je $\text{Im}(\phi) = H$, onda su grupe G/K i H izomorfne. ■

Korolar 1.1. Ako je $\phi: G \rightarrow H$ homomorfizam, onda sljedeći dijagram komutira

$$\begin{array}{ccc} G & \xrightarrow{\phi} & H \\ \pi \downarrow & \nearrow \psi & \\ G/\ker(\phi) & & \end{array} \quad (1.37)$$

gdje je π kanonska projekcija $\pi(x) = x\ker(\phi)$ i $\psi(x\ker(\phi)) = \phi(x)$.

Kada kažemo da dijagram (1.37) komutira, to znači da slika elementa $x \in G$ ne ovisi o tome koje strelice slijedimo u dijagramu jer je $\psi \circ \pi = \phi$. Ako je G konačna grupa, onda je prema Lagrangeovom teoremu $|G| = [G : \ker(\phi)] |\ker(\phi)|$. Međutim, $G/\ker(\phi) \simeq \text{Im}(\phi)$ implicira da je $[G : \ker(\phi)] = |\text{Im}(\phi)|$ pa dobivamo zanimljivu formulu za red grupe

$$|G| = |\ker(\phi)| |\text{Im}(\phi)|.$$

Neka je $\phi: G \rightarrow H$ homomorfizam i neka je N normalna podgrupa od G . Pretpostavimo da želimo definirati preslikavanje ψ na kvocijentnoj grupi s

$$\psi: G/N \rightarrow H, \quad \psi(xN) = \phi(x).$$

Tada treba provjeriti da ψ ne ovisi o predstavniku susjedne klase xN . Međutim, prema prvom teoremu o izomorfizmu ψ je dobro definiran na G/N ako i samo ako je $N \subseteq \ker(\phi)$, pa je dovoljno provjeriti da je $N \subseteq \ker(\phi)$.

U sljedećim primjerima ćemo pokazati kako se pomoću prvog teorema o izomorfizmu mogu opisati strukture nekih kvocijentnih grupa.

U ovim primjerima $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ i $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ označavaju grupe u odnosu na množenje.

Primjer 1.21. Pokažimo da je $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \simeq \mathbb{R}^*$. Preslikavanje $\varphi: GL(n, \mathbb{R}) \rightarrow \mathbb{R}^*$ definirano s $\varphi(A) = \det(A)$ je homomorfizam jer prema Binet-Cauchyevom teoremu vrijedi

$$\varphi(AB) = \det(AB) = \det(A)\det(B) = \varphi(A)\varphi(B).$$

Preslikavanje φ je surjekcija jer za svaki $x \in \mathbb{R}^*$ dijagonalna matrica

$$A = \begin{pmatrix} x & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \in GL(n, \mathbb{R})$$

ima determinantu $\det(A) = x$. Jezgra homomorfizma je dana sa

$$\ker(\varphi) = \{A \in GL(n, \mathbb{R}) \mid \det(A) = 1\} = SL(n, \mathbb{R}),$$

pa je prema teoremu 1.11

$$GL(n, \mathbb{R})/SL(n, \mathbb{R}) \simeq \mathbb{R}^*.$$

Dakle, kvocijentna grupa $GL(n, \mathbb{R})/SL(n, \mathbb{R})$ ima strukturu Abelove grupe $\mathbb{R}^*$. $\square$

Primjer 1.22. Neka je $\varphi: \mathbb{R}^* \rightarrow \mathbb{R}^*$ definirano s $\varphi(x) = |x|$. Preslikavanje φ je homomorfizam jer je $\varphi(xy) = |xy| = |x||y| = \varphi(x)\varphi(y)$. Jezgra homomorfizma je dana s

$$\ker(\varphi) = \{x \in \mathbb{R}^* \mid |x| = 1\} = \{-1, 1\},$$

Sliku homomorfizma $\text{Im}(\varphi)$ čine svi pozitivni realni brojevi $\mathbb{R}^+$, stoga iz teorema 1.11 slijedi

$$\mathbb{R}^*/\{-1, 1\} \simeq \mathbb{R}^+.$$

□

Primjer 1.23. Pokažimo da je $\mathbb{R}/\mathbb{Z} \simeq U(1)$ gdje je $U(1) = \{e^{i\theta} \mid \theta \in \mathbb{R}\}$ unitarna grupa. Neka je $\phi: \mathbb{R} \rightarrow U(1)$ preslikavanje s aditivne grupe $(\mathbb{R}, +)$ na grupu $U(1)$ definirano s $\phi(x) = e^{i2\pi x}$. Tada je

$$\phi(x+y) = e^{i2\pi(x+y)} = e^{i2\pi x} e^{i2\pi y} = \phi(x)\phi(y),$$

stoga je ϕ homomorfizam. Za svaki $e^{i\theta} \in U(1)$ postoji $x = \theta/(2\pi) \in \mathbb{R}$ takav da je $e^{i2\pi x} = e^{i\theta}$, stoga je ϕ surjekcija. Jezgru homomorfizma čine svi cijeli brojevi jer je

$$e^{i2\pi x} = 1 \quad \text{ako i samo ako je} \quad x \in \mathbb{Z}.$$

Dakle, $\text{Im}(\phi) = U(1)$ i $\ker(\phi) = \mathbb{Z}$, pa iz teorema 1.11 slijedi da je

$$\mathbb{R}/\mathbb{Z} \simeq U(1).$$

□

Primjer 1.24. Neka je $\text{Aut}(G)$ grupa svih automorfizama grupe G . Unutarnji automorfizmi $\text{Inn}(G) = \{I_g \mid g \in G\}$, gdje je $I_g(x) = gxg^{-1}$, tvore podgrupu od $\text{Aut}(G)$. Pokažimo da je $G/Z(G) \simeq \text{Inn}(G)$. Definirajmo $\varphi: G \rightarrow \text{Aut}(G)$ sa $\varphi(g) = I_g$. Za svaki $x \in G$ vrijedi

$$\varphi(gh)(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = I_g(I_h(x)) = \varphi(g) \circ \varphi(h)(x).$$

Dakle, φ je homomorfizam. Očigledno je $\text{Im}(\varphi) = \text{Inn}(G)$. Nadalje, jezgra homomorfizma je dana sa $\ker(\varphi) = \{g \in G \mid I_g = \text{id}_G\}$. Primijetimo da je $g \in \ker(\varphi)$ ako i samo ako je $gxg^{-1} = x$ za svaki $x \in G$ što povlači da je $\ker(\varphi) = Z(G)$. Prema prvom teoremu o izomorfizmu je $G/Z(G) \simeq \text{Inn}(G)$. □

Primjer 1.25. U kompleksnoj ravnini korijen $\sqrt[m]{1}$ ima m različitih vrijednosti danih sa $e^{i\frac{k2\pi}{m}}$, $k = 0, 1, 2, \dots, m-1$. Skup

$$H_m = \left\{ e^{i\frac{k2\pi}{m}} \mid k \in \mathbb{Z} \right\}$$

je grupa u odnosu na množenje čiji elementi su m -ti korijeni iz jedinice. Definirajmo $\varphi: \mathbb{Z} \rightarrow H_m$ sa $\varphi(k) = e^{i\frac{k2\pi}{m}}$. Lako se vidi da je $\varphi(k+l) = \varphi(k)\varphi(l)$ pa je φ epimorfizam na grupu H_m . Jezgra epimorfizma je $\ker(\varphi) = \{k \in \mathbb{Z} \mid e^{i\frac{k2\pi}{m}} = 1\}$. Očigledno je $e^{i\frac{k2\pi}{m}} = 1$ ako i samo ako je $k = mn$ za neki $n \in \mathbb{Z}$ što povlači da je $\ker(\varphi) = m\mathbb{Z}$. Sada prema teoremu 1.11 vrijedi $\mathbb{Z}/m\mathbb{Z} \simeq H_m$. □

Teorem 1.12 (Drugi teorem o izomorfizmu). *Neka je G grupa koja ima podgrupe H i N i neka je $N \triangleleft G$. Tada je*

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

Dokaz Prema teoremu 1.10(i) skup HN je podgrupa od G i vrijedi $N \triangleleft HN$ jer je $N \subseteq HN$. Stoga je kvocijentna grupa HN/N dobro definirana. Promotrimo preslikavanje

$$\varphi: H \rightarrow HN/N, \quad \varphi(h) = hN.$$

Primijetimo da je $hN = hgN$ za svaki $g \in N$ pa je $\varphi(h) \in HN/N$. Nadalje, φ je očigledno homomorfizam i $\text{Im}(\varphi) = HN/N$. Jezgra homomorfizma je dana s

$$\ker(\varphi) = \{h \in H \mid hN = N\} = \{h \in H \mid h \in N\} = H \cap N$$

jer je $hN = N$ ako i samo ako je $h \in N$. Iz prvog teorema o izomorfizmu slijedi $H/(H \cap N) \simeq HN/N$. ■

Sljedeći teorem o izomorfizmu poznat je i kao teorem o dvostrukom kvocijentu jer podsjeća na pravilo za računanje dvostrukih razlomaka.

Teorem 1.13 (Treći teorem o izomorfizmu). *Neka su H i K normalne podgrupe grupe G i neka je $K \subseteq H$. Tada je*

$$(G/K)/(H/K) \simeq G/H.$$

Dokaz Definirajmo preslikavanje $\varphi: G/K \rightarrow G/H$ s $\varphi(xK) = xH$. Pokažimo da je φ dobro definirano. Ako je $xK = yK$, onda je $x^{-1}y \in K$ što povlači $x^{-1}y \in H$ jer je $K \subseteq H$. Odavde slijedi $xH = yH$, dakle φ je dobro definirano. Nadalje, za svaki $x, y \in G$ vrijedi

$$\varphi((xK)(yK)) = \varphi(xyK) = xyH = (xH)(yH) = \varphi(xK)\varphi(yK),$$

što pokazuje da je φ homomorfizam. Preslikavanje φ je očigledno surjekcija jer je

$$\text{Im}(\varphi) = \{xH \mid xK \in G/K\} = \{xH \mid x \in G\} = G/H.$$

Jezgra homomorfizma je dana s

$$\ker(\varphi) = \{xK \mid xH = H\} = \{xK \mid x \in H\} = H/K,$$

pa iz prvog teorema o izomorfizmu slijedi

$$(G/K)/(H/K) \simeq G/H.$$

1.6 Cikličke grupe

Neka je G grupa i neka je $a \in G$. Prisjetimo se da potencije elementa $a \in G$ definiramo sa

$$a^0 = e, \quad a^k = \underbrace{a \cdot a \cdot \dots \cdot a}_{k \text{ puta}}, \quad a^{-k} = \underbrace{a^{-1} a^{-1} \cdot \dots \cdot a^{-1}}_{k \text{ puta}}, \quad k \in \mathbb{N}.$$

Lako se pokazuje da je

$$a^k (a^l)^{-1} = a^{k-l} \quad \text{za sve } k, l \in \mathbb{Z},$$

stoga je skup svih potencija $\{a^k \mid k \in \mathbb{Z}\}$ podgrupa od G što motivira sljedeću definiciju.

Definicija 1.16. Kažemo da je H ciklička grupa ako postoji $a \in H$ takav da je

$$H = \{a^k \mid k \in \mathbb{Z}\}.$$

Tada pišemo $H = \langle a \rangle$ i kažemo da je element a generator grupe H .

Ako je H aditivna grupa, onda pišemo

$$H = \{ka \mid k \in \mathbb{Z}\}.$$

Generator grupe općenito ne mora biti jedinstven. Na primjer, oba elementa a i a^{-1} su generatori grupe H . Također se može pokazati da u cikličkoj grupi prostog reda svaki njezin element različit od jedinice generira cijelu grupu (vidi propoziciju 1.6).

Primjer 1.26. Abelova grupa $(\mathbb{Z}, +)$ je ciklička grupa generirana elementom $1 \in \mathbb{Z}$ jer je $n = n \cdot 1$ za svaki $n \in \mathbb{Z}$. Primijetimo da -1 također generira $\mathbb{Z}$. Grupa $\mathbb{Z}$ je primjer cikličke grupe beskonačnog reda. $\square$

Primjer 1.27. Svaka podgrupa grupe $(\mathbb{Z}, +)$ je ciklička. Neka je H netrivialna podgrupa od $\mathbb{Z}$. Ako je $x \in H$, onda je $-x \in H$, stoga H sadrži pozitivne i negativne cijele brojeve. Neka je a najmanji prirodni broj u H . Tada je $\langle a \rangle = \{ka \mid k \in \mathbb{Z}\} \subseteq H$ jer je H zatvorena na zbrajanje i oduzimanje. Neka je $x \in H$. Tada postoje $q, r \in \mathbb{Z}$ takvi da je

$$x = qa + r, \quad 0 \leq r < a,$$

što povlači $r = x - qa \in H$ jer je H podgrupa. Odavde slijedi $r = 0$ jer je a najmanji prirodni broj u H . Dakle, $x = qa \in \langle a \rangle$, pa zaključujemo da je $H \subseteq \langle a \rangle$. Time je dokazano $H = \langle a \rangle$. $\square$

Primjer 1.28. Neka je $i = \sqrt{-1}$ imaginarna jedinica i neka je G multiplikativna grupa

$$G = \{1, -1, i, -i\}.$$

Tada je G ciklička grupa generirana elementom i jer je $i^{2n} = \pm 1$ i $i^{2n+1} = \pm i$ za svaki $n \in \mathbb{Z}$. Primijetimo da G također možemo generirati i elementom $-i$. G je ciklička grupa reda 4 čiji elementi leže na jediničnoj kružnici u Gaussovoj ravnini. $\square$

Definicija 1.17. Neka je G grupa i neka je $a \in G$. Ako postoji prirodni broj m takav da je $a^m = e$, onda najmanji takav m nazivamo red elementa a i označavamo s $|a|$. Ako takav broj ne postoji kažemo da je a beskonačnog reda i pišemo $|a| = \infty$.

Očigledno je $|a| = 1$ ako i samo ako je $a = e$.

Primjer 1.29. Promotrimo matrice $A, B \in GL(2, \mathbb{C})$,

$$A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad B = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}.$$

Očigledno je najmanja potencija $m \in \mathbb{N}$ za koju vrijedi $A^m = I$ jednaka $m = 4$, stoga je $|A| = 4$. S druge strane

$$B^m = \begin{pmatrix} \frac{1}{2^m} & 0 \\ 0 & \frac{1}{2^m} \end{pmatrix} \neq I \quad \text{za svaki } m \in \mathbb{N},$$

pa zaključujemo da je $|B| = \infty$. $\square$

Primjer 1.30. U multiplikativnoj grupi $G = \{1, -1, i, -i\}$ red elementa -1 jednak je 2, dok elementi i i $-i$ imaju red četiri. $\square$

Primjer 1.31. Element $e^{i\frac{2\pi}{n}} \in U(1)$, $n > 1$, ima red n . S druge strane, ako je α iracionalan broj, onda je red elementa $e^{i\alpha 2\pi}$ beskonačan. Doista, ako postoji $n \in \mathbb{N}$ takav da je $(e^{i\alpha 2\pi})^n = 1$, onda je $e^{i\alpha 2\pi}$ n -ti korijen iz jedinice, odnosno $e^{i\alpha 2\pi} = e^{i\frac{k2\pi}{n}}$ za $k = 0, 1, \dots, n-1$. Odavde slijedi $\alpha = \frac{k}{n} + m$, $m \in \mathbb{Z}$, što je u kontradikciji s pretpostavkom da je α iracionalan. $\square$

Propozicija 1.5. Neka je G grupa i neka je $a \in G$, $a \neq e$.

(i) Ako je $|a| = n$ za neki $n \in \mathbb{N}$, onda su elementi $e, a, a^2, \dots, a^{n-1}$ različiti pa vrijedi $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$.

(ii) Ako je $|a| = \infty$, onda je $a^k \neq a^l$ za sve $k, l \in \mathbb{Z}$, $k \neq l$.

Dokaz (i) Pretpostavimo da je $a^k = a^l$ za neke $0 \leq k, l \leq n-1$, $k > l$. Tada je $a^{k-l} = e$ što je u kontradikciji s pretpostavkom $|a| = n$ jer je $k-l < n$. Neka je sada $m \in \mathbb{Z}$. Prema teoremu o dijeljenju s ostatkom, postoje $q, r \in \mathbb{Z}$ takvi da je $m = qn + r$, $0 \leq r < n$. Odavde slijedi da je $a^m = (a^n)^q a^r = a^r$, stoga se svaka potencija a^m nalazi u skupu $\{e, a, a^2, \dots, a^{n-1}\}$. Zaključujemo da je $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$.

(ii) Ako je $a^k = a^l$ za neke $k, l \in \mathbb{Z}$, $k > l$, onda je $a^{k-l} = e$ što je u kontradikciji s pretpostavkom $|a| = \infty$. Dakle, sve potencije a^k , $k \in \mathbb{Z}$, su različite. $\blacksquare$

Iz propozicije 1.5 (i) slijedi da je red cikličke grupe $G = \langle a \rangle$ jednak redu generatora,

$$|G| = |a| \quad (1.38)$$

(ova jednakost vrijedi i za $|a| = \infty$ jer tada G ima beskonačno mnogo elemenata). Cikličke grupe konačnog reda n obično zapisujemo u obliku

$$G = \langle a \mid a^n = e \rangle \quad (1.39)$$

gdje izraz $a^n = e$ nazivamo relacija. Primjeri grupa definiranih generatorima i relacijama su diedralne grupe koje ćemo susresti u poglavlju 1.8.

Propozicija 1.6. *Neka je G konačna grupa reda $|G| \geq 2$ i neka je $a \in G$, $a \neq e$. Tada $|a|$ dijeli $|G|$. Nadalje, ako je $|G|$ prosti broj, onda je G ciklička grupa.*

Dokaz Prema propoziciji 1.5 (i) red cikličke podgrupe $\langle a \rangle$ jednak je $|\langle a \rangle| = |a|$, pa prema Lagrangeovom teoremu $|a|$ dijeli $|G|$. Ako je $|G| = p$ prosti broj, onda je $|a| = 1$ ili $|a| = p$. Kako $|a| = 1$ implicira $a = e$, zaključujemo da je $|a| = p$. Iz propozicije 1.5 (i) slijedi da niz $e, a, a^2, \dots, a^{p-1}$ ima p različitih elemenata grupe G , stoga se u njemu nalaze svi elementi od G . Dakle, G je ciklička grupa generirana elementom a . ■

Propozicija 1.6 implicira da ako je $|G| = p$ prosti broj, onda svaki element a^k , $1 \leq k \leq p-1$, generira cijelu grupu G . Stoga G ima $p-1$ različitih generatora $a, a^2, \dots, a^{p-1}$.

Teorem 1.14. *Neka je $G = \langle a \rangle$ ciklička grupa.*

- (i) *Ako je $|G| = \infty$, onda je G izomorfna grupi $(\mathbb{Z}, +)$.*
- (ii) *Ako je $|G| = n < \infty$, onda je G izomorfna grupi $(\mathbb{Z}_n, +)$.*

Dokaz (i) Preslikavanje $\varphi: \mathbb{Z} \rightarrow G$, $\varphi(k) = a^k$ je homomorfizam jer je

$$\varphi(k+l) = a^{k+l} = a^k a^l = \varphi(k)\varphi(l). \quad (1.40)$$

Ovo preslikavanje je surjekcija jer je G skup svih potencija a^k , $k \in \mathbb{Z}$. Također, φ je injekcija jer su prema propoziciji 1.5 (ii) sve potencije a^k , $k \in \mathbb{Z}$, različite. Dakle, $G \simeq \mathbb{Z}$.

(ii) Ako je $|G| = n$, onda prema relaciji (1.38) imamo $a^n = e$. Definirajmo $\varphi: \mathbb{Z}_n \rightarrow G$ s $\varphi(\bar{k}) = a^k$. Preslikavanje φ je dobro definirano jer ako je $\bar{k} = \bar{l}$, onda je $k = l + qn$ za neki $q \in \mathbb{Z}$ iz čega slijedi $a^k = a^l(a^n)^q = a^l$. Nadalje, φ je homomorfizam jer je

$$\varphi(\bar{k} + \bar{l}) = \varphi(\overline{k+l}) = a^{k+l} = a^k a^l = \varphi(\bar{k})\varphi(\bar{l}).$$

Preslikavanje φ je očigledno bijekcija jer se $\bar{0}, \bar{1}, \dots, \overline{n-1}$ preslikavaju u elemente $e, a, \dots, a^{n-1}$, redom. Dakle, $G \simeq \mathbb{Z}_n$. ■

Posljedica ovog teorema je da su dvije cikličke grupe istog reda izomorfne jer su obje izomorfne grupi $\mathbb{Z}$ ili $\mathbb{Z}_n$. Promotrimo sada podgrupe cikličkih grupa.

Teorem 1.15. *Neka je $G = \langle a \rangle$ ciklička grupa. Svaka podgrupa grupe G je ciklička.*

Dokaz Neka je H podgrupa od G . Tvrdnja trivijalno vrijedi za $H = \{e\}$, stoga pretpostavimo $H \neq \{e\}$. Tada postoji $k \in \mathbb{Z} \setminus \{0\}$ takav da je $a^k \in H$. Kako je $(a^k)^{-1} = a^{-k} \in H$ zaključujemo da postoji $k > 0$ takav da je $a^k \in H$. Neka je $d > 0$ najmanji prirodni broj za koji vrijedi $a^d \in H$. Tada je $\langle a^d \rangle \subseteq H$ jer je H podgrupa.

Odaberimo sada $x \in H$. Tada je $x = a^k$ za neki $k \in \mathbb{Z}$. Prema teoremu o dijeljenju s ostatkom postoje $q, r \in \mathbb{Z}$ takvi da je $k = qd + r$, $0 \leq r < d$. Odavde dobivamo

$$a^r = a^{k-qd} = a^k(a^d)^{-q} \in H \quad (1.41)$$

jer su $a^k, a^d \in H$. Relacija (1.41) implicira $r = 0$ jer je $d \in \mathbb{N}$ najmanja potencija sa svojstvom $a^d \in H$. Dakle, $k = qd$ iz čega slijedi $x = (a^d)^q \in \langle a^d \rangle$. Dakle, $H \subseteq \langle a^d \rangle$ što povlači $H = \langle a^d \rangle$. Time je dokazano da je H ciklička podgrupa. ■

Teorem 1.16. *Neka je G ciklička grupa reda n . Tada za svaki $m \in \mathbb{N}$ takav da $m \mid n$ postoji jedinstvena podgrupa od G reda m .*

Dokaz Neka je $G = \langle a \rangle$. Tada je $a^n = e$ jer je $|G| = n$. Pretpostavimo da $m \mid n$ i definirajmo $d = n/m$. Pokažimo da je red elementa a^d jednak m . Očigledno je $(a^d)^m = a^n = e$. Pretpostavimo da postoji $0 < m_1 < m$ takav da je $(a^d)^{m_1} = e$. Kako je $a^n = e$, ovo implicira $dm_1 = qn$ za neki $q \in \mathbb{N}$. Odavde slijedi $m_1 = qm \geq m$ što je u kontradikciji s $m_1 < m$. Dakle, m je najmanji prirodni broj takav da je $(a^d)^m = e$, odnosno $|a^d| = m$. Zaključujemo da je $\langle a^d \rangle$ ciklička podgrupa reda m .

Dokažimo sada jedinstvenost. Neka je H podgrupa od G reda m . Prema teoremu 1.15, $H = \langle a^k \rangle$ gdje je $k > 0$ najmanji prirodni broj takav da je $a^k \in H$. Kako je $|H| = |a^k| = m$, vrijedi $(a^k)^m = e = a^n$ što implicira $km = qn$ za neki $q \in \mathbb{N}$. Stoga je $k = qd$ za $d = n/m$. Odavde slijedi $a^k = (a^d)^q \in \langle a^d \rangle$ što pokazuje $H \subseteq \langle a^d \rangle$. S obzirom da podgrupe H i $\langle a^d \rangle$ imaju isti red m zaključujemo da je $H = \langle a^d \rangle$. ■

Ako je $G = \langle a \rangle$ ciklička grupa reda n , onda su sve njezine podgrupe oblika $\langle a^d \rangle$ gdje je $d = n/m$. U slučaju kada je n prosti broj, G ima samo trivijalne podgrupe.

Primjer 1.32. Primjenom teorema 1.16 lako možemo odrediti sve podgrupe grupe cikličke grupe $\mathbb{Z}_n$. Pri tome je potrebno odrediti sve prirodne brojeve m koji dijele n . Na primjer, $\mathbb{Z}_{12}$ ima netrivialne podgrupe reda $m = 2, 3, 4, 6$:

$$(a) \ H_1 = \langle \overline{6} \rangle = \{\overline{0}, \overline{6}\} \quad (m = 2),$$

- (b) $H_2 = \langle \bar{4} \rangle = \{\bar{0}, \bar{4}, \bar{8}\} \quad (m = 3),$
 (c) $H_3 = \langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\} \quad (m = 4),$
 (d) $H_4 = \langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\} \quad (m = 6).$

□

1.7 Grupe permutacija

U ovom poglavlju ćemo promotriti elementarna svojstva i pojmove vezane za grupu permutacija. Neka je X neprazan skup. Svako bijektivno preslikavanje $\sigma: X \rightarrow X$ nazivamo permutacija na skupu X . Skup svih bijekcija na X očigledno tvori grupu u odnosu na kompoziciju preslikavanja,

$$(f \circ g)(a) = f(g(a)), \quad a \in X, \quad (1.42)$$

a neutralni element u grupi je identiteta $id_X(a) = a$ za svaki $a \in X$. Ovo motivira sljedeću definiciju.

Definicija 1.18. *Neka je X neprazan skup. Grupa svih permutacija na skupu X naziva se simetrična grupa na X i označava sa S_X . Svaka podgrupa grupe S_X naziva se grupa permutacija na X .*

Ako je X konačan skup od n elemenata, onda S_X označavamo sa S_n i nazivamo simetrična grupa stupnja n . Na skupu X možemo uvesti uređaj i bez gubitka općenitosti elemente možemo označiti s $1, 2, \dots, n$. Tada se permutacija $\sigma \in S_n$ može zapisati u matričnom obliku

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix},$$

a neutralni element je matrica

$$e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Promotrimo za primjer grupu S_3 . Sve permutacije na skupu $X = \{1, 2, 3\}$ su dane sljedećim preslikavanjima:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad (1.43)$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \quad (1.44)$$

Umnožak permutacija računa se uobičajenim pravilom za kompoziciju preslikavanja. Na primjer,

$$\sigma_1 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e.$$

$\cdot$	σ_1	σ_2	σ_3	σ_4	σ_5
σ_1	σ_2	e	σ_5	σ_3	σ_4
σ_2	e	σ_1	σ_4	σ_5	σ_3
σ_3	σ_4	σ_5	e	σ_1	σ_2
σ_4	σ_5	σ_3	σ_2	e	σ_1
σ_5	σ_3	σ_4	σ_1	σ_2	e

Tablica 1.5. Tablica množenja u grupi S_3 .

Inverzni element se također lako nalazi iz matičnog zapisa,

$$\sigma_1^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_2.$$

Množenje u grupi S_3 prikazano je u tablici 1.5. Elementarnom kombinatorikom se pokazuje da na skupu od n elemenata imamo $n!$ permutacija, stoga je $|S_n| = n!$.

U simetričnoj grupi istaknuto mjesto zauzimaju permutacije koje neke elemente skupa X ciklički “rotiraju”. Takve permutacije nazivaju se cikličke permutacije.

Definicija 1.19. Neka je $\sigma \in S_n$. Ako postoje $x_1, x_2, \dots, x_r \in \{1, 2, \dots, n\}$ takvi da je

$$\begin{aligned} \sigma(x_i) &= x_{i+1}, & i &= 1, 2, \dots, r-1, \\ \sigma(x_r) &= x_1, \\ \sigma(x) &= x, & x &\notin \{x_1, x_2, \dots, x_r\}, \end{aligned}$$

onda permutaciju σ nazivamo ciklička permutacija duljine r i označavamo s $(x_1 x_2 \dots x_r)$. Cikličku permutaciju duljine dva nazivamo transpozicija.

Ciklička permutacija preslikava elemente $x_1, x_2, \dots, x_r$ prema pravilu

$$x_1 \mapsto x_2 \mapsto x_3 \mapsto \dots \mapsto x_r \mapsto x_1 \quad (1.45)$$

dok na ostalim elementima djeluje kao identiteta. Ciklička permutacija duljine jedan je identiteta koju zapisujemo (x) gdje je x bilo koji od brojeva $1, 2, \dots, n$. Na primjer, ciklička permutacija $(2\ 1\ 3)$ na skupu $X = \{1, 2, 3, 4\}$ je preslikavanje

$$2 \mapsto 1, \quad 1 \mapsto 3, \quad 3 \mapsto 2, \quad 4 \mapsto 4,$$

koju možemo zapisati kao

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

Ciklička permutacija $(x_1 x_2 \dots x_r)$ se može napisati na r različitih načina tako da svaki od elemenata $x_1, x_2, \dots, x_r$ bude na prvom mjestu. Za dvije cikličke permutacije $(x_1 x_2 \dots x_r)$

i $(y_1 y_2 \dots y_s)$ kažemo da su disjunktne ako nemaju zajedničkih elemenata, odnosno ako je $\{x_1, x_2, \dots, x_r\} \cap \{y_1, y_2, \dots, y_s\} = \emptyset$. Cikličke permutacije su osnovni blokovi na koje se može rastaviti proizvoljna permutacija.

Teorem 1.17. *Svaka permutacija $\sigma \in S_n$ je umnožak disjunktne cikličke permutacije. Ciklička faktorizacija je jedinstvena do na poredak cikličke permutacije i umetanje ili ispuštanje cikličke permutacije duljine jedan.*

Umjesto dokaza opišimo algoritam kojim se računa ciklička faktorizacija.

Algoritam za cikličku faktorizaciju

- (1) Prvu cikličku permutaciju započnite s $a_1 = 1$. Svaku sljedeću cikličku permutaciju započnite s najmanjim elementom $a_1 \in \{1, 2, \dots, n\}$ koji se ne nalazi u prethodnim cikličkim permutacijama.
- (2) Odredite $a_2 = \sigma(a_1)$. Ako je $a_2 = a_1$, onda ciklička permutacija ima duljinu jedan i pišemo (a_1) . Ako je $a_2 \neq a_1$, onda pišemo $(a_1 a_2)$ (bez desne zagrade!).
- (3) Odredite $a_3 = \sigma(a_2)$. Ako je $a_3 = a_1$, onda je ciklička permutacija dana s $(a_1 a_2)$. Ako je $a_3 \neq a_1$, onda pišemo $(a_1 a_2 a_3)$. Ponavljajte ovaj postupak dok se ciklička permutacija ne zatvori. Nakon toga vratite se na početak algoritma. Ponovite korake (1)–(3) dok se ne iscrpe svi brojevi u skupu $\{1, 2, \dots, n\}$.

Ilustrirajmo ovaj algoritam na primjeru permutacije $\sigma \in S_{13}$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 3 & 1 & 11 & 9 & 5 & 10 & 6 & 4 & 7 & 8 & 2 \end{pmatrix}.$$

Počevši algoritam s $a_1 = 1$ dobivamo

$$\sigma = (1 \ 12 \ 8 \ 10 \ 4)(2 \ 13)(3)(5 \ 11 \ 7)(6 \ 9).$$

Primijetimo da se ciklička permutacija (3) može ispustiti jer je svaka ciklička permutacija duljine jedan identiteta. Dakle,

$$\sigma = (1 \ 12 \ 8 \ 10 \ 4)(2 \ 13)(5 \ 11 \ 7)(6 \ 9). \quad (1.46)$$

Kako su cikličke permutacije u (1.46) disjunktne, možemo ih napisati u bilo kojem poretku.

Primijetimo da se svaka ciklička permutacija $(a_1 \ a_2 \ \dots \ a_m)$ može napisati kao umnožak transpozicija

$$(a_1 \ a_2 \ \dots \ a_m) = (a_1 \ a_m)(a_1 \ a_{m-1}) \dots (a_1 \ a_2).$$

Korolar 1.2. *Svaka permutacija se može napisati kao umnožak transpozicija.*

Ova faktORIZACIJA nije jedinstvena jer se permutacija σ može napisati kao umnožak različitog broja transpozicija. Međutim, može se pokazati da je njezina parnost jedinstvena. Drugim riječima, ako se σ može napisati kao umnožak n ili m transpozicija, onda su n i m ili oba parni ili oba neparni brojevi. Sljedeći primjer ilustrira ovo svojstvo. Množenjem transpozicija na desnoj strani jednakosti lako se provjeri da vrijedi

$$\begin{aligned}\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} &= (45)(35)(25)(15) \\ &= (53)(21)(35)(45)(23)(35).\end{aligned}$$

Dakle, permutacija σ je umnožak četiri ili šest transpozicija. U bilo kojem drugom rastavu σ se može napisati isključivo kao umnožak parnog broja transpozicija. Ovo motivira sljedeću definiciju.

Definicija 1.20. Kažemo da je permutacija $\sigma \in S_n$ parna (neparna) ako se može napisati kao umnožak parnog (neparnog) broja transpozicija. Predznak permutacije σ je definiran sa

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

Skup svih parnih permutacija u S_n , $n > 1$, nazivamo alternirajuća grupa A_n .

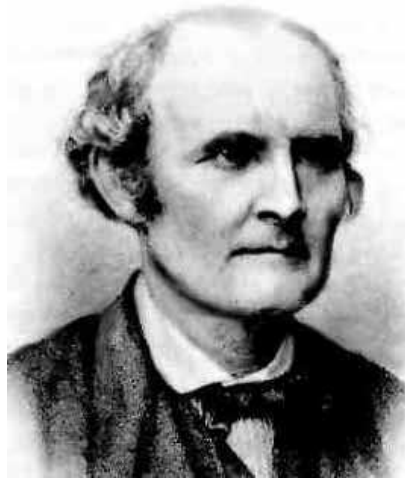
Lema 1.1. Neka je $n \geq 2$. Preslikavanje $\epsilon: S_n \rightarrow G$, gdje je $G = \{1, -1\}$ multiplikativna grupa, je epimorfizam.

Dokaz Neka su $\sigma_1, \sigma_2 \in S_n$. Ako su σ_1 i σ_2 obje parne ili obje neparne permutacije, onda je $\sigma_1\sigma_2$ parna permutacija. Ako je σ_1 neparna i σ_2 parna permutacija, onda je $\sigma_1\sigma_2$ neparna permutacija. Ovo implicira da u svakom slučaju vrijedi $\epsilon(\sigma_1\sigma_2) = \epsilon(\sigma_1)\epsilon(\sigma_2)$. Budući da S_n sadrži transpoziciju $\tau = (12)$, neutralni element $e \in S_n$ možemo rastaviti kao $e = (12)(21)$, pa je $\epsilon(e) = 1$. Nadalje, $\epsilon(\tau) = -1$, stoga je ϵ surjekcija. Dakle, $\epsilon: S_n \rightarrow G$ je epimorfizam. ■

Teorem 1.18. A_n je normalna podgrupa simetrične grupe S_n . Ako je $n \geq 2$, onda je red podgrupe A_n jednak $|A_n| = \frac{1}{2}n!$.

Dokaz Ako je $n = 1$, onda je $A_1 = S_1 = \{e\}$, stoga je A_1 trivijalno normalna podgrupa od S_1 . Neka je $n \geq 2$ i neka je $G = \{1, -1\}$ multiplikativna grupa iz leme 1.1. Prema lemi 1.1 preslikavanje $\epsilon: S_n \rightarrow G$ je epimorfizam, pa je prema prvom teoremu o izomorfizmu

$$S_n / \ker(\epsilon) \simeq G. \quad (1.47)$$



Slika 1.3. Arthur Cayley, 1821-1895. Najvažniji Cayleyev doprinos u razvoju algebre je rad na algebri matrica.

Jezgru homomorfizma tvore upravo parne permutacije jer je

$$\ker(\epsilon) = \{\sigma \in S_n \mid \epsilon(\sigma) = 1\} = A_n.$$

Stoga je A_n normalna podgrupa od S_n . Nadalje, iz relacije (1.47) slijedi $|S_n/A_n| = |G| = 2$, što povlači da je $[S_n : A_n] = 2$. Iz Lagrangeovog teorema dobivamo $|S_n| = [S_n : A_n] |A_n|$ što implicira

$$|A_n| = \frac{1}{[S_n : A_n]} |S_n| = \frac{1}{2} n!.$$

■

Promotrimo ponovo simetričnu grupu S_3 čiji elementi su dani permutacijama (1.43) i (1.44). Uvedimo oznake $\sigma = (1\ 2\ 3)$ i $\tau = (2\ 3)$. Lako se provjeri da je

$$\sigma^2 = \sigma_2, \sigma^3 = e, \tau^2 = e, \sigma^2\tau = \tau\sigma = \sigma_4, \sigma\tau = \sigma_5.$$

Dakle, svi elementi grupe S_3 se mogu zapisati kao

$$S_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}.$$

Umnožak bilo koja dva elementa u S_3 se može odrediti koristeći relacije

$$\sigma^3 = \tau^2 = e, \quad \sigma^2\tau = \tau\sigma. \quad (1.48)$$

Ove relacije potpuno određuju Cayleyevu tablicu grupe S_3 . Kažemo da su elementi σ i τ *generatori* grupe S_3 koji zadovoljavaju *definirajuće relacije* (1.48). Grupnu S_3 možemo zapisati koristeći generatore i relacije u obliku

$$S_3 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = e, \sigma^2\tau = \tau\sigma \rangle.$$

Važnost grupa permutacija se vidi iz sljedećeg teorema.

Teorem 1.19 (Cayleyev teorem). *Svaka grupa je izomorfna nekoj grupi permutacija.*

Dokaz Neka je G grupa. Svakom elementu $a \in G$ želimo pridružiti permutaciju na skupu G . Za odabrani $a \in G$ definirajmo

$$f_a: G \rightarrow G, \quad f_a(x) = ax.$$

Preslikavanje f_a je očigledno bijekcija jer $ax = ay$ implicira $x = y$, dok za proizvoljni $y \in G$ vrijedi $f_a(a^{-1}y) = y$. Dakle, $f_a \in S_G$. Promotrimo sada preslikavanje

$$\phi: G \rightarrow S_G, \quad \phi(a) = f_a,$$

koje elementu $a \in G$ pridružuje permutaciju $f_a \in S_G$. Za svaki $x \in G$ vrijedi

$$f_{ab}(x) = a(bx) = f_a(f_b(x)) = (f_a \circ f_b)(x). \quad (1.49)$$

Jednadžba (1.49) povlači $f_{ab} = f_a \circ f_b$, odnosno $\phi(ab) = \phi(a) \circ \phi(b)$. Dakle, ϕ je homomorfizam. Nadalje, ako je $\phi(a) = \phi(b)$, onda je $ax = bx$ za svaki $x \in G$. Za $x = e$ dobivamo $a = b$ što pokazuje da je ϕ injekcija. Iz navedenog zaključujemo da je $\phi: G \rightarrow \text{Im}(\phi)$ izomorfizam s G na grupu permutacija $\text{Im}(\phi) \subseteq S_G$. ■

Homomorfizam ϕ u Cayleyevom teoremu se naziva *lijeva regularna reprezentacija* ili *permutacijska reprezentacija* grupe G . Povijesno gledano, konačne grupe su se prvo proučavale kao podgrupe neke simetrične grupe S_n , a tek kasnije uveden je aksiomatski pristup u teoriji grupa. Prednost aksiomatskog pristupa je u tome što se mnogi rezultati mogu elegantno iskazati bez referiranja na konkretnu simetričnu grupu.

Primjer 1.33. Odredimo permutacijsku reprezentaciju cikličke grupe reda četiri $G = \{e, a, a^2, a^3\}$. Svaki element a^k definira permutaciju $f_{a^k}: G \rightarrow G$ na skupu G danu sa $f_{a^k}(a^l) = a^{k+l}$. Označimo elemente od G sa $e \mapsto 1, a \mapsto 2, a^2 \mapsto 3, a^3 \mapsto 4$ i odredimo slike elemenata $1, 2, 3, 4$ za svaki f_{a^k} . Na primjer, $f_{a^3}(a^2) = a^5 = a$ povlači da f_{a^3} preslikava 3 u 2 . Direktnim računom se lako pokaže da preslikavanja f_{a^k} daju sljedeće permutacije:

$$f_e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1), \quad (1.50)$$

$$f_a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1\ 2\ 3\ 4), \quad (1.51)$$

$$f_{a^2} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\ 3)(2\ 4), \quad (1.52)$$

$$f_{a^3} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1\ 4\ 3\ 2). \quad (1.53)$$

□

1.8 Diedralne grupe

Teorija grupa ima važnu ulogu u proučavanju simetrija, posebno u prirodnim znanostima. Intuitivno, kažemo da neki objekt posjeduje simetriju ako je invarijantan u odnosu na određene transformacije. Na primjer, sfera u $\mathbb{R}^3$ je invarijantna u odnosu na svaku rotaciju oko osi koja prolazi središtem sfere, pa kažemo da sfera ima rotacijsku simetriju. U ovom poglavlju definirat ćemo simetrije geometrijskih objekata i pobliže opisati simetrije pravilnih poligona. Neka je X podskup prostora $\mathbb{R}^n$ na kojem je definirana Euklidska udaljenost

$$d(x, y) = \left(\sum_{i=1}^n (x_i - y_i)^2 \right)^{\frac{1}{2}}, \quad x, y \in \mathbb{R}^n.$$

Definicija 1.21. *Permutacija $\sigma \in S_X$ naziva se simetrija na skupu $X \subseteq \mathbb{R}^n$ ako je*

$$d(\sigma(x), \sigma(y)) = d(x, y) \quad \text{za sve } x, y \in X.$$

Drugim riječima, simetrija na skupu X je svaka bijekcija $\sigma: X \rightarrow X$ koja čuva udaljenost između svake dvije točke u X . Primijetimo da u gornjoj definiciji X može biti konačan ili beskonačan skup.

Označimo sa T_X skup svih simetrija na skupu X . Pokažimo da je T_X podgrupa simetrične grupe S_X . Ako su $\sigma, \tau \in T_X$, onda je

$$\begin{aligned} d(\tau\sigma^{-1}(x), \tau\sigma^{-1}(y)) &= d(\sigma^{-1}(x), \sigma^{-1}(y)) \\ &= d(\sigma\sigma^{-1}(x), \sigma\sigma^{-1}(y)) = d(x, y) \quad \forall x, y \in X, \end{aligned}$$

što pokazuje da je $\tau\sigma^{-1} \in T_X$. Dakle, $T_X \leq S_X$.

Definicija 1.22. *Grupu T_X nazivamo grupa simetrija na skupu X .*

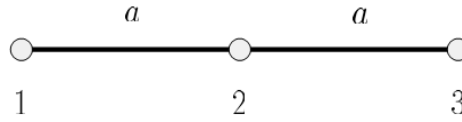
Primjer 1.34. Neka je $S^1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ jedinična kružnica sa središtem u ishodištu i neka je R_θ operator rotacije za kut θ u pozitivnom smjeru. Preslikavanje $R_\theta: S^1 \rightarrow S^1$ je očigledno bijekcija i za svake dvije točke $T_1, T_2 \in S^1$ vrijedi

$$d(R_\theta T_1, R_\theta T_2) = d(T_1, T_2) \tag{1.54}$$

pa je R_θ simetrija na skupu S^1 za svaki $\theta \in \mathbb{R}$. Prema jednadžbi (1.9), operatori rotacije se mogu prikazati kao matrice

$$R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}, \quad \theta \in \mathbb{R},$$

koje tvore specijalnu ortogonalnu grupu $SO(2)$. Stoga je $SO(2)$ podgrupa grupe simetrija jedinične kružnice S^1 . Punu grupu simetrija čine $SO(2)$ i sve osne simetrije s obzirom na pravce kroz ishodište. $\square$

Slika 1.4. Skup točaka X .

Primjer 1.35. Neka je X skup točaka na pravcu u oznakama 1, 2, 3 koje su poredane kao na slici 1.4. Za udaljenosti točaka skupa X vrijedi

$$d(1, 2) = d(2, 3) = a, \quad d(1, 3) = 2a.$$

Simetrije skupa X tvore podgrupu simetrične grupe S_3 definirane permutacijama (1.43) i (1.44). Promotrimo djelovanje permutacija na točke iz skupa X . Permutacije $\sigma_1, \sigma_2, \sigma_3$ i σ_5 nisu simetrije jer

$$\begin{aligned} d(\sigma_1(2), \sigma_1(3)) &= d(3, 1) \neq d(2, 3), \\ d(\sigma_2(1), \sigma_2(2)) &= d(3, 1) \neq d(1, 2), \\ d(\sigma_3(1), \sigma_3(2)) &= d(1, 3) \neq d(1, 2), \\ d(\sigma_5(2), \sigma_5(3)) &= d(1, 3) \neq d(2, 3). \end{aligned}$$

Međutim, za permutaciju σ_4 vrijedi

$$\begin{aligned} d(\sigma_4(1), \sigma_4(2)) &= d(3, 2) = d(1, 2), \\ d(\sigma_4(2), \sigma_4(3)) &= d(2, 1) = d(2, 3), \\ d(\sigma_4(1), \sigma_4(3)) &= d(3, 1) = d(1, 3), \end{aligned}$$

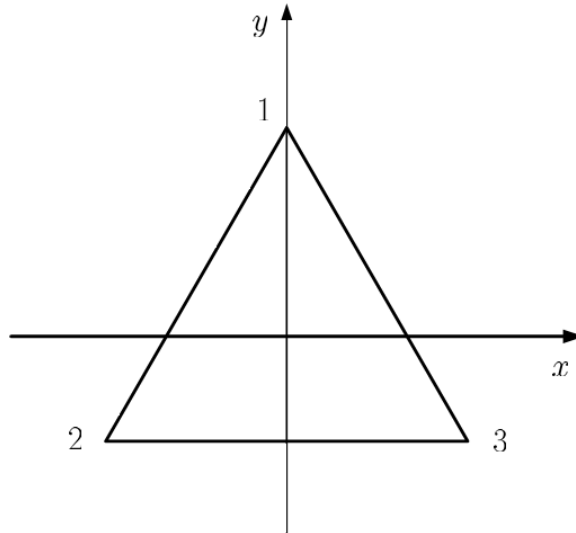
pa zaključujemo da je σ_4 simetrija skupa X . Dakle, grupa simetrija skupa X ima dva elementa, $T_X = \{e, \sigma_4\}$. $\square$

Važna grupa simetrija su simetrije pravilnog poligona P_n , $n \geq 3$, koje permutiraju vrhove tog poligona. Pretpostavimo da se središte poligona nalazi u ishodištu koordinatnog sustava. Vrhove poligona označimo s $1, 2, \dots, n$ u smjeru suprotno od kazaljke na satu. Slika 3 prikazuje tako označeni trokut P_3 . Simetrija poligona P_n čuva udaljenost između svakog para vrhova poligona.

Definicija 1.23. Grupa simetrija pravilnog poligona P_n naziva se diedralna grupa D_n .

Promotrimo поближе elemente grupe D_n . Permutacija σ je simetrija poligona P_n ako i samo ako σ preslikava dva susjedna vrha u dva susjedna vrha. Rotacija R za kut $2\pi/n$ (koju dogovorno uzimamo u smjeru suprotno od kazaljke na satu) očigledno pripada grupi D_n . Rotacija R preslikava vrh k u vrh $k + 1$, stoga je R ciklička permutacija

$$R = (1 \ 2 \ 3 \ \dots \ n). \quad (1.55)$$

Slika 1.5. Trokut P_3 .

Kompozicija od n rotacija preslikava svaki vrh u samoga sebe što znači da je $R^n = \mathbf{1}$ gdje $\mathbf{1}$ označava jedinicu u S_n . Osim rotacija, u grupi D_n imamo i refleksiju D obzirom na pravac koji prolazi vrhom 1 i središtem poligona P_n (umjesto vrha 1 možemo odabrati bilo koji drugi fiksni vrh). Refleksija D je permutacija dana s

$$D = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & n & n-1 & \dots & 2 \end{pmatrix}. \quad (1.56)$$

Primijetimo da je $D^2 = \mathbf{1}$. Pokažimo da grupa D_n ima $2n$ elemenata. Simetrija poligona je potpuno određena preslikavanjem dva susjedna vrha, na primjer vrhova 1 i 2. Pretpostavimo da simetrija $\sigma \in D_n$ preslikava vrh 1 u vrh k , tj. pretpostavimo da je $\sigma(1) = k$. Kako je vrh 2 susjedan vrhu 1, $\sigma(2)$ može biti samo $k-1$ ili $k+1$ (gdje je $n+1 \equiv 1$ i $1-1 \equiv n$). Za vrh 1 imamo n mogućnosti, a za vrh 2 dvije mogućnosti što ukupno daje $2n$ različitih slika uređenog para $(1,2)$. Odavde slijedi da grupa D_n ima $2n$ različitih elemenata. Obzirom da u skupu $\mathbf{1}, R, R^2, \dots, R^{n-1}, D, DR, DR^2, \dots, DR^{n-1}$ imamo $2n$ različitih elemenata grupe D_n zaključujemo da je

$$D_n = \{\mathbf{1}, R, R^2, \dots, R^{n-1}, D, DR, DR^2, \dots, DR^{n-1}\}$$

Na primjer, sve simetrije trokuta na slici 1.5 su dane elementima $D^i R^j$ za $i = 0, 1$ i $j = 0, 1, 2$. Promatranjem kako rotacija i refleksija djeluju na vrhove poligona $\{1, 2, \dots, n\}$ lako se vidi da je $RD = DR^{-1}$. Odavde indukcijom dobivamo da je $R^k D = DR^{-k}$ za sve $0 \leq k \leq n$. Stoga množenje u grupi D_n zadovoljava relacije

$$R^n = D^2 = \mathbf{1}, \quad R^k D = DR^{-k}, \quad 0 \leq k \leq n. \quad (1.57)$$

Umnožak bilo koja dva elementa grupe D_n se može svesti na oblik $D^i R^j$ za neki $i = 0, 1$ i $j = 0, 1, \dots, n-1$ korištenjem relacija (1.57). Na primjer, ako je $n = 12$, onda je

$$(DR^9)(DR^6) = D(R^9 D)R^6 = D(DR^{-9})R^6 = D^2 R^{-3} = R^{-3} = R^9.$$

$\cdot$	a	b	c
a	e	c	b
b	c	e	a
c	b	a	e

Tablica 1.6. Tablica množenja u Kleinovoj 4-grupi.

Diedralna grupa D_n generirana je elementima R i D i relacijama (1.57). Grupu D_n simbolički zapisujemo u obliku

$$D_n = \langle R, D \mid R^n = D^2 = 1, RD = DR^{-1} \rangle.$$

Generatori diedralne grupe se mogu osim permutacijama (1.55) i (1.56) prikazati i matricama reda 2,

$$R = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}, \quad D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Lako se provjeri da matrice R i D zadovoljavaju relacije (1.57). Matricu R interpretiramo kao rotaciju u ravnini (x, y) za kut $2\pi/n$ u pozitivnom smjeru, a D predstavlja transformaciju $(x, y) \mapsto (y, x)$ odnosno refleksiju obzirom na pravac $y = x$. Na primjeru diedralne grupe vidimo da se ista algebarska struktura može realizirati na više načina koristeći elemente različitih skupova.

Kleinova 4-grupa

Navedimo još jedan primjer grupe definirane generatorima i relacijama. Promotrimo matrice

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad b = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad c = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (1.58)$$

Lako se provjeri da a, b, c i e zadovoljavaju relacije

$$a^2 = b^2 = c^2 = e, \quad ab = c, \quad bc = a, \quad ca = b.$$

Grupa generirana elementima a, b i c se naziva Kleinova 4-grupa K_4 . Tablica množenja u K_4 dobiva se iz relacija (1.59). Na primjer,

$$ac = a(ab) = a^2b = b.$$

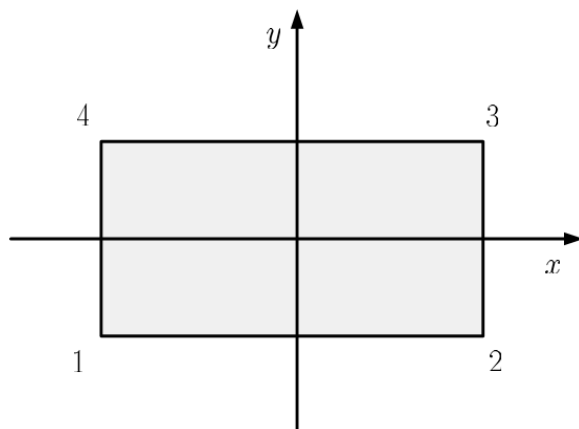
Kleinovu 4-grupu možemo zapisati kao

$$K_4 = \langle a, b, c \mid a^2 = b^2 = c^2 = e, ab = c, bc = a, ca = b \rangle. \quad (1.59)$$

Kleinova 4-grupa je grupa simetrija pravokutnika prikazanog na slici 1.6. Simetrije su dane permutacijama

$$E = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad (1.60)$$

$$B = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}. \quad (1.61)$$



Slika 1.6. Pravokutnik.

Geometrijski promatrano, A je rotacija za kut π , dok su B i C refleksije u odnosu na osi x i y . Primijetimo da rotacija za kut $\pi/2$ nije simetrija jer pravokutnik nije pravilan. Permutacije E , A , B i C zadovoljavaju iste relacije kao matrice e , a , b i c , stoga je K_4 izomorfna grupi simetrija (1.60)-(1.61). U ovom primjeru algebarska struktura (1.59) ima dvije različite realizacije, jednu pomoću matrica (1.58) i drugu pomoću permutacija (1.60)-(1.61).

1.9 Djelovanje grupe

U ovom poglavlju ćemo promatrati djelovanje grupa na skupove. Proučavanjem djelovanja neke grupe na samu sebe možemo doznati više o algebarskoj strukturi grupe koju promatramo. Ideja djelovanja grupe se javlja i kod proučavanja drugih algebarskih struktura kao što su moduli, vektorski prostori i polja.

Definicija 1.24. Kažemo da grupa G djeluje na skup A ako postoji preslikavanje $G \times A \rightarrow A$, $(g, a) \mapsto g \cdot a$, koje zadovoljava sljedeća svojstva:

$$(1) \quad g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a \text{ za sve } g_1, g_2 \in G, a \in A,$$

$$(2) \quad e \cdot a = a \text{ za svaki } a \in A,$$

gdje je e jedinica u G .

Naglasimo da $g \cdot a$ nije binarna operacija jer su skupovi G i A općenito različiti. Uvjeti (1) i (2) impliciraju da je djelovanje grupe kompatibilno sa strukturom grupe.

Djelovanje grupe na skup A inducira permutacije na skupu A . Svakom elementu $g \in G$ možemo pridružiti preslikavanje

$$\sigma_g: A \rightarrow A, \quad \sigma_g(a) = g \cdot a.$$

Pokažimo da je σ_g bijekcija na A . Doista, σ_g ima inverz na skupu A jer je

$$\sigma_g \sigma_{g^{-1}}(a) = g \cdot (g^{-1} \cdot a) = (gg^{-1}) \cdot a = e \cdot a = a,$$

a slično se pokazuje $\sigma_{g^{-1}} \sigma_g(a) = a$. Dakle, σ_g je permutacija na skupu A , tj. $\sigma_g \in S_A$.

Teorem 1.20. *Neka grupa G djeluje na skup A .*

(i) *Preslikavanje $\varphi: G \rightarrow S_A$ dano s $\varphi(g) = \sigma_g$ je homomorfizam.*

(ii) *Svaki homomorfizam $\varphi: G \rightarrow S_A$ inducira djelovanje grupe G na skup A .*

Dokaz (i) Neka su $g, h \in G$. Tada je

$$\varphi(gh)(a) = \sigma_{gh}(a) = (gh) \cdot a = g \cdot (h \cdot a) = \sigma_g(\sigma_h(a)) = \sigma_g \sigma_h(a) = \varphi(g)\varphi(h)(a)$$

za svaki $a \in A$. Dakle, $\varphi(gh) = \varphi(g)\varphi(h)$.

(ii) Neka je $\varphi: G \rightarrow S_A$ homomorfizam. Tada je $\varphi(g): A \rightarrow A$ bijekcija za svaki $g \in G$. Definirajmo

$$g \cdot a = \varphi(g)(a), \quad a \in A. \quad (1.62)$$

Sada imamo

$$(gh) \cdot a = \varphi(gh)(a) = \varphi(g)\varphi(h)(a) = \varphi(g)(\varphi(h)(a)) = g \cdot (h \cdot a), \quad (1.63)$$

$$e \cdot a = \varphi(e)(a) = a, \quad (1.64)$$

jer je $\varphi(e) = id_A$ identiteta u S_A prema teoremu 1.1. Dakle, preslikavanje (1.62) definira djelovanje grupe G na skup A . ■

Ovaj teorem pokazuje da su djelovanje grupe G na skup A i homomorfizmi $\varphi: G \rightarrow S_A$ u bijektivnoj korespondenciji, stoga predstavljaju isti pojam u različitim terminima. Svaki homomorfizam $\varphi: G \rightarrow S_A$ nazivamo *permutacijska reprezentacija* grupe G u simetričnu grupu S_A . Ako skup A ima n elemenata, onda je $S_A = S_n$ simetrična grupa stupnja n . Permutacijska reprezentacija od G je analogna matricnoj reprezentaciji linearnog operatora na vektorskom prostoru. Odabir uređenja na skupu A odgovara odabiru baze u odnosu na koju definiramo matricu operatora.

Primjer 1.36. Specijalna ortogonalna grupa $SO(2)$ djeluje na Euklidski prostor $\mathbb{R}^2$ matičnim množenjem:

$$R_\theta \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \cos \theta - y \sin \theta \\ x \sin \theta + y \cos \theta \end{pmatrix}, \quad R_\theta \in SO(2).$$

Matrica R_θ je operator rotacije koja točku (x, y) zakreće za kut θ u pozitivnom smjeru. Djelovanje grupe $SO(2)$ je izometrija Euklidskog prostora jer je

$$\|R_\theta \cdot P\| = \|P\| \quad (1.65)$$

za svaku točku $P = \begin{pmatrix} x \\ y \end{pmatrix}$ gdje je $\|P\| = \sqrt{x^2 + y^2}$ udaljenost točke od ishodišta. Primijetimo da $SO(2)$ preslikava kružnicu sa središtem u ishodištu na samu sebe, dakle $SO(2)$ djeluje na svaku kružnicu $K = \{x^2 + y^2 = R^2\}$, $R > 0$. S druge strane, $SO(2)$ ne djeluje na pravac $y = x$ jer element R_θ zakreće pravac za kut θ te se pravac preslikava na samoga sebe samo ako je $\theta = k\pi$, $k \in \mathbb{Z}$. $\square$

Primjer 1.37. Neka je $G = D_4$ i neka je $A = \{x_1, x_2, x_3, x_4\}$ skup vrhova pravilnog četverokuta. Diedralna grupa D_4 djeluje na A sa

$$\sigma \cdot x_i = x_{\sigma(i)}, \quad \sigma \in D_4, \quad 1 \leq i \leq 4, \quad (1.66)$$

gdje je σ permutacijska realizacija elemenata grupe D_4 dana sa (1.55) i (1.56). $\square$

Primjer 1.38. Grupa G djeluje na samu sebe lijevom translacijom $g \cdot a = ga$ i desnom translacijom $g \cdot a = ag^{-1}$. Nadalje, grupa djeluje na samu sebe konjugacijom

$$g \cdot a = gag^{-1}.$$

Lako se pokazuje da ove operacije definiraju djelovanje. Na primjer, za konjugaciju vrijedi

$$\begin{aligned} (gh) \cdot a &= (gh)a(gh)^{-1} = g(hah^{-1})g^{-1} = g \cdot (h \cdot a), \\ e \cdot a &= eae^{-1} = a. \end{aligned}$$

$\square$

Primjer 1.39. Neka je N normalna podgrupa od G . Grupa G djeluje na kvocijentnu grupu G/N pravilom

$$g \cdot (aN) = gag^{-1}N.$$

Doista, ako su $g, h \in G$ i $aN \in G/N$, onda imamo

$$\begin{aligned} (gh) \cdot aN &= (gh)a(gh)^{-1}N = g(hah^{-1})g^{-1}N = g \cdot (hah^{-1}N) = g \cdot (h \cdot (aN)), \\ e \cdot (aN) &= eae^{-1}N = aN. \end{aligned}$$

$\square$

Definicija 1.25. Neka G djeluje na skup A , i neka je $a \in A$. Skup

$$G_a = \{g \in G \mid g \cdot a = a\}$$

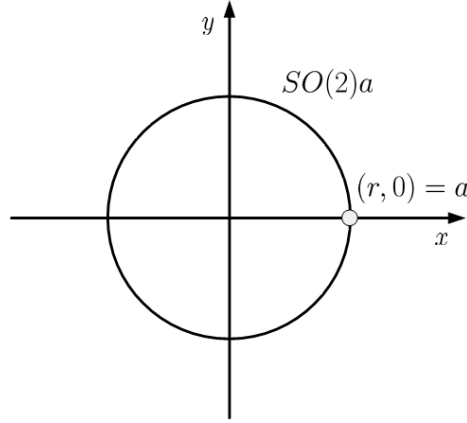
nazivamo stabilizator elementa a u G . Skup

$$Ga = \{g \cdot a \mid g \in G\}$$

nazivamo orbita elementa a u G .

Lako se pokazuje da je G_a podgrupa od G . Ako G djeluje na sebe konjugacijom, $g \cdot a = gag^{-1}$, onda je stabilizator elementa $a \in G$ jednak normalizatoru od a u G ,

$$G_a = \{g \in G \mid gag^{-1} = a\} = N(a),$$



Slika 1.7. Orbita točke $(r, 0)$ pod djelovanjem grupe $SO(2)$.

a orbita elementa a je klasa konjugacije

$$Ga = \{gag^{-1} \mid g \in G\} = C(a).$$

Očigledno je $a \in Ga$ jer je $e \cdot a = a$. Na primjer, ako grupa $SO(2)$ djeluje na ravninu $\mathbb{R}^2$ kao u primjeru (1), onda je orbita točke $(r, 0) \in \mathbb{R}^2$ kružnica radijusa $|r| > 0$ sa središtem u ishodištu (vidi sliku 1.7). Djelovanje ove grupe slikovito ilustrira naziv “orbita”. Primijetimo da je

$$N(a) = G \quad \text{i} \quad C(a) = \{a\} \quad \text{ako i samo ako je} \quad a \in Z(G) \quad (1.67)$$

gdje je $Z(G)$ centar grupe G .

Teorem 1.21. *Pretpostavimo da grupa G djeluje na skup A . Definirajmo relaciju na A sa*

$$a \sim b \iff a = g \cdot b \quad \text{za neki} \quad g \in G. \quad (1.68)$$

Onda je $\sim$ relacija ekvivalencije pa skup A možemo rastaviti po orbitama kao disjunktну uniju

$$A = \bigcup_{a \in C} Ga \quad (1.69)$$

gdje C sadrži točno jedan element iz svake orbite.

Drugim riječima, elementi $a, b \in A$ su u relaciji (ekvivalencije) ako pripadaju istoj orbiti, a različite orbite tvore particiju skupa A .

Dokaz Očigledno je $a \sim a$ jer je $e \cdot a = a$ za svaki $a \in A$ pa je relacija (1.68) refleksivna. Ako je $a \sim b$, onda postoji $g \in G$ takav da je $a = g \cdot b$. U tom slučaju

$$g^{-1} \cdot a = g^{-1} \cdot (g \cdot b) = (g^{-1}g) \cdot b = e \cdot b = b,$$

odnosno $b \sim a$ pa je relacija simetrična. Nadalje, ako je $a \sim b$ i $b \sim c$, onda je $a = g \cdot b$ i $b = h \cdot c$ za neke $g, h \in G$. Oдавde slijedi

$$a = g \cdot b = g \cdot (h \cdot c) = (gh) \cdot c,$$

odnosno $a \sim c$ što pokazuje da je relacija (1.68) tranzitivna. Dakle, (1.68) je relacija ekvivalencije na skupu A . Klasa ekvivalencije elementa $a \in A$ je orbita Ga jer je

$$\bar{a} = \{b \in A \mid b = g \cdot a, g \in G\} = Ga,$$

stoga je $A = \cup_{a \in C} Ga$ disjunktna unija gdje C sadrži točno jedan element iz svake orbite. ■

Definicija 1.26. Kažemo da grupa G djeluje tranzitivno na skup A ako za svaka dva elementa $a, b \in A$ postoji $g \in G$ takav da je $b = g \cdot a$.

Ako G djeluje tranzitivno na skup A , onda A ima samo jednu orbitu jer je $A = G \cdot a$ za svaki $a \in A$. Istražimo sada vezu između orbite i stabilizatora elementa. Intuitivno očekujemo da je orbita elementa manja što je stabilizator veći. Precizna formulacija ove tvrdnje je dana sljedećim teoremom.

Teorem 1.22. Neka grupa G djeluje na skup A . Kardinalni broj orbite Ga jednak je indeksu stabilizatora G_a u G , tj.

$$|Ga| = [G : G_a]. \quad (1.70)$$

Dokaz Definirajmo preslikavanje $f : Ga \rightarrow G/G_a$ sa $f(g \cdot a) = gG_a$ gdje je G/G_a skup svih lijevih susjednih klasa podgrupe G_a . Pokažimo da je f dobro definirano. Ako je $g \cdot a = h \cdot a$ za neke $g, h \in G$, onda djelovanjem sa h^{-1} na oba elementa dobivamo $(h^{-1}g) \cdot a = a$. Stoga je $h^{-1}g \in G_a$ što povlači $gG_a = hG_a$.

Preslikavanje f je očigledno surjekcija jer za svaki $gG_a \in G/G_a$ imamo $f(g \cdot G_a) = gG_a$. Pokažimo da je f injekcija. Ako je $f(g \cdot a) = f(h \cdot a)$, onda je $gG_a = hG_a$ što implicira $h^{-1}g \in G_a$. Oдавde slijedi da je $(h^{-1}g) \cdot a = a$ pa djelovanjem s h na oba elementa dobivamo $g \cdot a = h \cdot a$. Dakle, f je bijekcija što implicira $|Ga| = |G/G_a| = [G : G_a]$. ■

Ako je G konačna grupa, onda je prema Lagrangeovom teoremu $|G| = |G_a| [G : G_a]$ pa iz (1.70) slijedi

$$|G| = |G_a| |Ga| \quad \text{za svaki } a \in A. \quad (1.71)$$

Ako je A konačni skup, onda iz (1.69) i (1.70) slijedi da je broj elemenata skupa jednak

$$|A| = \sum_{a \in C} |Ga| = \sum_{a \in C} [G : G_a].$$

Time smo dokazali

Korolar 1.3. *Neka je A konačni skup na kojeg djeluje grupa G . Tada je*

$$|A| = \sum_{a \in C} [G : G_a]$$

gdje skup C sadrži točno jedan element iz svake orbite.

Neka je $A_g = \{a \in A \mid g \cdot a = a\}$ skup svih elemenata u A koji su stabilizirani elementom $g \in G$. Ako su A i G konačni skupovi, onda se broj orbita u A može izraziti kao prosječni broj elemenata u A koji su stabilizirani elementima iz G .

Teorem 1.23 (Burnside). *Neka je G konačna grupa koja djeluje na konačni skup A . Tada je broj orbita u A , u oznaci $|A/G|$, jednak*

$$|A/G| = \frac{1}{|G|} \sum_{g \in G} |A_g|. \quad (1.72)$$

Dokaz Definirajmo skup $S = \{(g, a) \in G \times A \mid g \cdot a = a\}$. Za fiksni $g \in G$ broj uređenih parova u S jednak je $|A_g|$, odnosno broju elemenata $a \in A$ koji su stabilizirani s g . Za fiksni $a \in A$ broj uređenih parova u S jednak je $|G_a|$, odnosno broju elemenata $g \in G$ koji stabiliziraju a . Stoga je

$$|S| = \sum_{g \in G} |A_g| = \sum_{a \in A} |G_a|. \quad (1.73)$$

Iz relacije (1.71) imamo $|G_a| = |G|/|Ga|$ pa je

$$\sum_{a \in A} |G_a| = |G| \sum_{a \in A} \frac{1}{|Ga|}. \quad (1.74)$$

Prema teoremu 1.21 skup A možemo rastaviti po orbitama $A = \cup_{a \in C} Ga$ gdje skup C sadrži točno jedan element iz svake orbite. Kako su orbite disjunktne, suma po elementima $a \in A$ se može napisati kao suma po elementima orbita Gb , $b \in C$. Ovo povlači da je

$$\sum_{a \in A} \frac{1}{|Ga|} = \sum_{b \in C} \sum_{a \in Gb} \frac{1}{|Ga|}. \quad (1.75)$$

Međutim, $a \in Gb$ povlači da su a i b u istoj orbiti pa je $|Ga| = |Gb|$ za svaki $a \in Gb$. Stoga je

$$\sum_{a \in Gb} \frac{1}{|Ga|} = \sum_{a \in Gb} \frac{1}{|Gb|} = |Gb| \frac{1}{|Gb|} = 1 \quad (1.76)$$

pa iz (1.75) dobivamo

$$\sum_{a \in A} \frac{1}{|Ga|} = \sum_{b \in C} 1 = |C| \quad (1.77)$$

gdje je $|C|$ broj orbita u A koji ćemo označiti s $|A/G|$. Sada iz relacija (1.73), (1.74) i (1.77) odmah slijedi

$$\sum_{g \in G} |A_g| = |G| \sum_{a \in A} \frac{1}{|Ga|} = |G| |A/G|, \quad (1.78)$$

odnosno

$$|A/G| = \frac{1}{|G|} \sum_{g \in G} |A_g|. \quad (1.79)$$

■

Prema teoremu 1.21 djelovanje grupe G na samu sebe konjugacijom tvori particiju od G na klase konjugacije $C(a) = \{gag^{-1} \mid g \in G\}$. Ako je G konačna grupa, ovo ima za posljedicu sljedeći važni rezultat.

Teorem 1.24 (Jednadžba klase). *Neka je G konačna grupa i neka su $a_1, a_2, \dots, a_n$ predstavnici klase konjugacije koje imaju više od jednog elementa. Tada je*

$$|G| = |Z(G)| + \sum_{i=1}^n [G : N(a_i)].$$

Dokaz Neka su $a_1, a_2, \dots, a_n, a_{n+1}, \dots, a_m$ predstavnici svih klase konjugacije u G gdje $a_{n+1}, \dots, a_m$ predstavljaju klase s jednim elementom, odnosno $C(a_k) = \{a_k\}$ za $k = n+1, \dots, m$. Tada je centar grupe dan sa $Z(G) = \{a_{n+1}, a_{n+2}, \dots, a_m\}$ pa imamo

$$|G| = \sum_{i=1}^m |C(a_i)| = \sum_{i=1}^n |C(a_i)| + \sum_{i=n+1}^m |C(a_i)| = |Z(G)| + \sum_{i=1}^n |C(a_i)|. \quad (1.80)$$

Prema teoremu 1.22 vrijedi

$$|C(a_i)| = [G : G_{a_i}] = [G : N(a_i)] \quad (1.81)$$

jer je stabilizator G_{a_i} jednak normalizatoru $N(a_i)$. Sada iz jednadžbi (1.80) i (1.81) dobivamo jednadžbu klase

$$|G| = |Z(G)| + \sum_{i=1}^n [G : N(a_i)].$$

■

Iz jednadžbe klase možemo izvesti određene zaključke o strukturi grupe. Kao prvu primjenu navodimo činjenicu da grupa reda p^n , gdje je p prost broj, ima netrivialan centar.

Teorem 1.25. *Neka je G grupa reda p^n , $n \geq 1$, gdje je p prosti broj. Tada je centar grupe G netrivialan.*

Dokaz Za grupu G jednačba klase glasi

$$p^n = |Z(G)| + \sum_{i=1}^r [G : N(a_i)], \quad (1.82)$$

gdje su $a_1, a_2, \dots, a_r$ predstavnici klasa konjugacije koje imaju više od jednog elementa. Prema Lagrangeovom teoremu vrijedi

$$p^n = |N(a_i)| [G : N(a_i)] \quad \text{za sve } i = 1, 2, \dots, r. \quad (1.83)$$

Prisjetimo se da je $N(a) = G$ ako i samo ako je $a \in Z(G)$. Stoga je $|N(a_i)| < |G|$ jer $a_i \notin Z(G)$ pa je $|N(a_i)| = p^l$ za neki $l < n$. Sada iz (1.83) slijedi da je

$$[G : N(a_i)] = p^{n-l} \quad (1.84)$$

što implicira da $p \mid [G : N(a_i)]$ za sve $i = 1, 2, \dots, r$, odnosno $p \mid \sum_{i=1}^r [G : N(a_i)]$. Iz jednačbe (1.82) slijedi da $p \mid |Z(G)|$ jer je $|Z(G)| = p^n - \sum_{i=1}^r [G : N(a_i)]$. Dakle, $Z(G)$ je netrivialan jer ima barem p elemenata. ■

1.10 Direktni i poludirektni umnožak grupa

U proučavanju strukture neke grupe G korisno je G razložiti na manje podgrupe koje čine sastavne blokove grupe G . Ako poznamo strukturu sastavnih blokova, onda možemo odrediti strukturu čitave grupe. U ovom i idućem poglavlju ćemo upoznati dva načina na koje se zadana grupa može rastaviti kao umnožak svojih podgrupa, naime direktni umnožak i poludirektni umnožak grupa. Posebno, razmotrit ćemo rastav konačno generiranih Abelovih grupa na direktni umnožak svojih podgrupa.

1.10.1 Direktni umnožak

U ovom poglavlju ćemo upoznati vanjski i unutarnji direktni umnožak grupa koji su važni u proučavanju strukture grupa. Vanjski direktni umnožak je način na koji se nove grupe mogu konstruirati od zadanih grupa, dok je unutarnji direktni umnožak način na koji se zadana grupa može napisati kao umnožak svojih podgrupa.

Definicija 1.27. *Direktni umnožak grupa $G_1, G_2, \dots, G_n$ je kartezijev umnožak $\times_{i=1}^n G_i = G_1 \times G_2 \cdots \times G_n$ s binarnom operacijom*

$$(g_1, g_2, \dots, g_n)(h_1, h_2, \dots, h_n) = (g_1 h_1, g_2 h_2, \dots, g_n h_n), \quad g_i, h_i \in G_i. \quad (1.85)$$

Binarne operacije na grupama $G_1, G_2, \dots, G_n$ su općenito različite, ali ih radi jednostavnosti označavamo istim simbolom. Jedinica u direktnom umnošku je element $(e_1, e_2, \dots, e_n)$ gdje je e_i jedinica u G_i , a inverz elementa $(g_1, g_2, \dots, g_n)$ je

$$(g_1, g_2, \dots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \dots, g_n^{-1}). \quad (1.86)$$

Asocijativnost množenja u $\times_{i=1}^n G_i$ se naslijeđuje od asocijativnosti množenja u grupama $G_1, G_2, \dots, G_n$.

Ako su $G_1, G_2, \dots, G_n$ konačne grupe, onda je očito red grupe $G = \times_{i=1}^n G_i$ jednak

$$|G| = \prod_{i=1}^n |G_i|.$$

Za primjer promotrimo direktni umnožak Abelove grupe $G_1 = (\mathbb{R}, +)$ i opće linearne grupe $G_2 = GL(n, \mathbb{R})$. Množenje u $G_1 \times G_2$ je definirano s

$$(x, A)(y, B) = (x + y, AB).$$

Neutralni element je

$$e = (0, I)$$

gdje je I jedinična matrica reda n , dok je inverzni element dan s

$$(x, A)^{-1} = (-x, A^{-1}).$$

Sljedeća propozicija pokazuje da direktni umnožak $\times_{i=1}^n G_i$ sadrži izomorfnu kopiju svake grupe G_i koja je normalna podgrupa od $\times_{i=1}^n G_i$. Također, za svaku grupu G_i postoji projekcijski homomorfizam sa $\times_{i=1}^n G_i$ na G_i .

Propozicija 1.7. *Neka je $G = \times_{i=1}^n G_i$ direktni umnožak grupa $G_1, G_2, \dots, G_n$.*

(i) *Skup*

$$\bar{G}_i = \left\{ (e_1, \dots, e_{i-1}, g_i, e_{i+1}, \dots, e_n) \mid g_i \in G_i \right\}$$

je normalna podgrupa od G i $\bar{G}_i \simeq G_i$. Nadalje,

$$G/\bar{G}_i \simeq \times_{\substack{j=1 \\ j \neq i}}^n G_j.$$

(ii) *Projekcija $\pi_i: G \rightarrow G_i$,*

$$\pi_i(g_1, g_2, \dots, g_n) = g_i,$$

je epimorfizam s jezgrom

$$\ker(\pi_i) \simeq \times_{\substack{j=1 \\ j \neq i}}^n G_j.$$

Dokaz (i) Preslikavanje

$$g_i \mapsto (e_1, \dots, e_{i-1}, g_i, e_{i+1}, \dots, e_n) \in \bar{G}_i$$

je očigledno izomorfizam sa G_i na $\bar{G}_i$ pa je $\bar{G}_i$ izomorfna kopija grupe G_i u grupi G . Nadalje, projekcija $\varphi_i: G \rightarrow \times_{\substack{j=1 \\ j \neq i}}^n G_j$,

$$\varphi_i(g_1, g_2, \dots, g_n) = (g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_n),$$

koja ispušta element g_i je epimorfizam s jezgrom

$$\ker(\varphi_i) = \{(e_1, \dots, e_{i-1}, g_i, e_{i+1}, \dots, e_n) \mid g_i \in G_i\} = \bar{G}_i.$$

Dakle, $\bar{G}_i$ je normalna podgrupa od G pa je po Prvom teoremu o izomorfizmu

$$G/\bar{G}_i \simeq \times_{\substack{j=1 \\ j \neq i}}^n G_j. \quad (1.87)$$

(ii) Projekcija $\pi_i: G \rightarrow G_i$ dana sa $\pi_i(g_1, g_2, \dots, g_n) = g_i$ je homomorfizam s jezgrom

$$\ker(\pi_i) = \{(g_1, \dots, g_{i-1}, e_i, g_{i+1}, \dots, g_n) \mid g_j \in G_j\}.$$

Preslikavanje $\psi_i: \ker(\pi_i) \rightarrow \times_{\substack{j=1 \\ j \neq i}}^n G_j$,

$$\psi_i(g_1, \dots, g_{i-1}, e_i, g_{i+1}, \dots, g_n) = (g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_n),$$

je izomorfizam, stoga je

$$\ker(\pi_i) \simeq \times_{\substack{j=1 \\ j \neq i}}^n G_j.$$

Iz relacije (1.87) također slijedi da je $\ker(\pi_i) \simeq G/\bar{G}_i$. ■

Ako je $G = G_1 \times G_2 \times \dots \times G_n$ direktni umnožak grupa, onda se svaki element iz G može napisati kao

$$(g_1, g_2, \dots, g_n) = (g_1, e_2, e_3, \dots, e_n)(e_1, g_2, e_3, \dots, e_n) \dots (e_1, \dots, e_{n-1}, g_n) \quad (1.88)$$

gdje elementi na desnoj strani pripadaju grupama $\bar{G}_1, \bar{G}_2, \dots, \bar{G}_n$ redom. Stoga se G može napisati kao umnožak

$$G = \bar{G}_1 \bar{G}_2 \dots \bar{G}_n \quad (1.89)$$

gdje podgrupe $\bar{G}_i$ zadovoljavaju sljedeće uvjete:

- (i) $\bar{G}_i \triangleleft G$
- (ii) $\bar{G}_i \cap (\bar{G}_1 \dots \bar{G}_{i-1} \bar{G}_{i+1} \dots \bar{G}_n) = \{e\}$.

Definicija 1.28. Grupa G je unutarnji direktni umnožak podgrupa $G_1, G_2, \dots, G_n$ ako je $G = G_1 G_2 \dots G_n$ i podgrupe G_i zadovoljavaju uvjete

- (i) $G_i \triangleleft G$,
- (ii) $G_i \cap (G_1 \dots G_{i-1} G_{i+1} \dots G_n) = \{e\}$

za sve $1 \leq i \leq n$.

Sljedeći teorem nam kazuje da su vanjski i unutarnji direktni umnošci izomorfni i daje kriterij kada se neka grupa može rastaviti na vanjski direktni umnožak svojih podgrupa.

Teorem 1.26. *Ako je $G = G_1 G_2 \dots G_n$ unutarnji direktni umnožak podgrupa $G_1, G_2, \dots, G_n$, onda je $G \simeq G_1 \times G_2 \times \dots \times G_n$.*

Dokaz Pokažimo da svaki $x \in G$ ima jedinstveni prikaz u obliku $x = g_1 g_2 \dots g_n$ gdje je $g_i \in G_i$. Prvo ćemo pokazati da elementi iz različitih podgrupa komutiraju, odnosno $g_i g_j = g_j g_i$ za sve $g_i \in G_i$ i $g_j \in G_j$ gdje je $i \neq j$. Primijetimo da je $G_j \subseteq G_1 \dots G_{i-1} G_{i+1} \dots G_n$ za $j \neq i$ pa uvjet (ii) definicije 1.28 implicira $G_i \cap G_j = \{e\}$. Neka su $g_i \in G_i$ i $g_j \in G_j$. Tada je $g_j^{-1} g_i g_j \in G_i$ jer je G_i normalna podgrupa od G što povlači $(g_j^{-1} g_i g_j) g_i^{-1} \in G_i$. Slično, $g_i g_j g_i^{-1} \in G_j$ što povlači $g_j^{-1} (g_i g_j g_i^{-1}) \in G_j$. Dakle, $g_j^{-1} g_i g_j g_i^{-1} \in G_i \cap G_j = \{e\}$ pa slijedi da je $g_i g_j = g_j g_i$.

Pretpostavimo sada da se element $x \in G$ može napisati na dva načina kao umnožak

$$x = g_1 g_2 \dots g_n = h_1 h_2 \dots h_n, \quad g_i, h_i \in G_i. \quad (1.90)$$

Odavde slijedi

$$h_1^{-1} g_1 = (h_2 h_3 \dots h_n) (g_2 g_3 \dots g_n)^{-1} = h_2 h_3 \dots h_n g_n^{-1} \dots g_3^{-1} g_2^{-1}. \quad (1.91)$$

Kako je $h_i g_i^{-1} \in G_i$, a elementi iz različitih podgrupa komutiraju, umnožak (1.91) se može zapisati kao

$$h_1^{-1} g_1 = (h_2 g_2^{-1}) (h_3 g_3^{-1}) \dots (h_n g_n^{-1}). \quad (1.92)$$

Ovo implicira da je $h_1^{-1} g_1 \in G_1 \cap (G_2 G_3 \dots G_n) = \{e\}$ pa zaključujemo da je $g_1 = h_1$. Sada iz jednakosti (1.90) slijedi

$$g_2 g_3 \dots g_n = h_2 h_3 \dots h_n. \quad (1.93)$$

Ponavljanjem postupka se pokaže da je $g_i = h_i$ za svaki $1 \leq i \leq n$ pa je zapis (1.90) jedinstven. Stoga možemo definirati bijektivno preslikavanje

$$\varphi: G_1 G_2 \dots G_n \rightarrow G_1 \times G_2 \times \dots \times G_n \quad (1.94)$$

sa $\varphi(g_1 g_2 \dots g_n) = (g_1, g_2, \dots, g_n)$. Ako je $x = g_1 g_2 \dots g_n$ i $y = h_1 h_2 \dots h_n$, onda zbog komutativnosti elemenata iz različitih podgrupa G_i imamo

$$\varphi(xy) = \varphi((g_1 g_2 \dots g_n)(h_1 h_2 \dots h_n)) = \varphi(g_1 h_1 g_2 h_2 \dots g_n h_n) \quad (1.95)$$

$$= (g_1, g_2, \dots, g_n)(h_1, h_2, \dots, h_n) = \varphi(x)\varphi(y). \quad (1.96)$$

Dakle, φ je izomorfizam pa je $G_1 G_2 \dots G_n \simeq G_1 \times G_2 \times \dots \times G_n$. ■

Primijetimo da vanjski direktni umnožak uvijek postoji dok je unutarnji direktni umnožak definiran samo ako podgrupe $G_1, G_2, \dots, G_n$ zadovoljavaju uvjete teorema 1.26. Ako je G Abelova grupa, onda unutarnji direktni umnožak označavamo sa $G = G_1 \oplus G_2 \oplus \dots \oplus G_n$ i nazivamo direktna suma grupa $G_1, G_2, \dots, G_n$.

Primjer 1.40. Neka je G konačna grupa takva da je red svakog elementa $a \neq e$ jednak 2. Pokažimo da je $|G| = 2^n$ i $G \simeq C_1 \times C_2 \times \cdots \times C_n$ gdje je C_i ciklička grupa reda 2.

Ako je $x \in G$, onda je $x^2 = e$ pa je $x = x^{-1}$ za svaki $x \in G$. Ako su $a, b \in G$, onda imamo

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba \quad (1.97)$$

što povlači da je G Abelova grupa. Odaberimo $a_1 \in G$, $a_1 \neq e$. Ako je $G = \langle a_1 \rangle$, onda je G ciklička grupa reda 2 i dokaz je gotov. U protivnom postoji $a_2 \notin \langle a_1 \rangle$. G je Abelova grupa pa su $\langle a_1 \rangle$ i $\langle a_2 \rangle$ normalne podgrupe od G . Nadalje, $a_1 \neq a_2$ povlači da je $\langle a_1 \rangle \cap \langle a_2 \rangle = \{e\}$ pa iz teorema 1.26 slijedi da je $\langle a_1 \rangle \langle a_2 \rangle \simeq \langle a_1 \rangle \times \langle a_2 \rangle$. Ako je $G = \langle a_1 \rangle \langle a_2 \rangle$, dokaz je gotov; u protivnom postoji $a_3 \notin \langle a_1 \rangle \langle a_2 \rangle$. S obzirom da je $a_i \neq a_j$ za $i \neq j$, slijedi da je

$$\langle a_1 \rangle \cap \langle a_2 \rangle \langle a_3 \rangle = \{e\}, \quad \langle a_2 \rangle \cap \langle a_1 \rangle \langle a_3 \rangle = \{e\}, \quad \langle a_3 \rangle \cap \langle a_1 \rangle \langle a_2 \rangle = \{e\} \quad (1.98)$$

pa zaključujemo da je $\langle a_1 \rangle \langle a_2 \rangle \langle a_3 \rangle \simeq \langle a_1 \rangle \times \langle a_2 \rangle \times \langle a_3 \rangle$. Nastavljajući postupak dolazimo do niza cikličkih podgrupa $\langle a_1 \rangle, \langle a_2 \rangle, \dots, \langle a_n \rangle$ reda 2 koje ispunjavaju uvjete iz teorema 1.26 i $G = \langle a_1 \rangle \langle a_2 \rangle \cdots \langle a_n \rangle$. Stoga je $G \simeq \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_n \rangle$. $\square$

Primjer 1.41. Neka je G grupa reda četiri. Onda je G ili ciklička grupa reda četiri ili je $G \simeq H \times K$ gdje su H i K cikličke grupe reda dva.

Pretpostavimo da G nije ciklička grupa reda četiri. Neka je $a \in G$, $a \neq e$. Onda $|a|$ dijeli 4 pa je $|a| = 2$ ($|a| \neq 4$ jer G nije ciklička grupa reda četiri). Stoga je $H = \{e, a\}$ ciklička podgrupa od G reda dva. Nadalje, postoji $b \in G \setminus H$ takav da je $|b| = 2$ pa je $K = \{e, b\}$ ciklička podgrupa od G reda dva. Elementi grupe G su dani sa $G = \{e, a, b, ab\} = HK$ jer G ima četiri elementa. Primijetimo da je $H \cap K = \{e\}$ i $[G: H] = [G: K] = 2$ pa su po propoziciji 1.4 H i K normalne podgrupe od G . Sada iz teorema 1.26 slijedi da je $G \simeq H \times K$. Cayleyevu tablicu za grupu G je lako konstruirati ako uočimo da je $ab = ba$ jer $ba \in \{e, a, b\}$ vodi na kontradikciju. Dakle, G je generirana elementima a i b koji zadovoljavaju relacije $a^2 = b^2 = e$ i $ab = ba$ što je dovoljno da se napiše tablica množenja za grupu G . $\square$

Na kraju promotrimo čemu je izomorfan vanjski direktni umnožak dvaju kvocijentnih grupa.

Teorem 1.27. Neka su G_1 i G_2 grupe, i neka su $N_1 \triangleleft G_1$ i $N_2 \triangleleft G_2$. Tada je

$$(G_1 \times G_2)/(N_1 \times N_2) \simeq (G_1/N_1) \times (G_2/N_2).$$

Dokaz Definirajmo preslikavanje $\phi: G_1 \times G_2 \rightarrow (G_1/N_1) \times (G_2/N_2)$ s $\phi(x_1, x_2) = (x_1N_1, x_2N_2)$. Pokažimo da je ϕ homomorfizam. Imamo

$$\begin{aligned} \phi((x_1, x_2)(y_1, y_2)) &= \phi(x_1y_1, x_2y_2) = (x_1y_1N_1, x_2y_2N_2) \\ &= ((x_1N_1)(y_1N_1), (x_2N_2)(y_2N_2)) \\ &= (x_1N_1, x_2N_2)(y_1N_1, y_2N_2) = \phi(x_1, x_2)\phi(y_1, y_2). \end{aligned}$$

Preslikavanje ϕ je surjektivno jer je

$$\text{Im}(\phi) = \{(x_1N_1, x_2N_2) \mid x_1 \in G_1, x_2 \in G_2\} = (G_1/N_1) \times (G_2/N_2).$$

Nadalje, jezgra homomorfizma je dana s

$$\begin{aligned} \ker(\phi) &= \{(x_1, x_2) \mid (x_1N_1, x_2N_2) = (N_1, N_2)\} \\ &= \{(x_1, x_2) \mid x_1N_1 = N_1, x_2N_2 = N_2\} \\ &= \{(x_1, x_2) \mid x_1 \in N_1, x_2 \in N_2\} = N_1 \times N_2. \end{aligned}$$

Dakle, prema prvom teoremu o izomorfizmu, vrijedi

$$(G_1 \times G_2)/(N_1 \times N_2) \simeq (G_1/N_1) \times (G_2/N_2).$$

■

1.10.2 Poludirektni umnožak

Poludirektni umnožak je generalizacija direktnog umnoška $G = HK \simeq H \times K$ kada je H normalna u G , ali K nije nužno normalna podgrupa od G . Ako su H i K komutativne grupe, onda je $H \times K$ također komutativna grupa. Međutim, poludirektni umnožak H i K ne mora biti komutativan pa ovim umnoškom možemo konstruirati puno veću klasu grupa.

Da bismo motivirali definiciju poludirektnog umnoška, pretpostavimo da G sadrži dvije podgrupe H i K sa sljedećim svojstvima:

- (a) $H \triangleleft G$,
- (b) $H \cap K = \{e\}$.

Prema teoremu 1.10, HK je podgrupa od G . Ako su $h_1k_1, h_2k_2 \in HK$, onda je njihov umnožak jednak

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2k_1^{-1})(k_1k_2) = h_3k_3, \quad (1.99)$$

gdje je $k_3 = k_1k_2$ i $h_3 = h_1k_1h_2k_1^{-1} \in H$ jer je H normalna podgrupa. Element $k_1h_2k_1^{-1}$ možemo pisati kao $C_{k_1}(h_2)$, gdje je $C_k(x) = kxk^{-1}$ konjugacija elementom $k \in K$. Definirajmo preslikavanje

$$\varphi: K \rightarrow \text{Aut}(H), \quad \varphi(k) = C_k.$$

Tada umnožak (1.99) možemo pisati u obliku

$$(h_1k_1)(h_2k_2) = (h_1\varphi(k_1)(h_2))(k_1k_2). \quad (1.100)$$

Primijetimo da je φ homomorfizam jer za svaki $h \in H$ vrijedi

$$\begin{aligned} \varphi(k_1k_2)(h) &= (k_1k_2)h(k_1k_2)^{-1} = k_1(k_2hk_2^{-1})k_1^{-1} \\ &= \varphi(k_1)(\varphi(k_2)(h)) = (\varphi(k_1) \circ \varphi(k_2))(h). \end{aligned}$$

Dakle, $\varphi(k_1k_2) = \varphi(k_1) \circ \varphi(k_2)$. Kako je $H \cap K = \{e\}$ svaki element grupe HK je na jedinstven način prikazan umnoškom hk , $h \in H$, $k \in K$, pa ga možemo identificirati s uređenim parom (h, k) . Stoga umnožak (1.100) možemo zapisati kao

$$(h_1, k_1)(h_2, k_2) = (h_1\varphi(k_1)(h_2), k_1k_2). \quad (1.101)$$

Umnožak (1.101) pretpostavlja da G sadrži podgrupe H i K . U poludirektnom umnošku se ova konstrukcija generalizira za dvije proizvoljne grupe H i K te zadani homomorfizam $\varphi: K \rightarrow \text{Aut}(H)$. Homomorfizam φ inducira djelovanje grupe K na grupu H definirano sa

$$k \cdot h = \varphi(k)(h).$$

Neutralni element $e_K \in K$ djeluje kao identiteta na H jer je $\varphi(e_K) = \text{id}_H$, tj.

$$e_K \cdot h = \text{id}_H(h) = h.$$

Također vrijedi

$$k \cdot e_H = \varphi(k)(e_H) = e_H$$

jer automorfizam $\varphi(k)$ preslikava jedinicu u samu sebe. Djelovanje umnoška $k_1 k_2$ je dano s

$$(k_1 k_2) \cdot h = \varphi(k_1 k_2)(h) = (\varphi(k_1) \circ \varphi(k_2))(h) = \varphi(k_1)(\varphi(k_2)(h)) = k_1 \cdot (k_2 \cdot h). \quad (1.102)$$

Nadalje, k djeluje na umnožak $h_1 h_2$ kao

$$k \cdot (h_1 h_2) = \varphi(k)(h_1 h_2) = \varphi(k)(h_1) \varphi(k)(h_2) = (k \cdot h_1)(k \cdot h_2) \quad (1.103)$$

jer je $\varphi(k)$ homomorfizam. Ova razmatranja motiviraju sljedeći teorem.

Teorem 1.28. *Neka su H i K grupe, i neka je $\varphi: K \rightarrow \text{Aut}(H)$ homomorfizam. Skup $G = H \times K$ je grupa obzirom na umnožak*

$$(h_1, k_1)(h_2, k_2) = (h_1(k_1 \cdot h_2), k_1 k_2) \quad (1.104)$$

gdje je $\cdot: K \times H \rightarrow H$ djelovanje definirano sa $k \cdot h = \varphi(k)(h)$.

(i) Neutralni element je $e = (e_H, e_K)$, a inverz elementa (h, k) je dan sa

$$(h, k)^{-1} = (k^{-1} \cdot h^{-1}, k^{-1}).$$

(ii) Podgrupe $\bar{H} = H \times \{e_K\}$ i $\bar{K} = \{e_H\} \times K$ su izomorfne grupama H i K , redom.

(iii) $\bar{H}$ je normalna podgrupa od G .

(iv) $\bar{H} \cap \bar{K} = \{e\}$.

Dokaz (i) Dokažimo asocijativnost množenja (1.104). Imamo

$$\begin{aligned} ((h_1, k_1)(h_2, k_2))(h_3, k_3) &= (h_1(k_1 \cdot h_2), k_1 k_2)(h_3, k_3) \\ &= (h_1(k_1 \cdot h_2)(k_1 k_2 \cdot h_3), (k_1 k_2)k_3). \end{aligned} \quad (1.105)$$

S druge strane,

$$\begin{aligned} (h_1, k_1)((h_2, k_2)(h_3, k_3)) &= (h_1, k_1)(h_2(k_2 \cdot h_3), k_2 k_3) \\ &= (h_1(k_1 \cdot (h_2(k_2 \cdot h_3))), k_1(k_2 k_3)). \end{aligned} \quad (1.106)$$

Primjenom relacija (1.102) i (1.103) dobivamo

$$(k_1 \cdot h_2)(k_1 k_2) \cdot h_3 = (k_1 \cdot h_2)(k_1 \cdot (k_2 \cdot h_3)) = k_1 \cdot (h_2(k_2 \cdot h_3)), \quad (1.107)$$

pa supstitucija izraza (1.107) u jednadžbu (1.106) povlači

$$(h_1, k_1)((h_2, k_2)(h_3, k_3)) = (h_1(k_1 \cdot h_2)(k_1 k_2) \cdot h_3, k_1(k_2 k_3)) = ((h_1, k_1)(h_2, k_2))(h_3, k_3).$$

Lako se provjeri da je (e_H, e_K) neutralni element zdesna jer je

$$(h, k)(e_H, e_K) = (h(k \cdot e_H), ke_K) = (he_H, k) = (h, k),$$

a slično se pokazuje i da je $(e_H, e_K)(h, k) = (h, k)$. Dakle, (e_H, e_K) je jedinica u G . Provjerimo da je inverzni element dan sa

$$(h, k)^{-1} = (k^{-1} \cdot h^{-1}, k^{-1}).$$

Doista,

$$\begin{aligned} (h, k)(k^{-1} \cdot h^{-1}, k^{-1}) &= (h k \cdot (k^{-1} \cdot h^{-1}), k k^{-1}) \\ &= (h(k k^{-1}) \cdot h^{-1}, e_K) = (h(e_K \cdot h^{-1}), e_K) = (e_H, e_K). \end{aligned}$$

Slično se pokazuje da je $(k^{-1} \cdot h^{-1}, k^{-1})(h, k) = (e_H, e_K)$.

(ii) Pokažimo da je $\bar{H}$ podgrupa od G . Ako su $(h_1, e_K), (h_2, e_K) \in \bar{H}$, onda je

$$\begin{aligned} (h_1, e_K)(h_2, e_K)^{-1} &= (h_1, e_K)(e_K \cdot h_2^{-1}, e_K) \\ &= (h_1 e_K \cdot (e_K \cdot h_2^{-1}), e_K) = (h_1 h_2^{-1}, e_K) \in \bar{H}. \end{aligned}$$

Preslikavanje $\psi: \bar{H} \rightarrow H$, $\psi(h, e_K) = h$, je očigledno bijekcija. Također,

$$\begin{aligned} \psi((h_1, e_K)(h_2, e_K)) &= \psi(h_1(e_K \cdot h_2), e_K) \\ &= \psi(h_1 h_2, e_K) = h_1 h_2 = \psi(h_1, e_K)\psi(h_2, e_K), \end{aligned}$$

stoga je ψ izomorfizam s $\bar{H}$ na H . Slično se pokazuje da je $\bar{K} \simeq K$.

(iii) Neka je $(h, e_K) \in \bar{H}$, i neka je $(h_1, k_1) \in G$. Tada imamo

$$\begin{aligned} (h_1, k_1)(h, e_K)(h_1, k_1)^{-1} &= (h_1(k_1 \cdot h), k_1)(k_1^{-1} \cdot h_1^{-1}, k_1^{-1}) \\ &= (h_1(k_1 \cdot h)k_1 \cdot (k_1^{-1} \cdot h_1^{-1}), e_K) \\ &= (h_1(k_1 \cdot h)h_1^{-1}, e_K) \in \bar{H}, \end{aligned}$$

čime je pokazano da je $\bar{H}$ normalna podgrupa od G .

(iv) Ako je $(h, k) \in \bar{H} \cap \bar{K}$, onda je $(h, k) \in \bar{H}$ i $(h, k) \in \bar{K}$ iz čega slijedi da je $h = e_H$ i $k = e_K$. Dakle, $\bar{H} \cap \bar{K} = \{(e_H, e_K)\}$. ■

Definicija 1.29. Neka su H i K grupe, i neka je $\varphi: K \rightarrow \text{Aut}(H)$ homomorfizam. Skup $H \times K$ zajedno s operacijom množenja

$$(h_1, k_1)(h_2, k_2) = (h_1(k_1 \cdot h_2), k_1 k_2)$$

gdje je $k \cdot h = \varphi(k)(h)$ nazivamo poludirektni produkt grupa H i K i označavamo s

$$H \rtimes_{\varphi} K.$$

Ako je iz konteksta jasno o kojem se homomorfizmu φ radi, onda pišemo $H \rtimes K$.

Grupa Euklidskih gibanja $ISO(2)$

Grupu transformacija $E(2)$ tvore izometrije u ravnini $\mathbb{R}^2$, odnosno transformacije koje čuvaju Euklidsku metriku $d(x, y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2}$, $x = (x_1, x_2)$ i $y = (y_1, y_2)$. Podgrupa transformacija od $E(2)$ koje čuvaju orijentaciju sastoji se od translacija i rotacija, i označava s $ISO(2)$. Svaki element grupe $ISO(2)$ je kompozicija translacije i rotacije

$$x \mapsto R(x + v), \quad R \in SO(2), \quad x, v \in \mathbb{R}^2,$$

ili kompozicija rotacije i translacije

$$x \mapsto Rx + v.$$

Grupa $ISO(2)$ ima primjene u klasičnoj mehanici gdje prikazuje sva moguća gibanja krutog tijela u ravnini.

Pokazat ćemo da je $ISO(2)$ poludirektni umnožak grupe translacija $\mathbf{T}$ i grupe rotacija $SO(2)$. Svaka translacija T_v za vektor $v \in \mathbb{R}^2$,

$$T_v(x) = x + v,$$

je jedinstveno određena tim vektorom, stoga T_v možemo identificirati s vektorom v . Preslikavanje $T_v \mapsto v$ na prirodan način daje izomorfizam s grupe $\mathbf{T}$ na grupu $(\mathbb{R}^2, +)$. Elementi grupe rotacija su matrice

$$R_{\theta} = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}, \quad \theta \in \mathbb{R}.$$

Za svaki $R_{\theta} \in SO(2)$ definirajmo preslikavanje $\varphi(R_{\theta}): \mathbb{R}^2 \rightarrow \mathbb{R}^2$ kao matrično množenje

$$\varphi(R_{\theta})(v) = R_{\theta}v, \quad v \in \mathbb{R}^2.$$

Preslikavanje $\varphi(R_{\theta}): \mathbb{R}^2 \rightarrow \mathbb{R}^2$ je očigledno bijekcija jer je matrica R_{θ} invertibilna. Također, $\varphi(R_{\theta})$ je homomorfizam jer je

$$\varphi(R_{\theta})(u + v) = R_{\theta}(u + v) = R_{\theta}u + R_{\theta}v = \varphi(R_{\theta})(u) + \varphi(R_{\theta})(v).$$

Stoga je $\varphi(R_\theta) \in \text{Aut}(\mathbb{R}^2)$. Nadalje,

$$\varphi(R_\theta R_\sigma)(v) = R_\theta(R_\sigma v) = \varphi(R_\theta)(\varphi(R_\sigma)(v)) = (\varphi(R_\theta) \circ \varphi(R_\sigma))(v)$$

za svaki $v \in \mathbb{R}^2$, pa zaključujemo da je preslikavanje $\varphi: SO(2) \rightarrow \text{Aut}(\mathbb{R}^2)$ također homomorfizam. Oдавde slijedi da grupa $SO(2)$ djeluje na $\mathbb{R}^2$ množenjem slijeva,

$$R_\theta \cdot v = \varphi(R_\theta)(v) = R_\theta v. \quad (1.108)$$

Koristeći djelovanje (1.108) možemo definirati poludirektni umnožak $\mathbb{R}^2 \rtimes SO(2)$ s binarnom operacijom

$$(u, R_\theta)(v, R_\sigma) = (u + R_\theta v, R_\theta R_\sigma). \quad (1.109)$$

$\mathbb{R}^2 \rtimes SO(2)$ je grupa euklidskih gibanja koja čuva orijentaciju, i označavamo je s $ISO(2)$.

Operacija (1.109) se može na vrlo zgodan način prikazati kao matrično množenje ako uređeni par (u, R_θ) uložimo u matricu trećeg reda na sljedeći način:

$$(u, R_\theta) \mapsto \begin{pmatrix} R_\theta & u \\ 0 & 1 \end{pmatrix}. \quad (1.110)$$

Lako se provjeri da operacija (1.109) odgovara umnošku matrica koje predstavljaju uređene parove (u, R_θ) i (v, R_σ) :

$$\begin{pmatrix} R_\theta & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} R_\sigma & v \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} R_\theta R_\sigma & R_\theta v + u \\ 0 & 1 \end{pmatrix}.$$

Stoga je $ISO(2)$ izomorfna matričnoj grupi

$$\left\{ \begin{pmatrix} R_\theta & v \\ 0 & 1 \end{pmatrix} \mid R_\theta \in SO(2), v \in \mathbb{R}^2 \right\}.$$

Neutralni element je jedinična matrica koja odgovara rotaciji za kut od $\theta = 0$ radijana i translaciji za nul-vektor $v = 0$. Inverzni element je dan s

$$\begin{pmatrix} R_\theta & v \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} R_\theta^{-1} & -R_\theta^{-1}v \\ 0 & 1 \end{pmatrix}.$$

Podgrupe

$$H = \left\{ \begin{pmatrix} I & v \\ 0 & 1 \end{pmatrix} \mid v \in \mathbb{R}^2 \right\}, \quad K = \left\{ \begin{pmatrix} R_\theta & 0 \\ 0 & 1 \end{pmatrix} \mid R_\theta \in SO(2) \right\}$$

su izomorfne grupama translacija $\mathbf{T}$ i rotacija $SO(2)$, redom, dok je H normalna podgrupa grupe $ISO(2)$.

1.11 Konačno generirane Ablove grupe

U proučavanju algebarskih struktura često nailazimo na sljedeći problem. Ako je zadana grupa G i podskup $A \subseteq G$, kako pronaći najmanju podgrupu od G koja sadrži skup A ? Ovaj problem smo već susreli kod cikličkih podgrupa. Ciklička podgrupa generirana elementom $x \in G$ se formira tako da se skupu $\{x\}$ dodaju sve cjelobrojne potencije elementa x . Na taj način prošireni skup postaje zatvoren na operacije množenja i invertiranja. Ovu konstrukciju ćemo sada generalizirati na proizvoljne podskupove grupe G .

Definicija 1.30. *Neka je G grupa i neka je $A \subseteq G$. Podgrupa generirana skupom A je najmanja podgrupa od G koja sadrži A . Podgrupu generiranu skupom A označavamo s $\langle A \rangle$.*

$\langle A \rangle$ je najmanja podgrupa od G koja sadrži A u sljedećem smislu: ako je H podgrupa od G takva da je $A \subseteq H$, onda je $\langle A \rangle \subseteq H$. Podgrupa $\langle A \rangle$ je presjek svih podgrupa od G koje sadrže skup A , tj.

$$\langle A \rangle = \bigcap_{\substack{H \leq G \\ A \subseteq H}} H.$$

Ako je A konačan skup $\{a_1, a_2, \dots, a_n\}$, onda pišemo

$$\langle A \rangle = \langle a_1, a_2, \dots, a_n \rangle.$$

Podgrupa $\langle A \rangle$ se tvori tako da se A proširi elementima iz G tako da $\langle A \rangle$ bude zatvoreno u odnosu na množenje i invertiranje u grupi G . Ovo proširenje mora biti minimalno u smislu gornje definicije. Na primjer, ako je $A = \{x\}$, onda skup A proširujemo svim potencijama x^k , $k \in \mathbb{Z}$, i dobivamo cikličku grupu

$$\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}.$$

U trivijalnim slučajevima kada je $A = \{e\}$ ili $A = G$ očito je $\langle e \rangle = \{e\}$ i $\langle G \rangle = G$.

Propozicija 1.8. *Neka je G grupa, i neka je A neprazan podskup od G . Tada je*

$$\langle A \rangle = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \dots a_n^{\epsilon_n} \mid n \geq 1, a_i \in A, \epsilon_i = \pm 1\}.$$

U ovoj propoziciji elementi a_i ne moraju biti nužno različiti, broj faktora u umnošku je proizvoljan, a skup A ne mora biti konačan niti čak prebrojiv.

Dokaz Definirajmo skup $H = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \dots a_n^{\epsilon_n} \mid n \geq 1, a_i \in A, \epsilon_i = \pm 1\}$. Pokažimo da je H podgrupa od G . Ako su

$$a = a_1^{\epsilon_1} a_2^{\epsilon_2} \dots a_n^{\epsilon_n} \quad \text{i} \quad b = b_1^{\delta_1} b_2^{\delta_2} \dots b_m^{\delta_m}, \quad \epsilon_i = \pm 1, \delta_i = \pm 1,$$

onda je

$$ab^{-1} = a_1^{\epsilon_1} a_2^{\epsilon_2} \dots a_n^{\epsilon_n} b_m^{-\delta_m} b_{m-1}^{-\delta_{m-1}} \dots b_1^{-\delta_1} \in H$$

jer je $-\delta_i = \pm 1$ za svaki i . Dakle, $H \leq G$. Očigledno je $A \subseteq H$ za $n = 1$ i $\epsilon_1 = 1$ što implicira $\langle A \rangle \subseteq H$. S druge strane, podgrupa $\langle A \rangle$ je zatvorena na množenje i invertiranje pa sadrži sve elemente oblika

$$a_1^{\epsilon_1} a_2^{\epsilon_2} \dots a_n^{\epsilon_n}, \quad a_i \in A, \quad n \geq 0, \quad \epsilon_i = \pm 1,$$

što implicira da je $H \subseteq \langle A \rangle$. Stoga zaključujemo da je $H = \langle A \rangle$. ■

Primijetimo da ako je G Abelova grupa i $A = \{a_1, a_2, \dots, a_n\} \subseteq G$ konačan skup, onda iz gornje propozicije slijedi da je

$$\langle A \rangle = \{a_1^{k_1} a_2^{k_2} \dots a_n^{k_n} \mid k_i \in \mathbb{Z}, \}.$$

Definicija 1.31. Kažemo da je grupa G konačno generirana ako postoji konačan podskup $A \subseteq G$ takav da je $G = \langle A \rangle$.

Svaka konačna grupa G je očito konačno generirana jer možemo uzeti $A = G$. Međutim, konačno generirana grupa ne mora biti konačna. Na primjer, $(\mathbb{Z}, +)$ je beskonačna grupa generirana brojem 1.

Definicija 1.32. *Direktni umnožak*

$$\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z} \quad (r \text{ kopija})$$

naziva se slobodna Abelova grupa ranga r .

Grupa $\mathbb{Z}^r$ je generirana elementima

$$x_i = (0, \dots, 0, 1, 0, \dots, 0), \quad i = 1, 2, \dots, r,$$

gdje se broj 1 u elementu x_i nalazi na i -tom mjestu.

Struktura konačno generiranih Abelovih grupa može se potpuno opisati sljedećim teoremom koji kazuje da je svaka takva grupa izomorfna direktnom umnošku slobodne Abelove grupe ranga $r \geq 0$ i konačnog broja cikličkih grupa $\mathbb{Z}_n$.

Teorem 1.29 (Fundamentalni teorem o konačno generiranim Abelovim grupama). *Neka je G konačno generirana Abelova grupa. Onda G ima jedinstveni rastav*

$$G \simeq \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k} \quad (1.111)$$

gdje $r, n_1, \dots, n_k$ zadovoljavaju sljedeće uvjete:

- (i) $r \geq 0$, $n_i \geq 2$ za svaki i ,
- (ii) $n_{i+1} \mid n_i$ za $1 \leq i \leq k-1$.

Definicija 1.33. Broj $r \geq 0$ naziva se slobodni rang ili Bettijev broj grupe G , a brojevi $n_1, n_2, \dots, n_k$ nazivaju se invarijantni faktori grupe G .

Relaciju (1.111) nazivamo rastav grupe G na invarijantne faktore. Uvjet (ii) implicira da invarijantni faktori tvore padajući niz

$$n_1 \geq n_2 \geq n_3 \geq \cdots \geq n_k.$$

Dvije konačno generirane Abelove grupe su izomorfne ako i samo ako imaju isti rang i invarijantne faktore. Primijetimo da je Abelova grupa G konačna ako i samo ako je $r = 0$ i u tom slučaju imamo

$$G \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$$

gdje je red grupe jednak $|G| = n_1 n_2 \dots n_k$.

Teorem 1.29 nam omogućava klasifikaciju konačnih Abelovih grupa. Ako želimo pronaći sve Abelove grupe reda n , onda se problem svodi na nalaženje svih invarijantnih faktora n_i takvih da je

- (i) $n_i \geq 2$,
- (ii) $n_{i+1} \mid n_i$,
- (iii) $n = n_1 n_2 \dots n_k$.

Ako je p prosti broj koji dijeli n , onda $p \mid n_i$ za neki $i \geq 1$. Zbog svojstva (ii) ovo implicira da $p \mid n_1$. Ovo zapažanje nam daje važno svojstvo najvećeg invarijantnog faktora n_1 :

$$\text{Svaki prosti djelitelj broja } n \text{ dijeli } n_1. \quad (1.112)$$

Posebno, ako je $n = p_1 p_2 \dots p_s$ gdje su $p_1, p_2, \dots, p_s$ različiti prosti brojevi, onda (1.112) implicira da $p_i \mid n_1$ za svaki i , pa postoji samo jedan mogući invarijantni faktor $n_1 = n$. Odavde slijedi

Korolar 1.4. *Ako je $n = p_1 p_2 \dots p_s$ umnožak različitih prostih brojeva $p_1, p_2, \dots, p_s$, onda je svaka Abelova grupa reda n izomorfna cikličkoj grupi $\mathbb{Z}_n$.*

Primjer 1.42. Prema korolaru 1.4, grupa $\mathbb{Z}_2 \times \mathbb{Z}_3$ je izomorfna grupi $\mathbb{Z}_6$ jer je $6 = 2 \cdot 3$ gdje su 2 i 3 prosti brojevi. Lako se provjeri da element $g = (\bar{1}, \bar{2}) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ ima red 6, pa g generira cikličku grupu $\mathbb{Z}_6$.

Primjer 1.43. Odredimo strukturu Abelovih grupa reda 180. Potrebno je odrediti sve invarijantne faktore n_i takve da je $180 = n_1 n_2 \dots n_k$.

- (1) U prvom koraku n se faktorizira na potencije prostih brojeva:

$$n = 2^2 \cdot 3^2 \cdot 5.$$

- (2) U drugom koraku određuje se najveći invarijantni faktor n_1 imajući na umu da svi prosti faktori broja n dijele n_1 i $n_1 \mid n$. Dakle, moguće vrijednosti za n_1 su

$$n_1 = 2 \cdot 3 \cdot 5, \quad 2^2 \cdot 3 \cdot 5, \quad 2 \cdot 3^2 \cdot 5, \quad n_1 = 2^2 \cdot 3^2 \cdot 5.$$

- (3) Treći korak se sastoji u određivanju ostalih invarijantnih faktora $n_2, n_3 \dots$ za svaku moguću vrijednost broja n_1 . Ovi invarijantni faktori imaju svojstvo da $n_2 \mid n_1$ i $n_1 n_2 \mid n$, $n_3 \mid n_2$ i $n_1 n_2 n_3 \mid n$, i tako dalje.

Invarijantni faktori	Abelove grupe
$2 \cdot 3 \cdot 5, 6$	$\mathbb{Z}_{30} \times \mathbb{Z}_6$
$2^2 \cdot 3 \cdot 5, 3$	$\mathbb{Z}_{60} \times \mathbb{Z}_3$
$2 \cdot 3^2 \cdot 5, 2$	$\mathbb{Z}_{90} \times \mathbb{Z}_2$
$2^2 \cdot 3^2 \cdot 5$	$\mathbb{Z}_{180}$

Tablica 1.7. Klasifikacija Abelovih grupa reda 180.

Na primjer, ako je $n_1 = 2 \cdot 3 \cdot 5$, onda su kandidati za n_2 dani s $n_2 = 2, 3, 6$. Ostale kombinacije djelitelja n_1 nisu dozvoljene jer u tom slučaju $n_1 n_2 \nmid n$. Ako je $n_2 = 2$, onda $n_3 \mid n_2$ implicira $n_3 = 2$. Ovo vodi na kontradikciju jer $n_1 n_2 n_3 = 2^3 \cdot 3 \cdot 5 \nmid n$. Isti zaključak vrijedi za $n_2 = 3$. Dakle, jedina mogućnost za n_2 je $n_2 = 6$. Tada je

$$6 \cdot (2 \cdot 3 \cdot 5) = 180,$$

pa su $n_1 = 2 \cdot 3 \cdot 5$ i $n_2 = 6$ invarijantni faktori koji daju rastav

$$\mathbb{Z}_{30} \times \mathbb{Z}_6.$$

Sličnim argumentima se određuju invarijantni faktori za ostale vrijednosti n_1 . Primijetimo da u posljednjem slučaju imamo $n = n_1$. Kompletan lista invarijantnih faktora s odgovarajućim rastavima dana je u tablici 1.7. $\square$

1.12 Sylowljevi teoremi

Ako je G konačna grupa, onda prema Lagrangeovom teoremu red bilo koje podgrupe od G dijeli $|G|$. Prirodno se nameće pitanje: Ako k dijeli $|G|$, da li G nužno ima podgrupu reda k ? Ako malo razmislimo, vidjet ćemo da obrat ne vrijedi. Na primjer, alternirajuća grupa A_4 koja ima 12 elemenata ne sadrži podgrupu reda 6 što se vidi iz sljedećeg razmatranja. Pretpostavimo da je H podgrupa od A_4 i $|H| = 6$. Tada je $[A_4 : H] = 2$ pa je H normalna podgrupa od A_4 prema propoziciji 1.4. Kvocijentna grupa A_4/H ima dva elementa pa je kvadrat svakog elementa u A_4/H jednak jedinici, $(gH)^2 = g^2H = H$ za svaki $g \in A_4$. Ovo povlači da je $g^2 \in H$ za svaki $g \in A_4$. Ako je $g \in A_4$ element reda 3, onda imamo $g = (g^2)^2 \in H$ pa zaključujemo da H sadrži sve elemente od A_4 reda 3. Međutim, to je kontradikcija jer A_4 ima 8 cikličkih permutacija duljine 3, odnosno 8 elemenata reda 3, dok je $|H| = 6$. Dakle, A_4 nema podgrupu reda 6. Općenito se može pokazati grupa A_n nema podgrupu reda $n!/4$ za $n \geq 5$.

Parcijalni obrat Lagrangeovog teorema ipak vrijedi u nekim posebnim slučajevima. Ovu činjenicu otkrio je L. Sylow koji je pokazao da ako p^i dijeli $|G|$ gdje je p prosti broj, onda G ima podgrupu reda p^i .



Slika 1.8. Ludwig Sylow, 1832-1918. Sylow je bio srednjoškolski profesor koji je 1872. dokazao jedan od najvažnijih rezultata u teoriji konačnih grupa.

Definicija 1.34. *Neka je G konačna grupa i neka je p prosti broj.*

- (i) *Grupa G naziva se p -grupa ako je $|G| = p^k$ za neki $k > 0$.*
- (ii) *Podgrupa od G reda p^i naziva se p -podgrupa od G .*
- (iii) *Podgrupa reda p^k , gdje je p^k najveća potencija od p koja dijeli $|G|$, naziva se Sylowljeva p -podgrupa od G .*

Primijetimo da ako je $|G| = p^k m$ gdje $p \nmid m$, onda Sylowljeva p -podgrupa ima red p^k . Skup Sylowljevih p -podgrupa od G označavamo sa $Syl_p(G)$, a broj Sylowljevih p -podgrupa s n_p .

Primjer 1.44. Grupa $\mathbb{Z}_{12}$ čiji red je $12 = 2^2 \cdot 3$ ima jednu Sylowljevu 2-podgrupu reda 4

$$\{\bar{0}, \bar{3}, \bar{6}, \bar{9}\},$$

i jednu Sylowljevu 3-podgrupu reda 3

$$\{\bar{0}, \bar{4}, \bar{8}\}.$$

□

Primjer 1.45. Simetrična grupa S_3 reda $6 = 2 \cdot 3$ ima tri Sylowljeve 2-podgrupe

$$\{(1), (12)\}, \quad \{(1), (23)\}, \quad \{(1), (13)\},$$

i jednu Sylowljevu 3-podgrupu

$$\{(1), (123), (132)\}.$$

□

Primjer 1.46. Diedralna grupa D_6 reda $12 = 2^2 \cdot 3$ je definirana s

$$D_6 = \{1, R, \dots, R^5, D, DR, \dots, DR^5 \mid R^6 = D^2 = 1, R^k D = DR^{-k}\}.$$

Grupa D_6 ima tri Sylowljeve 2-podgrupe

$$\{1, R^3, D, DR^3\}, \quad \{1, R^3, DR^5, DR^2\}, \quad \{1, R^3, DR^4, DR\},$$

i jednu Sylowljevu 3-podgrupu

$$\{1, R^2, R^4\}.$$

□

U ovim primjerima svaka grupa reda $p^k m$, gdje je p prosti broj i $p \nmid m$, ima barem jednu podgrupu reda p^k .

Teorem 1.30 (Prvi Sylowljev teorem). *Neka je G grupa reda $p^k m$ gdje je p prosti broj i $p \nmid m$. Tada G ima podgrupe reda p^i za svaki $1 \leq i \leq k$. Posebno, G ima barem jednu Sylowljevu p -podgrupu.*

Sylowljeva p -podgrupa od G je maksimalna podgrupa u smislu da je p^k najveća potencija od p koja dijeli $|G|$. Sljedeći teorem daje neka svojstva ovih grupa.

Teorem 1.31 (Drugi Sylowljev teorem).

(i) *Ako su P_1 i P_2 Sylowljeve p -podgrupe od G , onda postoji $g \in G$ takav da*

$$P_2 = gP_1g^{-1}.$$

(ii) *Broj Sylowljevih p -podgrupa je oblika $n_p = 1 + kp$ za neki $k \geq 0$, odnosno*

$$n_p \equiv 1 \pmod{p}.$$

Nadalje, n_p dijeli indeks $[G: P]$ gdje je P bilo koja Sylowljeva p -podgrupa od G .

(iii) *Bilo koja p -podgrupa od G sadržana je u nekoj Sylowljevoj p -podgrupi od G .*

Prvi dio teorema 1.31 kaže da se svaka Sylowljeva p -podgrupa može dobiti konjugacijom jedne Sylowljeve p -podgrupe. Drugim riječima, konjugacija djeluje tranzitivno na skup Sylowljevih p -podgrupa.

Neka je $|G| = p^k m$ gdje $p \nmid m$, i neka je P Sylowljeva p -podgrupa. Tada je $|P| = p^k$ pa iz Lagrangeovog teorema slijedi $[G: P] = m$. Stoga $n_p \mid m$ prema drugom dijelu teorema 1.31.

Sylowljevi teoremi su važni u klasifikaciji konačnih grupa. Zaključimo ovo poglavlje s nekim rezultatima o strukturi grupa koji su posljedica Sylowljevih teorema.

- (1) Ako je G grupa reda p^n , gdje je p prosti broj, koja sadrži točno po jednu podgrupu reda $p, p^2, \dots, p^{n-1}$, onda je G ciklička grupa.
- (2) Postoje samo dvije nekomutativne grupe reda 8:
- (a) Oktička grupa generirana elementima a i b koji zadovoljavaju relacije

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

- (b) Grupa kvaterniona generirana elementima a i b koji zadovoljavaju relacije

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

- (3) Neka je G grupa reda pq gdje su p i q prosti brojevi i $p < q$. Tada postoje najviše dvije grupe reda pq :

- (a) Ciklička grupa reda pq .
- (b) Ako $p \mid q - 1$, grupa generirana elementima a i b koji zadovoljavaju relacije

$$a^p = b^q = e, \quad a^{-1}ba = b^r$$

za neki $r \in \mathbb{Z}$ takav da je $r^p \equiv 1 \pmod{q}$ i $r \not\equiv 1 \pmod{q}$.

02

Prsteni

2.1 Osnovna svojstva prstena

Prsteni su algebarske strukture na kojima su definirane dvije binarne operacije koje nazivamo zbrajanje i množenje, i koje su povezane zakonom distributivnosti. Prototip prstena je skup cijelih brojeva $\mathbb{Z}$ sa standardnim operacijama zbrajanja i množenja. U ovom poglavlju ćemo proučiti elementarna svojstva prstena, posebno konstrukcije koje su analogne onim u teoriji grupa kao što su podprsteni, ideali (koji su analogni normalnim podgrupama), kvocijentni prsteni i homomorfizmi prstena. Kratko ćemo se osvrnuti i na pitanje multiplikativnog inverza koje prirodno vodi do konstrukcije polja.

Definicija 2.1. *Prsten je neprazan skup R s dvije binarne operacije $+$ i $\cdot$ koje nazivamo zbrajanje i množenje, i koje za svaki $a, b, c \in R$ zadovoljavaju sljedeća svojstva:*

(i) $(R, +)$ je Abelova grupa,

(ii) množenje je asocijativno:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$

(iii) množenje je distributivno u odnosu na zbrajanje s lijeva i zdesna:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Neutralni element u Abelovoj grupi $(R, +)$ označavamo s 0 , a inverzni element s $-a$. Dakle, u prstenu vrijedi

$$a + (-a) = 0 \quad \text{za svaki } a \in R.$$

Radi jednostavnosti pisanja množenje označavamo s $a \cdot b \equiv ab$.

Definicija 2.2. *Ako je množenje u prstenu R komutativno, onda R nazivamo komutativni prsten. Kažemo da je R prsten s jedinicom ako postoji element $1_R \in R$ takav da je*

$$1_R a = a 1_R = a \quad \text{za svaki } a \in R.$$

Jedinicu u prstenu R označavamo s 1_R kako bi je razlikovali od realnog broja 1. Međutim, ako nema opasnosti od zabune, jedinicu u prstenu ćemo jednostavno označiti s 1. Zanimljivo je primijetiti da je komutativnost zbrajanja u R uvjetovana zahtjevom distributivnosti množenja u R . Pretpostavimo na trenutak da $(R, +)$ nije komutativna grupa i da R ima jedinicu $1 \in R$. Tada se umnožak $(1 + 1)(a + b)$ može izračunati na dva različita načina:

$$(1 + 1)(a + b) = (1 + 1)a + (1 + 1)b = a + a + b + b, \quad (2.1)$$

$$(1 + 1)(a + b) = 1(a + b) + 1(a + b) = a + b + a + b. \quad (2.2)$$

Usporedbom (2.1) i (2.2) zaključujemo da je $a + b = b + a$ jer bismo inače imali kontradikciju. Dakle, $(R, +)$ mora biti Abelova grupa kako bi zbrajanje bilo kompatibilno s uvjetom distributivnosti.

Primjer 2.1. Neka je $(R, +)$ Abelova grupa. Ako na R definiramo množenje s $ab = 0$ za svaki $a, b \in R$, onda dobivamo trivijalni prsten. Trivijalni prsten nema jedinicu osim ako je $R = \{0\}$. U tom je slučaju $1 = 0$. $\square$

Primjer 2.2. Standardni primjeri prstena s jedinicom su skupovi brojeva $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$ sa standardnim operacijama zbrajanja i množenja. $\square$

Primjer 2.3. Neka je $M(n, \mathbb{F})$ skup kvadratnih matrica reda n nad $\mathbb{F} = \mathbb{R}$ ili $\mathbb{C}$. $M(n, \mathbb{F})$ je prsten s operacijama matričnog zbrajanja i množenja. Nula u prstenu je nul matrica, a jedinica je jedinična matrica. $\square$

Primjer 2.4. Skup 2×2 matrica nad poljem $\mathbb{F}$ definiran sa

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{F} \right\} \quad (2.3)$$

je nekomutativni prsten. Primijetimo da R nema jedinicu. Pretpostavimo da postoji $\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \in R$ takav da je

$$\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \quad (2.4)$$

za sve $a, b \in \mathbb{F}$. Jednadžba (2.4) implicira $ax = a$, $ay = b$ i $xb = b$ što vodi na kontradikciju ako je $a = 0$ i $b \neq 0$. Jedinična matrica $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ je jedinica u prstenu $M(2, \mathbb{F})$, ali $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin R$. $\square$

Primjer 2.5. Sa $\mathbb{R}[x]$ označimo skup polinoma s realnim koeficijentima

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \quad a_i \in \mathbb{R}.$$

Standardne operacije zbrajanja i množenja polinoma zadovoljavaju aksiome prstena. Nula u $\mathbb{R}[x]$ je nul polinom $\mathbf{0}(x) = 0$, a jedinica je konstantni polinom $\mathbf{1}(x) = 1$. Svojstva polinoma s koeficijentima u proizvoljnom prstenu ćemo detaljnije proučiti u poglavlju 2.10. $\square$

Primjer 2.6. Skup neprekidnih funkcija $f: [a, b] \rightarrow \mathbb{R}$ je prsten sa zbrajanjem i množenjem po točkama:

$$(f + g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x) \quad x \in [a, b].$$

Jedinica u prstenu je konstantna funkcija

$$\mathbf{1}(x) = 1 \quad \text{za svaki } x \in [a, b].$$

Ovaj prsten označavamo s $C[a, b]$. $\square$

Primjer 2.7. Promotrimo Abelovu grupu $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$. Množenje u $\mathbb{Z}_n$ definirano kao

$$\bar{x} \cdot \bar{y} = \overline{xy},$$

zadovoljava aksiome prstena. $\mathbb{Z}_n$ je prsten s jedinicom $\bar{1}$ koji ima konačno mnogo elemenata. $\square$

Elementarna svojstva prstena dana su sljedećim teoremom.

Teorem 2.1. *Neka je R prsten. Tada za svaki $a, b, c \in R$ vrijedi*

$$(i) \quad a0 = 0a = 0,$$

$$(ii) \quad a(-b) = -(ab) = (-a)b,$$

$$(iii) \quad a(b - c) = ab - ac, \quad (a - b)c = ac - bc.$$

Dokaz

(i) Iz distribucije množenja slijedi

$$a0 = a(0 + 0) = a0 + a0,$$

što prema definiciji neutralnog elementa implicira $a0 = 0$. Slično se pokazuje da je $0a = 0$.

(ii) Distributivnost množenja daje

$$0 = a0 = a(b + (-b)) = ab + a(-b),$$

pa iz definicije inverznog elementa slijedi

$$a(-b) = -(ab).$$

Slično se pokazuje relacija $-(ab) = (-a)b$.

(iii) Koristeći svojstvo (ii) dobivamo

$$a(b - c) = a(b + (-c)) = ab + a(-c) = ab - ac,$$

i slično

$$(a - b)c = (a + (-b))c = ac + (-b)c = ac - bc.$$



Množenje u prstenu je asocijativno pa umnožak elemenata a_1, a_2 i a_3 jednostavno zapisujemo kao $a_1 a_2 a_3$ jer nije važno kako grupiramo elemente. Isto vrijedi za umnožak elemenata $a_1, a_2, \dots, a_n$ koji zapisujemo kao

$$\prod_{i=1}^n a_i = a_1 a_2 \dots a_n.$$

Također, zbog asocijativnosti zbrajanja suma elemenata $a_1, a_2, \dots, a_n$ se zapisuje kao

$$\sum_{i=1}^n a_i = a_1 + a_2 + \dots + a_n.$$

Sljedeća propozicija daje generalizaciju aksioma o distributivnosti, i lako se dokazuje indukcijom po n i m .

Propozicija 2.1. *Neka je R prsten, i neka su $a_i, b_j \in R$, $1 \leq i \leq n$, $1 \leq j \leq m$. Tada je*

$$\left(\sum_{i=1}^n a_i \right) \left(\sum_{j=1}^m b_j \right) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j.$$

Ako je $a \in R$ i $m \in \mathbb{N}$, onda definiramo

$$\begin{aligned} a^m &= \underbrace{a a \dots a}_{m \text{ puta}}, & ma &= \underbrace{a + a + \dots + a}_{m \text{ puta}}, \\ a^{-m} &= (a^{-1})^m & \text{ako } a \text{ ima multiplikativni inverz } a^{-1}, \\ -ma &= \underbrace{(-a) + (-a) + \dots + (-a)}_{m \text{ puta}}. \end{aligned}$$

Ako R ima jedinicu, onda definiramo $a^0 = 1$. Iz ovih definicija indukcijom se lako pokazuje sljedeći teorem.

Teorem 2.2. *Neka je R prsten, i neka su $a, b \in R$. Tada za svaki $n, m \in \mathbb{N}$ vrijedi*

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

$$(ii) \quad (a^m)^n = a^{mn}.$$

Također, za svaki $n, m \in \mathbb{Z}$ imamo

$$(i) \quad ma + na = (m + n)a,$$

$$(ii) \quad m(na) = (mn)a,$$

$$(iii) \quad (ma)(nb) = (mn)(ab) = (na)(mb).$$

2.2 Vrste prstena

S obzirom na svojstva množenja, razlikujemo nekoliko vrsta prstena.

Definicija 2.3. *Neka je R prsten s jedinicom gdje je $1 \neq 0$. Ako svaki element $a \in R$, $a \neq 0$, ima multiplikativni inverz u R , onda R nazivamo prsten s dijeljenjem. Komutativni prsten s dijeljenjem nazivamo polje.*

Ako je R prsten s jedinicom, onda skup invertibilnih elemenata tvori multiplikativnu grupu R^* . Na primjer, u prstenu cijelih brojeva je $\mathbb{Z}^* = \{1, -1\}$. U prstenu s dijeljenjem multiplikativna grupa jednaka je $R^* = R \setminus \{0\}$.

Standardni primjeri prstena s dijeljenjem (odnosno polja) su prsteni brojeva $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$. Primijetimo da $\mathbb{Z}$ nije prsten s dijeljenjem jer cijeli brojevi osim 1 i -1 nemaju multiplikativni inverz u $\mathbb{Z}$. Prsten matrica $M(n, \mathbb{R})$ nije prsten s dijeljenjem jer matrica $A \neq 0$ ne mora nužno imati inverz. Na primjer,

$$A = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, \quad a, b \neq 0,$$

nije nul-matrica, ali A^{-1} ne postoji jer je $\det(A) = 0$.

Definicija 2.4. *Prsten R nazivamo integralna domena ako $xy = 0$, $x, y \in R$, povlači $x = 0$ ili $y = 0$.*

Ako je R prsten s dijeljenjem, onda je R integralna domena. Posebno, svako polje je integralna domena. Ako je R integralna domena i $x, y \in R \setminus \{0\}$, onda je $xy \neq 0$. Napomenimo da neki autori definiraju integralnu domenu kao komutativni prsten s jedinicom koji zadovoljava definiciju 2.4.

Prsten cijelih brojeva $\mathbb{Z}$ je očigledno integralna domena. Lako se pokazuje da je prsten Gaussovih cijelih brojeva

$$\mathbb{Z}[i] = \left\{ m + in \mid m, n \in \mathbb{Z}, i = \sqrt{-1} \right\}$$

također integralna domena.

Primjer 2.8. Promotrimo prsten neprekidnih funkcija $C[0, 1]$. Definirajmo

$$f(x) = \begin{cases} 0, & 0 \leq x \leq \frac{1}{2}, \\ x - \frac{1}{2}, & \frac{1}{2} < x \leq 1, \end{cases}$$

$$g(x) = \begin{cases} -x + \frac{1}{2}, & 0 \leq x \leq \frac{1}{2}, \\ 0, & \frac{1}{2} < x \leq 1. \end{cases}$$

Tada su $f, g \in C[0, 1]$ i $f \neq 0, g \neq 0$. Međutim, $f(x)g(x) = 0$ za svaki $x \in [0, 1]$, odnosno $fg = 0$, pa zaključujemo da $C[0, 1]$ nije integralna domena. $\square$

Prsten $\mathbb{Z}$ je komutativna integralna domena s jedinicom, ali nije polje jer za $n \in \mathbb{Z} \setminus \{0, 1, -1\}$ vrijedi $n^{-1} = \frac{1}{n} \notin \mathbb{Z}$. Međutim, parcijalni obrat vrijedi u sljedećem slučaju.

Propozicija 2.2. *Neka je R komutativna integralna domena s jedinicom. Ako je R konačan skup, onda je R polje.*

Dokaz Odaberimo $a \in R, a \neq 0$, i definirajmo preslikavanje $\varphi: R \rightarrow R$ s $\varphi(x) = ax$. Pokažimo da je φ injekcija. Ako je $ax = ay$, onda je $a(x - y) = 0$ što implicira da je $x - y = 0$ jer je R integralna domena i $a \neq 0$. Dakle, $x = y$. Injektivnost implicira da je $\varphi: R \rightarrow R$ surjekcija jer je R konačan skup. Odavde slijedi da za $1 \in R$ postoji jedinstveni $b \in R$ takav da je $\varphi(b) = 1$, odnosno $ab = ba = 1$. Time je dokazano da svaki element $a \neq 0$ ima multiplikativni inverz. Stoga je R polje. $\blacksquare$

Definicija 2.5. *Neka je R prsten. Element $x \in R$ naziva se lijevi djelitelj nule ako postoji $y \in R, y \neq 0$, takav da je $xy = 0$. Slično se definira desni djelitelj nule. Ako je x lijevi i desni djelitelj nule, onda se x naziva djelitelj nule.*

Očito je $0 \in R$ trivijalni djelitelj nule u svakom prstenu R . Primijetimo da je R integralna domena ako i samo ako je $0 \in R$ jedini djelitelj nule u R . Primjeri prstena s netrivialnim djeliteljima nule su $M(n, \mathbb{R})$ za $n \geq 2$ i $\mathbb{Z}_m$ gdje je m složeni broj.

Neka su

$$A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix}, \quad a, b \neq 0,$$

matrice u prstenu $M(2, \mathbb{R})$. Tada je $AB = 0$ što povlači da je A lijevi djelitelj, a B desni djelitelj nule u $M(2, \mathbb{R})$.

Netrivialni djelitelji nule u prstenu $\mathbb{Z}_n$ su elementi $\bar{a} \in \mathbb{Z}_n, \bar{a} \neq \bar{0}$, takvi da je najveći zajednički djelitelj $\text{nzd}(a, n) > 1$. Neka je $d = \text{nzd}(a, n) > 1$. Onda je $n = bd$ i $a = cd$ za neki $b \in \mathbb{N}$ i $c \in \mathbb{Z}$. Kako je $d > 1$ imamo $0 < b < n$, stoga je $\bar{b} \neq \bar{0}$. Nadalje, $ab = cdb = cn$ što implicira da je $\bar{a}\bar{b} = \overline{ab} = \bar{0}$. Dakle, $\bar{a}$ je djelitelj nule jer je $\bar{b} \neq \bar{0}$. Na primjer, djelitelji nule u prstenu $\mathbb{Z}_6$ su $\bar{2}, \bar{3}$ i $\bar{4}$ jer 2, 3 i 4 nisu relativno prosti u odnosu na 6.

Definirajmo još nekoliko korisnih pojmova u teoriji prstena.

Definicija 2.6. *Neka je R prsten. Za element $a \in R$ kažemo da je nilpotentan ako postoji $n \in \mathbb{N}$ takav da je $a^n = 0$.*

Neutralni element $0 \in R$ je očigledno nilpotentan. Matrica

$$A = \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}, \quad x \in \mathbb{R},$$

je nilpotentan element u prstenu $M(2, \mathbb{R})$ jer je

$$A^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Ako je R integralna domena, onda R ne sadrži nilpotentne elemente $a \neq 0$. Doista, ako je $a \neq 0$ nilpotentan, onda jednakost $a^n = aa^{n-1} = 0$ implicira $a^{n-1} = 0$. Iteracijom po n zaključujemo da je $a = 0$, što je kontradikcija. Dakle, jedini nilpotentni element u integralnoj domeni je $0 \in R$.

Definicija 2.7. Neka je R prsten. Kažemo da je element $a \in R$ idempotentan ako je $a^2 = a$.

Očito je da su 0 i 1 idempotentni elementi u svakom prstenu R (ako R ima jedinicu). Za matricu

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \in M(2, \mathbb{R})$$

vrijedi $A^2 = A$, stoga je A idempotentan element u $M(2, \mathbb{R})$.

2.3 Podprsten i karakteristika prstena

Definicija 2.8. Neka je $(R, +, \cdot)$ prsten, i neka je $S \subseteq R$ neprazan podskup. Ako je $(S, +, \cdot)$ prsten, onda S nazivamo podprsten od R .

Binarne operacije u S su iste kao u R . Slično se definira podpolje nekog polja. Svaki prsten R ima trivijalne podprstene: $\{0\}$ i R .

Propozicija 2.3. Neka je R prsten. Neprazan podskup $S \subseteq R$ je podprsten od R ako za svaki $a, b \in S$ vrijedi $a - b \in S$ i $ab \in S$.

Dokaz Ako je $a - b \in S$ za svaki $a, b \in S$, onda je $(S, +)$ aditivna podgrupa grupe $(R, +)$. Nadalje, ako je $ab \in S$ za svaki $a, b \in S$, onda je S zatvoren na množenje, dok se asocijativnost i distributivnost množenja naslijeđuju iz R . ■

Lako se pokazuje da je presjek konačnog broja podprstena od R također podprsten od R .

Definicija 2.9. *Neka je R prsten. Skup*

$$Z(R) = \{a \in R \mid xa = ax \text{ za svaki } x \in R\}$$

naziva se centar prstena R .

Centar $Z(R)$ je neprazan skup jer je $0 \in Z(R)$.

Teorem 2.3. *Centar prstena je podprsten.*

Dokaz Neka su $a, b \in Z(R)$ i $x \in R$. Tada je

$$(a - b)x = ax - bx = xa - xb = x(a - b),$$

što pokazuje da je $a - b \in Z(R)$. Nadalje,

$$(ab)x = a(bx) = a(xb) = (ax)b = x(ab),$$

pa slijedi da je $ab \in Z(R)$. Prema propoziciji 2.3, $Z(R)$ je podprsten od R . ■

Definicija 2.10. *Neka je R prsten. Pretpostavimo da postoji $n \in \mathbb{N}$ takav da je $na = 0$ za svaki $a \in R$. Najmanji takav prirodni broj naziva se karakteristika prstena R . Ako takav broj ne postoji, onda kažemo da R ima karakteristiku nula.*

Karakteristiku prstena R označavamo s $\text{char}(R)$. Očigledno je da prsten cijelih brojeva ima karakteristiku $\text{char}(\mathbb{Z}) = 0$.

Primjer 2.9. Pokažimo da je karakteristika prstena $\mathbb{Z}_n$ jednaka n . Ako je $n = 1$, onda je $\mathbb{Z}_1 = \{\bar{0}\}$ i trivijalno vrijedi $1 \cdot \bar{0} = \bar{0}$ pa je $\text{char}(\mathbb{Z}_1) = 1$. Neka je $n \geq 2$. Onda za svaki $\bar{k} \in \mathbb{Z}_n$ imamo

$$n\bar{k} = \underbrace{\bar{k} + \bar{k} + \cdots + \bar{k}}_{n \text{ puta}} = \overline{nk} = \overline{n\bar{k}} = \bar{0}$$

jer je $\overline{n\bar{k}} = \bar{0}$. Tvrdimo da je n najmanji prirodni broj sa svojstvom $n\bar{k} = \bar{0}$ za svaki $\bar{k} \in \mathbb{Z}_n$. Pretpostavimo da postoji $1 \leq m < n$ takav da je $m\bar{k} = \bar{0}$ za svaki $\bar{k} \in \mathbb{Z}_n$. Tada za $k = 1$ dobivamo

$$m\bar{1} = \underbrace{\bar{1} + \bar{1} + \cdots + \bar{1}}_{m \text{ puta}} = \overline{m} = \bar{0},$$

što implicira $m = pn$ za neki $p \geq 1$. Ovo vodi na kontradikciju jer je $m < n$. Dakle, $m = n$.

□

Teorem 2.4. *Neka je F polje. Tada je $\text{char}(F)$ nula ili prost broj.*

Dokaz Pretpostavimo da je $n \neq 0$ karakteristika polja F . Onda je $n 1_F = 0_F$ gdje su 0_F i 1_F nula i jedinica u polju F . Ako n nije prosti broj, onda se n može faktorizirati kao $n = n_1 n_2$ gdje je $1 < n_1 < n$ i $1 < n_2 < n$. Sada $(n_1 n_2) 1_F = 0_F$ implicira $(n_1 1_F)(n_2 1_F) = 0_F$ što daje $n_1 1_F = 0_F$ ili $n_2 1_F = 0_F$ jer je F integralna domena. Ovo dalje implicira $n_1 a = 0$ ili $n_2 a = 0$ za svaki $a \in F$, čime dobivamo kontradikciju jer su $n_1, n_2 < n$. Zaključujemo da n nije složen, odnosno da je n prosti broj. ■

Primjer 2.10. Polja $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ imaju karakteristiku nula. □

Primjer 2.11. Prsten $\mathbb{Z}_p$, gdje je p prosti broj, je polje karakteristike p . $\mathbb{Z}_p$ je komutativni prsten s jedinicom $\bar{1}$ pa je dovoljno pokazati da svaki $\bar{a} \in \mathbb{Z}_p$, $\bar{a} \neq \bar{0}$, ima multiplikativni inverz u $\mathbb{Z}_p$. Ako je $0 < a < p$, onda je najveći zajednički djelitelj brojeva a i p jednak 1. Stoga postoje $m, n \in \mathbb{Z}$ takvi da je

$$ma + np = 1. \quad (2.5)$$

Odavde slijedi da je

$$\bar{m}\bar{a} + \bar{n}\bar{p} = \bar{m}\bar{a} = \bar{1} \quad (2.6)$$

jer je $\bar{p} = \bar{0}$. Stoga je $\bar{m}\bar{a} = \bar{a}\bar{m} = \bar{1}$, odnosno $\bar{a}^{-1} = \bar{m}$, gdje m možemo odabrati tako da je $0 < m < p$. Prema primjeru 2.9 je $\text{char}(\mathbb{Z}_p) = p$ pa je $\mathbb{Z}_p$ polje karakteristike p . □

2.4 Prsten kvaterniona

1843. godine irski matematičar W.R. Hamilton konstruirao je prvi primjer nekomutativnog prstena s dijeljenjem. Elemente tog prstena nazvao je kvaternioni jer su definirani pomoću četiri realna broja. Kvaternioni nalaze široku primjenu u matematici, fizici i tehnici. Na primjer, kvaternionima se opisuju prostorne rotacije pa se stoga primjenjuju u 3D računalnoj grafici, teorijskoj mehanici i teoriji kontrole. Interesantno je spomenuti da se položaj svemirskih satelita u orbiti kontrolira pomoću kvaterniona. Kvaternioni su imali važan utjecaj na razvoj algebre jer su doveli do istraživanja drugih “hiperkompleksnih” brojevnih sustava.

U ovom odjeljku ćemo konstruirati kvaternione promatrajući kompleksne matrice

$$A = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}, \quad a, b \in \mathbb{C}, \quad (2.7)$$

gdje $\bar{a}$ označava konjugaciju broja a . Neka je $\mathbb{H}$ skup svih matrica oblika (2.7). Pokažimo da je $\mathbb{H}$ podprsten prstena $M(2, \mathbb{C})$. Ako su $A_1, A_2 \in \mathbb{H}$, onda je

$$A_1 - A_2 = \begin{pmatrix} a_1 & b_1 \\ -\bar{b}_1 & \bar{a}_1 \end{pmatrix} - \begin{pmatrix} a_2 & b_2 \\ -\bar{b}_2 & \bar{a}_2 \end{pmatrix} = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ -(\bar{b}_1 - \bar{b}_2) & \bar{a}_1 - \bar{a}_2 \end{pmatrix} \in \mathbb{H}.$$



Slika 2.1. William Rowan Hamilton, 1805-1865. Hamilton je otkrio kvaternione 1843. godine, što je primjer prve nekomutativne algebre.

Također,

$$A_1 A_2 = \begin{pmatrix} a_1 & b_1 \\ -\bar{b}_1 & \bar{a}_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ -\bar{b}_2 & \bar{a}_2 \end{pmatrix} = \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}$$

gdje je $u = a_1 a_2 - b_1 \bar{b}_2$ i $v = a_1 b_2 + b_1 \bar{a}_2$, pa je $\mathbb{H}$ zatvoren na množenje. Prema propoziciji 2.3, $\mathbb{H}$ je podprsten od $M(2, \mathbb{C})$.

Pokažimo sada da je $\mathbb{H}$ prsten s dijeljenjem. Neka je $A \in \mathbb{H}$, $A \neq 0$. Tada je $a \neq 0$ ili $b \neq 0$, što povlači da je $\det(A) = |a|^2 + |b|^2 > 0$. Dakle, matrica A je invertibilna i vrijedi

$$A^{-1} = \frac{1}{|a|^2 + |b|^2} \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix}.$$

Primijetimo da je A^{-1} također matrica oblika (2.7) jer je $a = \bar{\bar{a}}$ i $b = -(-b)$, pa zaključujemo da je $A^{-1} \in \mathbb{H}$. Time je dokazano da je $\mathbb{H}$ prsten s dijeljenjem.

Ako kompleksne brojeve a i b rastavimo na realni i imaginarni dio, $a = \alpha_1 + i\alpha_2$ i $b = \beta_1 + i\beta_2$, onda matricu A možemo napisati kao zbroj

$$A = \alpha_1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \alpha_2 \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + \beta_1 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + \beta_2 \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Definirajmo matrice

$$\mathbf{e} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Ove matrice zadovoljavaju tablicu množenja 2.1. Stoga se umnožak u prstenu $\mathbb{H}$ može računati korištenjem tablice 2.1 i distribucije matričnog množenja. Ovo motivira sljedeću definiciju.

$\cdot$	$\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$\mathbf{e}$	$\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$\mathbf{i}$	$\mathbf{i}$	$-\mathbf{e}$	$\mathbf{k}$	$-\mathbf{j}$
$\mathbf{j}$	$\mathbf{j}$	$-\mathbf{k}$	$-\mathbf{e}$	$\mathbf{i}$
$\mathbf{k}$	$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{i}$	$-\mathbf{e}$

Tablica 2.1. Tablica množenja kvaterniona

Definicija 2.11. Brojevi oblika

$$x = a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}, \quad a, b, c, d \in \mathbb{R}, \quad (2.8)$$

gdje simboli $\mathbf{e}$, $\mathbf{i}$, $\mathbf{j}$ i $\mathbf{k}$ zadovoljavaju tablicu množenja 2.1 nazivaju se realni kvaternioni.

Zbroj dvaju kvaterniona x_1 i x_2 je dan sa

$$x_1 + x_2 = (a_1 + a_2)\mathbf{e} + (b_1 + b_2)\mathbf{i} + (c_1 + c_2)\mathbf{j} + (d_1 + d_2)\mathbf{k}.$$

Umnožak

$$x_1 x_2 = (a_1\mathbf{e} + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k})(a_2\mathbf{e} + b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k})$$

se računa primjenom tablice 2.1 i distributivnosti množenja. Na primjer, ako su $x_1 = 2\mathbf{e} + \mathbf{i} - \mathbf{k}$ i $x_2 = -2\mathbf{j} + \mathbf{k}$, onda je

$$\begin{aligned} x_1 x_2 &= (2\mathbf{e} + \mathbf{i} - \mathbf{k})(-2\mathbf{j} + \mathbf{k}) \\ &= -4\mathbf{e}\mathbf{j} - 2\mathbf{i}\mathbf{j} + 2\mathbf{k}\mathbf{j} + 2\mathbf{e}\mathbf{k} + \mathbf{i}\mathbf{k} - \mathbf{k}^2 \\ &= -4\mathbf{j} - 2\mathbf{k} - 2\mathbf{i} + 2\mathbf{k} - \mathbf{j} + \mathbf{e} \\ &= \mathbf{e} - 2\mathbf{i} - 5\mathbf{j}. \end{aligned}$$

Nula u prstenu je

$$0 = 0\mathbf{e} + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}, \quad (2.9)$$

a jedinica je

$$1 = 1\mathbf{e} + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}. \quad (2.10)$$

Inverz kvaterniona jednak je

$$(a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})^{-1} = \frac{a\mathbf{e} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}}{a^2 + b^2 + c^2 + d^2}$$

uz uvjet da je barem jedan od brojeva a , b , c ili d različit od nule. Primijetimo da prsten kvaterniona $\mathbb{H}$ sadrži podprstene $\mathbb{R}$ i $\mathbb{C}$ jer realne i kompleksne brojeve možemo identificirati s kvaternionima kao

$$a \equiv a\mathbf{e}, \quad a + ib \equiv a\mathbf{e} + b\mathbf{i}.$$

Dakle, $\mathbb{H}$ predstavlja proširenje polja kompleksnih brojeva $\mathbb{C}$, ali množenje u proširenom prstenu $\mathbb{H}$ nije komutativno.

2.5 Prsten matrica

Pojam matrice nad poljem realnih ili kompleksnih brojeva se može proširiti na proizvoljan prsten. Neka je A matrica reda n s elementima u nekom prstenu R ,

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}, \quad a_{ij} \in R, \quad 1 \leq i, j \leq n.$$

Matricu kraće označavamo s $A = (a_{ij})$ gdje je a_{ij} element matrice A u i -tom retku i j -tom stupcu. Prsten matrica $M(n, R)$ je skup matrica reda n na kojem zbrajanje i množenje definiramo na standardni način:

$$A + B = (a_{ij} + b_{ij}), \quad (2.11)$$

$$AB = \left(\sum_{k=1}^n a_{ik} b_{kj} \right). \quad (2.12)$$

Lako se pokazuje da zbrajanje i množenje definirano s (2.11) i (2.12) zadovoljava aksiome prstena. Nula u prstenu $M(n, R)$ je nul matrica čiji su svi elementi $0 \in R$. Ako R ima jedinicu $1 \in R$, onda je jedinica u prstenu $M(n, R)$ jedinična matrica

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

U tom slučaju svaku matricu A možemo napisati kao linearnu kombinaciju s koeficijentima u R ,

$$A = \sum_{i,j=1}^n a_{ij} E_{ij},$$

gdje matrica E_{ij} ima u i -tom retku i j -tom stupcu jedinicu a na ostalim mjestima nulu. Za umnožak matrica E_{ij} vrijedi pravilo

$$E_{ij} E_{kl} = \delta_{jk} E_{il} \quad (2.13)$$

gdje je δ_{jk} Kroneckerov delta simbol

$$\delta_{jk} = \begin{cases} 1, & j = k, \\ 0, & j \neq k. \end{cases}$$

Matrice E_{ii} su idempotentne jer je $E_{ii}^2 = E_{ii}$ za svaki $i = 1, 2, \dots, n$. Ako je $n > 1$, onda prema pravilu (2.13) imamo

$$\begin{aligned} E_{11} E_{12} &= \delta_{11} E_{12} = E_{12}, \\ E_{12} E_{11} &= \delta_{21} E_{11} = 0. \end{aligned}$$

Stoga je $M(n, R)$ nekomutativni prsten za $n > 1$.

Pretpostavimo da je R komutativni prsten s jedinicom. U tom slučaju standardni rezultati iz linearne algebre analogno vrijede i u prstenu $M(n, R)$. Posebice, možemo definirati determinantu matrice kao

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

gdje se suma uzima po svim permutacijama skupa $\{1, 2, \dots, n\}$, a $\operatorname{sgn}(\sigma)$ je predznak permutacije σ . Za determinantu vrijedi Binet-Cauchyeva formula

$$\det(AB) = \det(A)\det(B) \quad \text{za svaki } A, B \in M(n, R). \quad (2.14)$$

Prisjetimo se da je kofaktor elementa a_{ij} definiran s

$$A_{ij} = (-1)^{i+j} \Delta_{ij},$$

gdje je Δ_{ij} subdeterminanta matrice A koja se dobije tako da se iz A izbriše i -ti redak i j -ti stupac. Adjunkta matrice A je matrica $\tilde{A} = (\alpha_{ij})$ gdje je $\alpha_{ij} = A_{ji}$. Za svaku matricu $A \in M(n, R)$ vrijedi

$$\tilde{A}A = A\tilde{A} = \det(A)I \quad (2.15)$$

gdje je $I \in M(n, R)$ jedinična matrica.

Teorem 2.5. *Neka je R komutativni prsten s jedinicom. Tada je $A \in M(n, R)$ invertibilna matrica ako i samo ako je $\det(A)$ invertibilna u R .*

Dokaz Neka je A invertibilna matrica. Tada postoji $A^{-1} \in M(n, R)$ takva da je $AA^{-1} = A^{-1}A = I$. Iz jednadžbe (2.14) dobivamo

$$\det(A)\det(A^{-1}) = \det(A^{-1})\det(A) = \det(I) = 1,$$

što pokazuje da je $\det(A)$ invertibilna u R . Pretpostavimo sada da je $\Delta = \det(A)$ invertibilna u R , odnosno da postoji $\Delta^{-1} \in R$ takav da je $\Delta\Delta^{-1} = \Delta^{-1}\Delta = 1$. Kako je R komutativni prsten, za svaki $a \in R$ i $B \in M(n, R)$ vrijedi $aB = Ba$. Množenjem jednadžbe (2.15) s Δ^{-1} i koristeći svojstvo komutativnosti u prstenu R dobivamo

$$(\Delta^{-1}\tilde{A})A = A(\Delta^{-1}\tilde{A}) = I.$$

Oдавде slijedi da je A invertibilna matrica i da je

$$A^{-1} = \Delta^{-1}\tilde{A}.$$

■

Kako svi elementi nekog polja koji su različiti od nule imaju multiplikativni inverz, poseban slučaj ovog teorema je

Korolar 2.1. *Neka je F polje. Tada je $A \in M(n, F)$ invertibilna ako i samo ako je $\det(A) \neq 0$.*

2.6 Prsten grupe

Neka je R prsten s jedinicom $1 \neq 0$ i neka je $G = \{g_1, g_2, \dots, g_n\}$ konačna grupa. Označimo s $R[G]$ skup svih formalnih suma

$$a_1g_1 + a_2g_2 + \dots + a_ng_n, \quad a_i \in R, \quad g_i \in G.$$

Ako je $g_1 = e$ neutralni element u G , onda kraće pišemo $ag_1 = a$ za $a \in R$, i slično $1g_i = g_i$. Zbrajanje u $R[G]$ se definira po komponentama, tj.

$$\sum_{i=1}^n a_i g_i + \sum_{i=1}^n b_i g_i = \sum_{i=1}^n (a_i + b_i) g_i.$$

Množenje se definira tako da prvo definiramo

$$(ag_i)(bg_j) = (ab)g_k \tag{2.16}$$

gdje je $g_k = g_i g_j$, a zatim (2.16) proširimo na formalne sume koristeći distributivnost. Ako je

$$\left(\sum_{i=1}^n a_i g_i \right) \left(\sum_{j=1}^n b_j g_j \right) = \sum_{k=1}^n c_k g_k,$$

onda je koeficijent elementa g_k jednak

$$c_k = \sum_{g_i g_j = g_k} a_i b_j.$$

Ovako definirano zbrajanje i množenje u $R[G]$ zadovoljava svojstva prstena. Asocijativnost množenja u $R[G]$ se naslijeđuje od asocijativnosti množenja u R i G . Nadalje, element $1e = 1$ je jedinica u $R[G]$. Time skup $R[G]$ dobiva strukturu prstena s jedinicom kojeg nazivamo prsten grupe.

Primjer 2.12. Promotrimo diedralnu grupu

$$D_4 = \langle R, D \mid R^4 = D^2 = 1, R^k D = D R^{-k} \rangle$$

i prsten $\mathbb{Z}$. Neka su $x = 2R^2 - 3D$ i $y = R + 2DR^3$. Tada je

$$\begin{aligned} xy &= (2R^2 - 3D)(R + 2DR^3) \\ &= 2R^3 - 3DR + 4R^2DR^3 - 6D^2R^3 \\ &= 2R^3 - 3DR + 4DR^{-2}R^3 - 6R^3 = -4R^3 + DR. \end{aligned}$$

Ako je R komutativni prsten i G Abelova grupa, onda je prsten $R[G]$ komutativan. Preslikavanjem $a \mapsto ae$ s R u RG dobivamo ulaganje prstena R u prsten $R[G]$. Slično, preslikavanje $g \mapsto 1g$ s G u RG predstavlja ulaganje grupe G u prsten $R[G]$. Stoga $R[G]$ sadrži kopije prstena R i grupe G . $\square$

Interesantno je primijetiti da ako je G konačna grupa i $|G| > 1$, onda $R[G]$ ima djelitelje nule. Neka je $g \in G$, $g \neq e$ element reda $m > 1$. Po definiciji prstena grupe, formalne sume $e - g$ i $e + g + g^2 + \cdots + g^{m-1}$ nisu nula. Međutim

$$(e - g)(e + g + g^2 + \cdots + g^{m-1}) = e - g^m = 0,$$

što pokazuje da je $e - g$ djelitelj nule u $R[G]$.

2.7 Ideali i kvocijentni prsten

Koncept ideala u prstenu je analogan normalnoj podgrupi. Kvocijentni prsteni se tvore na sličan način kao kvocijentne grupe, a veza između ideala i homomorfizama prstena je analogna vezi između normalnih podgrupa i homomorfizama grupa.

Definicija 2.12. *Neprazan podskup I prstena R naziva se ideal ako vrijedi*

- (i) $a - b \in I$ za svaki $a, b \in I$,
- (ii) $ra \in I$ i $ar \in I$ za svaki $a \in I$, $r \in R$.

Ako umjesto svojstva (ii) vrijedi $ra \in I$ za svaki $a \in I$, $r \in R$, onda I nazivamo lijevi ideal prstena R . Slično definiramo desni ideal u R . Ideal je lijevi i desni ideal, pa se ponekad naziva dvostrani ideal. Ako je R komutativni prsten, onda je svaki ideal u R dvostran. Svaki ideal je podprsten jer je I Abelova podgrupa od R prema svojstvu (i), a iz svojstva (ii) slijedi da je I zatvoren na množenje u R . Međutim, podprsten nije nužno ideal jer ne mora vrijediti svojstvo (ii). Svaki prsten R ima trivijalne ideale $\{0\}$ i R .

Primjer 2.13. Svaki podprsten u prstenu cijelih brojeva $\mathbb{Z}$ je ideal. Neka je $S \subseteq \mathbb{Z}$ podprsten. Ako je $r \in \mathbb{Z}$ i $a \in S$, onda je

$$ra = \begin{cases} \underbrace{a + a + \cdots + a}_r, & r > 0, \\ 0, & r = 0, \\ \underbrace{-a - a - \cdots - a}_{|r|}, & r < 0. \end{cases}$$

U svakom slučaju je $ra \in S$ jer je S aditivna podgrupa od $\mathbb{Z}$. Stoga je S ideal u $\mathbb{Z}$. $\square$

Primjer 2.14. Neka je R prsten gornje-trokutastih kvadratnih matrica reda 2 nad poljem $\mathbb{R}$. Tada je podskup

$$I = \left\{ \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R} \right\}$$

ideal u R . Doista, I je očito aditivna podgrupa od R . Za svaku matricu $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in R$ imamo

$$\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & xa \\ 0 & 0 \end{pmatrix} \in I,$$

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} 0 & az \\ 0 & 0 \end{pmatrix} \in I,$$

pa zaključujemo da je I ideal u R . Ako I promatramo kao podskup prstena R' kvadratnih matrica reda 2 nad $\mathbb{R}$, onda I nije ni lijevi ni desni ideal u R' . Dakle, svojstvo ideala ne ovisi samo o skupu I već i o prstenu u kojem ga promatramo. $\square$

Primjer 2.15. Neka je R prsten, i neka je $a \in R$. Tada je

$$aR = \{ar \mid r \in R\}$$

desni ideal u R , a

$$Ra = \{ra \mid r \in R\}$$

lijevi ideal u R . Ako R nema jedinicu, a ne mora biti element skupa aR ili Ra . Pokažimo da je aR desni ideal. Odaberimo $ar_1, ar_2 \in aR$. Tada je

$$ar_1 - ar_2 = a(r_1 - r_2) \in aR$$

jer je $r_1 - r_2 \in R$. Dakle, aR je Abelova podgrupa od R . Nadalje, za svaki $r \in R$ imamo

$$(ar_1)r = a(r_1r) \in aR$$

jer je $r_1r \in R$, pa zaključujemo da je aR desni ideal u R . Slično se pokazuje da je Ra lijevi ideal u R . $\square$

Primjer 2.16. Neka je R prsten, i neka je $a \in R$. Definirajmo

$$RaR = \left\{ \sum_i r_i a s_i \mid r_i, s_i \in R \right\} \quad (2.17)$$

gdje $\sum_i$ označava konačnu sumu. Razlika dviju ovakvih suma je opet suma oblika (2.17), dakle RaR je Abelova podgrupa od R . Također, za $r, s \in R$ imamo

$$r \left(\sum_i r_i a s_i \right) = \sum_i (rr_i) a s_i \in RaR,$$

$$\left(\sum_i r_i a s_i \right) s = \sum_i r_i a (s_i s) \in RaR,$$

što pokazuje da je RaR (dvostrani) ideal u R . $\square$

Teorem 2.6. Neka su A i B ideali u prstenu R . Tada je skup

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

ideal u prstenu R .

Dokaz Odaberimo $x, y \in A + B$. Tada je $x = a + b$ i $y = a' + b'$ za neke $a, a' \in A$ i $b, b' \in B$, pa vrijedi $x - y = (a - a') + (b - b') \in A + B$ jer je $a - a' \in A$ i $b - b' \in B$. Za svaki $r \in R$ imamo $rx = ra + rb \in A + B$ jer je $ra \in A$ i $rb \in B$. Slično, $xr \in A + B$ pa je time je dokazano da je $A + B$ ideal od R . ■

Propozicija 2.4. *Neka je $\{I_k\}_{k \in J}$ familija ideala prstena R . Tada je $\bigcap_{k \in J} I_k$ također ideal prstena R .*

Dokaz Odaberimo $a, b \in \bigcap_{k \in J} I_k$ i $r \in R$. Tada je $a - b \in I_k$ za svaki $k \in J$ pa je $a - b \in \bigcap_{k \in J} I_k$. Nadalje, $ra, ar \in I_k$ za svaki $k \in J$ što povlači $ra, ar \in \bigcap_{k \in J} I_k$ pa zaključujemo da je $\bigcap_{k \in J} I_k$ ideal od R . ■

Definicija 2.13. *Neka je S podskup prstena R . Najmanji ideal koji sadrži S naziva se ideal generiran skupom S , i označava sa (S) . Ako je S konačan skup, $S = \{a_1, a_2, \dots, a_m\}$, onda koristimo oznaku $(S) = (a_1, a_2, \dots, a_m)$. Ideal (a) generiran jednim elementom $a \in R$ nazivamo glavni ideal.*

Ideal generiran skupom $S \subseteq R$ se tvori na sljedeći način. Neka je $\mathcal{A} = \{A_k\}_{k \in J}$ familija ideala od R takvih da je $S \subseteq A_k$ za svaki $k \in J$. Primijetimo da je $\mathcal{A}$ neprazan skup jer je $R \in \mathcal{A}$. Prema propoziciji 2.4, $\bigcap_{k \in J} A_k$ je ideal od R i $S \subseteq \bigcap_{k \in J} A_k$. Ako je B bilo koji drugi ideal od R koji sadrži S , onda je $B \in \mathcal{A}$ pa je $\bigcap_{k \in J} A_k \subseteq B$. Dakle, $\bigcap_{k \in J} A_k$ je najmanji ideal koji sadrži skup S , pa je

$$(S) = \bigcap_{k \in J} A_k.$$

Analogne definicije i tvrdnje se mogu formulirati za lijeve i desne ideale.

Neka je R prsten s jedinicom. Lako se provjeri da je

$$(a) = \left\{ \sum_i r_i a s_i \mid r_i, s_i \in R \right\} = RaR,$$

gdje $\sum_i$ označava konačnu sumu. Ako je R također komutativan, onda je

$$(a) = \{ra \mid r \in R\} = Ra = aR.$$

Vodeći se analogijom u konstrukciji kvocijentne grupe, sada ćemo definirati kvocijentni prsten. Neka je I ideal u prstenu R . Definirajmo relaciju ekvivalencije $\sim$ na R s

$$a \sim b \quad \text{ako i samo ako je} \quad a - b \in I.$$

Klasa ekvivalencije elementa $a \in R$ je

$$\bar{a} = \{b \in R \mid a - b \in I\} = \{a + r \mid r \in I\} = a + I.$$

Skup svih klasa ekvivalencije $\bar{a}$ označimo s

$$R/I = \{a + I \mid a \in R\}.$$

Na skupu R/I možemo definirati zbrajanje i množenje na prirodan način:

$$(a + I) + (b + I) = (a + b) + I, \quad (2.18)$$

$$(a + I)(b + I) = ab + I. \quad (2.19)$$

Pokažimo da su operacije (2.18) i (2.19) dobro definirane, odnosno da ne ovise o predstavniku klase ekvivalencije. Ako je $a + I = a' + I$ i $b + I = b' + I$, onda je $a' - a = r \in I$ i $b' - b = s \in I$. Sada imamo

$$(a' + b') + I = (a + b + r + s) + I = (a + b) + I$$

jer je $r + s \in I$. Nadalje,

$$a'b' + I = (a + r)(b + s) + I = (ab + rb + as + rs) + I = ab + I$$

jer zbog dvostranosti ideala I imamo $rb, as, rs \in I$. Dakle, zbrajanje i množenje u R/I je dobro definirano. Lako se provjeri da skup R/I s operacijama (2.18) i (2.19) zadovoljava aksiome prstena. Operacije (2.18) i (2.19) možemo kraće zapisati kao

$$\bar{a} + \bar{b} = \overline{a + b}, \quad \bar{a}\bar{b} = \overline{ab} \quad \text{za sve } a, b \in R.$$

Nula u prstenu R/I je klasa ekvivalencije $\bar{0} = I$. Ako R ima jedinicu $1 \in R$, onda je jedinica u R/I dana s $\bar{1} = 1 + I$.

Definicija 2.14. *Neka je I ideal u prstenu R . Tada se prsten $(R/I, +, \cdot)$ naziva kvocijentni prsten R modulo I .*

Ako je $I = R$, onda je R/I nul-prsten jer je $\bar{r} = r + I = \bar{0}$ za svaki $r \in R$. Ako je $I = (0)$, onda se R/I može identificirati s R ako $a + (0)$ identificiramo s a .

Primjer 2.17. Odaberimo $n \in \mathbb{N}$ i promotrimo kvocijentni prsten

$$\mathbb{Z}/(n) = \{k + (n) \mid k \in \mathbb{Z}\}.$$

Prema teoremu o dijeljenju s ostatkom, svaki $k \in \mathbb{Z}$ se može zapisati kao $k = qn + l$ za neki $q \in \mathbb{Z}$ i $0 \leq l < n$. Stoga je

$$\mathbb{Z}/(n) = \{l + (n) \mid l = 0, 1, \dots, n-1\}$$

pa je $\mathbb{Z}/(n)$ jednak prstenu $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ sa zbrajanjem i množenjem modulo n . $\square$

Primjer 2.18. Promotrimo prsten gornje trokutastih matrica

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\} \quad (2.20)$$

i dvostrani ideal

$$I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in \mathbb{R} \right\}. \quad (2.21)$$

Kvocijentni prsten je dan sa

$$R/I = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + I \mid a, b, c \in \mathbb{R} \right\}. \quad (2.22)$$

Svaki element iz R/I se može napisati kao

$$\begin{aligned} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + I &= \left[\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} + \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \right] + I \\ &= \left[\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} + I \right] + \left[\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} + I \right] = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} + I \end{aligned} \quad (2.23)$$

jer je

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} + I = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + I. \quad (2.24)$$

Dakle, kvocijentni prsten sadrži dijagonalne matrice modulo I ,

$$R/I = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} + I \mid a, c \in \mathbb{R} \right\}. \quad (2.25)$$

□

Primjer 2.19. Neka je (x) ideal generiran polinomom x u prstenu $\mathbb{R}[x]$. Promotrimo kvocijentni prsten

$$\mathbb{R}[x]/(x) = \left\{ f(x) + (x) \mid f(x) \in \mathbb{R}[x] \right\}.$$

Ako je $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$, onda je

$$\overline{f(x)} = f(x) + (x) = a_0 + (x) = \bar{a}_0$$

jer je $a_kx^k \in (x)$ za svaki $k \geq 1$. Dakle,

$$\mathbb{R}[x]/(x) = \{a + (x) \mid a \in \mathbb{R}\}.$$

Ako element $a + (x)$ identificiramo s realnim brojem a , onda se zbrajanje i množenje u $\mathbb{R}[x]/(x)$ svodi na zbrajanje i množenje u skupu $\mathbb{R}$,

$$\begin{aligned} (a + (x)) + (b + (x)) &= (a + b) + (x), \\ (a + (x))(b + (x)) &= ab + (x). \end{aligned}$$

Stoga kvocijentni prsten $\mathbb{R}[x]/(x)$ možemo identificirati s poljem realnih brojeva $\mathbb{R}$. □

Primjer 2.20. Promotrimo sada kvocijentni prsten

$$\mathbb{R}[x]/(x^2 + 1) = \left\{ f(x) + (x^2 + 1) \mid f(x) \in \mathbb{R}[x] \right\}.$$

Da bismo odredili elemente prstena $\mathbb{R}[x]/(x^2 + 1)$ primijetimo da $x^2 + 1 \in (x^2 + 1)$ implicira

$$\overline{x^2 + 1} = \overline{x^2} + \overline{1} = \overline{0}.$$

Dakle, $\overline{x^2} = -\overline{1}$ odakle slijedi da su potencije elementa $\overline{x} \in \mathbb{R}[x]/(x^2 + 1)$ dane s

$$\overline{x^{2n}} = (-1)^n \overline{1}, \quad \overline{x^{2n+1}} = (-1)^n \overline{x}, \quad n \geq 1. \quad (2.26)$$

Ako je $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$, onda iz (2.26) slijedi da je

$$\overline{f(x)} = \overline{a_0} + \overline{a_1}\overline{x} + \overline{a_2}\overline{x^2} + \cdots + \overline{a_m}\overline{x^m} = \overline{\alpha} + \overline{\beta}\overline{x}$$

za neke $\alpha, \beta \in \mathbb{R}$, gdje se α i β dobiju grupiranjem koeficijenata uz parne i neparne potencije od $\overline{x}$. Zaključujemo da je

$$\mathbb{R}[x]/(x^2 + 1) = \{\overline{\alpha} + \overline{\beta}\overline{x} \mid \alpha, \beta \in \mathbb{R}\} \quad \text{gdje je } \overline{x^2} = -\overline{1}. \quad (2.27)$$

Ako $\overline{\alpha}$ i $\overline{\beta}$ identificiramo s realnim brojevima α i β , te $\overline{x}$ identificiramo s imaginarnom jedinicom $i = \sqrt{-1}$, onda je zbrajanje i množenje u $\mathbb{R}[x]/(x^2 + 1)$ istovjetno zbrajanju i množenju kompleksnih brojeva. Dakle, $\mathbb{R}[x]/(x^2 + 1)$ možemo identificirati s poljem kompleksnih brojeva $\mathbb{C}$. $\square$

2.8 Homomorfizmi prstena

Neka je I ideal u prstenu R . Definirajmo preslikavanje

$$\pi: R \rightarrow R/I, \quad \pi(a) = a + I. \quad (2.28)$$

Iz definicije binarnih operacija u R/I slijedi da π zadovoljava

$$\pi(a + b) = \pi(a) + \pi(b), \quad \pi(ab) = \pi(a)\pi(b).$$

Preslikavanje π naziva se *projekcija* ili *kanonski homomorfizam* s prstena R na prsten R/I . Ovo motivira sljedeću definiciju.

Definicija 2.15. Neka su R i S prsteni. Preslikavanje $f: R \rightarrow S$ koje zadovoljava svojstva

$$(i) \quad f(a + b) = f(a) + f(b),$$

$$(ii) \quad f(ab) = f(a)f(b),$$

za sve $a, b \in R$ naziva se *homomorfizam prstena*.

Ako je f injekcija, odnosno surjekcija, onda kažemo da je f monomorfizam, odnosno epimorfizam prstena. Ako je f bijekcija, onda je f *izomorfizam* prstena i kažemo da su prsteni R i S izomorfni. U tom slučaju je inverzno preslikavanje $f^{-1}: S \rightarrow R$ također izomorfizam prstena.

Primjer 2.21. Kompleksna konjugacija $f: \mathbb{C} \rightarrow \mathbb{C}$, $f(z) = \bar{z}$, je očigledno izomorfizam na prstenu $\mathbb{C}$. $\square$

Primjer 2.22. Neka je R prsten matrica

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \mid a, b \in \mathbb{R} \right\} \quad (2.29)$$

i neka je preslikavanje $f: R \rightarrow \mathbb{R}$ definirano sa

$$f \left(\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \right) = a. \quad (2.30)$$

Neka su $A = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ i $B = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}$. Onda je

$$f(A + B) = f \left(\begin{bmatrix} a+c & b+d \\ 0 & 0 \end{bmatrix} \right) = a+c = f(A) + f(B).$$

S druge strane

$$f(AB) = f \left(\begin{bmatrix} ac & ad \\ 0 & 0 \end{bmatrix} \right) = ac = f(A)f(B).$$

Dakle, f je homomorfizam prstena. $\square$

Definicija 2.16. Neka je $f: R \rightarrow S$ homomorfizam prstena. Jezgra homomorfizma je skup

$$\ker(f) = \{a \in R \mid f(a) = 0\}.$$

Primijetimo da svojstvo (i) iz definicije 2.15 implicira da je svaki homomorfizam prstena $f: R \rightarrow S$ također homomorfizam iz grupe $(R, +)$ u grupu $(S, +)$. Stoga dokaz sljedećeg teorema izostavljamo jer su analogne tvrdnje dokazane u teoremima 1.1 i 1.2.

Teorem 2.7. Neka je $f: R \rightarrow S$ homomorfizam iz prstena R u prsten S . Tada vrijedi:

- (i) $f(0) = 0'$ gdje su 0 i $0'$ nule u prstenovima R i S , redom,
- (ii) $f(-a) = -f(a)$ za svaki $a \in R$,
- (iii) f je injektivna homomorfizam ako i samo ako je $\ker(f) = \{0\}$.

Primjer 2.23. Odredimo sve homomorfizme iz prstena cijelih brojeva $\mathbb{Z}$ u $\mathbb{Z}$. Primijetimo da je trivijalno preslikavanje $f(n) = 0$ za sve $n \in \mathbb{Z}$ homomorfizam prstena. Pretpostavimo da je $f \neq 0$. Tada $f(n) = f(1 \cdot n) = f(1)f(n)$ implicira

$$f(n)(1 - f(1)) = 0 \quad (2.31)$$

odakle slijedi $f(1) = 1$ jer je $\mathbb{Z}$ integralna domena. Sada za svaki $n > 0$ imamo

$$f(n) = f(1) + f(1) + \cdots + f(1) = nf(1) = n. \quad (2.32)$$

Prema teoremu 2.7 vrijedi $f(-n) = -n$ dok je $f(0) = 0$. Ovo povlači da je preslikavanje f identiteta na $\mathbb{Z}$. Dakle, jedini homomorfizmi na $\mathbb{Z}$ su $f = 0$ i $f = id_{\mathbb{Z}}$. $\square$

Navedimo još neka svojstva homomorfizma prstena.

Teorem 2.8. *Neka su R i S prstenovi i neka je $f: R \rightarrow S$ homomorfizam.*

- (i) *Jezgra $\ker(f)$ je ideal u R .*
- (ii) *Slika $\operatorname{Im}(f)$ je podprsten od S .*
- (iii) *Ako R ima jedinicu 1 , onda je $f(1)$ jedinica u $\operatorname{Im}(f)$.*
- (iv) *Ako je R komutativni prsten, onda je $\operatorname{Im}(f)$ komutativni podprsten od S .*

Dokaz (i) Jezgra $\ker(f)$ je Abelova podgrupa od R . Neka su $r \in R$ i $a \in \ker(f)$. Tada je

$$f(ra) = f(r)f(a) = f(r)0 = 0.$$

Slično se pokazuje $f(ar) = 0$. Dakle, $ra \in \ker(f)$ i $ar \in \ker(f)$ što pokazuje da je $\ker(f)$ ideal u R .

(ii) Neka su $x, y \in \operatorname{Im}(f) \subseteq S$. Tada postoje $a, b \in R$ takvi da je $f(a) = x$ i $f(b) = y$. Sada imamo

$$\begin{aligned} x - y &= f(a) - f(b) = f(a - b) \in \operatorname{Im}(f), \\ xy &= f(a)f(b) = f(ab) \in \operatorname{Im}(f). \end{aligned}$$

Slijedi da je $\operatorname{Im}(f)$ podprsten od S .

(iii) Pretpostavimo da je R prsten s jedinicom $1 \in R$. Tada za svaki $f(a) \in \operatorname{Im}(f)$, $a \in R$, vrijedi

$$f(a) = f(1 \cdot a) = f(1)f(a),$$

i slično $f(a) = f(a)f(1)$. Dakle, $f(1)$ je jedinica u podprstenu $\operatorname{Im}(f)$.

(iv) Pretpostavimo da je R komutativni prsten. Neka su $f(a), f(b) \in \operatorname{Im}(f)$ za neke $a, b \in R$. Množenje u $\operatorname{Im}(f)$ je komutativno jer je

$$f(a)f(b) = f(ab) = f(ba) = f(b)f(a).$$

Dakle, $\operatorname{Im}(f)$ je komutativni podprsten u S . ■

Naglasimo da $f(1) \in S$ ne mora biti jedinica u prstenu S . Doista, preslikavanje $f: \mathbb{R} \rightarrow M(2, \mathbb{R})$ dano sa $f(a) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ je homomorfizam prstena pa je $f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ jedinica u podprstenu

$$\operatorname{Im}(f) = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R} \right\}. \quad (2.33)$$

Međutim, $f(1)$ nije jedinica u $M(2, \mathbb{R})$.

Iako prsten ne mora imati jedinicu, svaki prsten se može uložiti u prsten s jedinicom.

Teorem 2.9. *Neka je R prsten. Tada postoji injektivni homomorfizam prstena $f: R \rightarrow S$ gdje je S prsten s jedinicom.*

Dokaz Neka je S kartezijev umnožak $S = R \times \mathbb{Z}$. Na skupu S definirajmo binarne operacije

$$(a, m) + (b, n) = (a + b, m + n), \quad (2.34)$$

$$(a, m)(b, n) = (ab + mb + na, mn), \quad (2.35)$$

gdje su $a, b \in R$ i $m, n \in \mathbb{Z}$. Lako se provjeri da operacije (2.34) i (2.35) zadovoljavaju aksiome prstena. Uređeni par $(0_R, 1)$ (gdje je 0_R nula u R) je jedinica u S jer je

$$(a, m)(0_R, 1) = (a0_R + m0_R + a, m) = (a, m),$$

$$(0_R, 1)(a, m) = (0_Ra + a + m0_R, m) = (a, m).$$

Definirajmo preslikavanje $f: R \rightarrow S$ s $f(a) = (a, 0)$. Iz definicije binarnih operacija u S imamo

$$f(a + b) = (a + b, 0) = (a, 0) + (b, 0) = f(a) + f(b),$$

$$f(ab) = (ab, 0) = (a, 0)(b, 0) = f(a)f(b).$$

Preslikavanje f je očigledno injekcija pa je f monomorfizam iz prstena R u prsten S . ■

Prema teoremu 2.9, svaki prsten R možemo identificirati s podprstenom $f(R) \subseteq S$, ali jedinica u S nije sadržana u $f(R)$. Ako R ima jedinicu $1_R \in R$, onda je $f(1_R)$ jedinica u $f(R)$, ali $f(1_R)$ nije jedinica u S jer za $(a, n) \in S$, $n \neq 0$, imamo

$$(1_R, 0)(a, n) = (a + n1_R, 0) \neq (a, n). \quad (2.36)$$

Sljedeći teorem je analogan prvom teoremu o izomorfizmu u teoriji grupa.

Teorem 2.10 (Prvi teorem o homomorfizmu prstena). *Neka je $f: R \rightarrow S$ homomorfizam iz prstena R u prsten S . Tada je*

$$R/\ker(f) \simeq \text{Im}(f).$$

Dokaz Označimo $K = \ker(f)$. Definirajmo preslikavanje $h: R/K \rightarrow S$ s $h(\bar{a}) = f(a)$ gdje je $\bar{a} = a + K$. Ako je $\bar{a} = \bar{b}$, onda je $a - b \in K$ što implicira $f(a - b) = 0$, odnosno $f(a) = f(b)$. Dakle, preslikavanje h je dobro definirano. Pokažimo da je h homomorfizam prstena. Za svaki $\bar{a}, \bar{b} \in R/K$ vrijedi

$$h(\bar{a} + \bar{b}) = h(\overline{a + b}) = f(a + b) = f(a) + f(b) = h(\bar{a}) + h(\bar{b}),$$

$$h(\bar{a}\bar{b}) = h(\overline{ab}) = f(ab) = f(a)f(b) = h(\bar{a})h(\bar{b}).$$

Nadalje, h je očigledno surjekcija na $\text{Im}(f)$ jer je

$$\text{Im}(h) = \{h(a + K) \mid a \in R\} = \{f(a) \mid a \in R\} = \text{Im}(f).$$

Preostaje nam dokazati da je h injekcija. Ako je $h(\bar{a}) = h(\bar{b})$, onda je $f(a) = f(b)$ što povlači $f(a - b) = 0$, odnosno $a - b \in K$. Odavde slijedi $a + K = b + K$, odnosno $\bar{a} = \bar{b}$. Time je dokazano da je $h: R/K \rightarrow \text{Im}(f)$ izomorfizam. ■

Primjer 2.24. Prvi teorem o homomorfizmu možemo iskoristiti kako bismo pojednostavnili prikaz kvocijentnog prstena. Promotrimo prsten

$$R = \left\{ \begin{pmatrix} n & r \\ 0 & 0 \end{pmatrix} \mid n \in \mathbb{Z}, r \in \mathbb{Q} \right\}. \quad (2.37)$$

Lako se provjeri da je skup

$$A = \left\{ \begin{pmatrix} 0 & s \\ 0 & 0 \end{pmatrix} \mid s \in \mathbb{Q} \right\} \quad (2.38)$$

dvostrani ideal u R . Doista,

$$\begin{pmatrix} n & r \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & s \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ns \\ 0 & 0 \end{pmatrix} \in A, \quad (2.39)$$

$$\begin{pmatrix} 0 & s \\ 0 & 0 \end{pmatrix} \begin{pmatrix} n & r \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in A. \quad (2.40)$$

Kvocijentni prsten je dan sa

$$R/A = \left\{ \begin{pmatrix} n & r \\ 0 & 0 \end{pmatrix} + A \mid n \in \mathbb{Z}, r \in \mathbb{Q} \right\} = \left\{ \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix} + A \mid n \in \mathbb{Z} \right\}. \quad (2.41)$$

Preslikavanje $f: R/A \rightarrow \mathbb{Z}$ definirano sa

$$f \left(\begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix} + A \right) = n \quad (2.42)$$

je izomorfizam prstena, stoga je $R/A \simeq \mathbb{Z}$. □

Neka je $f: R \rightarrow S$ homomorfizam prstena. Zanima nas u kakvom su odnosu ideali u S s idealima u R . Ova korespondencija dana je sljedećim teoremom.

Teorem 2.11. *Neka je $f: R \rightarrow S$ epimorfizam prstena. Neka je I_R skup svih ideala u R koji sadrže jezgru $\ker(f)$ i neka je I_S skup svih ideala u S . Tada je preslikavanje $\psi: I_R \rightarrow I_S$ definirano s $\psi(A) = f(A)$ bijekcija.*

Dokaz Tvrdnju ćemo dokazati u dva koraka.

(i) Pokažimo da je ψ surjekcija. Neka je X ideal u S . Pokažimo da je skup

$$f^{-1}(X) = \{a \in R \mid f(a) \in X\}$$

ideal u R koji sadrži $\ker(f)$. Neka su $a, b \in f^{-1}(X)$. Tada su $f(a), f(b) \in X$, pa vrijedi $f(a - b) = f(a) - f(b) \in X$, dakle je $a - b \in f^{-1}(X)$. Za svaki $r \in R$ imamo $f(ra) =$

$f(r)f(a) \in X$, stoga je $ra \in f^{-1}(X)$. Slično se pokazuje $ar \in f^{-1}(X)$, pa zaključujemo da je $f^{-1}(X)$ ideal u R .

Ako je $a \in \ker(f)$, onda je $f(a) = 0 \in X$, odnosno $a \in f^{-1}(X)$, što implicira da je $\ker(f) \subseteq f^{-1}(X)$. Kako je $f: R \rightarrow S$ surjekcija, na nivou skupova je $X = f(f^{-1}(X))$. Dakle, ideal X je oblika $f(A)$ gdje je $A = f^{-1}(X)$ ideal u R koji sadrži $\ker(f)$. Time je dokazano da je ψ surjekcija.

(ii) Sada ćemo pokazati da je ψ injekcija. Pretpostavimo da je $f(A) = f(B)$ gdje su $A, B \in I_R$. Pokažimo da je $A = f^{-1}(f(A))$. Kako je

$$f^{-1}(f(A)) = \{x \in R \mid f(x) \in f(A)\},$$

trivijalno slijedi da je $A \subseteq f^{-1}(f(A))$. Odaberimo sada $x \in f^{-1}(f(A))$. Tada je $f(x) = f(a)$ za neki $a \in A$. Odavde slijedi $f(x - a) = 0$, odnosno $x - a \in \ker(f) \subseteq A$. Stoga je $x = a + a' \in A$ za neki $a' \in A$, što implicira $f^{-1}(f(A)) \subseteq A$. Time je pokazano da je $A = f^{-1}(f(A))$, i slično $B = f^{-1}(f(B))$. Sada iz jednakosti $f(A) = f(B)$ odmah slijedi $A = B$, čime je dokazano da je ψ injekcija. ■

Ovaj teorem pokazuje da ako je $f: R \rightarrow S$ epimorfizam prstena, onda su ideali u S u 1-1 korespondenciji s idealima u R koji sadrže $\ker(f)$. Važna posljedica ovog teorema je sljedeći rezultat koji se odnosi na ideale u kvocijentalnom prstenu.

Teorem 2.12. *Neka je I ideal u prstenu R . Tada je svaki ideal u R/I oblika A/I gdje je $A \subseteq R$ ideal koji sadrži I .*

Dokaz Neka je $\varphi: R \rightarrow R/I$ kanonski homomorfizam, $\varphi(a) = a + I$. Kako je φ surjekcija, prema teoremu 2.11 svaki ideal u prstenu R/I je oblika $\varphi(A)$ gdje je A ideal u R i $A \supseteq \ker(\varphi) = I$. Također, vrijedi

$$\varphi(A) = \{\varphi(a) = a + I \mid a \in A\} = A/I,$$

čime je teorem dokazan. ■

2.9 Euklidska domena i domena glavnih ideala

Poznato je da u prstenu cijelih brojeva $\mathbb{Z}$ i prstenu polinoma $\mathbb{R}[x]$ elemente možemo dijeliti s ostatkom pri čemu je ostatak pri dijeljenju u izvjesnom smislu "manji" od elementa kojim se dijeli.

Teorem 2.13 (Dijeljenje s ostatkom). *Neka su $a, b \in \mathbb{Z}$, $b > 0$. Tada postoje jedinstveni $q, r \in \mathbb{Z}$ takvi da je*

$$a = bq + r, \quad 0 \leq r < b. \quad (2.43)$$

Dokaz Promotrimo skup

$$S = \{a - bk \mid k \in \mathbb{Z}, a - bk \geq 0\}.$$

Primijetimo da je S neprazan skup jer je $a - b(-n) \geq 0$ za dovoljno veliki $n \in \mathbb{N}$. Budući je S omeđen odozdo, S ima minimalni element $r \geq 0$ i vrijedi

$$r = a - bq \quad \text{za neki } q \in \mathbb{Z}.$$

Ako je $r \geq b$, onda je $r - b = a - b(q + 1) \geq 0$ pa je $r - b \in S$, što je u kontradikciji s pretpostavkom da je r minimalni element od S . Dakle, $0 \leq r < b$ čime je dokazana egzistencija q i r .

Prepostavimo sada da postoje $q', r' \in \mathbb{Z}$ takvi da je

$$a = bq + r = bq' + r', \quad 0 \leq r, r' < b.$$

Onda je

$$b(q - q') = r' - r. \quad (2.44)$$

Budući je $|r' - r| < b$, iz (2.44) slijedi da je $b|q - q'| < b$, odnosno $|q - q'| < 1$. Dakle, $q = q'$ jer su q i q' cijeli brojevi. Sada (2.44) implicira $r = r'$ pa zaključujemo da je rastav (2.43) jedinstven. ■

Algoritam dijeljenja s ostatkom se može proširiti na druge prstene ako se na njima na prikladan način može definirati norma koja mjeri veličinu elementa u prstenu.

Definicija 2.17. *Neka je R prsten. Svaka funkcija $\phi: R \rightarrow \mathbb{N}_0$ sa svojstvom $\phi(0) = 0$ i $\phi(a) > 0$ za $a \neq 0$ se naziva norma na prstenu R .*

Primijetimo da je ova definicija prilično općenita pa isti prsten može imati više različitih normi. Prsten na kojem je moguće definirati normu koja daje algoritam dijeljenja s ostatkom nazivamo euklidska domena. Preciznije, uvodimo sljedeću definiciju.

Definicija 2.18. *Neka je R komutativna integralna domena s jedinicom. Kažemo da je R euklidska domena ako postoji norma $\phi: R \rightarrow \mathbb{N}_0$ takva da za sve $a, b \in R$, $b \neq 0$, postoje $q, r \in R$ takvi da je*

$$a = bq + r \quad \text{gdje je } \phi(r) < \phi(b). \quad (2.45)$$

Element q nazivamo kvocijent, a r ostatak pri dijeljenju. Primijetimo da (2.45) uključuje i slučaj kada je $r = 0$ jer je tada $\phi(0) = 0 < \phi(b)$ za svaki $b \neq 0$.

Pojam algoritma dijeljenja s ostatkom se može proširiti i na nekomutativne prstene. U tom slučaju razlikujemo lijevi euklidski prsten u kojem vrijedi rastav

$$a = bq + r, \quad \phi(r) < \phi(b),$$

i desni euklidski prsten u kojem je

$$a = qb + r, \quad \phi(r) < \phi(b).$$

Međutim, u primjenama, na primjer u teoriji brojeva, se dijeljenje s ostatkom gotovo uvijek razmatra u komutativnim prstenima.

Primjer 2.25. Prema Teoremu 2.13 prsten cijelih brojeva $\mathbb{Z}$ je Euklidska domena s normom $\phi(n) = |n|$. $\square$

Primjer 2.26. Svako polje F je euklidska domena. Definirajmo normu na F sa $\phi(0) = 0$ i $\phi(a) = 1$ za $a \neq 0$. Onda za sve $a, b \in F$, $b \neq 0$, vrijedi

$$a = (ab^{-1})b + 0, \quad \phi(0) < \phi(b).$$

Budući je u polju ostatak pri dijeljenju uvijek nula, normu na F možemo definirati kao bilo koju funkciju ϕ takvu da je $\phi(0) = 0$ i $\phi(a) > 0$ za $a \neq 0$. $\square$

Primjer 2.27. Prsten Gaussovih cijelih brojeva je definiran sa

$$\mathbb{Z}[i] = \{m + in \mid m, n \in \mathbb{Z}, i = \sqrt{-1}\}.$$

Definirajmo normu

$$\phi(m + in) = |m + in|^2 = m^2 + n^2.$$

Neka su $a, b \in \mathbb{Z}[i]$, $b \neq 0$. Tada je $ab^{-1} = \alpha + i\beta$ za neke $\alpha, \beta \in \mathbb{Q}$. Za racionalne brojeve α i β neka su $\alpha_0, \beta_0 \in \mathbb{Z}$ takvi da je α_0 najbliži α i β_0 najbliži β . Tada je $|\alpha - \alpha_0| \leq \frac{1}{2}$ i $|\beta - \beta_0| \leq \frac{1}{2}$. Sada imamo

$$\begin{aligned} a &= b(\alpha + i\beta) = b((\alpha - \alpha_0) + i(\beta - \beta_0) + \alpha_0 + i\beta_0) \\ &= b(\alpha_0 + i\beta_0) + b(\alpha - \alpha_0 + i(\beta - \beta_0)). \end{aligned}$$

Definirajmo $q = \alpha_0 + i\beta_0$ i $r = b(\alpha - \alpha_0 + i(\beta - \beta_0))$. Tada je $a = bq + r$.

Očigledno je $q \in \mathbb{Z}[i]$, pa slijedi da je $r = a - bq \in \mathbb{Z}[i]$. Nadalje,

$$\begin{aligned} \phi(r) &= |b|^2 |\alpha - \alpha_0 + i(\beta - \beta_0)|^2 = |b|^2 ((\alpha - \alpha_0)^2 + (\beta - \beta_0)^2) \\ &\leq |b|^2 \left(\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 \right) < |b|^2 = \phi(b). \end{aligned}$$

Time smo pokazali da je $\mathbb{Z}[i]$ Euklidska domena. $\square$

Definicija 2.19. Prsten u kojem je svaki ideal glavni naziva se prsten glavnih ideala. Komutativna integralna domena s jedinicom u kojoj je svaki ideal glavni naziva se domena glavnih ideala.

Prema ovoj definiciji, u domeni R glavnih ideala svaki ideal je oblika $(a) = Ra$ za neki $a \in R$ jer je R komutativni prsten s jedinicom.

Teorem 2.14. *Svaka Euklidska domena je domena glavnih ideala.*

Dokaz Neka je R Euklidska domena s normom $\phi: R \rightarrow \mathbb{N} \cup \{0\}$, i neka je I ideal u R . Ako je $I = \{0\}$ nul-ideal, onda je $I = (0)$. Stoga pretpostavimo $I \neq \{0\}$. Skup $S = \{\phi(a) \mid a \in I, a \neq 0\}$ je omeđen odozdo, pa postoji $d \in I, d \neq 0$, koji ima minimalnu normu u S . Pokažimo da je $I = (d)$. Očigledno je $(d) \subseteq I$. Odaberimo $a \in I, a \neq 0$. Kako je R Euklidska domena, postoje $q, r \in R$ takvi da je $a = dq + r$ i $\phi(r) < \phi(d)$. Primijetimo da je $r = a - dq \in I$. Ako je $r \neq 0$, onda iz $0 < \phi(r) < \phi(d)$ dobivamo kontradikciju zbog minimalnosti norme $\phi(d)$. Dakle, $r = 0$ što implicira $a = dq \in (d)$. Zaključujemo da je $I \subseteq (d)$, što povlači $I = (d)$. ■

Svaki ideal I u Euklidskoj domeni je generiran nekim elementom $d \in I$ koji ima minimalnu normu u I . Element d ne mora biti jedinstven. Na primjer, prsten cijelih brojeva $\mathbb{Z}$ je domena glavnih ideala gdje je svaki ideal I generiran elementom d koji ima najmanju apsolutnu vrijednost u I . Stoga, ako je $I \neq \{0\}$, onda je I generiran elementima d i $-d$.

2.10 Prsten polinoma

Polinome s realnim ili kompleksnim koeficijentima možemo proširiti na polinome s koeficijentima u proizvoljnom prstenu R . Ako želimo zadržati komutativnost množenja polinoma i monične polinome x^k , promatrat ćemo komutativne prstene s jedinicom.

Definicija 2.20. *Neka je R komutativni prsten s jedinicom. Formalna suma*

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \quad a_i \in R, \quad (2.46)$$

naziva se polinom u varijabli x .

Element $a_n \neq 0$ nazivamo vodeći koeficijent, a a_nx^n vodeći član polinoma $f(x)$. Polinom $f(x) = a_0, a_0 \neq 0$, nazivamo konstantni polinom. Ako je $a_0 = 0$, onda $f(x) = 0$ nazivamo nul-polinom. Stupanj polinoma definiramo sa $\deg(f(x)) = n$ gdje je $a_n \neq 0$ vodeći koeficijent polinoma, dok stupanj nul-polinoma definiramo sa $\deg(0) = -\infty$ uz standardnu konvenciju

$$-\infty < n, \quad -\infty + (-\infty) = -\infty, \quad -\infty + n = -\infty \quad \forall n \geq 0. \quad (2.47)$$

Prema ovoj definiciji, konstantni polinom ima stupanj 0, a nul-polinom ima stupanj $-\infty$. Skup svih polinoma oblika (2.46) označavamo sa $R[x]$.

Na skupu $R[x]$ možemo definirati strukturu prstena ako zbrajanje i množenje polinoma uvedemo na standardni način. Zbroj polinoma $f(x) = \sum_{k=0}^n a_kx^k$ i $g(x) = \sum_{k=0}^m b_kx^k$, $n \geq m$, definiramo sa

$$f(x) + g(x) = \sum_{k=0}^n (a_k + b_k)x^k \quad (2.48)$$

gdje smo uzeli da je $b_{m+1} = b_{m+2} = \dots = b_n = 0$. Umnožak polinoma je definiran sa

$$\begin{aligned} f(x)g(x) &= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots + a_nb_mx^{n+m} \\ &= \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_ib_j \right) x^k. \end{aligned} \quad (2.49)$$

Lako se provjeri da operacije (2.48) i (2.49) zadovoljavaju aksiome prstena. Stoga je $R[x]$ komutativni prsten s jedinicom gdje je jedinica u $R[x]$ konstantni polinom $f(x) = 1$. Prsten R možemo promatrati kao podprsten konstantnih polinoma i pišemo $R \subset R[x]$.

Primijetimo da za stupanj polinoma vrijede nejednakosti

$$\begin{aligned} \deg(f(x) + g(x)) &\leq \max(\deg(f(x)), \deg(g(x))), \\ \deg(f(x)g(x)) &\leq \deg(f(x)) + \deg(g(x)), \end{aligned}$$

koje vrijede i za $f(x) = 0$ ili $g(x) = 0$ uzevši u obzir konvenciju (2.47). Na primjer, ako je $f(x) = 0$, $g(x) \neq 0$ i $\deg(g(x)) = n$, onda je

$$\deg(f(x)g(x)) = -\infty = -\infty + n = \deg(f(x)) + \deg(g(x)).$$

Propozicija 2.5. *Neka je R integralna domena. Tada je*

- (i) $R[x]$ integralna domena,
- (ii) $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$.

Dokaz Neka su zadani polinomi $f(x) = \sum_{k=0}^n a_k x^k \neq 0$ i $g(x) = \sum_{k=0}^m b_k x^k \neq 0$. Tada su $a_n \neq 0$ i $b_m \neq 0$ pa je $a_nb_m \neq 0$ jer je R integralna domena. Ovo povlači da je $f(x)g(x) \neq 0$ jer je vodeći član umnoška $a_nb_mx^{n+m} \neq 0$. Oдавде slijedi da je $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$. Dakle, $R[x]$ je integralna domena jer nema djelitelja nule osim nul-polinoma. ■

Svojstva polinoma u mnogome ovise o prstenu R . Promotrimo sljedeće primjere.

Primjer 2.28. Odredite umnožak polinoma $f(x) = 3x^2 + 4x$ i $g(x) = 2x + 5$ u prstenu $\mathbb{Z}_2[x]$ i $\mathbb{Z}_6[x]$. U prstenu $\mathbb{Z}_2[x]$ imamo

$$(3x^2 + 4x)(2x + 5) = 6x^3 + 23x^2 + 20x = x^2$$

jer je $6 = 0$, $23 = 1$ i $20 = 0$ u $\mathbb{Z}_2$. S druge strane, u prstenu $\mathbb{Z}_6[x]$ dobivamo

$$(3x^2 + 4x)(2x + 5) = 5x^2 + 2x \quad (2.50)$$

jer je $6 = 0$, $23 = 5$ i $20 = 2$ u $\mathbb{Z}_6$. □

Sljedeći teorem pokazuje da se Euklidov algoritam dijeljenja polinoma s ostatkom u prstenu $\mathbb{R}[x]$ može proširiti na znatno veću klasu prstena.

Teorem 2.15 (Euklidov algoritam). *Neka je R komutativni prsten s jedinicom, i neka su $f(x), g(x) \in R[x]$ gdje je $g(x) \neq 0$. Ako je vodeći koeficijent od $g(x)$ invertibilan u R , onda postoje jedinstveni polinomi $q(x), r(x) \in R[x]$ takvi da je*

$$f(x) = g(x)q(x) + r(x), \quad \deg(r(x)) < \deg(g(x)). \quad (2.51)$$

Dokaz Ako je $f(x) = 0$, onda su $q(x) = r(x) = 0$. Pretpostavimo da je $f(x) = \sum_{k=0}^n a_k x^k \neq 0$ i neka je $g(x) = \sum_{k=0}^m b_k x^k$ gdje je $b_m^{-1} \in R$. Ako je $\deg(g(x)) > \deg(f(x))$, onda u relaciji (2.51) možemo uzeti $q(x) = 0$ i $r(x) = f(x)$. Stoga je dovoljno promatrati slučaj $\deg(g(x)) \leq \deg(f(x))$, pa dokaz možemo provesti indukcijom po $n = \deg(f(x))$.

Ako je $n = 0$, onda je $f(x) = a_0$ i $g(x) = b_0$ pa možemo uzeti $q(x) = b_0^{-1}a_0$ i $r(x) = 0$. Primijetimo da je $\deg(r(x)) = -\infty < 0 = \deg(g(x))$. Pretpostavimo sada da tvrdnja (2.51) vrijedi za svaki polinom $f(x)$ stupnja $< n$. Promotrimo

$$\begin{aligned} a_n b_m^{-1} x^{n-m} g(x) &= a_n b_m^{-1} x^{n-m} (b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0) \\ &= a_n x^n + a_n b_m^{-1} (b_{m-1} x^{n-1} + \cdots + b_0 x^{n-m}) \\ &= a_n x^n + g_1(x) \end{aligned}$$

gdje je $\deg(g_1(x)) \leq n - 1$. Sada je

$$f(x) - a_n b_m^{-1} x^{n-m} g(x) = a_{n-1} x^{n-1} + \cdots + a_0 - g_1(x) = f_1(x) \quad (2.52)$$

gdje je $\deg(f_1(x)) \leq n - 1$. Po pretpostavci indukcije postoje $q_1(x), r(x) \in R[x]$ takvi da je

$$f_1(x) = g(x)q_1(x) + r(x), \quad \deg(r(x)) < \deg(g(x)). \quad (2.53)$$

Iz jednadžbi (2.52) i (2.53) slijedi

$$f(x) = g(x)(a_n b_m^{-1} x^{n-m} + q_1(x)) + r(x).$$

Definirajmo $q(x) = a_n b_m^{-1} x^{n-m} + q_1(x)$. Time je dokazana egzistencija polinoma $q(x)$ i $r(x)$.

Za jedinstvenost rastava (2.51) pretpostavimo da je

$$f(x) = g(x)q_1(x) + r_1(x) = g(x)q_2(x) + r_2(x)$$

gdje je $\deg(r_i(x)) < \deg(g(x))$ za $i = 1, 2$. Odavde dobivamo

$$g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x). \quad (2.54)$$

Kako je vodeći koeficijent u $g(x)$ invertibilan, to je

$$\deg(g(x)(q_1(x) - q_2(x))) = \deg(g(x)) + \deg(q_1(x) - q_2(x)).$$

Također, $\deg(r_1(x) - r_2(x)) < \deg(g(x))$ što zajedno s jednadžbom (2.54) povlači

$$\deg(g(x)) + \deg(q_1(x) - q_2(x)) < \deg(g(x)).$$

Ova nejednakost vrijedi ako i samo ako je $\deg(q_1(x) - q_2(x)) = -\infty$, odnosno $q_1(x) = q_2(x)$. Sada iz jednadžbe (2.54) dobivamo $r_1(x) = r_2(x)$. ■

U primjenama nas često zanimaju polinomi nad poljem F , na primjer $F = \mathbb{R}$, $\mathbb{C}$ ili $\mathbb{Z}_p$ gdje je p prosti broj. Ako je $g(x) \neq 0$ u $F[x]$, onda vodeći koeficijent od $g(x)$ ima inverz u F pa Teorem 2.15 povlači da u prstenu $F[x]$ polinome možemo dijeliti s ostatkom. Normu na $F[x]$ možemo definirati sa $\phi(f(x)) = 2^{\deg(f(x))}$ uz konvenciju $2^{-\infty} = 0$ koja osigurava da je $\phi(0) = 0$. Sada rastav (2.51) možemo pisati u obliku

$$f(x) = g(x)q(x) + r(x), \quad \phi(r(x)) < \phi(g(x))$$

jer je ϕ rastuća funkcija. Stoga je $F[x]$ euklidska domena pa iz Teorema 2.14 slijedi da je $F[x]$ domena glavnih ideala. Time smo dokazali

Teorem 2.16. *Ako je F polje, onda je prsten $F[x]$ domena glavnih ideala.*

Prema ovom teoremu, svaki ideal u $F[x]$ je oblika

$$(p(x)) = p(x)F[x] = \{p(x)f(x) \mid f(x) \in F[x]\}$$

za neki polinom $p(x) \in F[x]$.

2.10.1 Ireducibilni polinomi

Promotrimo sada поближе problem ireducibilnosti i faktorizacije polinoma. Posebno nas zanima uvjet kada se u faktorizaciji polinoma javlja linearni faktor, odnosno polinom stupnja jedan.

Definicija 2.21. *Neka je F polje. Kažemo da je polinom $f(x) \in F[x]$ ireducibilan nad poljem F ako je $\deg(f(x)) \geq 1$ i ako*

$$f(x) = g(x)h(x), \quad g(x), h(x) \in F[x],$$

povlači $g(x) \in F$ ili $h(x) \in F$.

Drugim riječima, ako je $f(x)$ ireducibilan, onda u faktorizaciji $f(x) = g(x)h(x)$ jedan od polinoma $g(x)$ ili $h(x)$ mora biti konstantan. Primijetimo da je prema definiciji 2.21 polinom prvog stupnja ireducibilan. Ako je $f(x) = g(x)h(x)$, onda kažemo da $g(x)$, odnosno $h(x)$, dijeli $f(x)$. Faktorizacija polinoma u mnogome ovisi o polju u kojem se nalaze njegovi koeficijenti. Na primjer, polinom $x^2 + 1$ je ireducibilan nad $\mathbb{R}$, ali nad poljem $\mathbb{C}$ se može faktorizirati kao

$$x^2 + 1 = (x - i)(x + i).$$

Isti polinom se također može faktorizirati u prstenu $\mathbb{Z}_2[x]$ kao

$$x^2 + \bar{1} = (x + \bar{1})(x + \bar{1})$$

jer je $\bar{2} = \bar{0}$. Neka je R prsten i neka je $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in R[x]$. Za svaki $\alpha \in R$ možemo definirati evaluacijsko preslikavanje sa $R[x]$ na R , $f(x) \mapsto f(\alpha)$, gdje je $f(\alpha) = a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_0$.

Definicija 2.22. Neka je R podprsten komutativnog prstena S , i neka je $f(x) \in R[x]$. Kažemo da je $\alpha \in S$ korijen polinoma $f(x)$ u S ako je $f(\alpha) = 0$.

Ova definicija uzima u obzir činjenicu da korijen polinoma ne mora biti u istom prstenu kao i njegovi koeficijenti. Na primjer, korijeni polinoma $x^2 + 1 \in \mathbb{Z}[x]$ su $\pm i$ koji leže u prstenu $\mathbb{C}$.

Teorem 2.17. Neka je F polje i neka je $f(x) \in F[x]$, $\deg(f(x)) = n \geq 1$.

- (i) $\alpha \in F$ je korijen polinoma $f(x)$ ako i samo ako $x - \alpha$ dijeli $f(x)$.
- (ii) $f(x)$ ima najviše n korijena u polju F .

Dokaz (i) Ako $x - \alpha$ dijeli $f(x)$, onda je $f(x) = (x - \alpha)q(x)$ za neki $q(x) \in F[x]$, pa je očigledno $f(\alpha) = 0$. Pretpostavimo da je $f(\alpha) = 0$. Prema teoremu 2.15 postoje jedinstveni polinomi $q(x), r(x) \in F[x]$ takvi da je

$$f(x) = (x - \alpha)q(x) + r(x) \quad (2.55)$$

gdje je $r(x) = 0$ ili $r(x) = c \neq 0$. Kako je $f(\alpha) = 0$, iz jednadžbe (2.55) slijedi $r(\alpha) = 0$, što implicira $r(x) = 0$. Dakle, $x - \alpha$ dijeli $f(x)$.

(ii) Pretpostavimo da su $\alpha_1, \alpha_2, \dots, \alpha_m \in F$ različiti korijeni polinoma $f(x)$. Tada je

$$f(x) = (x - \alpha_1)q_1(x) \quad \text{za neki} \quad q_1(x) \in F[x], \deg(q_1(x)) = n - 1 \geq 0.$$

Nadalje, $f(\alpha_2) = (\alpha_2 - \alpha_1)q_1(\alpha_2) = 0$ povlači $q_1(\alpha_2) = 0$ jer je $\alpha_2 - \alpha_1 \neq 0$. Sada postoji $q_2(x) \in F[x]$ takav da je $q_1(x) = (x - \alpha_2)q_2(x)$. Ponavljanjem postupka zaključujemo da polinom $(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_m)$ dijeli $f(x)$ pa je očito $m \leq n$. ■

Iz teorema 2.17 odmah slijedi da ako polinom $f(x) \in F[x]$ stupnja ≥ 2 ima korijen $\alpha \in F$, onda je $f(x)$ reducibilan u F . U tom slučaju možemo $f(x)$ napisati kao umnožak polinoma koji nisu konstantni, tj. kao

$$f(x) = (x - \alpha)q(x) \quad \text{za neki} \quad q(x) \in F[x].$$

Primijetimo da reducibilan polinom u $F[x]$ ne mora imati korijen u F . Na primjer, $x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1)$ je reducibilan nad $\mathbb{R}$ ali nema realne korijene. Međutim, za polinome stupnja 2 ili 3 vrijedi obrat.

Propozicija 2.6. *Neka je F polje i neka je $f(x) \in F[x]$ polinom stupnja 2 ili 3. Ako je $f(x)$ reducibilan nad F , onda $f(x)$ ima korijen u F .*

Dokaz Ako je $f(x)$ reducibilan polinom stupnja 2 ili 3, onda je $f(x) = g(x)h(x)$ gdje $g(x)$ i $h(x)$ nisu konstantni polinomi. Dakle, jedan od polinoma $g(x)$ ili $h(x)$ ima stupanj 1. Pretpostavimo da je $g(x) = ax + b$, $a \neq 0$. Tada je $g(-ba^{-1}) = 0$ pa zaključujemo da je $-ba^{-1} \in F$ korijen polinoma $f(x)$. ■

Vrlo često nas zanima problem faktorizacije u prstenu $R[x]$ gdje je R podprsten polja F . Prirodno je zapitati se kako se faktorizacija u $F[x]$ može iskoristiti da saznamo nešto o faktorizaciji u $R[x]$. Sljedeći rezultati koje navodimo bez dokaza daju neke kriterije ireducibilnosti u prstenima $\mathbb{Z}[x]$ i $\mathbb{Q}[x]$.

Lema 2.1. *Neka je $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ polinom u $\mathbb{Z}[x]$. Pretpostavimo da $f(x)$ ima korijen $r/s \in \mathbb{Q}$ gdje je r/s potpuno skraćeni razlomak.*

(i) *Tada $r \mid a_0$ i $s \mid a_n$.*

(ii) *Ako je $a_n = 1$ i $f(d) \neq 0$ za svaki $d \in \mathbb{Z}$ koji dijeli a_0 , onda $f(x)$ nema korijen u $\mathbb{Q}$.*

Primjer 2.29. Neka su $f(x) = x^2 - p$ i $g(x) = x^3 - p$ polinomi u $\mathbb{Z}[x]$ gdje je p prosti broj. Jedini djelitelji slobodnog člana za oba polinoma su ± 1 i $\pm p$. Međutim, $f(d) \neq 0$ i $g(d) \neq 0$ za $d = \pm 1, \pm p$, pa polinomi $f(x)$ i $g(x)$ nemaju korijen u $\mathbb{Q}$. Iz propozicije 2.6 sada slijedi da su $f(x)$ i $g(x)$ ireducibilni u $\mathbb{Q}[x]$.

Teorem 2.18 (Eisensteinov kriterij). *Neka je $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$, $n \geq 1$. Ako postoji prosti broj p takav da $p \mid a_k$ za $k = 0, 1, \dots, n-1$, $p \nmid a_n$ i $p^2 \nmid a_0$, onda je $f(x)$ ireducibilan nad $\mathbb{Q}$.*

Primjer 2.30. Promotrimo polinom $f(x) = 2x^5 - 5x^4 + 5 \in \mathbb{Z}[x]$. Prost broj $p = 5$ ne dijeli vodeći koeficijent 2 dok su svi ostali koeficijenti djeljivi s 5. Nadalje, $p^2 = 25$ ne dijeli slobodni koeficijent 5 pa je prema Eisensteinovom kriteriju $f(x)$ ireducibilan nad $\mathbb{Q}$. □

Primjer 2.31. Neka je p prost broj. Tada je polinom $f_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ ireducibilan nad $\mathbb{Q}$. Na ovom polinomu ne možemo direktno primijeniti Eisensteinov kriterij, ali možemo napraviti sljedeću transformaciju. Primijetimo da je

$$f_p(x)(x-1) = x^p - 1,$$

pa transformacijom varijabli $x \mapsto x+1$ i primjenom binomne formule dobivamo

$$f_p(x+1)x = (x+1)^p - 1 = \binom{p}{1}x + \binom{p}{2}x^2 + \dots + \binom{p}{p}x^p.$$

Dakle,

$$f_p(x+1) = \binom{p}{1} + \binom{p}{2}x + \cdots + \binom{p}{p}x^{p-1}.$$

Broj p dijeli $\binom{p}{k}$ za $k = 1, 2, \dots, p-1$, ali $p \nmid \binom{p}{p} = 1$. Također, $p^2 \nmid \binom{p}{1} = p$, pa je $f_p(x+1)$ ireducibilan nad $\mathbb{Q}$ prema Eisensteinovom kriteriju. Ovo implicira da je $f_p(x)$ ireducibilan nad $\mathbb{Q}$. $\square$

Za polje F kažemo da je algebarski zatvoreno ako svaki polinom $f(x) \in F[x]$ stupnja ≥ 1 ima korijen u F . Na primjer, dobro je poznato da je polje $\mathbb{C}$ algebarski zatvoreno, dok polje $\mathbb{R}$ nije. Može se pokazati da je svako polje sadržano u nekom polju koje je algebarski zatvoreno. Ako je F algebarski zatvoreno polje, onda su ireducibilni polinomi u $F[x]$ upravo polinomi prvog stupnja. U tom slučaju svaki polinom $f(x) \in F[x]$, $\deg(f(x)) \geq 1$, se može faktorizirati kao

$$f(x) = c \prod_{i=1}^m (x - \alpha_i)^{k_i}$$

gdje je $c \in F$, $c \neq 0$, $k_i \in \mathbb{N}$ i $\alpha_1, \alpha_2, \dots, \alpha_m \in F$ su korijeni polinoma $f(x)$.

2.11 Maksimalni ideali

Važna klasa ideala su oni koji nisu sadržani ni u jednom pravom idealu. Takve ideale nazivamo maksimalni ideali. U ovom poglavlju proučavamo svojstva maksimalnih ideala i njihovu vezu s prostim prstenima.

Definicija 2.23. *Kažemo da je R prosti prsten ako R nema netrivialnih ideala.*

Drugim riječima, jedini ideali u prostom prstenu su nul-ideal $\{0\}$ i cijeli prsten R . Svako polje F je trivijalno prosti prsten. Ako je $I \neq \{0\}$ ideal u F , onda postoji $a \in I$, $a \neq 0$, što povlači da je $a^{-1}a = 1 \in I$. Odavde slijedi da je $x = x \cdot 1 \in I$ za svaki $x \in F$ što implicira $I = F$.

Definicija 2.24. *Neka je R prsten. Kažemo da je ideal $A \subset R$ maksimalni ideal u R ako vrijedi:*

(i) $A \neq R$,

(ii) *ako je B ideal u R i $B \supseteq A$, onda je $B = A$ ili $B = R$.*

Primijetimo da je $\{0\}$ maksimalni ideal u polju F . Doista, ako je $I \supseteq \{0\}$ ideal u F i $I \neq \{0\}$, onda je $I = F$ jer je F prosti prsten.

Teorem 2.19. *Neka je R prsten, i neka je $A \neq R$ ideal u R . Onda je A maksimalni ideal ako i samo ako je R/A prosti prsten.*

Dokaz Pretpostavimo da je A maksimalni ideal u R . Neka je J ideal u R/A . Prema Teoremu 2.12, $J = B/A$ za neki ideal $B \subseteq R$ takav da $B \supseteq A$. Obzirom da je A maksimalni ideal, $B = A$ ili $B = R$. Ovo implicira $J = A/A = \{\bar{0}\}$ ili $J = R/A$. Dakle, R/A je prosti prsten.

Pretpostavimo da je R/A prosti prsten. Neka je $B \supseteq A$ ideal u R . Ako je $B \neq A$, onda postoji $x \in B \setminus A$. Ideali A i (x) su sadržani u B što povlači

$$J = A + (x) \subseteq B. \quad (2.56)$$

Uvedimo oznaku $J = A + (x)$. Kvocijent J/A je ideal u R/A i vrijedi $J/A \neq \{\bar{0}\}$ jer je J pravi nadskup od A . Ovo implicira $J/A = R/A$ jer je po pretpostavci R/A prosti prsten. Stoga je $J = R$ pa iz relacije (2.56) slijedi $B = R$. Dakle, $B = A$ ili $B = R$ što povlači da je A maksimalni ideal u R . ■

Ako je R komutativni prsten s jedinicom, onda vrijedi sljedeći rezultat.

Teorem 2.20. *Neka je R komutativni prsten s jedinicom. Ideal $M \subset R$ je maksimalan ako i samo ako je R/M polje.*

Dokaz Neka je M maksimalni ideal u R . Primijetimo da je $\bar{R} = R/M$ komutativni prsten s jedinicom $\bar{1} = 1 + M$, $1 \in R$. Dovoljno je dokazati da svaki element $\bar{a} \in \bar{R}$, $\bar{a} \neq \bar{0}$, ima multiplikativni inverz u $\bar{R}$. Prema Teoremu 2.19, $\bar{R}$ je prosti prsten što povlači $(\bar{a}) = \bar{R}$ jer je $(\bar{a}) \neq \{\bar{0}\}$. Nadalje, $(\bar{a}) = \bar{a} \bar{R} = \bar{R} \bar{a}$ jer je $\bar{R}$ komutativni prsten s jedinicom. Sada iz $\bar{R} = \bar{a} \bar{R} = \bar{R} \bar{a}$ slijedi da postoji $\bar{b} \in \bar{R}$ takav da je $\bar{1} = \bar{a} \bar{b} = \bar{b} \bar{a}$, odnosno $\bar{b} = \bar{a}^{-1}$. Dakle, $\bar{R}$ je polje.

Pretpostavimo sada da je $\bar{R}$ polje. Neka je $K \supseteq M$ ideal u R . Onda je K/M ideal u polju $\bar{R}$, pa je $K/M = \{\bar{0}\}$ ili $K/M = \bar{R}$ jer je svako polje prosti prsten. Ovo implicira $K = M$ ili $K = R$, stoga je M maksimalni ideal u R . ■

Ako je prsten bogat maksimalnim idealima, onda primjenom teorema 2.20 možemo konstruirati različita polja.

Primjer 2.32. Neka su R i S prsteni matrica nad poljem F definirani sa

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in F \right\}, \quad S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in F \right\}. \quad (2.57)$$

Preslikavanje $f: R \rightarrow S$ dano sa

$$f: \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \quad (2.58)$$

je epimorfizam prstena s jezgrom

$$\ker(f) = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in F \right\}. \quad (2.59)$$

Prema Fundamentalnom teoremu o izomorfizmu imamo $R/M \simeq S$ gdje je $M = \ker(f)$. Primijetimo da je $S \simeq F$ jer je preslikavanje $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mapsto a$ izomorfizam. Stoga je $R/M \simeq F$ pa iz Teorema 2.19 slijedi da je M maksimalni ideal u R . Naglasimo da zaključak ne možemo izvesti iz Teorema 2.20 jer R nije komutativni prsten s jedinicom. $\square$

Primjer 2.33. Neka je $\mathbb{R}[x]$ prsten polinoma nad poljem realnih brojeva $\mathbb{R}$. U prošlom odjeljku smo pokazali da su kvocijentni prsteni $\mathbb{R}[x]/(x)$ i $\mathbb{R}[x]/(x^2 + 1)$ izomorfni poljima $\mathbb{R}$ i $\mathbb{C}$:

$$\mathbb{R}[x]/(x) \simeq \mathbb{R}, \quad \mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}.$$

Prema teoremu 2.20, (x) i $(x^2 + 1)$ su maksimalni ideali u $\mathbb{R}[x]$. $\square$

Primjer 2.34. Pokažimo da je M maksimalni ideal u prstenu $\mathbb{Z}$ ako i samo ako je $M = (p)$ gdje je p prosti broj. Neka je M maksimalni ideal u $\mathbb{Z}$. Onda je $M = (p)$ za neki $p > 0$ jer je $\mathbb{Z}$ domena glavnih ideala. Prema Teoremu 2.20, kvocijentni prsten $\mathbb{Z}/(p)$ je polje. Pokažimo da je p prosti broj. Ako p nije prost, onda p možemo faktorizirati kao $p = n_1 n_2$ za neke $1 < n_1, n_2 < p$. Ovo implicira $\bar{p} = \bar{n}_1 \bar{n}_2 = \bar{0}$ što je kontradikcija s $\bar{n}_1, \bar{n}_2 \neq \bar{0}$ jer polje nema djelitelja nule. Dakle, p je prosti broj.

Pretpostavimo sada da je p prosti broj. Tvrđimo da je $\mathbb{Z}/(p)$ polje. Dovoljno je pokazati da svaki $\bar{a} \in \mathbb{Z}/(p)$, $\bar{a} \neq \bar{0}$, ima multiplikativni inverz u $\mathbb{Z}/(p)$. Ako je $0 < a < p$, onda je najveći zajednički djelitelj brojeva a i p jednak 1. Stoga postoje $m, n \in \mathbb{Z}$ takvi da je

$$ma + np = 1. \quad (2.60)$$

U kvocijentnom prstenu, jednakost (2.60) postaje

$$\bar{m} \bar{a} + \bar{n} \bar{p} = \bar{m} \bar{a} = \bar{1}$$

jer je $\bar{p} = \bar{0}$. Stoga je $\bar{m} \bar{a} = \bar{a} \bar{m} = \bar{1}$, odnosno $\bar{m} = \bar{a}^{-1}$ (gdje m uvijek možemo odabrati tako da je $0 < m < p$). Dakle, $\mathbb{Z}/(p)$ je polje pa iz Teorema 2.20 slijedi da je (p) maksimalni ideal u $\mathbb{Z}$. $\square$

Za kraj dokažimo rezultat koji opisuje maksimalne ideale u prstenu polinoma $F[x]$ gdje je F zadano polje.

Teorem 2.21. Neka je F polje. Onda je $M \subseteq F[x]$ maksimalni ideal u $F[x]$ ako i samo ako je $M = (p(x))$ gdje je $p(x)$ ireducibilni polinom u $F[x]$.

Dokaz Neka je $p(x) \in F[x]$ ireducibilan polinom. Prema teoremu 2.16 prsten $F[x]$ je domena glavnih ideala. Neka je $(h(x))$ ideal u $F[x]$ takav da $(h(x)) \supseteq (p(x))$. Tada je $p(x) \in (h(x))$ što povlači $p(x) = g(x)h(x)$ za neki $g(x) \in F[x]$. Kako je $p(x)$ ireducibilan polinom, to je

$g(x) = c$ ili $h(x) = c$. Ako je $g(x) = c$, onda je $(p(x)) = (c h(x)) = (h(x))$. Ako je $h(x) = c$, onda je $(h(x)) = (c) = F[x]$. Dakle, $(h(x)) = (p(x))$ ili $(h(x)) = F[x]$ što povlači da je $(p(x))$ maksimalni ideal u $F[x]$.

Pretpostavimo sada da je $(p(x))$ maksimalni ideal u $F[x]$, i neka je

$$p(x) = g(x)h(x) \tag{2.61}$$

za neke $g(x), h(x) \in F[x]$. Tada je $(p(x)) \subseteq (g(x))$ što povlači $(g(x)) = (p(x))$ ili $(g(x)) = F[x]$. Ako je $(g(x)) = (p(x))$, onda je $g(x) = k(x)p(x)$ za neki $k(x) \in F[x]$. Supstitucijom ovog izraza u (2.61) dobivamo

$$p(x) = k(x)p(x)h(x)$$

što implicira da su $k(x)$ i $h(x)$ konstantni polinomi. S druge strane, ako je $(g(x)) = F[x]$, onda je $g(x)$ konstantan polinom. U svakom slučaju iz jednačbe (2.61) dobivamo $g(x) = c$ ili $h(x) = c$ za neki $c \in F$ što pokazuje da je $p(x)$ ireducibilan polinom. ■

03

Moduli

3.1 Definicija i primjeri modula

U ovom poglavlju dajemo kratki osvrt na module i njihova osnovna svojstva. Modul je Abelova grupa čije elemente možemo množiti elementima nekog prstena. Na primjer, vektori u $\mathbb{R}^n$ tvore modul nad poljem $\mathbb{R}$ jer vektore možemo množiti realnim brojevima. Polinomi s koeficijentima u prstenu R također tvore modul nad R jer takve polinome možemo množiti elementima prstena R .

Definicija 3.1. Neka je R prsten, i neka je $(M, +)$ Abelova grupa. Kažemo da je M lijevi R -modul ako postoji preslikavanje $R \times M \rightarrow M$, $(r, m) \mapsto rm$, sa svojstvima

$$(i) \quad r(m_1 + m_2) = rm_1 + rm_2,$$

$$(ii) \quad (r_1 + r_2)m = r_1m + r_2m,$$

$$(iii) \quad (r_1r_2)m = r_1(r_2m),$$

$$(iv) \quad 1m = m \text{ ako je } 1 \in R,$$

za sve $r, r_1, r_2 \in R$ i $m, m_1, m_2 \in M$.

Ako je R polje, onda M nazivamo *vektorski prostor* nad poljem R . Operacija $(r, m) \mapsto rm$ naziva se množenje skalarom r , a prsten R se često naziva prsten skalara. Svojstva (i) i (ii) su zakoni distributivnosti u odnosu na zbrajanje u M i R , a svojstvo (iii) je zakon miješane asocijativnosti. Modul M se naziva lijevi R -modul jer je množenje rm definirano slijeva. Slično se definira desni R -modul.

Ako je R komutativni prsten i M je lijevi R -modul, onda M postaje desni R -modul ako definiramo

$$mr = rm, \quad r \in R, m \in M.$$

Lako se provjeri da za ovu definiciju vrijede aksiomi (i)-(iv) gdje je množenje skalarom

definirano zdesna. Za ilustraciju dokažimo svojstvo (iii). Zbog komutativnosti u R imamo

$$m(r_1r_2) = (r_1r_2)m = (r_2r_1)m = r_2(r_1m) = r_2(mr_1) = (mr_1)r_2.$$

U ovom slučaju lijevi R -modul je istovjetan desnom R -modulu pa ih ne trebamo razlikovati. Takve module jednostavno nazivamo R -moduli ili moduli nad prstenom R . U daljnjem tekstu R -modul će uvijek značiti lijevi modul osim ako nije naglašeno drugačije.

Primjer 3.1. Svaki prsten R je očigledno lijevi i desni R -modul. $\square$

Primjer 3.2. Ako je G aditivna Abelova grupa, onda je G lijevi $\mathbb{Z}$ -modul jer za sve $k, k_1, k_2 \in \mathbb{Z}$ i $g, g_1, g_2 \in G$ vrijedi

$$\begin{aligned} k(g_1 + g_2) &= kg_1 + kg_2, \\ (k_1 + k_2)g &= k_1g + k_2g, \\ (k_1k_2)g &= k_1(k_2g), \\ 1g &= g. \end{aligned}$$

$\square$

Primjer 3.3. Neka je $\mathbb{R}^n$ skup svih uređenih n -torki

$$(x_1, x_2, \dots, x_n), \quad x_i \in \mathbb{R}.$$

Skup $\mathbb{R}^n$ je Abelova grupa u odnosu na zbrajanje

$$(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n).$$

Neutralni element je

$$0 = (0, 0, \dots, 0),$$

a suprotni element je definiran s

$$-(x_1, x_2, \dots, x_n) = (-x_1, -x_2, \dots, -x_n).$$

Ako definiramo množenje $\mathbb{R} \times \mathbb{R}^n \rightarrow \mathbb{R}^n$ s

$$r(x_1, x_2, \dots, x_n) = (rx_1, rx_2, \dots, rx_n),$$

onda $\mathbb{R}^n$ postaje modul nad poljem $\mathbb{R}$. Ovaj modul nazivamo n -dimenzionalni realni vektorski prostor. $\square$

Primjer 3.4. Neka je $M(n, R)$ aditivna grupa matrica reda n nad prstenom R . Definirajmo množenje $R \times M(n, R) \rightarrow M(n, R)$ s

$$r[a_{ij}] = [ra_{ij}] \tag{3.1}$$

gdje je $[a_{ij}]$ matrica u $M(n, R)$. Tada množenje dano sa (3.1) daje strukturu lijevog R -modula na $M(n, R)$. $\square$

Neka su M i N lijevi moduli nad prstenom R . Ako na Kartezijevom umnošku $M \times N$ definiramo operacije

$$(x, y) + (x', y') = (x + x', y + y'),$$

$$r(x, y) = (rx, ry)$$

za sve $(x, y), (x', y') \in M \times N$ i $r \in R$, onda skup $M \times N$ postaje lijevi R -modul. Ovaj modul naziva se direktni umnožak modula M i N .

Navedimo neka elementarna svojstva R -modula M :

- (i) $0m = 0, m \in M, 0 \in R$,
- (ii) $r0 = 0, r \in R, 0 \in M$,
- (iii) $(-r)m = -(rm) = r(-m), r \in R, m \in M$.

Kada je iz konteksta jasno, nulu iz prstena R i nulu iz modula M označavamo istim simbolom 0 . Svojstva (i)–(iii) dokazuju se slično kao kod prstena, pa dokaz izostavljamo.

3.2 Podmoduli i direktne sume

U daljnjem tekstu svi rezultati se odnose na lijeve R -module koje ćemo jednostavno nazivati R -moduli. Analogni rezultati vrijede za desne R -module.

Definicija 3.2. Neka je M modul nad R . Neprazan podskup $N \subseteq M$ je podmodul od M ako vrijedi

- (i) $a - b \in N$ za sve $a, b \in N$,
- (ii) $ra \in N$ za sve $a \in N, r \in R$.

Ako je R polje, onda N nazivamo *vektorski podprostor* od M . Drugim riječima podmodul je Abelova podgrupa od M koja je zatvorena na množenje elementima iz prstena R . Očigledno su $\{0\}$ i M trivijalni podmoduli od M .

Primjer 3.5. Ako je I lijevi ideal u prstenu R , onda je I podmodul R -modula R . $\square$

Primjer 3.6. Neka je M modul nad R i neka je $x \in M$. Tada je skup

$$Rx = \{rx \mid r \in R\}$$

podmodul od M . Doista,

$$r_1x - r_2x = (r_1 - r_2)x \in Rx,$$

$$r_1(r_2x) = (r_1r_2)x \in Rx,$$

za sve $r_1, r_2 \in R$. Podmodul Rx općenito ne sadrži x osim ako R ima jedinicu jer je tada $x = 1x \in Rx$. $\square$

Primjer 3.7. Prsten polinoma $F[x]$ je vektorski prostor nad poljem F . Neka je $F_n[x]$ skup svih polinoma iz $F[x]$ do uključivo reda n . Tada je $F_n[x]$ vektorski podprostor prostora $F[x]$. $\square$

Definicija 3.3. Neka je M modul nad prstenom R i neka je $x \in M$. Najmanji podmodul od M koji sadrži x se naziva podmodul generiran elementom x .

Pokažimo da je skup

$$K = \{rx + nx \mid r \in R, n \in \mathbb{Z}\}$$

podmodul od M generiran elementom $x \in M$. Primijetimo da ovdje nx označava sumu $x + x + \cdots + x$ za $n > 0$, odnosno $-x - x \cdots - x$ za $n < 0$. K je Abelova podgrupa od M jer za svaki $r, s \in R$ i $n, m \in \mathbb{Z}$ vrijedi

$$(rx + nx) - (sx + mx) = (r - s)x + (n - m)x \in K.$$

Ako je $a \in R$, onda je

$$a(rx + nx) = (ar + na)x \in Rx$$

jer je $ar + na \in R$. Time je dokazano da je K podmodul od M . Nadalje, za $r = 0$ i $n = 1$ dobivamo $x \in K$. Neka je sada L bilo koji podmodul od M koji sadrži x . Tada prema definiciji 3.2 vrijedi $rx \in L$ i $nx \in L$ za svaki $r \in R$ i $n \in \mathbb{Z}$. Stoga je $rx + nx \in L$ što povlači $K \subseteq L$. Dakle, K je najmanji podmodul od M koji sadrži x .

Pretpostavimo sada da R ima jedinicu 1. Pokažimo da je u tom slučaju $K = Rx$. Doista, kako je $x = 1x$ imamo

$$rx + nx = (r + 1 + 1 + \cdots + 1)x \quad (\text{za } n > 0),$$

odnosno

$$rx + nx = (r - 1 - 1 - \cdots - 1)x \quad (\text{za } n < 0).$$

Dakle, ako R ima jedinicu, onda je $rx + nx = (r + n1)x \in Rx$ što povlači $K \subseteq Rx$. Inkluzija $Rx \subseteq K$ je trivijalna (za $n = 0$), pa zaključujemo da je $K = Rx$.

Teorem 3.1. Neka je $\{N_i\}_{i \in I}$ familija podmodula R -modula M . Tada je $\bigcap_{i \in I} N_i$ također podmodul od M .

Dokaz Neka su $x, y \in \bigcap_{i \in I} N_i$ i $a \in R$. Tada su $x, y \in N_i$ za svaki $i \in I$ iz čega slijedi $x - y \in N_i$ i $ax \in N_i$ za svaki $i \in I$. Dakle, $x - y \in \bigcap_{i \in I} N_i$ i $ax \in \bigcap_{i \in I} N_i$ što dokazuje da je $\bigcap_{i \in I} N_i$ podmodul od M . $\blacksquare$

Neka je S neprazan podskup R -modula M . Najmanji podmodul od M koji sadrži skup S nazivamo podmodul generiran skupom S i označavamo sa (S) . Ako je $S = \{x_1, x_2, \dots, x_n\}$,

onda koristimo oznaku $(S) = (x_1, x_2, \dots, x_n)$. Podmodul generiran skupom S tvori se na sljedeći način. Neka je $\mathcal{F} = \{N_k\}_{k \in J}$ familija podmodula od M koji sadrže skup S , $N_k \supseteq S$. $\mathcal{F}$ je neprazan skup jer je $M \in \mathcal{F}$. Prema teoremu 3.1 presjek $\bigcap_{k \in J} N_k$ je podmodul od M i $S \subseteq \bigcap_{k \in J} N_k$. Ako je N bilo koji podmodul koji sadrži S , onda je $N \in \mathcal{F}$ pa je $\bigcap_{k \in J} N_k \subset N$. Dakle, $\bigcap_{k \in J} N_k$ je najmanji podmodul koji sadrži S , tj.

$$(S) = \bigcap_{k \in J} N_k.$$

Definicija 3.4. Kažemo da je R -modul M konačno generirani modul ako je $M = (x_1, x_2, \dots, x_n)$ za neke $x_i \in M$, $1 \leq i \leq n$. Elemente x_i nazivamo generatori modula M . Ako je $M = (x)$ za neki $x \in M$, onda M nazivamo ciklički modul.

Neka su $x_1, x_2, \dots, x_n \in M$. Izraz

$$r_1x_1 + r_2x_2 + \dots + r_nx_n \quad (3.2)$$

nazivamo *linearna kombinacija* elemenata $x_1, x_2, \dots, x_n$. Skup svih takvih linearnih kombinacija označavamo s

$$\sum_{i=1}^n Rx_i = \{r_1x_1 + r_2x_2 + \dots + r_nx_n \mid r_i \in R, x_i \in M\}.$$

Sljedeći rezultat pokazuje da ako R ima jedinicu, onda se konačno generirani R -moduli sastoje točno od linearnih kombinacija (3.2).

Teorem 3.2. Neka je R prsten s jedinicom i neka je M modul nad R . Ako je M konačno generiran elementima $x_1, x_2, \dots, x_n$, onda je

$$M = \sum_{i=1}^n Rx_i. \quad (3.3)$$

Dokaz Pokažimo da je skup $\sum_{i=1}^n Rx_i$ podmodul od M . Neka su $m_1 = \sum_{i=1}^n r_i x_i$ i $m_2 = \sum_{i=1}^n s_i x_i$. Tada je

$$m_1 - m_2 = \sum_{i=1}^n (r_i - s_i)x_i \in \sum_{i=1}^n Rx_i.$$

Ako je $a \in R$, onda je

$$am_1 = \sum_{i=1}^n (ar_i)x_i \in \sum_{i=1}^n Rx_i.$$

Dakle, $\sum_{i=1}^n Rx_i$ je podmodul od M . Nadalje, svi generatori modula M su sadržani u $\sum_{i=1}^n Rx_i$ jer je $x_k = 1x_k \in \sum_{i=1}^n Rx_i$ za svaki $k = 1, 2, \dots, n$. Stoga je

$$(x_1, x_2, \dots, x_n) \subseteq \sum_{i=1}^n Rx_i \quad (3.4)$$

jer je $(x_1, x_2, \dots, x_n)$ najmanji modul koji sadrži sve generatore $x_1, x_2, \dots, x_n$. Po pretpostavci je $M = (x_1, x_2, \dots, x_n)$, pa iz relacije (3.4) slijedi $M = \sum_{i=1}^n Rx_i$. ■

Dakle, svaki element m konačno generiranog modula je linearna kombinacija $m = \sum_{i=1}^n r_i x_i$. Generatori nekog modula ne moraju biti jedinstveni. Neka je $F_n[x]$ vektorski prostor polinoma nad poljem F do uključivo stupnja n . Tada su

$$\{1, x, x^2, \dots, x^n\} \quad \text{i} \quad \{1, 1+x, x^2, \dots, x^n\}$$

dva različita skupa generatora prostora $F_n[x]$.

Definicija 3.5. Neka su $N_1, N_2, \dots, N_k$ podmoduli R -modula M . Podmodul generiran unijom $\bigcup_{i=1}^k N_i$ nazivamo suma podmodula N_i i označavamo s $\sum_{i=1}^k N_i$.

Prema ovoj definiciji je

$$\left(\bigcup_{i=1}^k N_i \right) = \sum_{i=1}^k N_i. \quad (3.5)$$

Ako je $M = \sum_{i=1}^k N_i$, onda kažemo da je M generiran podmodulima N_i . Struktura podmodula (3.5) karakterizirana je sljedećim teoremom (koji ujedno objašnjava oznaku $\sum_{i=1}^k N_i$).

Teorem 3.3. Neka su $N_1, N_2, \dots, N_k$ podmoduli R -modula M . Tada je

$$\sum_{i=1}^k N_i = \left\{ \sum_{i=1}^k x_i \mid x_i \in N_i \right\}. \quad (3.6)$$

Dokaz Neka je S skup svih konačnih suma $\sum_{i=1}^k x_i$, $x_i \in N_i$. Pokažimo da je S podmodul od M . Neka su $\sum_{i=1}^k x_i, \sum_{i=1}^k y_i \in S$, i neka je $a \in R$. Onda je

$$\sum_{i=1}^k x_i - \sum_{i=1}^k y_i = \sum_{i=1}^k (x_i - y_i) \in S$$

jer je $x_i - y_i \in N_i$ za svaki $1 \leq i \leq k$, i

$$a \sum_{i=1}^k x_i = \sum_{i=1}^k ax_i \in S$$

jer je $ax_i \in N_i$ za svaki $1 \leq i \leq k$. Očigledno je $\bigcup_{i=1}^k N_i \subseteq S$ jer je $N_i \subseteq S$ za svaki $1 \leq i \leq k$. Pokažimo da je S najmanji podmodul od M koji sadrži $\bigcup_{i=1}^k N_i$. Neka je K podmodul od M takav da $K \supseteq \bigcup_{i=1}^k N_i$. Tada K sadrži sve elemente oblika $\sum_{i=1}^k x_i$, $x_i \in N_i$, pa je $S \subseteq K$. Dakle, S je podmodul generiran skupom $\bigcup_{i=1}^k N_i$, pa je $\sum_{i=1}^k N_i$ dan izrazom (3.6). ■

Definicija 3.6. Neka su $N_1, N_2, \dots, N_k$ podmoduli R -modula M . Suma podmodula $\sum_{i=1}^k N_i$ naziva se direktna suma ako se svaki element $x \in \sum_{i=1}^k N_i$ može na jedinstven način zapisati kao $x = \sum_{i=1}^k x_i$, $x_i \in N_i$. Direktnu sumu označavamo s

$$N_1 \oplus N_2 \cdots \oplus N_k.$$

Ako direktna suma daje cijeli modul M , onda pišemo

$$M = N_1 \oplus N_2 \cdots \oplus N_k.$$

Za ilustraciju promotrimo vektorski prostor $V = \mathbb{R}^3$ nad poljem $\mathbb{R}$. Odaberimo vektore $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$ i $e_3 = (0, 0, 1)$. Svaki vektor $x = (x_1, x_2, x_3) \in V$ se može na jedinstven način napisati kao

$$x = x_1(1, 0, 0) + x_2(0, 1, 0) + x_3(0, 0, 1) = x_1e_1 + x_2e_2 + x_3e_3.$$

Stoga je $V = \mathbb{R}e_1 \oplus \mathbb{R}e_2 \oplus \mathbb{R}e_3$, direktna suma podprostora $\mathbb{R}e_i = \{re_i \mid r \in \mathbb{R}\}$.

Teorem 3.4. Neka su N_1 i N_2 podmoduli R -modula M . Tada je $M = N_1 \oplus N_2$ ako i samo ako je $M = N_1 + N_2$ i $N_1 \cap N_2 = \{0\}$.

Dokaz Pretpostavimo da je $M = N_1 \oplus N_2$. Tada je očigledno $M = N_1 + N_2$. Ako je $x \in N_1 \cap N_2$, onda x možemo rastaviti na sume

$$x = x + 0, \quad x \in N_1, 0 \in N_2 \quad \text{i} \quad x = 0 + x, \quad 0 \in N_1, x \in N_2.$$

Kako suma mora biti jedinstvena zaključujemo da je $x = 0$. Dakle $N_1 \cap N_2 = \{0\}$.

Pretpostavimo sada da je $M = N_1 + N_2$ i $N_1 \cap N_2 = \{0\}$. Tada se svaki $x \in M$ može napisati kao $x = x_1 + x_2$, $x_i \in N_i$. Pokažimo da je suma jedinstvena. Ako je $x = y_1 + y_2$ za neke $y_i \in N_i$, onda je $x_1 + x_2 = y_1 + y_2$, odnosno $x_1 - y_1 = y_2 - x_2$. Ovo povlači da je $x_1 - y_1 \in N_1 \cap N_2$ i $y_2 - x_2 \in N_1 \cap N_2$. Kako je $N_1 \cap N_2 = \{0\}$ zaključujemo da je $x_1 = y_1$ i $x_2 = y_2$. Time je dokazano da je $M = N_1 \oplus N_2$. ■

Na sličan način se pokazuje da je $M = N_1 \oplus N_2 \cdots \oplus N_k$ ako i samo ako je

$$M = \sum_{i=1}^k N_i \quad \text{i} \quad N_i \cap \sum_{j \neq i}^k N_j = \{0\} \quad \text{za sve } i = 1, 2, \dots, k.$$

3.3 Homomorfizmi modula i kvocijentni moduli

Definicija 3.7. Neka su M i N moduli nad prstenom R , i neka je $f: M \rightarrow N$ preslikavanje koje zadovoljava

$$(i) \quad f(x + y) = f(x) + f(y),$$

$$(ii) \quad f(rx) = rf(x),$$

za svaki $x, y \in M, r \in R$. Tada se f naziva linearno preslikavanje ili homomorfizam iz modula M u modul N . Ako je R polje, onda kažemo da je f linearna transformacija iz vektorskog prostora M u vektorski prostor N .

Skup svih homomorfizama $f: M \rightarrow N$ označavamo s $\text{Hom}_R(M, N)$. Ako je $M = N$, onda kažemo da je f endomorfizam modula M . Skup svih endomorfizama modula M označavamo s $\text{End}_R(M)$. Svaki homomorfizam modula $f: M \rightarrow N$ je također homomorfizam Abelovih grupa M i N , pa vrijedi

$$(i) \quad f(0) = 0,$$

$$(ii) \quad f(-x) = -f(x),$$

$$(iii) \quad f(x - y) = f(x) - f(y),$$

za svaki $x, y \in M$. Jezgra homomorfizma

$$\ker(f) = \{x \in M \mid f(x) = 0\}$$

je podmodul modula M , a slika homomorfizma

$$\text{Im}(f) = \{f(x) \mid x \in M\}$$

je podmodul modula N . Homomorfizam $f: M \rightarrow N$ je injekcija ako i samo ako je $\ker(f) = \{0\}$. Ako je homomorfizam $f: M \rightarrow N$ bijekcija, onda kažemo da je f izomorfizam modula. U tom slučaju su moduli M i N izomorfni i pišemo $M \simeq N$.

Primjer 3.8. Neka je R komutativni prsten, i neka je M modul nad R . Odaberimo $a \in R$ i definirajmo $f_a: M \rightarrow M$ s

$$f_a(x) = ax.$$

Tada je f_a homomorfizam. Doista, $f_a(x + y) = f_a(x) + f_a(y)$ slijedi trivijalno, a zbog komutativnosti prstena imamo

$$f_a(rx) = a(rx) = (ar)x = (ra)x = rf_a(x)$$

za svaki $x \in M, r \in R$. $\square$

Primjer 3.9. Definirajmo preslikavanje $\lambda_i: \mathbb{R}^n \rightarrow \mathbb{R}$ s

$$\lambda_i(x_1, x_2, \dots, x_n) = x_i.$$

λ_i je linearna transformacija iz $\mathbb{R}^n$ na $\mathbb{R}$ koju nazivamo projekcija na i -tu komponentu vektora x . $\square$

Primjer 3.10. Neka je $C^k(a, b)$ vektorski prostor funkcija $f: (a, b) \rightarrow \mathbb{R}$ koje imaju neprekidnu derivaciju do uključivo k -tog reda. Tada je derivacija $D: C^k(a, b) \rightarrow C^{k-1}(a, b)$,

$$D(f) = \frac{df}{dx}$$

linearna transformacija iz prostora $C^k(a, b)$ na prostor $C^{k-1}(a, b)$. $\square$

Skup $\text{Hom}_R(M, N)$ je Abelova grupa u kojoj je zbrajanje definirano po točkama,

$$(f + g)(x) = f(x) + g(x), \quad x \in M. \quad (3.7)$$

Ako je R komutativni prsten, onda možemo definirati množenje $R \times \text{Hom}_R(M, N) \rightarrow \text{Hom}_R(M, N)$ s

$$(rf)(x) = rf(x), \quad x \in M. \quad (3.8)$$

Doista, rf je linearno preslikavanje jer za svaki $x, y \in M$ i $a \in R$ vrijedi

$$(rf)(x + y) = rf(x + y) = rf(x) + rf(y) = (rf)(x) + (rf)(y), \quad (3.9)$$

$$(rf)(ax) = rf(ax) = (ra)f(x) = (ar)f(x) = a(rf)(x). \quad (3.10)$$

Primijetimo da je relacija (3.10) posljedica komutativnosti prstena R . Lako se pokazuje da zbrajanje i množenje definirano izrazima (3.7) i (3.8) zadovoljavaju aksiome modula, pa je $\text{Hom}_R(M, N)$ modul nad komutativnim prstenom R .

3.4 Kvocijentni modul

Definirajmo sada pojam kvocijentnog modula. Konstrukcija kvocijentnog modula sasvim je analogna konstrukciji kvocijentne grupe ili kvocijentnog prstena. Stoga su neki detalji ostavljeni čitatelju za provjeru. Neka je N podmodul R -modula M . Definirajmo relaciju ekvivalencije $\sim$ na M s

$$a \sim b \Leftrightarrow a - b \in N.$$

Klasa ekvivalencije koja sadrži element $a \in M$ je skup

$$\bar{a} = \{a + x \mid x \in N\} = a + N.$$

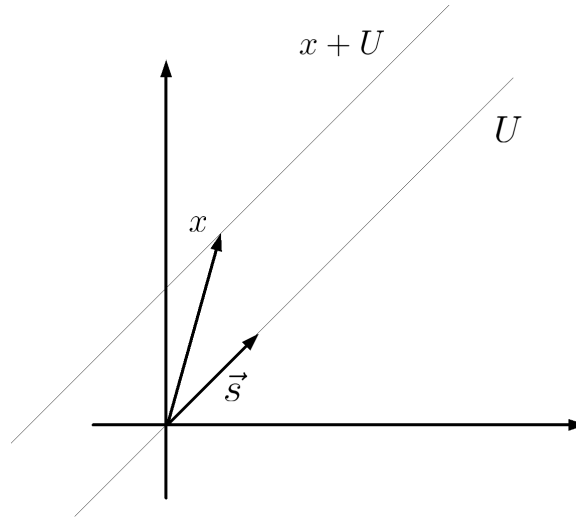
Skup svih klasa ekvivalencije na M označavamo s M/N ,

$$M/N = \{a + N \mid a \in M\}.$$

Na skupu M/N možemo definirati zbrajanje i množenje na sljedeći način:

$$(a + N) + (b + N) = (a + b) + N, \quad (3.11)$$

$$r(a + N) = ra + N, \quad (3.12)$$



Slika 3.1. Kvocijentni prostor se sastoji od pravaca koji su paralelni s pravcem U .

za svaki $a, b \in M$, $r \in R$. Može se pokazati da su operacije (3.11) i (3.12) dobro definirane, odnosno da ne ovise o predstavniku klase ekvivalencije. Ove operacije zadovoljavaju aksiome modula na skupu M/N kojeg nazivamo *kvocijentni modul*. Ako je R polje, onda M/N nazivamo *kvocijentni prostor*. Preslikavanje $\varphi: M \rightarrow M/N$,

$$\varphi(x) = x + N$$

naziva se *kanonska projekcija*. Zbog relacija (3.11) i (3.12) kanonska projekcija je očigledno homomorfizam iz modula M na modul M/N .

Kao primjer promotrimo podprostor vektorskog prostora $V = \mathbb{R}^3$ definiran s

$$U = \{(ts_1, ts_2, ts_3) \mid t \in \mathbb{R}\}, \quad s_1^2 + s_2^2 + s_3^2 > 0.$$

Podprostor U predstavlja pravac s vektorom smjera $s = (s_1, s_2, s_3) \neq 0$ koji prolazi ishodištem (vidi sliku 3.1). Opišimo kvocijentni prostor

$$V/U = \{x + U \mid x \in \mathbb{R}^3\}.$$

Klasa ekvivalencije

$$x + U = \{(x_1 + ts_1, x_2 + ts_2, x_3 + ts_3) \mid t \in \mathbb{R}\}$$

predstavlja pravac koji prolazi točkom $x = (x_1, x_2, x_3)$ i ima vektor smjera $\vec{s}$. Dakle, kvocijentni prostor V/U se sastoji od svih pravaca koji su paralelni sa zadanim pravcem U .

Sljedeći rezultat je analogan fundamentalnom teoremu o homomorfizmima grupa ili prstena.

Teorem 3.5. *Neka su M i N moduli nad R i neka je $f: M \rightarrow N$ homomorfizam modula. Tada je*

$$M/\ker(f) \simeq \operatorname{Im}(f).$$

Dokaz Dokaz je sličan dokazu teorema 2.10 pa detalje izostavljamo. Definirajmo podmodul $K = \ker(f)$ i preslikavanje

$$\varphi: M/K \rightarrow N, \quad \varphi(x + K) = f(x).$$

Preslikavanje φ je dobro definirano. Ako je $x + K = y + K$, onda je $x - y \in K$ što implicira $f(x - y) = 0$, odnosno $f(x) = f(y)$. Lako se pokazuje da je φ homomorfizam modula:

$$\begin{aligned} \varphi((x + K) + (y + K)) &= f(x + y) = f(x) + f(y) = \varphi(x + K) + \varphi(y + K), \\ \varphi(r(x + K)) &= f(rx) = rf(x) = r\varphi(x + K), \end{aligned}$$

za sve $x, y \in M, r \in R$. Nadalje, φ je injekcija jer $\varphi(x + K) = \varphi(y + K)$ povlači $f(x) = f(y)$, odnosno $f(x - y) = 0$ pa je $x - y \in K$. Odavde slijedi $x + K = y + K$. Kako je $\text{Im}(\varphi) = \text{Im}(f)$ preslikavanje $\varphi: M/K \rightarrow \text{Im}(f)$ je bijekcija. Stoga su moduli $M/\ker(f)$ i $\text{Im}(f)$ izomorfni. ■

Kao primjenu teorema 3.5 navedimo sljedeći rezultat.

Teorem 3.6. *Neka je R prsten s jedinicom $1 \in R$, i neka je M modul nad R . Tada je M ciklički modul ako i samo ako je $M \simeq R/I$ za neki lijevi ideal $I \subseteq R$.*

Dokaz Pretpostavimo da je $M = Rx$ ciklički modul. Definirajmo preslikavanje $f: R \rightarrow Rx$, $f(r) = rx$, gdje R promatramo kao R -modul. Očigledno je f surjekcija i homomorfizam modula jer je $f(r + s) = rx + sx = f(r) + f(s)$ i $f(rs) = (rs)x = rf(s)$. Prema teoremu 3.5 je $R/\ker(f) \simeq Rx$. Jezgra homomorfizma f , $\ker(f) = \{r \in R \mid rx = 0\}$, naziva se anihilator elementa $x \in M$ i označava s $\text{Ann}(x)$. Dakle,

$$R/\text{Ann}(x) \simeq Rx = M.$$

Pretpostavimo sada da je $M \simeq R/I$ za neki lijevi ideal $I \subseteq R$. R -modul R/I je generiran elementom $1 + I$ jer je $R/I = \{r(1 + I) \mid r \in R\} = R(1 + I)$. Stoga je M ciklički modul. ■

04

Pregled ostalih algebarskih struktura

U ovom poglavlju dajemo pregled nekih algebarskih struktura koje su važne u različitim granama matematike i fizike. Poglavlje je isključivo informativnog karaktera i služi da studenta upozna s osnovnim pojmovima iz teorije asocijativnih algebri, Liejevih i Weylovih algebri. Stoga je prezentacija nužno nepotpuna i donosi samo letimičan pregled ideja vezanih za ove algebarske strukture prema autorovom odabiru.

4.1 Asocijativne algebre

Definicija 4.1. *Asocijativna algebra nad poljem $\mathbb{F}$ je vektorski prostor nad $\mathbb{F}$ na kojem je definirano bilinearano preslikavanje $m: A \times A \rightarrow A$, $m(a, b) = ab$, koje zadovoljava $a(bc) = (ab)c$ za sve $a, b, c \in A$.*

Preslikavanje $m: A \times A \rightarrow A$ nazivamo množenje u algebri A . Primijetimo da bilinearnost množenja povlači da za sve $a, b, c \in A$ i $\lambda \in \mathbb{F}$ vrijedi

- (i) $(a + b)c = ac + bc$,
- (ii) $a(b + c) = ab + ac$,
- (iii) $(\lambda a)b = a(\lambda b) = \lambda(ab)$.

Asocijativnost i distributivnost množenja povlače da je A prsten u kojem su zbrajanje i množenje isti kao u algebri A .

Definicija 4.2. *Kažemo da je A unitalna algebra ili algebra s jedinicom ako postoji element $1 \in A$ takav da je $1a = a1 = a$ za svaki $a \in A$.*

Ako postoji, jedinični element je jedinstven. Napomenimo da se definicija algebre ponešto razlikuje ovisno o literaturi. Neki autori podrazumijevaju da algebra A uvijek ima jedinicu ili da je $\mathbb{F}$ komutativni prsten s jedinicom.

Primjer 4.1. Neka je V vektorski prostor nad poljem $\mathbb{F}$ i neka je $\text{End}_{\mathbb{F}}(V)$ skup svih linearnih transformacija na prostoru V . Na $\text{End}_{\mathbb{F}}(V)$ su definirane operacije zbrajanja i kompozicije, te množenja skalarom:

$$(f + g)(u) = f(u) + g(u),$$

$$(f \circ g)(u) = f(g(u)),$$

$$(\lambda f)(u) = \lambda f(u),$$

za sve $\lambda \in \mathbb{F}$ i $u \in V$. $\text{End}_{\mathbb{F}}(V)$ je vektorski prostor nad $\mathbb{F}$ u odnosu na ove operacije. Množenje definirano kompozicijom $m(f, g) = f \circ g$ je bilinearно jer su f i g linearna preslikavanja. $\text{End}_{\mathbb{F}}(V)$ je algebra nad $\mathbb{F}$ s jedinicom id_V gdje je id_V identiteta na V . $\square$

Primjer 4.2. Prsten kvaterniona $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$ s tablicom množenja

$$i^2 = j^2 = k^2 = -1, \quad (4.1)$$

$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j. \quad (4.2)$$

je algebra nad poljem realnih brojeva $\mathbb{R}$. $\square$

Primjer 4.3. Skup $M(n, \mathbb{F})$ matrica reda n nad poljem $\mathbb{F}$ je algebra nad $\mathbb{F}$ s operacijama zbrajanja i množenja matrica, te množenja matrica skalarom. Jedinica u $M(n, \mathbb{F})$ je jedinična matrica I_n . $\square$

Primjer 4.4. Prsten polinoma $\mathbb{F}[x]$ je algebra nad poljem $\mathbb{F}$ gdje je množenje skalarom definirano s

$$\lambda \left(\sum_{k=0}^n \alpha_k x^k \right) = \sum_{k=0}^n (\lambda \alpha_k) x^k.$$

Konstantni polinom $p(x) = 1$ je jedinica u algebri $\mathbb{F}[x]$. $\square$

Primjer 4.5. Neka je $G = \{g_1 = e, g_2, \dots, g_n\}$ konačna grupa i neka je $\mathbb{F}$ polje. Neka je $\mathbb{F}[G]$ vektorski prostor nad $\mathbb{F}$ čija baza je skup G . Elementi prostora $\mathbb{F}[G]$ su konačne linearne kombinacije $\sum_i \alpha_i g_i$, $\alpha_i \in \mathbb{F}$. Zbrajanje i množenje skalarom je definirano na prirodan način, dok je umnožak u $\mathbb{F}[G]$ definiran s

$$\left(\sum_i \alpha_i g_i \right) \left(\sum_j \beta_j g_j \right) = \sum_{i,j} \alpha_i \beta_j (g_i g_j).$$

Algebra $\mathbb{F}[G]$ s ovako definiranim operacijama zbrajanja i množenja naziva se algebra konačne grupe. Jedinica u algebri $\mathbb{F}[G]$ je jedinica u grupi G , tj. $1 = e$. $\square$

Definicija 4.3. Algebra A je komutativna ako je $ab = ba$ za svaki $a, b \in A$.

Algebre $\text{End}_{\mathbb{F}}(V)$ za $\dim V \geq 2$ i $M(n, \mathbb{F})$ za $n \geq 2$, te algebra kvaterniona $\mathbb{H}$ su nekomutativne, dok je $\mathbb{F}[x]$ komutativna algebra.

Definicija 4.4. *Dimenzija algebre A je dimenzija vektorskog prostora A nad poljem $\mathbb{F}$.*

Algebre mogu biti konačno i beskonačno dimenzionalne. Na primjer, $M(n, \mathbb{F})$ je n^2 -dimenzionalna algebra s bazom

$$E_{ij} = \begin{pmatrix} 0 & \vdots & 0 \\ \cdots & 1 & \cdots \\ 0 & \vdots & 0 \end{pmatrix}, \quad 1 \leq i, j \leq n,$$

gdje se element 1 nalazi u i -tom retku i j -tom stupcu, a ostali elementi su jednaki nuli. S druge strane, algebra polinoma $\mathbb{F}[x]$ je beskonačno dimenzionalna jer je prostor $\mathbb{F}[x]$ razapet monomima $\{1, x, x^2, \dots\}$.

Definicija 4.5. *Neka je A algebra nad poljem $\mathbb{F}$. Podskup $B \subseteq A$ je podalgebra od A ako je B podprsten prstena A i podprostor vektorskog prostora A .*

Primjer 4.6. Skup kompleksnih brojeva $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ je podalgebra algebre kvaterniona $\mathbb{H}$. $\square$

Definicija 4.6. *Neka su A i B algebre nad poljem $\mathbb{F}$. Preslikavanje $\varphi: A \rightarrow B$ koje za sve elemente $a, b \in A$ i $\lambda \in \mathbb{F}$ zadovoljava*

$$(i) \quad \varphi(\lambda a) = \lambda \varphi(a),$$

$$(ii) \quad \varphi(a + b) = \varphi(a) + \varphi(b),$$

$$(iii) \quad \varphi(ab) = \varphi(a)\varphi(b),$$

naziva se homomorfizam algebri. Ako je φ bijekcija, onda je φ izomorfizam algebri.

Od posebnog su značaja homomorfizmi algebri koje nazivamo *reprezentacije*.

Definicija 4.7. *Neka je A asocijativna algebra nad poljem $\mathbb{F}$. Reprezentacija algebre A je uređeni par (ρ, V) gdje je V vektorski prostor nad $\mathbb{F}$ i $\rho: A \rightarrow \text{End}_{\mathbb{F}}(V)$ je homomorfizam algebri. Ako A ima jedinicu 1, onda je $\rho(1) = \text{id}_V$.*

Neka je A unitalna algebra nad poljem $\mathbb{F}$. Svakom elementu $a \in A$ možemo pridružiti linearno preslikavanje $a_L \in \text{End}_{\mathbb{F}}(A)$ dano s $a_L(x) = ax$. Definirajmo $\rho: A \rightarrow \text{End}_{\mathbb{F}}(A)$, $\rho(a) = a_L$.

Pokažimo da je ρ homomorfizam algebri. Za sve $a, b, x \in A$ i $\lambda \in \mathbb{F}$ imamo

$$\begin{aligned}\rho(a+b)(x) &= (a+b)x = ax + bx = \rho(a)(x) + \rho(b)(x), \\ \rho(\lambda a)(x) &= (\lambda a)x = \lambda(ax) = \lambda\rho(a)(x), \\ \rho(ab)(x) &= (ab)x = a(bx) = \rho(a)(\rho(b)(x)) = \rho(a) \circ \rho(b)(x).\end{aligned}$$

Zaključujemo da je $\rho(a+b) = \rho(a) + \rho(b)$, $\rho(\alpha a) = \alpha\rho(a)$ i $\rho(ab) = \rho(a) \circ \rho(b)$, stoga je ρ reprezentacija algebre A na vektorskom prostoru A . Preslikavanje $a \mapsto \rho(a)$ je injektivno jer je A unitalna algebra. Doista, ako je $\rho(a) = \rho(b)$, onda $\rho(a)(1) = \rho(b)(1)$ implicira $a1 = b1$, odnosno $a = b$. Ovu reprezentaciju nazivamo *regularna reprezentacija*.

Pretpostavimo da je A konačno dimenzionalna algebra dimenzije n . Tada svakoj linearnoj transformaciji a_L možemo pridružiti matricu $[a_L]$ s obzirom na odabranu bazu prostora A . U tom slučaju homomorfizam $\rho: A \rightarrow M(n, \mathbb{F})$, $\rho(a) = [a_L]$, nazivamo regularna matrična reprezentacija od A .

Primjer 4.7. Neka je $\mathbb{H}$ kvaternionska algebra nad $\mathbb{R}$ s bazom $\mathcal{B} = \{1, i, j, k\}$ gdje elementi baze zadovoljavaju relacije (4.1)-(4.2). Odredimo regularnu matričnu reprezentaciju $\rho: \mathbb{H} \rightarrow M(4, \mathbb{R})$ u odnosu na bazu $\mathcal{B}$. Neka je $u = a_01 + a_1i + a_2j + a_3k \in \mathbb{H}$. Matrica transformacije $\rho(u) = [u_L]$ je dana s

$$[u_L] = [u_L(1) \mid u_L(i) \mid u_L(j) \mid u_L(k)]$$

gdje se u stupcima nalaze komponente vektora $u_L(b) = ub$, $b \in \mathcal{B}$. Nalazimo

$$\begin{aligned}u_L(1) &= u \cdot 1 = a_01 + a_1i + a_2j + a_3k, \\ u_L(i) &= u \cdot i = -a_1 + a_0i + a_3j - a_2k, \\ u_L(j) &= u \cdot j = -a_2 - a_3i + a_0j + a_1k, \\ u_L(k) &= u \cdot k = -a_3 + a_2i - a_1j + a_0k.\end{aligned}$$

Dakle, regularna reprezentacija je dana s

$$\rho(u) = \begin{pmatrix} a_0 & -a_1 & -a_2 & -a_3 \\ a_1 & a_0 & -a_3 & a_2 \\ a_2 & a_3 & a_0 & -a_1 \\ a_3 & -a_2 & a_1 & a_0 \end{pmatrix}.$$

□

4.2 Liejeve algebre

Liejeve algebre su neasocijativne algebre koje imaju važnu primjenu u matematici i teorijskoj fizici. Otkriće Liejevih algebri vezano je uz pojam Liejevih grupa koje je uveo norveški matematičar Sophus Lie u proučavanju neprekidnih simetrija diferencijalnih jednadžbi. U daljnjem tekstu $\mathbb{F}$ označava polje realnih ili kompleksnih brojeva.



Slika 4.1. Marius Sophus Lie, 1842-1899. Lie je tvorac teorije neprekidnih simetrija koje su našle primjenu u proučavanju diferencijalnih jednažbi.

Definicija 4.8. Liejeva algebra $\mathfrak{g}$ je vektorski prostor nad poljem $\mathbb{F}$ na kojem je definirano preslikavanje $[\cdot, \cdot]: \mathfrak{g} \times \mathfrak{g} \rightarrow \mathfrak{g}$ koje zadovoljava sljedeće uvjete:

(i) linearnost

$$[ax + by, z] = a[x, z] + b[y, z] \text{ za sve } a, b \in \mathbb{F} \text{ i } x, y, z \in \mathfrak{g},$$

(ii) antisimetričnost

$$[x, y] = -[y, x] \text{ za sve } x, y \in \mathfrak{g},$$

(iii) Jacobijev identitet

$$[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0 \text{ za sve } x, y, z \in \mathfrak{g}.$$

Preslikavanje $[\cdot, \cdot]$ nazivamo Liejeva zagrada. Iz uvjeta (i) i (ii) slijedi da je Liejeva zagrada bilinearно preslikavanje, dok uvjet (ii) povlači da je

$$[x, x] = 0 \text{ za svaki } x \in \mathfrak{g}.$$

Ako je $\mathbb{F} = \mathbb{R} (\mathbb{C})$, onda kažemo da je $\mathfrak{g}$ realna (kompleksna) Liejeva algebra. Dimenzija Liejeve algebre je dimenzija vektorskog prostora $\mathfrak{g}$ nad $\mathbb{F}$. Liejevu algebru možemo interpretirati kao algebru čiji je umnožak $[x, y]$ antikomutativan, a umjesto asocijativnosti zadovoljava Jacobijev identitet. Navedimo neke važne primjere Liejevih algebri.

Primjer 4.8. Neka je A asocijativna algebra. Tada $[a, b] = ab - ba$ definira Liejevu zgradu na A . Jacobijev identitet slijedi iz asocijativnosti množenja u A :

$$\begin{aligned} [a, [b, c]] + [b, [c, a]] + [c, [a, b]] &= a(bc - cb) - (bc - cb)a \\ &\quad + b(ca - ac) - (ca - ac)b \\ &\quad + c(ab - ba) - (ab - ba)c = 0. \end{aligned}$$

Posebno važan primjer je asocijativna algebra $\text{End}_{\mathbb{F}}(V)$ linearnih operatora na vektorskom prostoru V s operacijama zbrajanja i kompozicije operatora. Tada je $[A, B] = A \circ B - B \circ A$ Liejeva zagrada na $\text{End}_{\mathbb{F}}(V)$. $\square$

Primjer 4.9. Ako je $A = M(n, \mathbb{F})$ algebra matrica reda n nad poljem $\mathbb{F}$, onda je A n^2 -dimenzionalna Liejeva algebra sa zagradom $[A, B] = AB - BA$. U tom slučaju Liejevu zagradu nazivamo komutator matrica A i B . $\square$

Primjer 4.10. Neka je $\mathbb{R}^3$ realni vektorski prostor s elementima $\vec{u} = (u_1 \ u_2 \ u_3)^t$, gdje t označava transponiranje, na kojem je zagrada definirana kao vektorski umnožak

$$[\vec{u}, \vec{v}] = \vec{u} \times \vec{v} = \begin{pmatrix} u_2 v_3 - u_3 v_2 \\ u_3 v_1 - u_1 v_3 \\ u_1 v_2 - u_2 v_1 \end{pmatrix}. \quad (4.3)$$

Linearnost i antisimetričnost zagrade su očigledni iz svojstava vektorskog umnoška, dok Jacobijev identitet slijedi iz vektorskog identiteta

$$\vec{u} \times (\vec{v} \times \vec{w}) + \vec{v} \times (\vec{w} \times \vec{u}) + \vec{w} \times (\vec{u} \times \vec{v}) = \vec{0} \quad \text{za sve } \vec{u}, \vec{v}, \vec{w} \in \mathbb{R}^3.$$

Prostor $\mathbb{R}^3$ sa zagradom $[\vec{u}, \vec{v}] = \vec{u} \times \vec{v}$ je trodimenzionalna Liejeva algebra. $\square$

Primjer 4.11. Neka je $C^\infty(\mathbb{R}^{2n})$ prostor glatkih funkcija $f: \mathbb{R}^{2n} \rightarrow \mathbb{R}$,

$$f(q, p) = f(q_1, q_2, \dots, q_n, p_1, p_2, \dots, p_n).$$

Definirajmo zagradu na $C^\infty(\mathbb{R}^{2n})$ s

$$[f, g] = \sum_{i=1}^n \left(\frac{\partial f}{\partial q_i} \frac{\partial g}{\partial p_i} - \frac{\partial f}{\partial p_i} \frac{\partial g}{\partial q_i} \right). \quad (4.4)$$

Zagrada (4.4) naziva se Poissonova zagrada i igra važnu ulogu u fizici, naročito u teorijskoj mehanici. Poissonova zagrada je bilinearna jer su parcijalne derivacije linearni operatori, dok je antisimetričnost zagrade očigledna. Izravnim računom se provjeri da Jacobijev identitet vrijedi jer parcijalne derivacije drugog reda komutiraju,

$$\frac{\partial^2 f}{\partial q_i \partial p_j} = \frac{\partial^2 f}{\partial p_j \partial q_i}.$$

Prostor $C^\infty(\mathbb{R}^{2n})$ s Poissonovom zagradom (4.4) je primjer beskonačno dimenzionalne Liejeve algebre. $\square$

Primjer 4.12. *Heisenbergova Liejeva algebra.* Neka je $(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n, z)$ baza vektorskog prostora V nad poljem $\mathbb{F}$. Na V možemo definirati strukturu Liejeve algebre tako da definiramo zagradu sa

$$[x_i, y_i] = -[y_i, x_i] = z$$

i gdje su zagrade ostalih elemenata jednake nuli. Element z komutira sa svim elementima baze pa ga nazivamo centralni element. Heisenbergova algebra se može prikazati pomoću



Slika 4.2. Simeon Denis Poisson, 1781-1840, francuski matematičar i fizičar.

matrica na sljedeći način. Definirajmo redak vektore $e_i = (0, \dots, 1, \dots, 0) \in \mathbb{F}^n$ gdje se 1 nalazi na i -tom mjestu. Elementima baze pridružimo matrice

$$X_i = \begin{pmatrix} 0 & e_i & 0 \\ 0 & 0_n & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad Y_i = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0_n & e_i^t \\ 0 & 0 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0_n & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad (4.5)$$

gdje je 0_n nul-matrica reda n . Lako se provjeri da matrice (4.5) zadovoljavaju komutacijske relacije Heisenbergove algebre. Opći element algebre možemo prikazati kao linearnu kombinaciju

$$X = \sum_{i=1}^n u_i X_i + \sum_{i=1}^n v_i Y_i + cZ = \begin{pmatrix} 0 & u & c \\ 0 & 0_n & v^t \\ 0 & 0 & 0 \end{pmatrix}, \quad u_i, v_i, c \in \mathbb{F}.$$

□

Neka je $\mathfrak{g}$ n -dimenzionalna Liejeva algebra nad poljem $\mathbb{F}$ i neka je $\{E_1, E_2, \dots, E_n\}$ baza prostora $\mathfrak{g}$. Tada je

$$[E_i, E_j] = \sum_{k=1}^n C_{ij}^k E_k \quad (4.6)$$

za neke konstante $C_{ij}^k \in \mathbb{F}$ koje nazivamo *strukturne konstante* algebre $\mathfrak{g}$. Kažemo da je $\mathfrak{g}$ Liejeva algebra generirana elementima $E_1, E_2, \dots, E_n$. Antisimetričnost i Jacobijev identitet povlače da strukturne konstante zadovoljavaju

$$C_{ij}^k = -C_{ji}^k, \quad (4.7)$$

$$\sum_{m=1}^n (C_{ij}^m C_{mk}^r + C_{jk}^m C_{mi}^r + C_{ki}^m C_{mj}^r) = 0. \quad (4.8)$$

Struktura algebre $\mathfrak{g}$ potpuno je određena konstantama C_{ij}^k . Ako su poznati koeficijenti C_{ij}^k , onda zbog bilinearnosti Liejeve zgrade iz jednadžbe (4.6) možemo izračunati $[x, y]$ za sve

$x, y \in \mathfrak{g}$. Obrnuto, bilo koji skup konstanti C_{ij}^k koji zadovoljava uvjete (4.7) i (4.8) definira Liejevu algebru sa zagradom (4.6) koja se bilinearно proširuje na cijelu algebru $\mathfrak{g}$.

Definicija 4.9. Neka je $\mathfrak{g}$ Liejeva algebra sa zagradom $[\cdot, \cdot]$ i neka je $\mathfrak{h}$ vektorski podprostor od $\mathfrak{g}$. Ako je $[X, Y] \in \mathfrak{h}$ za sve $X, Y \in \mathfrak{h}$, onda kažemo da je $\mathfrak{h}$ Liejeva podalgebra od $\mathfrak{g}$.

Definicija 4.10. Neka su $\mathfrak{g}$ i $\mathfrak{h}$ Liejeve algebre nad poljem $\mathbb{F}$. Linearno preslikavanje $\varphi: \mathfrak{g} \rightarrow \mathfrak{h}$ koje zadovoljava uvjet

$$\varphi([x, y]) = [\varphi(x), \varphi(y)]$$

za sve $x, y \in \mathfrak{g}$ naziva se homomorfizam Liejevih algebri. Ako je φ bijektivno preslikavanje, onda φ nazivamo izomorfizam Liejevih algebri.

Važan primjer homomorfizma Liejevih algebri je adjungirana reprezentacija

$$\text{ad}: \mathfrak{g} \rightarrow \text{End}_{\mathbb{F}}(\mathfrak{g}).$$

Za svaki $x \in \mathfrak{g}$ operator $\text{ad}(x): \mathfrak{g} \rightarrow \mathfrak{g}$ je definiran s

$$\text{ad}(x)(y) = [x, y].$$

Zbog bilinearnosti Liejeve zagrade operator $\text{ad}(x)$ je linearan. Iz istog razloga je preslikavanje $x \mapsto \text{ad}(x)$ linearно. Da bismo pokazali da je adjungirana reprezentacija homomorfizam Liejevih algebri potrebno je provjeriti da je

$$\text{ad}([x, y]) = \text{ad}(x) \circ \text{ad}(y) - \text{ad}(y) \circ \text{ad}(x),$$

odnosno

$$[[x, y], z] = [x, [y, z]] - [y, [x, z]] \quad \text{za svaki } z \in \mathfrak{g}.$$

Primijetimo da je ovo svojstvo ekvivalentno Jacobijevom identitetu. Iz Jacobijevog identiteta također slijedi da $\text{ad}(x)$ zadovoljava Leibnizovo pravilo u odnosu na zagradu $[y, z]$:

$$\text{ad}(x)([y, z]) = [\text{ad}(x)(y), z] + [y, \text{ad}(x)(z)].$$

Linearno preslikavanje $D: \mathfrak{g} \rightarrow \mathfrak{g}$ za koje vrijedi $D([a, b]) = [D(a), b] + [a, D(b)]$ nazivamo derivacija, a preslikavanje $\text{ad}(x): \mathfrak{g} \rightarrow \mathfrak{g}$ naziva se unutarnja derivacija.

Primjer 4.13. Promotrimo vektorski prostor antisimetričnih matrica

$$\mathfrak{h} = \{X \in M(3, \mathbb{R}) \mid X^t + X = 0\}. \quad (4.9)$$

Pokažimo da je komutator $[X, Y] = XY - YX$ zatvoren u $\mathfrak{h}$ što implicira da je $\mathfrak{h}$ podalgebra Liejeve algebre $M(3, \mathbb{R})$. Ako su $X, Y \in \mathfrak{h}$, onda je $X^t = -X$ i $Y^t = -Y$ što povlači

$$[X, Y]^t = (XY)^t - (YX)^t = Y^t X^t - X^t Y^t = (-Y)(-X) - (-X)(-Y) = -[X, Y].$$

Dakle, $[X, Y] \in \mathfrak{h}$ za sve $X, Y \in \mathfrak{h}$. Svaka matrica $X \in \mathfrak{h}$ se može napisati u obliku

$$X = \begin{pmatrix} 0 & -c & b \\ c & 0 & -a \\ -b & a & 0 \end{pmatrix}$$

za neke $a, b, c \in \mathbb{R}$. Stoga se X može rastaviti na jedinstvenu linearnu kombinaciju

$$X = aL_1 + bL_2 + cL_3$$

gdje su

$$L_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}, \quad L_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix}, \quad L_3 = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Matrice L_1, L_2, L_3 tvore bazu vektorskog prostora $\mathfrak{h}$. Komutatori matrica L_i su dani s

$$[L_1, L_2] = L_3, \quad [L_2, L_3] = L_1, \quad [L_3, L_1] = L_2 \quad (4.10)$$

što kraće možemo zapisati kao

$$[L_i, L_j] = \sum_{k=1}^3 \varepsilon_{ijk} L_k \quad (4.11)$$

gdje je ε_{ijk} Levi-Civita simbol

$$\varepsilon_{ijk} = \begin{cases} +1, & (ijk) \text{ je parna permutacija od } (1\,2\,3), \\ -1, & (ijk) \text{ je neparna permutacija od } (1\,2\,3), \\ 0, & \text{ako se indeks } i, j \text{ ili } k \text{ ponavlja.} \end{cases}$$

Iz jednadžbe (4.11) vidimo da su strukturne konstante algebre (4.9) dane s $C_{ij}^k = \varepsilon_{ijk}$. Algebra (4.9) je primjer klasične Liejeve algebre koju nazivamo $so(3)$. $\square$

Algebra $\mathfrak{so}(3)$ je izomorfna Liejevoj algebri $\mathbb{R}^3$ s Liejevom zagradom $[\vec{u}, \vec{v}] = \vec{u} \times \vec{v}$. Neka su $\vec{e}_1 = (1\,0\,0)^t$, $\vec{e}_2 = (0\,1\,0)^t$ i $\vec{e}_3 = (0\,0\,1)^t$ vektori koji tvore kanonsku bazu prostora $\mathbb{R}^3$. Vektorski umnožak elemenata baze dan je s

$$\vec{e}_1 \times \vec{e}_2 = \vec{e}_3, \quad \vec{e}_2 \times \vec{e}_3 = \vec{e}_1, \quad \vec{e}_3 \times \vec{e}_1 = \vec{e}_2. \quad (4.12)$$

Usporedba s jednadžbom (4.10) sugerira da vektor $\vec{e}_i$ ima istu ulogu kao matrica L_i . Definirajmo linearno preslikavanje $\varphi: \mathbb{R}^3 \rightarrow \mathfrak{so}(3)$ s $\varphi(\vec{e}_i) = L_i$. Tada je φ izomorfizam Liejevih algebri jer iz relacija (4.10) i (4.12) dobivamo

$$\varphi([\vec{e}_i, \vec{e}_j]) = [L_i, L_j]$$

što povlači da je $\varphi([\vec{u}, \vec{v}]) = [\varphi(\vec{u}), \varphi(\vec{v})]$ za sve $\vec{u}, \vec{v} \in \mathbb{R}^3$.

4.3 Klasične Liejeve algebre

Klasične Liejeve algebre se prirodno pojavljuju u proučavanju određenih simetrija u matematici i teorijskoj fizici. Ovdje ćemo dati kratak opis nekih od njih.

4.3.1 Opća i specijalna linearna Liejeva algebra

Algebru $M(n, \mathbb{F})$ s matričnim komutatorom $[A, B] = AB - BA$ nazivamo opća linearna Liejeva algebra nad poljem $\mathbb{F}$ i označavamo s $\mathfrak{gl}(n, \mathbb{F})$.

Trag matrice $A = [a_{ij}]$ je funkcija $\text{Tr}(A) = \sum_{i=1}^n a_{ii}$. Primijetimo da je $\text{Tr}(AB) = \text{Tr}(BA)$ što implicira $\text{Tr}([A, B]) = \text{Tr}(AB) - \text{Tr}(BA) = 0$ za sve $A, B \in M(n, \mathbb{F})$. Stoga je vektorski prostor

$$\mathfrak{sl}(n, \mathbb{F}) = \{X \in M(n, \mathbb{F}) \mid \text{Tr}(X) = 0\} \quad (4.13)$$

zatvoren na matrični komutator, pa tvori Liejevu podalgebru od $M(n, \mathbb{F})$. Algebra (4.13) naziva se specijalna linearna Liejeva algebra nad poljem $\mathbb{F}$.

4.3.2 Ortogonalne Liejeve algebre

Neka su $p, q \geq 0$ cijeli brojevi i neka je $p + q = n$. Neka je I_{pq} blok matrica reda n

$$I_{pq} = \begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix} \quad (4.14)$$

gdje su I_p i I_q jedinične matrice reda p i q , redom. Specijalna ortogonalna Liejeva algebra $\mathfrak{so}(p, q)$ je definirana sa

$$\mathfrak{so}(p, q) = \{X \in M(n, \mathbb{R}) \mid X^t I_{pq} + I_{pq} X = 0\}. \quad (4.15)$$

Ako je $p = n$, onda $\mathfrak{so}(p, q)$ postaje algebra antisimetričnih matrica

$$\mathfrak{so}(n, \mathbb{R}) = \{X \in M(n, \mathbb{R}) \mid X^t + X = 0\}.$$

4.3.3 Simplektička Liejeva algebra

Neka je J antisimetrična matrica reda $2n$,

$$J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$$

gdje je I_n jedinična matrica reda n . Algebra

$$\mathfrak{sp}(n, \mathbb{F}) = \{X \in M(2n, \mathbb{F}) \mid X^t J + J X = 0\}$$

naziva se simplektička Liejeva algebra ranga n .

4.3.4 Unitarne Liejeve algebre

Neka su $p, q \geq 0$ cijeli brojevi, $p + q = n$, i neka je I_{pq} matrica dana izrazom (4.14). Algebra

$$\mathfrak{u}(p, q) = \{X \in M(n, \mathbb{C}) \mid X^* I_{pq} + I_{pq} X = 0\},$$

gdje je $X^* = \overline{X}^t$ adjungirana matrica matrice X , naziva se unitarna Liejeva algebra. Specijalna unitarna algebra definirana je kao $\mathfrak{su}(p, q) = \mathfrak{u}(p, q) \cap \mathfrak{sl}(n, \mathbb{C})$, odnosno

$$\mathfrak{su}(p, q) = \{X \in \mathfrak{u}(p, q) \mid \text{Tr}(X) = 0\}.$$

Osim navedenih algebri postoje i kvaternionske Liejeve algebre koje su definirane nad prstenom kvaterniona $\mathbb{H}$.



Slika 4.3. Hermann Weyl, 1885-1955. Jedan od najznačajnijih matematičara 20. stoljeća čiji rad je imao veliki utjecaj na razvoj matematičke fizike.

4.4 Weylove algebre

Weylove algebre, nazvane po njemačkom matematičaru Hermannu Weylu, uvedene su početkom 20. stoljeća kao algebre koje opisuju operatore položaja i impulsa u kvantnoj mehanici. Ovdje ćemo dati kratak opis Weylovih algebri kao asocijativnu algebru diferencijalnih operatora.

Neka je $\mathbb{F}$ polje realnih ili kompleksnih brojeva i neka je $\mathbb{F}[x] = \mathbb{F}[x_1, x_2, \dots, x_n]$ prsten polinoma u varijablama $x_1, x_2, \dots, x_n$. Prsten $\mathbb{F}[x]$ je beskonačno dimenzionalni vektorski prostor nad poljem $\mathbb{F}$. Bazu prostora tvore monomi

$$x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}, \quad k_i \geq 0,$$

gdje je $x_i^0 = 1$. Neka su $\hat{x}_i$ i ∂_i linearni operatori na $\mathbb{F}[x]$ definirani s

$$\hat{x}_i(f) = x_i f, \quad \partial_i(f) = \frac{\partial f}{\partial x_i}, \quad 1 \leq i \leq n.$$

Definicija 4.11. Weylova algebra $\mathcal{A}_n$ je podalgebra algebre $\text{End}_{\mathbb{F}}(\mathbb{F}[x])$ generirana operatorima $\hat{x}_i$ i ∂_i , $1 \leq i \leq n$. Za $n = 0$ definiramo $\mathcal{A}_0 = \mathbb{F}$.

Elementi algebre $\mathcal{A}_n$ su linearne kombinacije monoma u generatorima $\hat{x}_1, \hat{x}_2, \dots, \hat{x}_n$ i $\partial_1, \partial_2, \dots, \partial_n$. Algebra $\mathcal{A}_n$ nije komutativna jer operatori $\hat{x}_i$ i ∂_i ne komutiraju. Promotrimo kako operator $\partial_i \hat{x}_j$ djeluje na polinom $f \in \mathbb{F}[x]$:

$$(\partial_i \hat{x}_j)(f) = \partial_i(x_j f) = \frac{\partial}{\partial x_i}(x_j f) = \delta_{ij} f + x_j \frac{\partial f}{\partial x_i}$$

gdje je δ_{ij} Kroneckerov simbol. Iz ove jednadžbe dobivamo

$$(\partial_i \hat{x}_j)(f) = (\delta_{ij} 1 + x_j \partial_i)(f) \tag{4.16}$$

gdje 1 označava operator identitete dan sa $1(f) = f$ za svaki $f \in \mathbb{F}[x]$. Relaciju (4.16) možemo zapisati kao komutacijsku relaciju

$$[\partial_i, \hat{x}_j] = \delta_{ij}1, \quad 1 \leq i, j \leq n, \quad (4.17)$$

gdje definiramo $[a, b] = a \circ b - b \circ a$ za sve $a, b \in \text{End}_{\mathbb{F}}(\mathbb{F}[x])$. Očigledno je da ostali operatori komutiraju,

$$[\partial_i, \partial_j] = [\hat{x}_i, \hat{x}_j] = 0, \quad 1 \leq i, j \leq n.$$

Kada je iz konteksta jasno da se radi o operatoru množenja, $\hat{x}_i$ ćemo identificirati s varijablom x_i . Također, operator $\delta_{ij}1$ identificiramo s δ_{ij} .

Neka je $f \in \mathbb{F}[x]$. Promotrimo kako operator $[\partial_i, f]$ djeluje na polinom $h \in \mathbb{F}[x]$. Prema definiciji komutatora,

$$\begin{aligned} [\partial_i, f]h &= (\partial_i f)h - (f\partial_i)h = \frac{\partial}{\partial x_i}(fh) - f\frac{\partial h}{\partial x_i} \\ &= \frac{\partial f}{\partial x_i}h + f\frac{\partial h}{\partial x_i} - f\frac{\partial h}{\partial x_i} = \frac{\partial f}{\partial x_i}h. \end{aligned}$$

Dakle,

$$[\partial_i, f] = \frac{\partial f}{\partial x_i}, \quad (4.18)$$

što znači da je $[\partial_i, f]$ operator množenja polinomom $\frac{\partial f}{\partial x_i}$. Ako f ne ovisi o varijabli x_i , onda ∂_i i f komutiraju, odnosno $[\partial_i, f] = 0$. Iz relacije (4.17) imamo

$$\partial_i x_j = x_j \partial_i + \delta_{ij},$$

što pokazuje da svaki monom u ∂_i i x_i možemo napisati kao linearnu kombinaciju monoma u kojima su varijable x_i slijeva a derivacije ∂_i zdesna. Na primjer,

$$\begin{aligned} \partial_2 x_2^2 \partial_1 x_1^3 &= (x_2^2 \partial_2 + 2x_2)(x_1^3 \partial_1 + 3x_1^2) \\ &= x_2^2 \partial_2 x_1^3 \partial_1 + 2x_2 x_1^3 \partial_1 + 3x_2^2 \partial_2 x_1^2 + 6x_2 x_1^2 \\ &= x_2^2 x_1^3 \partial_2 \partial_1 + 2x_2 x_1^3 \partial_1 + 3x_2^2 x_1^2 \partial_2 + 6x_2 x_1^2. \end{aligned} \quad (4.19)$$

Ako je monom zapisan u obliku (4.19), onda kažemo da je zapisan u kanonskoj bazi. Za opisivanje baze Weylove algebre korisno je uvesti multi-indeks $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{N}_0^n$ gdje je $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Monom $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ kraće zapisujemo kao x^α , a stupanj monoma je duljina multi-indeksa $|\alpha| = \sum_{i=1}^n \alpha_i$. Može se pokazati da je baza Weylove algebre dana sa

$$\mathcal{B} = \{x^\alpha \partial^\beta \mid \alpha, \beta \in \mathbb{N}_0^n\}.$$

Uz prethodnu definiciju, $\mathcal{A}_0 = \mathbb{F}$ je jednodimenzionalna algebra dok je $\mathcal{A}_n$ beskonačno dimenzionalna za $n \geq 1$.

Literatura

1. D.S. Dummit, R.M. Foote, *Abstract algebra*, treće izdanje, John Wiley and Sons Inc., Hoboken, 2004.
2. G. T. Lee, *Abstract Algebra, An Introductory Course*, Springer, 2018.
3. P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul, *Basic Abstract Algebra*, drugo izdanje, Cambridge University Press, 1994.
4. N. Jacobson, *Basic Algebra I*, drugo izdanje, W.H. Freeman and Company, New York, 1985.
5. S. MacLane, G. Birkhoff, *Algebra*, treće izdanje, AMS Chelsea Publishing, Providence, 1999.
6. S. Lang, *Algebra*, revidirano treće izdanje, Springer, New York, 2002.
7. K. Erdmann, M.J. Wildon, *Introduction to Lie Algebras*, Springer, London, 2006.
8. R. Goodman, N.R. Wallach, *Symmetry, Representations, and Invariants*, Springer, New York, 2009.