Sveučilište Josipa Jurja Strossmayera
Odjel za matematiku

Darija Brajković

Algebra kroz primjere

Priručnik za vježbe

2018.

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

Odjel za Matematiku

Algebra kroz primjere

Priručnik za vježbe

Darija Brajković

Osijek, 2018.

Autor:
Darija Brajković
Odjel za matematiku
Sveučilište J.J. Strossmayera u Osijeku
Trg Ljudevita Gaja 6
HR-31000 Osijek

Izdavač:
Sveučilište Josipa Jurja Strossmayera u Osijeku – Odjel za matematiku

Recenzenti:
izv. prof. dr. sc. Ivan Matić, Odjel za matematiku,
Sveučilište Josipa Jurja Strossmayera u Osijeku
prof. dr. sc. Marcela Hanzer, PMF-Matematički odsjek,
Sveučilište u Zagrebu

Lektorica:
Marina Tomić

Tisak:
STUDIO HS Internet d.o.o., Osijek

CIP zapis dostupan je u računalnom katalogu Gradske i sveučilišne knjižnice Osijek pod brojem 140913057.

ISBN 978-953-8154-09-6

Priručnik se objavljuje uz suglasnost Senata Sveučilišta J.J. Strossmayera u Osijeku pod brojem 8/18.

Priručnik se objavljuje uz financijsku potporu Ministarstva znanosti i obrazovanja Republike Hrvatske.

Sadržaj

1

Grupe

"The only way to learn mathematics is to do mathematics."
- Paul Halmos

1.1 Definicija i osnovni primjeri grupa

Definicija 1.1.1. Neka je G neprazan skup. Binarna operacija na G funkcija je koja svakom uređenom paru elemenata od G pridružuje element od G, odnosno

$$(a, b) \mapsto a * b \in G \text{ za sve } a, b \in G.$$

Kažemo da je skup G zatvoren s obzirom na binarnu operaciju $*$ i uređeni par $(G, *)$ nazivamo grupoid.

Najčešće koristimo binarnu operaciju zbrajanja $+ \colon G \times G \to G$ i uređeni par $(G, +)$ zovemo aditivni grupoid te binarnu operaciju množenja $\cdot \colon G \times G \to G$ i uređeni par $(G, \cdot)$ zovemo multiplikativni grupoid. Kada je jasno o kojoj je operaciji riječ, govorit ćemo samo grupoid G. U nastavku, ukoliko nije posebno naznačeno o kojoj se binarnoj operaciji radi, binarnu operaciju nećemo označavati posebnim znakom, odnosno pisat ćemo $(a, b) \mapsto ab$.

Polugrupa je grupoid G u kome je binarna operacija asocijativna, to jest grupoid G u kome vrijedi $(ab)c = a(bc)$ za sve $a, b, c \in G$.

Lijeva jedinica ili lijevi neutralni element u grupoidu G svaki je element $l \in G$ takav da je $la = a$ za sve $a \in G$, a desna jedinica ili desni neutralni element u grupoidu G svaki je $d \in G$ takav da je $ad = a$ za sve $a \in G$. Element grupoida G koji je i lijevi i desni neutralni element, odnosno $e \in G$ takav da je $ea = ae = a$ za sve $a \in G$, naziva se jedinica, jedinični element ili neutralni element grupoida G i označava se s e ili s 1. Polugrupa s jedinicom naziva se monoid.

Neka je G monoid s jedinicom e i neka je $a \in G$. Kažemo da je $b_l \in G$ lijevi inverz ili lijevi inverzni element od a ako vrijedi $b_l a = e$, a da je $b_d \in G$ desni inverz ili desni inverzni element od a ako vrijedi $ab_d = e$. Element monoida G koji je i lijevi i desni inverz od $a \in G$ naziva se inverz ili inverzni element od a i označava se s a^{-1}. Kažemo da je $a \in G$ invertibilan element ako ima inverz. Skup svih invertibilnih elemenata monoida G označavat ćemo s G^*.

Napomena 1.1.2. Neka je $(G, +)$ monoid u kojemu element $a \in G$ ima inverz. Tada neutralni element označavamo s 0 i nazivamo nula, a inverzni element označavamo s $-a$ i nazivamo suprotni element.

Definicija 1.1.3. Kažemo da je grupoid G grupa ako vrijede sljedeća svojstva:

1) Asocijativnost. Binarna je operacija asocijativna, to jest vrijedi $(ab)c = a(bc)$ za sve a, b i c u G.

2) Postojanje neutralnog elementa. Postoji element e u G takav da je $ae = ea = a$ za sve a u G.

3) Postojanje inverznog elementa. Za svaki element a u G postoji element a^{-1} u G takav da je $aa^{-1} = a^{-1}a = e$.

Ako u grupi G vrijedi svojstvo komutativnosti, to jest ako je $ab = ba$ za sve elemente a, b u G, onda kažemo da je G komutativna ili Abelova grupa. (Analogno imamo komutativan grupoid, komutativnu polugrupu i komutativan monoid.)

Napomena 1.1.4. Neutralni je element u grupi G jedinstven.

Napomena 1.1.5. Za svaki element a u grupi G postoji jedinstveni inverzni element a^{-1} u grupi G.

Zadatak 1.1.1. Neka je G grupa. Dokažite sljedeće tvrdnje:

a) Za elemente a i b grupe G vrijedi $(ab)^{-1} = b^{-1}a^{-1}$.

b) Neka su a, b i c elementi grupe G. Ako je $ac = bc$, onda je $a = b$.

c) Neka su a, b i c elementi grupe G. Ako je $ca = cb$, onda je $a = b$.

Rješenje.

a) Kako je G grupa, elementi a, b i ab u G imaju inverzne elemente $a^{-1}, b^{-1}, (ab)^{-1}$ u G. Dakle, vrijedi $ab(ab)^{-1} = e$. Pomnožimo li sada tu jednakost slijeva s a^{-1}, dobijemo $b(ab)^{-1} = a^{-1}e = a^{-1}$. Ako sada dobivenu jednakost pomnožimo slijeva s b^{-1}, dobivamo upravo $(ab)^{-1} = b^{-1}a^{-1}$.

b) Pretpostavimo da je $ac = bc$ za elemente a, b i c u G. Kako je G grupa, element c u G ima inverz c^{-1} u G. Pomnožimo li jednakost $ac = bc$ zdesna s c^{-1}, dobijemo $(ac)c^{-1} = (bc)c^{-1}$ pa nam asocijativnost daje $a(cc^{-1}) = b(cc^{-1})$, odnosno $ae = be$. Prema tome, $a = b$, što smo htjeli dokazati.

c) Analogno kao u b) dijelu zadatka. ■

Zadatak 1.1.2. Dokažite da je grupa G Abelova grupa ako i samo ako vrijedi

$$a^2b^2 = (ab)^2 \text{ za sve } a, b \in G. \qquad \square$$

Zadatak 1.1.3. Ispitajte svojstva sljedećih struktura:

a) $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ uz operaciju zbrajanja.

b) $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ uz operaciju oduzimanja.

c) $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ uz operaciju množenja.

d) $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}, \mathbb{R}^* = \mathbb{R}\backslash\{0\}, \mathbb{C}^* = \mathbb{C}\backslash\{0\}$ uz operaciju množenja.

e) $\mathbb{N}, \mathbb{Z}\backslash\{0\}, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ uz operaciju dijeljenja.

Rješenje.

a)
- ▷ zatvorenost s obzirom na zbrajanje vrijedi ⇒ grupoidi
- ▷ zbrajanje je asocijativno ⇒ polugrupe
- ▷ neutralni element za zbrajanje u $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ jest 0, a u $\mathbb{N}$ ne postoji neutralni element za zbrajanje ($0 \notin \mathbb{N}$) ⇒ $\mathbb{N}$ je polugrupa, a $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ su monoidi
- ▷ u $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ postoje suprotni elementi ⇒ grupe
- ▷ svuda vrijedi komutativnost

Dakle, skup $\mathbb{N}$ uz zbrajanje komutativna je polugrupa, a skupovi $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ uz zbrajanje komutativne su grupe.

Napomena 1.1.6. Grupa $(\mathbb{Z}, +)$ zove se aditivna grupa cijelih brojeva, grupa $(\mathbb{Q}, +)$ aditivna grupa racionalnih brojeva, grupa $(\mathbb{R}, +)$ aditivna grupa realnih brojeva, a grupa $(\mathbb{C}, +)$ aditivna grupa kompleksnih brojeva.

b) Za vježbu.

c)
- ▷ zatvorenost s obzirom na množenje vrijedi ⇒ grupoidi
- ▷ množenje je asocijativno ⇒ polugrupe
- ▷ neutralni je element za množenje 1 ⇒ monoidi
- ▷ ne postoje inverzni elementi (u $\mathbb{N}$ za $n > 1$ imamo $\frac{1}{n} \notin \mathbb{N}$, a u ostalima 0 nema inverz)
- ▷ svuda vrijedi komutativnost

Prema tome, skupovi $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ uz množenje komutativni su monoidi.

d) Skupovi $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}, \mathbb{R}^* = \mathbb{R}\backslash\{0\}, \mathbb{C}^* = \mathbb{C}\backslash\{0\}$ uz množenje komutativne su grupe.

Posebno, koja svojstva vrijede u skupu $\mathbb{Z}\backslash\{0\}$ uz množenje?

Napomena 1.1.7. Grupa $(\mathbb{Q}^*, \cdot)$ zove se multiplikativna grupa racionalnih brojeva, grupa $(\mathbb{R}^*, \cdot)$ multiplikativna grupa realnih brojeva, a grupa $(\mathbb{C}^*, \cdot)$ multiplikativna grupa kompleksnih brojeva.

e) $\mathbb{N}, \mathbb{Z}\backslash\{0\}$:

- ▷ zatvorenost s obzirom na dijeljenje ne vrijedi jer, primjerice, $\frac{1}{2} \notin \mathbb{N}$ i $\frac{1}{2} \notin \mathbb{Z}\backslash\{0\}$

$\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$:

- ▷ zatvorenost s obzirom na dijeljenje vrijedi $\Rightarrow$ grupoidi
- ▷ asocijativnost ne vrijedi zbog

$$(a : b) : c = \frac{\frac{a}{b}}{c} = \frac{a}{bc}$$

$$a : (b : c) = \frac{a}{\frac{b}{c}} = \frac{ac}{b}$$

- ▷ iz $\frac{a}{e} = a$ slijedi da je $e = 1$ desni neutralni element, ali s druge strane imamo $\frac{e}{a} = a \Rightarrow e = a^2$ pa zaključujemo da ne postoji neutralni element
- ▷ inverz nema smisla gledati jer ne postoji neutralni element
- ▷ komutativnost ne vrijedi

Dakle, $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ su uz dijeljenje grupoidi u kojima postoji desni neutralni element. ■

Zadatak 1.1.4. Neka je S neprazan skup i $\mathcal{P}(S) = \{X : X \subseteq S\}$ partitivni skup skupa S. Ispitajte svojstva sljedećih struktura:

a) $(\mathcal{P}(S), \cup)$.

b) $(\mathcal{P}(S), \cap)$.

c) $(\mathcal{P}(S), \backslash)$, $A\backslash B = A \cap B^C$.

d) $(\mathcal{P}(S), \triangle)$, $A \triangle B = (A\backslash B) \cup (B\backslash A) = (A \cup B)\backslash(A \cap B)$.

Rješenje.

a)
- ▷ zatvorenost vrijedi jer za $A, B \in \mathcal{P}(S) \Rightarrow A \subseteq S$ i $B \subseteq S \Rightarrow A \cup B \subseteq S$, odnosno $A \cup B \in \mathcal{P}(S) \Rightarrow$ grupoid
- ▷ asocijativnost vrijedi $\Rightarrow$ polugrupa
- ▷ iz $A \cup E = A$ slijedi da je $E = \emptyset \in \mathcal{P}(S)$ desni neutralni element, a zatim iz $A \cup \emptyset = \emptyset \cup A = A$ zaključujemo da je prazan skup neutralni element $\Rightarrow$ monoid
- ▷ samo prazan skup ima inverz i u tom je slučaju on sam sebi inverz
- ▷ komutativnost vrijedi

Prema tome, $(\mathcal{P}(S), \cup)$ komutativan je monoid.

b) Za vježbu.

c) ▷ zatvorenost vrijedi ⇒ grupoid
▷ asocijativnost ne vrijedi
▷ iz $A\backslash E = A$ slijedi da je $E = \emptyset \in \mathcal{P}(S)$ desni neutralni element, ali lijevi neutralni element ne postoji pa ne postoji neutralni element
▷ inverz nema smisla gledati
▷ komutativnost ne vrijedi

Dakle, $(\mathcal{P}(S), \backslash)$ grupoid je koji ima desni neutralni element.

d) ▷ zatvorenost vrijedi ⇒ grupoid
▷ asocijativnost vrijedi ⇒ polugrupa
▷ iz $A \triangle E = A$, odnosno $(A \cup E)\backslash(A \cap E) = A$ slijedi da je $E = \emptyset$ desni neutralni element, a iz $E \triangle A = A$, odnosno $(A \cup E)\backslash(A \cap E) = A$ slijedi da je $E = \emptyset$ lijevi neutralni element; zaključujemo da je $E = \emptyset \in \mathcal{P}(S)$ neutralni element ⇒ monoid
▷ svaki skup sam je sebi inverz ⇒ grupa
▷ komutativnost vrijedi

Prema tome, $(\mathcal{P}(S), \triangle)$ komutativna je grupa. ■

Zadatak 1.1.5. Neka je S neprazan skup. Pokažite da je $(S^S, \circ)$, gdje je S^S skup svih funkcija $f\colon S \to S$, monoid. □

Napomena 1.1.8. Sa $(S^S)^* = B(S)$ označavamo skup svih bijekcija sa S na S. Takve se funkcije zovu permutacije skupa S, a $(B(S), \circ)$ nekomutativna je grupa koju zovemo grupa permutacija skupa S.

Zadatak 1.1.6. Pokažite da je skup $M_n(\mathbb{R}) = M(n, \mathbb{R})$ svih realnih kvadratnih matrica reda n monoid uz množenje matrica.

Rješenje. Zatvorenost vrijedi jer za matrice $A, B \in M(n, \mathbb{R})$ imamo $AB \in M(n, \mathbb{R})$. Asocijativnost općenito vrijedi za matrice. Neutralni je element jedinična matrica I odgovarajućeg reda jer je $A \cdot I = I \cdot A = A$ za sve $A \in M(n, \mathbb{R})$. S obzirom da inverz postoji onda i samo onda kada je matrica regularna, možemo zaključiti da je $M(n, \mathbb{R})$ uz množenje matrica monoid.

Štoviše, $M(n, \mathbb{R})$ je za $n \geq 2$ uz množenje matrica nekomutativan monoid. ■

Skup $M_n^*(\mathbb{R}) = M^*(n, \mathbb{R}) = GL_n(\mathbb{R}) = GL(n, \mathbb{R}) = \{A \in M(n, \mathbb{R})\colon \det A \neq 0\}$ grupa je uz množenje matrica koja se naziva opća linearna grupa. Ona je nekomutativna za $n \geq 2$. Nadalje, skup $SL_n(\mathbb{R}) = SL(n, \mathbb{R}) = \{A \in M(n, \mathbb{R})\colon \det A = 1\}$ grupa je uz množenje matrica koju zovemo specijalna linearna grupa i ona je nekomutativna za $n \geq 2$, a skup $O_n(\mathbb{R}) = O(n, \mathbb{R}) = \{A \in M(n, \mathbb{R})\colon AA^T = A^T A = I\}$ grupa je uz množenje matrica koju zovemo ortogonalna grupa.

Zadatak 1.1.7. Neka je G grupoid. Dokažite da je G grupa ako i samo ako zadovoljava sljedeća tri uvjeta:

a) Vrijedi asocijativnost, odnosno $(ab)c = a(bc)$ za sve $a, b, c \in G$.

b) Postoji $e \in G$ takav da je $ea = a$ za sve $a \in G$.

c) Za svaki $a \in G$ postoji $a^{-1} \in G$ takav da je $a^{-1}a = e$.

Rješenje. Nužnost je očita, a da bismo pokazali dovoljnost, trebamo pokazati da svojstva a), b) i c) povlače da postoji desni neutralni element i da svaki element u G ima desni inverz. Neka su a i a^{-1} elementi u G takvi da je $a^{-1}a = e$. Kako je G grupoid, element aa^{-1} je u G pa imamo

$$(aa^{-1})(aa^{-1}) \overset{a)}{=} a(a^{-1}a)a^{-1} \overset{c)}{=} aea^{-1} \overset{b)}{=} aa^{-1}. \tag{1.1}$$

Nadalje, kako je aa^{-1} element u $G \overset{c)}{\Rightarrow}$ postoji $(aa^{-1})^{-1}$ u G takav da je $(aa^{-1})^{-1}(aa^{-1}) = e$. Pomnožimo li sada jednakost (1.1) slijeva s $(aa^{-1})^{-1}$, dobijemo

$$aa^{-1} = (aa^{-1})^{-1}(aa^{-1}) = e.$$

Dakle, $a^{-1} \in G$ desni je inverz od $a \in G$. Pokažimo još da postoji desni neutralni element. Naime, kako sada znamo da vrijedi $a^{-1}a = aa^{-1} = e$, imamo

$$a \overset{b)}{=} ea = (aa^{-1})a \overset{a)}{=} a(a^{-1}a) \overset{c)}{=} ae.$$

Time smo pokazali dovoljnost. ■

Zadatak 1.1.8. Dan je skup $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ za $m \in \mathbb{N}$. Provjerite svojstva sljedećih struktura:

a) $(\mathbb{Z}_m, +_m)$, gdje je $+_m \colon \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ operacija definirana s $a +_m b = a + b \pmod m$.

b) $(\mathbb{Z}_m, \cdot_m)$, gdje je $\cdot_m \colon \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ operacija definirana s $a \cdot_m b = a \cdot b \pmod m$.

c) $(\mathbb{Z}_m \backslash \{0\}, \cdot_m)$, gdje je $\cdot_m \colon \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ operacija definirana s $a \cdot_m b = a \cdot b \pmod m$.

Rješenje.

a)
- ▷ zatvorenost vrijedi ⇒ grupoid
- ▷ zbrajanje modulo m je asocijativno ⇒ polugrupa
- ▷ komutativnost vrijedi ⇒ komutativna polugrupa
- ▷ iz $a = a +_m e = a + e \pmod m$ slijedi da je $e = 0$ desni neutralni element, pa, s obzirom da vrijedi komutativnost, imamo $a = a +_m e = e +_m a$ te zaključujemo da je $e = 0 \in \mathbb{Z}_m$ neutralni element ⇒ komutativan monoid
- ▷ iz $0 = a +_m b = a + b \pmod m$ zaključujemo da je $b = 0 \in \mathbb{Z}_m$ inverzni element od $a = 0 \in \mathbb{Z}_m$, a $b = m - a \in \mathbb{Z}_m$ inverzni element od $a \neq 0$ iz $\mathbb{Z}_m$ ⇒ komutativna grupa.

b) Za vježbu.

c) 1) m je složen broj
- ▷ ako je m složen broj, onda postoje $p, q \in \mathbb{Z}_m$ takvi da je $m = pq$, iz čega slijedi da je $p \cdot_m q \equiv 0 \pmod m$, pa zaključujemo da $p \cdot_m q \notin \mathbb{Z}_m \backslash \{0\}$ ⇒ zatvorenost ne vrijedi

2) m je prost broj
   - ▷ ako je m prost broj, onda je $p \cdot_m q \in \mathbb{Z}_m\backslash\{0\}$ za sve $p, q \in \mathbb{Z}_m\backslash\{0\} \Rightarrow$ grupoid
   - ▷ asocijativnost množenja modulo m vrijedi $\Rightarrow$ polugrupa
   - ▷ komutativnost vrijedi $\Rightarrow$ komutativna polugrupa
   - ▷ iz $a = a \cdot_m e = a \cdot e \pmod m$ slijedi da je $e = 1$ desni neutralni element, pa, s obzirom da vrijedi komutativnost, imamo $a = a \cdot_m e = e \cdot_m a$ te zaključujemo da je $e = 1 \in \mathbb{Z}_m\backslash\{0\}$ neutralni element $\Rightarrow$ komutativan monoid
   - ▷ kako su $a \in \mathbb{Z}_m\backslash\{0\}$ i m relativno prosti, postoje cijeli brojevi x, y takvi da je $ax+my = 1$, pa je $a \cdot_m x \equiv 1 \pmod m$ te zaključujemo da je $x \in \mathbb{Z}_m\backslash\{0\}$ desni inverzni element od $a \in \mathbb{Z}_m\backslash\{0\}$, a s obzirom da vrijedi komutativnost, zaključujemo da je $x \in \mathbb{Z}_m\backslash\{0\}$ inverzni element od $a \in \mathbb{Z}_m\backslash\{0\} \Rightarrow$ komutativna grupa; uočimo da je $\mathbb{Z}_m\backslash\{0\} = \mathbb{Z}_m^*$. ■

Napomena 1.1.9. Radi jednostavnosti ćemo $(\mathbb{Z}_m, +_m)$ pisati kao $(\mathbb{Z}_m, +)$ (analogno za ostale operacije). Također, kada je jasno uz koju je operaciju neki skup grupa, često se ta operacija izostavlja i kažemo samo G je grupa umjesto $(G, *)$ je grupa.

Primjer 1.1.1. Napravimo tablicu zbrajanja za grupu $(\mathbb{Z}_3, +)$:

$+$	**0**	**1**	**2**
0	0	1	2
1	1	2	0
2	2	0	1

Primjer 1.1.2. Napravimo tablicu množenja za grupu $(\mathbb{Z}_3^*, \cdot)$:

$\cdot$	**1**	**2**
1	1	2
2	2	1

Napomena 1.1.10. Tablice iz prethodnih dvaju primjera nazivaju se Cayleyeve tablice. U Cayleyevoj tablici grupe svaki element grupe pojavljuje se točno jednom u svakom retku i točno jednom u svakom stupcu. Što nam Cayleyeva tablica grupe govori o neutralnom elementu i inverznim elementima? Kako možemo iz Cayleyeve tablice grupe zaključiti je li grupa komutativna?

Zadatak 1.1.9. Pokažite da je skup $K_4 = \{1, -1, i, -i\}$ grupa uz množenje kompleksnih brojeva i napravite Cayleyevu tablicu za tu grupu. □

Zadatak 1.1.10. Ispitajte svojstva strukture $\mathbb{Q}$ uz operaciju $*$ definiranu s

$$a * b = a + b - ab \text{ za sve } a, b \in \mathbb{Q}.$$

Rješenje.

- ▷ zatvorenost vrijedi jer je $a * b = a + b - ab \in \mathbb{Q}$, $\forall a, b \in \mathbb{Q} \Rightarrow$ grupoid
- ▷ kako je

$$(a*b)*c = (a*b)+c-(a*b)c = a+b-ab+c-(a+b-ab)c = a+b-ab+c-ac-bc+abc$$

jednako

$$a*(b*c) = a+(b*c)-a(b*c) = a+b+c-bc-a(b+c-bc) = a+b+c-bc-ab-ac+abc,$$

asocijativnost vrijedi $\Rightarrow$ polugrupa

- ▷ komutativnost vrijedi jer imamo $a*b = a+b-ab = b+a-ba = b*a \Rightarrow$ komutativna polugrupa
- ▷ iz $a*e = a$, odnosno $a+e-ae = a$ imamo $e(1-a) = 0$, $\forall a \in \mathbb{Q}$, pa slijedi da je $e = 0$ desni neutralni element, a s obzirom da vrijedi komutativnost, zaključujemo da je $e = 0 \in \mathbb{Q}$ neutralni element $\Rightarrow$ komutativni monoid
- ▷ imamo $a*b = 0$, odnosno $a+b-ab = 0$, iz čega slijedi $b(1-a) = -a$, pa vidimo da element $a \neq 1$ u $\mathbb{Q}$ ima inverz $b = \frac{-a}{1-a} \in \mathbb{Q}$, a element $a = 1$ u $\mathbb{Q}$ nema inverz

Prema tome, $(\mathbb{Q}, *)$ komutativni je monoid. ■

Zadatak 1.1.11. Neka je $\mathbb{R}$ grupoid uz binarnu operaciju $*$ definiranu s

$$a*b = a+b-2a^2b^2 \text{ za sve } a, b \in \mathbb{R}.$$

Ispitajte je li grupoid $\mathbb{R}$ polugrupa, vrijedi li svojstvo komutativnosti te odredite neutralni element u grupoidu $\mathbb{R}$. □

Napomena 1.1.11. Neka su $(G_1, *)$, $(G_2, \star)$ grupe i neka je $G_1 \times G_2$ skup svih parova (a_1, a_2), gdje je $a_1 \in G_1$, a $a_2 \in G_2$. Na skupu $G_1 \times G_2$ definiramo binarnu operaciju s

$$(a_1, a_2)(b_1, b_2) = (a_1 * b_1, a_2 \star b_2) \text{ za sve } (a_1, a_2), (b_1, b_2) \in G_1 \times G_2$$

s obzirom na koju $G_1 \times G_2$ postaje grupa. Neutralni element grupe $G_1 \times G_2$ jest (e_1, e_2), gdje je e_1 neutralni element u G_1 i e_2 neutralni element u G_2, a inverzni element od (a_1, a_2) jest (a_1^{-1}, a_2^{-1}). Analogno, za konačno mnogo grupa $G_1, G_2, \ldots, G_n$ definiramo njihov produkt kao $G_1 \times G_2 \times \cdots \times G_n$.

Primjer 1.1.3. Skup $\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R} = \{(a_1, a_2, \ldots, a_n) \colon a_1, a_2, \ldots, a_n \in \mathbb{R}\}$ grupa je uz zbrajanje realnih brojeva po komponentama, to jest

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

za sve $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in \mathbb{R}^n$. Analogno vrijedi za $\mathbb{C}^n$.

Primjer 1.1.4. Skup $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(a, b) \colon a, b \in \mathbb{Z}_2\}$ grupa je uz operaciju

$$(a_1, b_1) + (a_2, b_2) = (a_1 +_2 a_2, b_1 +_2 b_2) \text{ za } (a_1, b_1), (a_2, b_2) \in \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Definicija 1.1.12. Broj elemenata grupe G naziva se red grupe G i označava s $|G|$. Kažemo da je grupa G konačna ako je G konačan skup, a u suprotnom kažemo da je grupa G beskonačna.

Primjer 1.1.5. $(\mathbb{Z}_4, +)$ konačna je grupa jer je $|\mathbb{Z}_4| = 4$.

Primjer 1.1.6. $(\mathbb{Z}, +)$ beskonačna je grupa.

Primjer 1.1.7. Neka je G grupa reda 2. Napravimo Cayleyevu tablicu za G.

Uzmimo $G = \{e, a\}$. Elementi a i e međusobno su različiti jer je grupa G reda 2. Očito je $ea = a$, $ae = a$ i $ee = e$. Sada je, kako se svaki element grupe G pojavljuje točno jednom u svakom retku i točno jednom u svakom stupcu, očito $aa = e$. No, to se može i lako pokazati. Pretpostavimo da je $aa = a$. Pomnožimo li tu jednakost zdesna s inverznim elementom od a, za kojeg znamo da postoji jer je a element grupe G, dobijemo da je $a = e$, što ne može biti. Dakle, $aa = e$. Odnosno, Cayleyeva je tablica grupe reda 2

	e	a
e	e	a
a	a	e

Primjer 1.1.8. Napravite Cayleyevu tablicu za grupu reda 3.

Primjer 1.1.9. Napravimo Cayleyevu tablicu za grupu reda 4.

Uzmimo $G = \{e, a, b, c\}$. Kako je G grupa, elementi a, b i c imaju inverzne elemente. Očito, jedan element mora sam sebi biti inverz i neka je to element b. Prema tome, $b = b^{-1}$, odnosno $bb = e$. Nadalje, znamo da je $xe = ex = x$ za sve elemente x u G. Krenimo s popunjavanjem tablice. Vidimo da element ac grupe G mora biti iz skupa elemenata $\{e, b\}$ jer se elementi a i c pojavljuju u tom retku, odnosno stupcu, pa imamo dva moguća slučaja.

Prvi slučaj. Neka je $ac = e$. Lako se pokaže da je onda i $ca = e$. Kako u svakom retku i svakom stupcu tablice može biti točno jedan element grupe G, sada možemo zaključiti da je onda $ab = c$ te $aa = b$, a zatim da je $ba = c$, $bc = a$ i $cb = a$. Na kraju, vidimo da je $cc = b$.

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Drugi slučaj. Neka je $ac = b$. Za vježbu.

1.2 Podgrupe

Definicija 1.2.1. Neka je G grupa i H podskup od G. Kažemo da je H podgrupa od G ako je H grupa s obzirom na istu operaciju.

Ako je H podgrupa grupe G, pišemo $H \leq G$. Svaka grupa G ima barem dvije podgrupe, a to su sama grupa G i $\{e\}$. Te podgrupe zovu se trivijalne podgrupe od G. Za podgrupu koja nije trivijalna kažemo da je netrivijalna podgrupa od G.

Ako je H podgrupa grupe G, ali nije jednaka grupi G, kažemo da je H prava podgrupa od G.

Teorem 1.2.2. *Podskup H podgrupa je od G ako i samo ako vrijede sljedeća tri uvjeta:*

1) $a, b \in H \Rightarrow ab \in H$,

2) $a \in H \Rightarrow a^{-1} \in H$,

3) $e \in H$.

Ukoliko je podskup H neprazan, uvjetima 1), 2) *i* 3) *ekvivalentan je uvjet:*

4) $a, b \in H \Rightarrow ab^{-1} \in H$.

Primjer 1.2.1. Vrijedi: $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$.

Napomena 1.2.3. Ponekad, kada želimo pokazati da je neki skup grupa, može biti lakše pokazati da je dani skup podgrupa neke grupe nego direktno provjeravati aksiome grupe.

Zadatak 1.2.1. Ispitajte jesu li sljedeće strukture grupe:

a) $(S^1, \cdot)$, gdje je $S^1 = \{z \in \mathbb{C} \colon |z| = 1\}$.

b) $(K_n, \cdot)$, gdje je $K_n = \{z \in \mathbb{C} \colon z^n = 1\}$ za $n \in \mathbb{N}$, skup n-tih korijena iz jedinice.

c) $(x\mathbb{Z}, +)$ za $x \in \mathbb{C}$.

Rješenje.

a) Znamo da je $z = |z|(\cos t + i \sin t) = |z|e^{it}$ za svaki realan broj t, pa je $S^1 = \{e^{it} \colon t \in \mathbb{R}\}$. Tvrdimo: $S^1 \leq \mathbb{C}^*$. Očito je skup S^1 podskup od $\mathbb{C}^*$ i neprazan. Neka su $z_1, z_2 \in S^1$. Tada je $z_1 = e^{it_1}$ i $z_2 = e^{it_2}$ za neke $t_1, t_2 \in \mathbb{R}$, pa je

$$z_1 \cdot z_2^{-1} = e^{it_1} \cdot e^{-it_2} = e^{i(t_1 - t_2)} \in S^1,$$

odnosno, prema teoremu 1.2.2, slijedi da je S^1 podgrupa od $\mathbb{C}^*$. Prema tome, $(S^1, \cdot)$ jest grupa.

b) Za vježbu.

c) Tvrdimo: $x\mathbb{Z} \leq \mathbb{C}$. Jasno je da je $x\mathbb{Z}$ podskup od $\mathbb{C}$ i da je $x\mathbb{Z}$ neprazan skup. Neka su $x_m, x_n \in x\mathbb{Z}$. Tada je $x_m = xm$, $x_n = xn$ za neke $m, n \in \mathbb{Z}$, pa je

$$x_m - x_n = xm - xn = x(m - n) \in x\mathbb{Z}.$$

Sada, prema teoremu 1.2.2, slijedi da je $x\mathbb{Z}$ podgrupa od $\mathbb{C}$. Prema tome, $(x\mathbb{Z}, +)$ jest grupa. ■

Zadatak 1.2.2. Pokažite da je $SL(n, \mathbb{R})$ podgrupa od $GL(n, \mathbb{R})$.

Rješenje. Skup $SL(n, \mathbb{R})$ neprazan je jer je, primjerice, $I \in SL(n, \mathbb{R})$, a iz definicije skupova $SL(n, \mathbb{R})$ i $GL(n, \mathbb{R})$ slijedi da je skup $SL(n, \mathbb{R})$ podskup od $GL(n, \mathbb{R})$. Uzmimo sada proizvoljne matrice $A, B \in SL(n, \mathbb{R})$. Dakle, $\det A = 1$ i $\det B = 1$, pa je

$$\det(AB^{-1}) = (\det A) \cdot (\det B^{-1}) = (\det A) \cdot (\det B)^{-1} = 1.$$

Time smo pokazali da je matrica $AB^{-1} \in SL(n, \mathbb{R})$, pa je, prema teoremu 1.2.2, $SL(n, \mathbb{R})$ podgrupa od $GL(n, \mathbb{R})$. ■

Zadatak 1.2.3. Ispitajte jesu li sljedeći skupovi grupe uz pripadne operacije:

a) $G_1 = \{m + n\sqrt{2} + k\sqrt{8} \colon m, n, k \in \mathbb{Z}\}$;

   a_1) uz zbrajanje realnih brojeva,

   a_2) uz množenje realnih brojeva.

b) $G_2 = \{(z, \overline{z}) \colon z \in \mathbb{C}\}$ uz zbrajanje kompleksnih brojeva po komponentama;

c) $G_3 = \{0, 2, 4\}$;

   c_1) uz zbrajanje modulo 5,

   c_2) uz množenje modulo 5.

Rješenje.

a) Najprije uočimo da je $m + n\sqrt{2} + k\sqrt{8} = m + n\sqrt{2} + 2k\sqrt{2} = m + (n + 2k)\sqrt{2}$, a $n + 2k \in \mathbb{Z}$, pa je $G_1 = \{m + s\sqrt{2} \colon m, s \in \mathbb{Z}\}$.

   (a_1) Dovoljno je provjeriti je li G_1 podgrupa od $\mathbb{R}$ jer je $(\mathbb{R}, +)$ grupa. Očito je G_1 neprazan skup i podskup od $\mathbb{R}$. Nadalje, uzmimo proizvoljne elemente $a, b \in G_1$. Tada je $a = m_1 + s_1\sqrt{2}$ i $b = m_2 + s_2\sqrt{2}$ za neke $m_1, m_2, s_1, s_2 \in \mathbb{Z}$, pa je

   $$a - b = m_1 - m_2 + (s_1 - s_2)\sqrt{2} \in G_1,$$

   odnosno G_1 je, prema teoremu 1.2.2, podgrupa od $\mathbb{R}$ uz zbrajanje realnih brojeva.

   (a_2) Uočimo da element $0 \in G_1$ nema inverzni element, stoga skup G_1 nije grupa uz množenje realnih brojeva.

b) Kako znamo da je $(\mathbb{C}^2, +)$ grupa, dovoljno je provjeriti da je G_2 podgrupa od $\mathbb{C}^2$. Očito je G_2 neprazan skup i podskup od $\mathbb{C}^2$. Uzmimo proizvoljne elemente $a, b \in G_2$. Tada je $a = (z_1, \overline{z_1})$ i $b = (z_2, \overline{z_2})$ za neke $z_1, z_2 \in \mathbb{C}$, pa je

   $$a - b = (z_1 - z_2, \overline{z_1} - \overline{z_2}) = (z_1 - z_2, \overline{z_1 - z_2}) \in G_2,$$

   odnosno $(G_2, +)$ je, prema teoremu 1.2.2, podgrupa od $(\mathbb{C}^2, +)$.

c) Očito je skup G_3 neprazan podskup od $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

   (c_1) Vidimo da $2 +_5 4 = 1$ nije u G_3, odnosno ne vrijedi zatvorenost, pa G_3 nije grupa uz zbrajanje modulo 5.

   (c_2) Vidimo da $2 \cdot_5 4 = 3$ nije u G_3, odnosno ne vrijedi zatvorenost, pa G_3 nije grupa uz množenje modulo 5. ■

Zadatak 1.2.4. Pokažite da $H = \{a + bi \colon a, b \in \mathbb{R}, ab \geq 0\}$ nije podgrupa od $\mathbb{C}$ uz zbrajanje kompleksnih brojeva.

Rješenje. Dovoljno je naći jedan kontraprimjer. Uzmimo elemente $x = 1 + 0 \cdot i$ i $y = 0 - 1 \cdot i$ iz H. Tada $x + y = 1 - i \notin H$ jer $1 \cdot (-1) = -1 \not\geq 0$. Dakle, prema teoremu 1.2.2, H nije podgrupa od $\mathbb{C}$. ■

Zadatak 1.2.5. Neka je H podgrupa od $\mathbb{R}$ uz zbrajanje realnih brojeva. Pokažite da je skup $K = \{2^a \colon a \in H\}$ podgrupa od $\mathbb{R}^*$ uz množenje realnih brojeva.

Rješenje. Očito je K podskup od $\mathbb{R}^*$. Kako je H podgrupa od $\mathbb{R}$, znamo da je element 0 u H pa je element $2^0 = 1$ u K. Prema tome, skup K je neprazan. Uzmimo sada proizvoljne $x, y \in K$. Tada je $x = 2^a$ i $y = 2^b$ za neke $a, b \in H$. S obzirom da je H podgrupa od $\mathbb{R}$, element $a - b$ jest u H, pa je

$$2^{a-b} = 2^a \cdot 2^{-b} = 2^a \cdot (2^b)^{-1} = x \cdot y^{-1} \in K$$

te je, prema teoremu 1.2.2, K podgrupa od $\mathbb{R}^*$. ■

Zadatak 1.2.6. Dokažite da je

$$H = \left\{ \begin{bmatrix} x & -y \\ y & x \end{bmatrix} : x, y \in \mathbb{R}, x^2 + y^2 = 1 \right\}$$

podgrupa od $GL(2, \mathbb{R})$. □

Definicija 1.2.4. Centar grupe G, u oznaci $Z(G)$, podskup je svih elemenata u G koji komutiraju sa svakim elementom od G, to jest

$$Z(G) = \{a \in G \colon ag = ga, \forall g \in G\}.$$

Teorem 1.2.5. *Centar grupe G podgrupa je od G.*

Napomena 1.2.6. Grupa G Abelova je ako i samo ako je $G = Z(G)$.

Zadatak 1.2.7. Dokažite da je $Z(GL(n, \mathbb{R})) = \{\lambda I \colon \lambda \in \mathbb{R}^*\}$.

Rješenje. Tražimo sve matrice $A \in GL(n, \mathbb{R})$ takve da je $AB = BA$, $\forall B \in GL(n, \mathbb{R})$. Uzmimo proizvoljnu realnu regularnu matricu A reda n.

Neka je B regularna dijagonalna matrica reda n s elementima $\lambda_1, \lambda_2, \ldots, \lambda_n$ na glavnoj dijagonali. Tada je $\lambda_1 \cdot \lambda_2 \cdots \lambda_n \neq 0$. Da bi matrica A bila u centru grupe $GL(n, \mathbb{R})$, mora biti $AB = BA$. Lako se pokaže da je tada $a_{ij} = 0$ za sve $i \neq j$. Dakle, matrica A dijagonalna je matrica s elementima $a_{11}, a_{22}, \ldots, a_{nn}$, koje možemo označiti redom s $a_1, a_2, \ldots, a_n$, na glavnoj dijagonali. Kako je matrica A regularna, slijedi da je $a_1 \cdot a_2 \cdots a_n \neq 0$.

Neka je sada matrica B gornje trokutasta matrica reda n u kojoj su svi nenul elementi jednaki 1. Matrica je B očito regularna jer je $\det B = 1$. Da bi matrica A bila u centru grupe $GL(n, \mathbb{R})$, mora biti $AB = BA$, pa se lako pokaže da je tada $a_i = a_j$, za sve $i \neq j$. Prema tome, $a_1 = a_2 = \cdots = a_n$, odnosno $A = \lambda I$ i time smo pokazali da je centar grupe $GL(n, \mathbb{R})$ skup $\{\lambda I \colon \lambda \in \mathbb{R}^*\}$. ■

1.3 Homomorfizmi grupa

Definicija 1.3.1. Neka su $(G_1, *)$ i $(G_2, \star)$ grupe. Preslikavanje $\varphi\colon G_1 \to G_2$ zove se homomorfizam grupa ako vrijedi

$$\varphi(a * b) = \varphi(a) \star \varphi(b) \text{ za sve } a, b \in G_1.$$

Skup svih homomorfizama s G_1 u G_2 označavamo s $\mathrm{Hom}(G_1, G_2)$.

Ako je φ homomorfizam grupa koji je injekcija, onda kažemo da je φ monomorfizam grupa, a ako je φ homomorfizam grupa koji je surjekcija, onda kažemo da je φ epimorfizam grupa.

Homomorfizam grupa koji je bijekcija nazivamo izomorfizam grupa. Ako postoji izomorfizam grupa $\varphi\colon G_1 \to G_2$, kažemo da je grupa G_1 izomorfna grupi G_2 i u tom slučaju pišemo $G_1 \cong G_2$. Relacija $\cong$ relacija je ekvivalencije. Izomorfizam grupa $\varphi\colon G \to G$ naziva se automorfizam i skup svih automorfizama od G označavamo s $\mathrm{Aut}(G)$.

Ako su $\varphi_1\colon G_1 \to G_2$ i $\varphi_2\colon G_2 \to G_3$ homomorfizmi grupa, onda je i njihova kompozicija $\varphi_2 \circ \varphi_1\colon G_1 \to G_3$ homomorfizam grupa. Analogno vrijedi za kompoziciju monomorfizama grupa, epimorfizama grupa i izomorfizama grupa.

Propozicija 1.3.2. *Neka je $\varphi\colon G_1 \to G_2$ homomorfizam grupa. Tada vrijedi:*

a) $\varphi(e_{G_1}) = e_{G_2}$,

b) $\varphi(a^{-1}) = [\varphi(a)]^{-1}$ *za sve* $a \in G_1$.

Definicija 1.3.3. Neka je $\varphi\colon G_1 \to G_2$ homomorfizam grupa. Skup

$$\mathrm{Im}\,\varphi = \{\varphi(a)\colon a \in G_1\}$$

nazivamo slika homomorfizma φ, a skup

$$\mathrm{Ker}\,\varphi = \{a \in G_1\colon \varphi(a) = e_{G_2}\}$$

nazivamo jezgra homomorfizma φ.

Propozicija 1.3.4. *Neka je $\varphi\colon G_1 \to G_2$ homomorfizam grupa. Tada je slika homomorfizma φ podgrupa od G_2, a jezgra homomorfizma φ podgrupa od G_1.*

Propozicija 1.3.5. *Homomorfizam grupa $\varphi\colon G_1 \to G_2$ monomorfizam je ako i samo ako je $Ker\,\varphi = \{e_{G_1}\}$.*

Zadatak 1.3.1. Dokažite da je preslikavanje $\varphi\colon GL(n, \mathbb{R}) \to \mathbb{R}^*$ definirano s

$$\varphi(A) = \det A$$

epimorfizam grupa i odredite mu jezgru.

Rješenje. Uzmimo proizvoljne matrice $A, B \in GL(n, \mathbb{R})$. Tada imamo

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

Prema tome, preslikavanje $\varphi\colon GL(n, \mathbb{R}) \to \mathbb{R}^*$ homomorfizam je grupa.

Pokažimo sada da je preslikavanje φ surjekcija. Neka je $x \in \mathbb{R}^*$. Tražimo matricu A takvu da je $\det A = x$. Za dijagonalnu matricu kojoj su na glavnoj dijagonali elementi $x, 1, \ldots, 1$ jest $\det A = x \neq 0$, pa je prema tome matrica A iz $GL(n, \mathbb{R})$. Dakle, preslikavanje φ epimorfizam je grupa.

Nadalje, jezgra od φ jednaka je

$$\operatorname{Ker} \varphi = \{A \in GL(n, \mathbb{R})\colon \varphi(A) = \det A = 1\} = SL(n, \mathbb{R}).$$

Posebno, uočite da preslikavanje φ nije monomorfizam grupa. ■

Zadatak 1.3.2. Pokažite da je preslikavanje $x \mapsto i^x$ homomorfizam grupe $(\mathbb{Z}, +)$ u grupu $(K_4, \cdot)$ te da je $\operatorname{Ker} \varphi = \{m \in \mathbb{Z}\colon m = 4k, k \in \mathbb{Z}\}$. Je li φ epimorfizam grupa? □

Zadatak 1.3.3. Neka je $\varphi\colon G_1 \to G_2$ homomorfizam grupa. Dokažite da ako je G_1 Abelova grupa, onda je i $\operatorname{Im} \varphi$ Abelova grupa.

Rješenje. Neka je G_1 Abelova grupa. Znamo da je $\operatorname{Im} \varphi$ grupa jer je podgrupa od G_2. Treba još pokazati da je ona Abelova grupa. Za proizvoljne elemente a_1, a_2 u G_1 postoje elementi b_1, b_2 u $\varphi(G_1)$ takvi da je $\varphi(a_1) = b_1$ i $\varphi(a_2) = b_2$. Sada imamo

$$b_1 b_2 = \varphi(a_1)\varphi(a_2) = \varphi(a_1 a_2) = \varphi(a_2 a_1) = \varphi(a_2)\varphi(a_1) = b_2 b_1,$$

jer je preslikavanje φ homomorfizam grupa i G_1 Abelova grupa. Prema tome, $\operatorname{Im} \varphi$ Abelova je grupa. ■

Zadatak 1.3.4. Neka je $\varphi\colon G \to H$ homomorfizam grupa. Dokažite da za sve prirodne brojeve n vrijedi

$$\varphi\left(\prod_{i=1}^{n} a_i\right) = \prod_{i=1}^{n} \varphi(a_i).$$ □

Zadatak 1.3.5. Dokažite da je grupa G Abelova grupa ako i samo ako je preslikavanje $\varphi\colon G \to G$ definirano s $\varphi(a) = a^{-1}$ automorfizam.

Rješenje. Pokažimo najprije nužnost. Neka je G Abelova grupa i $\varphi\colon G \to G$ preslikavanje definirano s $\varphi(a) = a^{-1}$. Uzmimo proizvoljne elemente a i b iz grupe G. Kako je

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

slijedi da je preslikavanje φ homomorfizam grupa. Još treba pokazati da je φ bijekcija. Injektivnost je očita. Naime, ako je $\varphi(a) = \varphi(b)$, slijedi da je $a^{-1} = b^{-1}$, odnosno $a = b$. Nadalje, za $a \in G$ je $\varphi(a^{-1}) = (a^{-1})^{-1} = a$, pa imamo surjektivnost.

Da bismo pokazali dovoljnost, pretpostavimo da je preslikavanje $\varphi\colon G \to G$ definirano s $\varphi(a) = a^{-1}$ automorfizam grupe G. Znamo da je G grupa, treba pokazati da je ona komutativna. Iz definicije imamo

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

a s druge strane, znamo da je

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

Prema tome, vrijedi $a^{-1}b^{-1} = b^{-1}a^{-1}$. Množimo li najprije s a zdesna pa s b zdesna, a zatim s a slijeva pa s b slijeva, slijedi traženo. ■

Zadatak 1.3.6. Neka je za dani element a iz grupe G definirano preslikavanje $\varphi_a \colon G \to G$ s

$$\varphi_a(x) = axa^{-1}.$$

a) Dokažite da je φ_a automorfizam grupe G. (Taj automorfizam naziva se unutrašnji automorfizam grupe G).

b) Neka je s $\mathrm{Int}(G)$ označen skup svih unutrašnjih automorfizama grupe G. Dokažite da je $\mathrm{Int}(G)$ grupa u odnosu na kompoziciju.

Rješenje.

a) Kako je

$$\varphi_a(x_1x_2) = ax_1x_2a^{-1} = ax_1a^{-1}ax_2a^{-1} = \varphi_a(x_1)\varphi_a(x_2)$$

za sve elemente x_1, x_2 iz G, slijedi da je φ_a homomorfizam grupa.

Za $\varphi_a(x_1) = \varphi_a(x_2)$ imamo $ax_1a^{-1} = ax_2a^{-1}$. Djelujemo li s a^{-1} slijeva, a s a zdesna, dobijemo $x_1 = x_2$, odnosno zaključujemo da je preslikavanje φ_a injekcija.

Nadalje, neka je $y \in G$ i tražimo $x \in G$ takav da $\varphi_a(x) = y$. Kako je $\varphi_a(x) = y$ ako i samo ako je $axa^{-1} = y$, slijedi da je $x = a^{-1}ya \in G$ traženi element. Prema tome, preslikavanje φ_a jest surjekcija.

Time smo pokazali da je preslikavanje φ_a automorfizam grupe G.

b) Zatvorenost vrijedi jer za $\varphi_a, \varphi_b \in \mathrm{Int}(G)$ imamo

$$(\varphi_a \circ \varphi_b)(x) = \varphi_a(\varphi_b(x)) = \varphi_a(bxb^{-1}) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = \varphi_{ab}(x) \in \mathrm{Int}(G).$$

Asocijativnost kompozicije vrijedi. Neutralni je element φ_e jer je $\varphi_a \circ \varphi_e = \varphi_{ae} = \varphi_a$ i $\varphi_e \circ \varphi_a = \varphi_{ea} = \varphi_a$. Nadalje, trebamo pronaći inverzni element od φ_a. Imamo $\varphi_a \circ \varphi_b = \varphi_e$, odnosno $\varphi_{ab} = \varphi_e$. Sada lako vidimo da je $(\varphi_a)^{-1} = \varphi_{a^{-1}}$.

Prema tome, $\mathrm{Int}(G)$ grupa je u odnosu na kompoziciju. ■

Zadatak 1.3.7. Dokažite da grupe $\mathbb{R}^*$ i $\mathbb{C}^*$ nisu izomorfne.

Rješenje. Pretpostavimo suprotno, to jest pretpostavimo da postoji izomorfizam grupa $\varphi \colon \mathbb{C}^* \to \mathbb{R}^*$. Znamo da homomorfizam grupa preslikava neutralni element u neutralni element pa znamo da je $\varphi(1) = 1$. Nadalje, $1 = \varphi(1) = \varphi((-1) \cdot (-1)) = \varphi(-1)\varphi(-1)$ jer je preslikavanje φ homomorfizam grupa. Prema tome, $\varphi(-1)$ jednak je 1 ili -1. S obzirom da je preslikavanje φ injektivno, slijedi da je $\varphi(-1) = -1$. Sada vidimo da je $-1 = \varphi(-1) = \varphi(i \cdot i) = \varphi(i)\varphi(i)$, iz čega zaključujemo da $\varphi(i) \notin \mathbb{R}^*$, čime smo došli do kontradikcije. Dakle, ne postoji izomorfizam između grupa $\mathbb{R}^*$ i $\mathbb{C}^*$. Drugim riječima, grupe $\mathbb{R}^*$ i $\mathbb{C}^*$ nisu izomorfne. ■

Napomena 1.3.6. Svaka grupa reda 4 izomorfna je ili grupi $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ ili grupi $(\mathbb{Z}_4, +)$.

Zadatak 1.3.8. Pokažite da grupe $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ i $(\mathbb{Z}_4, +)$ nisu izomorfne. □

1.4 Simetrična grupa

Neka je S neprazan skup. Prisjetimo se, permutacija skupa S bijekcija je sa S na S. Skup svih permutacija skupa S označavamo s $B(S)$, a $(B(S), \circ)$ grupa je permutacija skupa S koja je nekomutativna grupa za $|S| \geq 3$. Ako je $|S| = n$, onda se grupa permutacija skupa S naziva simetrična grupa $n-$tog reda i označava sa S_n. Red grupe S_n jest $n!$.

Ako su σ, τ u S_n, njihovu kompoziciju $\sigma \circ \tau$ označavat ćemo kraće s $\sigma\tau$ i zvati produkt permutacija σ i τ.

Permutaciju $\sigma\colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ zapisivat ćemo na sljedeći način:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Zadatak 1.4.1. Ako je $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ i $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$, odredite $\sigma\tau$, $\tau\sigma$, σ^{-1} i τ^{-1}.

Rješenje. Kompoziciju permutacija pronaći ćemo tako da idemo s desna na lijevo, i to od vrha prema dnu, a zatim opet od vrha prema dnu. Dakle, imamo

$$\sigma\tau(1) = \sigma(\tau(1)) = \sigma(4) = 4,$$

pa se u kompoziciji $\sigma\tau$ ispod elementa 1 nalazi element 4. Slično dobijemo ostale elemente. Prema tome,

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

Inverzna permutacija dobije se tako da dva retka zamijene mjesta, a zatim stupce poslo-žimo tako da u prvom retku ponovo budu redom brojevi $1, 2, \ldots, n$. Dakle,

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}.$$

Za vježbu odredite $\sigma\tau$ i σ^{-1}. ■

Definicija 1.4.1. Za permutaciju $\sigma \in S_n$ kažemo da je $k-$ciklus ili ciklus duljine k, gdje je $2 \leq k \leq n$ ako postoje $c_1, c_2, \ldots, c_k \in \{1, 2, \ldots, n\}$ takvi da je $\sigma(c_1) = c_2$, $\sigma(c_2) = c_3, \ldots, \sigma(c_{k-1}) = c_k, \sigma(c_k) = c_1$ i $\sigma(j) = j$ za sve $j \notin \{c_1, c_2, \ldots, c_k\}$. Takav $k-$ciklus označavamo sa

$$\sigma = (c_1, c_2, \ldots, c_k) \in S_n.$$

Za cikluse kažemo da su disjunktni ako su podskupovi od $\{1, 2, \ldots, n\}$ koje oni ciklički permutiraju međusobno disjunktni. Primjerice, ciklusi $(1, 4, 5)$ i $(2, 3)$ disjunktni su, a ciklusi $(1, 4, 5)$ i $(2, 4)$ nisu.

Napomena 1.4.2. Disjunktni ciklusi komutiraju.

Propozicija 1.4.3. *Svaka je permutacija $\sigma \in S_n$ ili ciklus ili produkt međusobno disjunktnih ciklusa koji su jedinstveno određeni sa σ.*

Primjer 1.4.1. Primjetimo da je

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

ciklus. Zaista, uzmemo li $c_1 = 1$, $c_2 = 4$ i $c_3 = 2$, tvrdnja slijedi iz definicije.

Primjer 1.4.2. Uočimo da

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

nije ciklus. Zaista, uzmemo li $c_1 = 1$, $c_2 = 4$, imamo ciklus $(1, 4)$, ali točke 2 i 3 nisu fiksne pa, prema definiciji, σ nije ciklus.

Zadatak 1.4.2. Prikažite permutaciju

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 3 & 8 & 1 & 2 & 7 & 5 \end{pmatrix} \in S_8$$

u obliku produkta disjunktnih ciklusa.

Rješenje. Imamo $\sigma = (1, 4, 8, 5)(2, 6)(3)(7) = (1, 4, 8, 5)(2, 6)$. ■

Zadatak 1.4.3. Napišite $\sigma\tau$ kao produkt disjunktnih ciklusa ako je $\sigma = (1, 3, 2, 4)(5, 6)$ i $\tau = (1, 5, 6)(2, 4, 3)$.

Rješenje. Imamo $\sigma\tau = (1, 6, 3, 4, 2)(5)$. ■

Zadatak 1.4.4. Odredite sve permutacije na skupu S_3 i napravite pripadnu Cayleyevu tablicu. □

Definicija 1.4.4. Ciklus duljine 2 ili $2-$ciklus naziva se transpozicija.

Propozicija 1.4.5. *Svaka je permutacija $\sigma \in S_n$, $\sigma \neq id$ ili transpozicija ili produkt transpozicija.*

Lema 1.4.6. *Svaki $k-$ciklus za $k > 2$ produkt je $k - 1$ transpozicija.*

Primjer 1.4.3. Imamo $(1, 2, 3, 4, 5) = (1, 5)(1, 4)(1, 3)(1, 2)$.

Definicija 1.4.7. Permutacija σ parna je ako se može prikazati kao produkt parnog broja transpozicija. U suprotnom kažemo da je permutacija σ neparna.

Definicija 1.4.8. Ako je permutacija σ parna, definiramo $\operatorname{sgn}\sigma = 1$, a ako je permutacija σ neparna, definiramo $\operatorname{sgn}\sigma = -1$. Broj $\operatorname{sgn}\sigma$ nazivamo predznak permutacije σ i preslikavanje

$$\operatorname{sgn}\colon (S_n, \circ) \to (\{-1, 1\}, \cdot)$$

homomorfizam je grupa.

Identiteta je parna permutacija. Predznak ciklusa duljine k jest $(-1)^{k-1}$ pa, rastavimo li permutaciju u produkt disjunktnih ciklusa, lako možemo izračunati predznak svake permutacije. Nadalje, $\operatorname{sgn}\sigma^{-1} = \operatorname{sgn}\sigma$.

S A_n označavamo skup svih parnih permutacija. Skup A_n podgrupa je od S_n koju nazivamo alternirajuća grupa. Red alternirajuće grupe A_n jest $\frac{n!}{2}$.

Zadatak 1.4.5. Odredite parnost permutacije $\sigma \in S_8$ zadane sa $\sigma = (1,2,4)(3,6)(5,7)$.

Rješenje. Očito je

$$\operatorname{sgn}\sigma = (\operatorname{sgn}(1,2,4))(\operatorname{sgn}(3,6))(\operatorname{sgn}(5,7)) = (-1)^2 \cdot (-1) \cdot (-1) = 1,$$

iz čega zaključujemo da je σ parna permutacija. ■

Napomena 1.4.9. Red $k-$ciklusa jest k. Red permutacije konačnog skupa zapisane kao produkt disjunktnih ciklusa najmanji je zajednički višekratnik redova ciklusa.

Zadatak 1.4.6. Odredite red permutacije $\sigma = (4,5)(2,3,7)$.

Rješenje. Permutacija σ očito je zapisana kao produkt disjunktnih ciklusa. Red ciklusa $(4,5)$ jest 2, a red ciklusa $(2,3,7)$ jest 3. Kako je $\operatorname{nzv}(2,3) = 6$, slijedi da je red permutacije σ jednak 6. ■

1.5 Normalne i kvocijentne podgrupe

Definicija 1.5.1. Neka je H podgrupa grupe G te neka su $a, b \in G$. Kažemo da je a desno kongruentan b modulo H ako je $b^{-1}a \in H$. Pišemo $a \sim^H b$.

Napomena 1.5.2. Relacija $\sim^H$ relacija je ekvivalencije na skupu G.

Napomena 1.5.3. Za $a \in G$ s $[a]$ označit ćemo klasu ekvivalencije u odnosu na relaciju $\sim^H$ u kojoj se nalazi element a:

$$[a] = \{b \in G\colon b \sim^H a\} = \{b \in G\colon a^{-1}b \in H\} = \{b \in G\colon b = ah, h \in H\}.$$

Lema 1.5.4. *Neka je H podgrupa grupe G i $a \in G$. Tada je*

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

Klase ekvivalencije $[a] = aH$ zovu se desne klase u grupi G u odnosu na podgrupu H ili, kraće, desne $H-$klase u G. Grupa G disjunktna je unija svojih desnih $H-$klasa.

Primjer 1.5.1. Neka je $n \in \mathbb{N}$, tada je $n\mathbb{Z} \leq \mathbb{Z}$. Uvjerite se u to za vježbu. Prema tome, $6\mathbb{Z} \leq \mathbb{Z}$. Uzmimo $a, b \in \mathbb{Z}$. Tada je

$$a \sim^{6\mathbb{Z}} b \Leftrightarrow -b + a \in 6\mathbb{Z} \Leftrightarrow 6 \mid a - b \Leftrightarrow a \equiv b \pmod 6.$$

Prema tome, u istoj klasi nalaze se oni elementi koji daju isti ostatak pri dijeljenju sa 6, pa imamo klase $[0] = \{\ldots, -6, 0, 6, \ldots\} = 0 + 6\mathbb{Z}$, $[1] = \{\ldots, -5, 1, 7, \ldots\} = 1 + 6\mathbb{Z}, \ldots,$ $[5] = \{\ldots, -1, 5, 11, \ldots\} = 5 + 6\mathbb{Z}$. Tada je

$$\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [5] = 6\mathbb{Z} \cup 1 + 6\mathbb{Z} \cup \cdots \cup 5 + 6\mathbb{Z}.$$

Analogno se definira relacija biti lijevo kongruentan modulo H:

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

Relacija ${}^{H}\!\sim$ relacija je ekvivalencije na skupu G, a klasa ekvivalencije koja sadrži element $a \in G$ jednaka je

$$[a] = \{ha \colon h \in H\} = Ha.$$

Klase Ha zovu se lijeve klase u grupi G u odnosu na podgrupu H ili, kraće, lijeve $H-$klase u G. Grupa G disjunktna je unija svojih lijevih $H-$klasa.

Napomena 1.5.5. U konačnoj grupi G vrijedi $|Ha| = |H| = |aH|$ za sve $a \in G$.

Teorem 1.5.6. *(Lagrange) Neka je G konačna grupa i H podgrupa od G. Tada je red grupe G djeljiv redom grupe H.*

Definicija 1.5.7. Broj različitih desnih (lijevih) $H-$klasa u G označava se s $[G \colon H]$ i naziva indeks podgrupe H u G. Za podgrupu H grupe G kažemo da je konačnog indeksa u grupi G ako ima samo konačno mnogo različitih desnih (lijevih) $H-$klasa u grupi G.

Primjer 1.5.2. Indeks podgrupe $6\mathbb{Z}$ u grupi $\mathbb{Z}$ jest 6, to jest $[\mathbb{Z} : 6\mathbb{Z}] = 6$.

Napomena 1.5.8. Ako je H podgrupa konačne grupe G, onda prema Lagrangeovom teoremu vrijedi:

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

Lema 1.5.9. *Ako je G konačna grupa prostog reda, onda G nema pravih podgrupa.*

Zadatak 1.5.1. Dokažite da grupa S_9 nema podgrupu reda 11.

Rješenje. Pretpostavimo suprotno, to jest pretpostavimo da postoji podgrupa H grupe S_9 reda 11. Kako je $|S_9| = 9!$, prema Lagrangeovom teoremu slijedi da $11 \mid 9!$, što ne vrijedi. Dakle, slijedi tvrdnja. ■

Zadatak 1.5.2. Neka je G grupa i $\varphi \colon \mathbb{Z}_{17} \to G$ homomorfizam koji nije monomorfizam. Odredite formulu za $\varphi(x)$.

Rješenje. Kako je jezgra od φ podgrupa od $\mathbb{Z}_{17}$, prema Lagrangeovom teoremu $|\operatorname{Ker}\varphi|$ dijeli $|\mathbb{Z}_{17}| = 17$. Prema tome, $|\operatorname{Ker}\varphi| \in \{1, 17\}$. S obzirom da φ nije monomorfizam, red jezgre od φ nije 1, odnosno $|\operatorname{Ker}\varphi| = 17$, pa preslikavanje φ očito sve elemente iz $\mathbb{Z}_{17}$ preslika u neutralni element od G. Dakle, $\varphi(x) = e_G$ za sve $x \in \mathbb{Z}_{17}$. ■

Zadatak 1.5.3. Neka je G Abelova grupa neparnog reda. Dokažite da je umnožak svih elemenata grupe G neutralni element te grupe.

Rješenje. Neka je $G = \{e, a_1, \ldots, a_{2n}\}$ Abelova grupa neparnog reda. Očito je $|G| = 2n+1$. Svaki element $a_i \neq e$ u G ima inverz $a_i^{-1} \in \{a_1, \ldots, a_{2n}\}$. Pretpostavimo da je a_i sam sebi inverz. Tada je $\{e, a_i\}$ podgrupa od G reda 2 pa prema Lagrangeovom teoremu $2 \mid |G|$, što ne može biti jer je G grupa neparnog reda. Dakle, svaki element $a_i \neq e$ ima inverz a_i^{-1} koji je različit od a_i pa zbog svojstva komutativnosti imamo

$$a_1 a_2 \cdots a_{2n} = a_1 a_1^{-1} a_2 a_2^{-1} \cdots a_n a_n^{-1} = e.$$

Prema tome, umnožak svih elemenata grupe G neutralni je element te grupe. ■

Definicija 1.5.10. Podgrupa H grupe G zove se normalna podgrupa od G, u oznaci $H \trianglelefteq G$, ako vrijedi

$$aH = Ha \text{ za sve } a \in G.$$

Napomena 1.5.11. Lako je vidjeti da je $H \trianglelefteq G$ ako i samo ako je $aHa^{-1} = H$ za sve $a \in G$.

Primjer 1.5.3. Centar $Z(G)$ grupe G normalna je podgrupa od G.

Primjer 1.5.4. Alternirajuća grupa A_n normalna je podgrupa od S_n.

Lema 1.5.12. *Svaka je podgrupa Abelove grupe normalna.*

Primjer 1.5.5. Kako je grupa $\mathbb{Z}$ komutativna grupa, iz leme 1.5.12 slijedi da je svaka njezina podgrupa normalna. Prema tome, podgrupa $6\mathbb{Z}$ normalna je podgrupa od $\mathbb{Z}$.

Zadatak 1.5.4. Dokažite da je $SL(n, \mathbb{R})$ normalna podgrupa od $GL(n, \mathbb{R})$.

Rješenje. Pokazali smo ranije da je $SL(n, \mathbb{R})$ podgrupa od $GL(n, \mathbb{R})$. Uzmimo matrice $A \in SL(n, \mathbb{R})$ i $B \in GL(n, \mathbb{R})$. Tada je

$$\det(BAB^{-1}) = (\det B) \cdot (\det A) \cdot (\det B)^{-1} = (\det B) \cdot (\det B)^{-1} = 1.$$

Prema tome, $BAB^{-1} \in SL(n, \mathbb{R})$, odnosno $SL(n, \mathbb{R})$ normalna je podgrupa od $GL(n, \mathbb{R})$. ■

Zadatak 1.5.5. Neka je $\varphi\colon G_1 \to G_2$ epimorfizam grupa. Ako je $N \trianglelefteq G_1$, dokažite da je onda $\varphi(N) \trianglelefteq G_2$. □

Definicija 1.5.13. Neka je G grupa i neka je H normalna podgrupa od G. Skup

$$G/H = \{aH\colon a \in G\}$$

svih $H-$klasa u G grupa je koju zovemo kvocijentna grupa po normalnoj podgrupi H uz operaciju

$$(aH)(bH) = abH.$$

Napomena 1.5.14. U kvocijentnoj grupi G/H, $a^{-1}H$ inverzni je element od aH, a $eH = H$ neutralni je element.

Primjer 1.5.6. Kako je $6\mathbb{Z}$ normalna podgrupa od $\mathbb{Z}$, onda je

$$\mathbb{Z}/6\mathbb{Z} = \{6\mathbb{Z}, 1 + 6\mathbb{Z}, \ldots, 5 + 6\mathbb{Z}\} = \{[0], [1], \ldots, [5]\}$$

kvocijentna grupa uz binarnu operaciju definiranu s

$$(a + 6\mathbb{Z}) + (b + 6\mathbb{Z}) = a + b + 6\mathbb{Z} \text{ za sve } a, b \in \mathbb{Z}.$$

Teorem 1.5.15. *Neka je $\varphi\colon G_1 \to G_2$ homomorfizam grupa.*

a) $Ker\varphi$ normalna je podgrupa od G_1.

b) Preslikavanje $\Phi\colon G_1/\,Ker\varphi \to Im\varphi$ definirano s

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

izomorfizam je kvocijentne grupe $G_1/\,Ker\varphi$ na grupu $Im\varphi$.

Napomena 1.5.16. Dio b) teorema 1.5.15 zove se Prvi teorem o izomorfizmu za grupe.

Primjer 1.5.7. Neka je preslikavanje $\varphi\colon \mathbb{Z} \to \mathbb{Z}_m$ definirano s $\varphi(z) = z \pmod m$. Lako se pokaže da je preslikavanje φ homomorfizam grupa, da je $\operatorname{Ker}\varphi = m\mathbb{Z}$ te da je φ epimorfizam, odnosno da je $\operatorname{Im}\varphi = \mathbb{Z}_m$. Sada, prema Prvom teoremu o izomorfizmu za grupe, slijedi da je

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m.$$

Primjer 1.5.8. Pokazali smo ranije da je preslikavanje $\varphi\colon GL(n,\mathbb{R}) \to \mathbb{R}^*$ definirano s $\varphi(A) = \det A$ epimorfizam grupa te da je $\operatorname{Ker}\varphi = SL(n,\mathbb{R})$. Sada, prema Prvom teoremu o izomorfizmu za grupe, slijedi da je

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

Zadatak 1.5.6. Dokažite da je grupa $\mathbb{C}^*/S^1$ izomorfna grupi $\mathbb{R}^*_+$.

Rješenje. Definirajmo preslikavanje $\varphi\colon \mathbb{C}^* \to \mathbb{R}^*_+$ s $\varphi(z) = |z|$ i neka su $z_1, z_2 \in \mathbb{C}^*$. Lako se pokaže da je preslikavanje φ dobro definirano i ono je homomorfizam grupa jer je

$$\varphi(z_1z_2) = |z_1z_2| = |z_1||z_2| = \varphi(z_1)\varphi(z_2).$$

Za svaki element x u $\mathbb{R}^*_+$ je $\varphi(x) = |x| = x$, pa je preslikavanje φ surjekcija, a

$$\operatorname{Ker}\varphi = \{z \in \mathbb{C}^*\colon \varphi(z) = |z| = 1\} = S^1.$$

Prema prvom teoremu o izomorfizmu za grupe slijedi da je $\mathbb{C}^*/S^1 \cong \mathbb{R}^*_+$. ■

Napomena 1.5.17. Homomorfizam grupa $\varphi\colon G \to H$ trivijalni je homomorfizam ako je

$$\varphi(g) = e_H \text{ za sve } g \in G.$$

Uočimo da je tada $|\operatorname{Im}\varphi| = 1$.

Zadatak 1.5.7. Neka je $\varphi\colon G \to H$ netrivijalni homomorfizam grupa i neka je $|G| = 24$, $|H| = 15$. Odredite red jezgre i slike preslikavanja φ.

Rješenje. Iz Prvog teorema o izomorfizmu za grupe imamo da je

$$G/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi.$$

Kako je izomorfizam bijekcija, znamo da je $|G/\operatorname{Ker}\varphi| = |\operatorname{Im}\varphi|$. Također, znamo da je

$$|G/\operatorname{Ker}\varphi| = [G : \operatorname{Ker}\varphi],$$

pa iz napomene 1.5.8 slijedi da je

$$|G| = |\operatorname{Im}\varphi| \cdot |\operatorname{Ker}\varphi|.$$

Nadalje, kako je jezgra preslikavanja φ podgrupa od G, a slika preslikavanja φ podgrupa od H, prema Lagrangeovom teoremu slijedi da $|\operatorname{Ker}\varphi| \mid 24$, a $|\operatorname{Im}\varphi| \mid 15$. S obzirom da je preslikavanje φ netrivijalni homomorfizam i da je $24 = |\operatorname{Im}\varphi| \cdot |\operatorname{Ker}\varphi|$, slijedi da je red slike od φ jednak 3, a onda se lako vidi da je red jezgre od φ jednak 8. ■

Zadatak 1.5.8. Neka je $\varphi\colon S_3 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ netrivijalni homomorfizam grupa. Odredite red slike preslikavanja φ.

Rješenje. Iz prethodnog zadatka znamo da je $|S_3| = |\operatorname{Ker}\varphi| \cdot |\operatorname{Im}\varphi|$. Također, znamo da je red grupe S_3 jednak $3! = 6$, a da je red grupe

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}$$

jednak 4. Sada, prema Lagrangeovom teoremu, slijedi da $|\operatorname{Im}\varphi| \mid 4$, pa je $|\operatorname{Im}\varphi| \in \{1,2,4\}$. Kako preslikavanje φ nije trivijalan homomorfizam, zaključujemo da je $|\operatorname{Im}\varphi| \in \{2,4\}$, pa iz $6 = |\operatorname{Ker}\varphi| \cdot |\operatorname{Im}\varphi|$ dobijemo da je red slike od φ jednak 2. ■

Teorem 1.5.18. *(Cayley) Neka je G grupa i $S(G)$ grupa permutacija skupa G. Tada postoji monomorfizam $\varphi\colon G \to S(G)$. Prema tome, svaka je grupa G izomorfna nekoj podgrupi grupe permutacija $S(G)$. Posebno, svaka konačna grupa reda n izomorfna je podgrupi grupe S_n.*

1.6 Cikličke grupe

Neka je G grupa i a element u G. Za $n \in \mathbb{N}$ definiramo $a^n = a \cdot a \cdots a$ (imamo n faktora) i pri tome je $a^0 = e$. Također, neka je $a^{-n} = (a^{-1})^n$, gdje je a^{-1} inverz od a. Lako se vidi da za $m, n \in \mathbb{Z}$ vrijedi $a^{m+n} = a^m a^n$.

Za neprazan podskup S grupe G, za najmanju podgrupu koja sadrži skup S kažemo da je generirana sa S i označavamo je sa $\langle S\rangle$. Posebno,

$$\langle a\rangle = \langle\{a\}\rangle$$

podgrupa je od G generirana elementom $a \in G$ i to je najmanja podgrupa od G koja sadrži a.

Definicija 1.6.1. Grupa G naziva se ciklička grupa ako je generirana jednim elementom, odnosno ako postoji element $a \in G$ takav da je $G = \{a^n\colon n \in \mathbb{Z}\}$ i označavamo ju s $G = \langle a\rangle$.

Lema 1.6.2. *Svaka je ciklička grupa Abelova.*

Lema 1.6.3. *Neka je K podgrupa aditivne grupe $\mathbb{Z}$. Tada je ili $K = \{0\}$ ili postoji $m \in \mathbb{N}$ takav da je $K = m\mathbb{Z}$.*

Propozicija 1.6.4. *Neka je G grupa i $a \in G$. Tada vrijedi jedna od sljedećih dviju mogućnosti:*

a) $\langle a\rangle$ je beskonačna grupa i tada je $\langle a\rangle = \{\ldots, a^{-2}, a^{-1}, e, a^1, a^2, \ldots\} \cong \mathbb{Z}$.

b) $\langle a\rangle$ je konačna grupa i tada je $\langle a\rangle = \{e, a, a^2, \ldots, a^{m-1}\} \cong \mathbb{Z}_m$ za neki $m \in \mathbb{N}$.

Definicija 1.6.5. Neka je G grupa i $a \in G$. Red cikličke grupe generirane s a nazivamo red ili period elementa a. To je najmanji $n \in \mathbb{N}$ takav da je $a^n = e$, ako takav postoji, i označava se s $|a|$. Ako takav n ne postoji, kažemo da je element a beskonačnog reda.

Lema 1.6.6.

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

b) U konačnoj grupi red elementa dijeli red grupe.

c) Za sve elemente a u konačnoj grupi G vrijedi $a^{|G|} = e$.

d) Neka je a element reda n u grupi G. Ako je $a^k = e$, onda n dijeli k.

Propozicija 1.6.7. *Ako je G grupa prostog reda i $a \in G$, $a \neq e$, onda je $\langle a\rangle = G$.*

Lema 1.6.8. *Neka je $\varphi\colon G_1 \to G_2$ homomorfizam grupa. Ako je element $g \in G_1$ konačnog reda, onda je red od g djeljiv redom od $\varphi(g)$.*

Primjer 1.6.1.

a) U grupi $\mathbb{Z}_4$ neutralni je element 0 i element 1 jest reda 4 jer je $1+1+1+1 = 0$. Element 2 jest reda 2 jer je $2 + 2 = 0$, a element 3 jest reda 4 jer je $3 + 3 + 3 + 3 = 0$.

b) U grupi $\mathbb{Z}_2 \times \mathbb{Z}_2$ neutralni je element $(0, 0)$ te je $|(0, 1)| = 2$ jer je $(0, 1) + (0, 1) = (0, 0)$, $|(1, 0)| = 2$ jer je $(1, 0) + (1, 0) = (0, 0)$ i $|(1, 1)| = 2$ jer je $(1, 1) + (1, 1) = (0, 0)$.

c) U grupi $\mathbb{Z}$ element 1 beskonačnog je reda.

Napomena 1.6.9. Uočimo da se u grupi $\mathbb{Z}_4$ nalaze neutralni element, dva elementa reda 4 i jedan reda 2, a da su u grupi $\mathbb{Z}_2 \times \mathbb{Z}_2$ svi elementi, izuzev neutralnog elementa, reda 2.

Zadatak 1.6.1. Odredite redove danih elemenata u zadanim grupama:

a) i u grupi $\mathbb{C}^*$,

b) 1 i 4 u grupi $\mathbb{Z}_6$,

c) $\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$ u grupi $GL(2, \mathbb{R})$.

Rješenje.

a) U grupi $\mathbb{C}^*$ neutralni je element 1 pa kako je $i^1 = i$, $i^2 = -1$, $i^3 = -i$, a $i^4 = 1$, očito je $|i| = 4$, odnosno element i jest reda 4.

b) Za vježbu.

c) U grupi $GL(2, \mathbb{R})$ neutralni je element jedinična matrica $I \in GL(2, \mathbb{R})$. Vidimo da je

$$\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I,$$

pa je element $\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$ reda 2. ■

Zadatak 1.6.2. Dokažite da u grupi G za sve elemente $a, b \in G$ vrijedi:

a) $|a| = |a^{-1}|$,

b) $|a| = |b^{-1}ab|$,

c) $|ab| = |ba|$.

Rješenje. Neka je $|a| = k$, to jest $a^k = e$ i $a^i \neq e$ za $1 \leq i < k$.

a) Neka je $|a^{-1}| = k'$. Tada je $(a^{-1})^k = (a^k)^{-1} = e^{-1} = e$, iz čega slijedi da je $k \geq k'$. S druge strane, $a^{k'} = ((a^{-1})^{-1})^{k'} = ((a^{-1})^{k'})^{-1} = e^{-1} = e$, pa slijedi da je $k' \geq k$. Dakle, $k = k'$, odnosno $|a| = |a^{-1}|$.

b) Uočimo najprije da je

$$(b^{-1}ab)^n = (b^{-1}ab)(b^{-1}ab)\cdots(b^{-1}ab) = b^{-1}a^nb.$$

Neka je $|b^{-1}ab| = l$. Sada imamo $(b^{-1}ab)^k = b^{-1}a^kb = b^{-1}eb = e$, pa je $k \geq l$. S druge strane, imamo $a^l = bb^{-1}a^lbb^{-1} = b(b^{-1}ab)^lb^{-1} = beb^{-1} = e$, pa je $l \geq k$. Prema tome, $k = l$, odnosno $|a| = |b^{-1}ab|$.

c) Za vježbu. ■

Zadatak 1.6.3. Ako grupa G sadrži točno jedan element reda 2, dokažite da je taj element iz centra grupe G.

Rješenje. Neka je element b jedini element reda 2 grupe G. Iz prethodnog zadatka znamo da je onda $|b| = |g^{-1}bg| = 2$ za sve elemente $g \in G$. Iz jedinstvenosti elementa b slijedi da je $b = g^{-1}bg$ pa, pomnožimo li tu jednakost slijeva s g, dobijemo da je $gb = bg$ za sve elemente $g \in G$, odnosno element b jest iz centra grupe G. ■

Zadatak 1.6.4. Neka su a i b međusobno različiti elementi grupe G koji su različiti od neutralnog elementa, a za koje vrijedi

$$a^3 = b^4 = e \text{ i } ba = ab^3.$$

Odredite red elementa ab.

Rješenje. Pretpostavimo da je $ab = e$, to jest da je element ab reda 1. Pomnožimo li tu jednakost slijeva s b, dobijemo $bab = b$. Kako je $ba = ab^3$, slijedi da je $ab^3b = b$, odnosno $ab^4 = b$. S obzirom da je $b^4 = e$, imamo da je $a = b$, što je kontradikcija s pretpostavkom zadatka. Prema tome, red elementa ab nije 1.

Provjerimo sada je li red elementa ab jednak 2. Imamo $(ab)^2 = abab = aab^3b = a^2b^4 = a^2$. Uvjerimo se najprije da je red elementa a zaista 3. Kako je $a \neq e$, očito red elementa a nije 1. Pretpostavimo da je red elementa a jednak 2. Tada je $a^2 = e$, odnosno $a^3 = a$ pa iz pretpostavke zadatka slijedi da je $e = a$, što znamo da ne vrijedi. Stoga, red je elementa a zaista 3, a onda zaključujemo da red elementa ab nije jednak 2.

Kako je $(ab)^3 = (ab)^2ab = a^2ab = a^3b = b \neq e$, slijedi da red elementa ab nije 3, a iz $(ab)^4 = (ab)^3ab = bab = ab^3b = ab^4 = a \neq e$ zaključujemo da red elementa ab nije niti 4. Provjerimo je li $|ab| = 5$. Imamo $(ab)^5 = (ab)^4ab = aab = a^2b$. Pretpostavimo da je $a^2b = e$. Pomnožimo li tu jednakost slijeva s a, imamo $a^3b = a$, odnosno $b = a$, čime smo došli do kontradikcije pa zaključujemo da red elementa ab nije 5.

Konačno, kako je $(ab)^6 = (ab)^5ab = a^2bab = a^2ab^3b = a^3b^4 = e$, slijedi da je $|ab| = 6$. ■

Zadatak 1.6.5. Pretpostavimo da grupa G sadrži elemente a i b takve da je $|a| = 4$, $|b| = 2$ te $a^3b = ba$. Odredite red elementa ab. □

Zadatak 1.6.6. Neka je G grupa reda 155 te neka su a i b elementi grupe G različitog reda i različiti od neutralnog elementa. Dokažite da ne postoji prava podgrupa od G koja sadrži elemente a i b.

Rješenje. Neka je H podgrupa od G koja sadrži elemente a i b. Prema Lagrangeovom je teoremu tada $|H| \in \{5, 31, 155\}$. Ako je $|H| = 5$, svi su elementi različiti od neutralnog elementa reda 5, čime smo došli do kontradikcije. Slično je ako je $|H| = 31$. Prema tome, $|H| = 155$, odnosno $H = G$. Dakle, ne postoji prava podgrupa od G koja sadrži elemente a i b. ■

Napomena 1.6.10. Red permutacije $\sigma \in S_n$ red je elementa grupe S_n, odnosno najmanji prirodan broj k takav da je $\sigma^k = e$. Zapišemo li permutaciju σ kao produkt disjunktnih ciklusa, za računanje reda dane permutacije koristimo napomenu 1.4.9.

Zadatak 1.6.7. Dan je homomorfizam $\varphi\colon \mathbb{Z}_{24} \to S_8$ takav da je

$$\varphi(1) = (2,5)(1,4,6,7).$$

Odredite $\varphi(14)$ i jezgru homomorfizma φ.

Rješenje. Kako je

$$\varphi(k) = \varphi(1)\varphi(1)\cdots\varphi(1) = \varphi(1)^k = (2,5)^k(1,4,6,7)^k,$$

slijedi da je $\varphi(14) = (2,5)^{14}(1,4,6,7)^{14}$. S obzirom da je $|(2,5)| = 2$, očito je $(2,5)^{14} = \mathrm{id}$, a kako je $|(1,4,6,7)| = 4$, zaključujemo da je $(1,4,6,7)^{14} = (1,4,6,7)^2$. Sada imamo

$$\varphi(14) = (1,4,6,7)^2 = (1,6)(4,7).$$

Nadalje, red permutacije $(2,5)(1,4,6,7)$ jest 4 jer je to najmanji zajednički višekratnik od 2 i 4. Dakle, da bi $\varphi(k) = (2,5)^k(1,4,6,7)^k$ bilo identiteta u S_8, k očito mora biti višekratnik od 4, pa je $\operatorname{Ker}\varphi = \{0, 4, 8, 12, 16, 20\}$. ■

Primjer 1.6.2. Odredimo generatore grupe $\mathbb{Z}_6$:

$\langle 0\rangle = \{0\}$
$\langle 1\rangle = \{1,2,3,4,5,0\} = \mathbb{Z}_6 \Rightarrow 1$ jest generator grupe $\mathbb{Z}_6$
$\langle 2\rangle = \{2,4,0\} \Rightarrow 2$ nije generator grupe $\mathbb{Z}_6$
$\langle 3\rangle = \{3,0\} \Rightarrow 3$ nije generator grupe $\mathbb{Z}_6$
$\langle 4\rangle = \{4,2,0\} \Rightarrow 4$ nije generator grupe $\mathbb{Z}_6$
$\langle 5\rangle = \{5,4,3,2,1,0\} = \mathbb{Z}_6 \Rightarrow 5$ jest generator grupe $\mathbb{Z}_6$.

Napomena 1.6.11. Grupa $\mathbb{Z}_m$ za $m \geq 1$ ciklička je grupa i cijeli je broj k generator grupe $\mathbb{Z}_m$ ako i samo ako su k i m relativno prosti.

Primjer 1.6.3. Grupa $(A, \cdot_8)$, gdje je $A = \{1,3,5,7\}$, nije ciklička grupa jer je generirana elementima 3 i 5, to jest $A = \langle 3,5\rangle$. Uvjerite se da je $(A, \cdot_8)$ zaista grupa.

Primjer 1.6.4. Grupa $\mathbb{Z}$ ciklička je grupa. Elementi 1 i -1 generatori su te grupe, odnosno

$$\mathbb{Z} = \langle 1\rangle \text{ i } \mathbb{Z} = \langle -1\rangle.$$

Napomena 1.6.12. U grupi $\langle a\rangle = \{e, a, a^2, \ldots, a^{m-1}\}$ jest a^k generator grupe ako i samo ako su k i m relativno prosti.

Propozicija 1.6.13. *Neka je G ciklička grupa.*

a) Svaka je podgrupa od G ciklička.

b) Kvocijentna grupa G/H ciklička je za svaku podgrupu H od G.

Zadatak 1.6.8. Nađite sve podgrupe od $\mathbb{Z}_6$.

Rješenje. Grupa $\mathbb{Z}_6$ ciklička je pa su prema propoziciji 1.6.13 sve njezine podgrupe cikličke grupe. One su generirane elementima iz $\mathbb{Z}_6$ i, koristeći propoziciju 1.6.4 te napomenu 1.6.11, vidimo da su podgrupe od $\mathbb{Z}_6$ sljedeće grupe: trivijalne podgrupe $\langle 0\rangle$ i $\mathbb{Z}_6$, $\langle 3\rangle = \{3, 0\} \cong \mathbb{Z}_2$ i $\langle 2\rangle = \langle 4\rangle = \{2, 4, 0\} \cong \mathbb{Z}_3$. ■

Primjer 1.6.5. Grupa $\mathbb{Z} \times \mathbb{Z}$ nije ciklička.

Napomena 1.6.14. Neka je G ciklička grupa reda m, a H ciklička grupa reda n, gdje su m i n relativno prosti prirodni brojevi. Tada je grupa $G \times H$ ciklička.

Primjer 1.6.6. Skup $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(a, b)\colon a \in \mathbb{Z}_2, b \in \mathbb{Z}_3\}$ grupa je uz operaciju

$$(a_1, b_1) + (a_2, b_2) = (a_1 +_2 a_2, b_1 +_3 b_2) \text{ za sve } (a_1, b_1), (a_2, b_2) \in \mathbb{Z}_2 \times \mathbb{Z}_3$$

koja je ciklička jer je $(|\mathbb{Z}_2|, |\mathbb{Z}_3|) = (2, 3) = 1$.

Primjer 1.6.7. Grupa $\mathbb{Z}_2 \times \mathbb{Z}_2$ nije ciklička grupa. Odredite najmanji skup koji ju generira.

Zadatak 1.6.9. Dokažite da grupa $(\mathbb{Q}, +)$ nije ciklička grupa.

Rješenje. Pretpostavimo suprotno, to jest pretpostavimo da postoje relativno prosti $m \in \mathbb{Z}$ i $n \in \mathbb{N}$ takvi da je $\mathbb{Q} = \langle \frac{m}{n}\rangle$. Tada za svaki element $q \in \mathbb{Q}$ postoji $k \in \mathbb{Z}$ takav da je

$$q = k \cdot \tfrac{m}{n}.$$

Uzmemo li, primjerice, $q = \frac{1}{2n}$, onda je $\frac{1}{2n} = k \cdot \frac{m}{n}$, odnosno $2km = 1$ i došli smo do kontradikcije jer su k i m cijeli brojevi. Prema tome, grupa $\mathbb{Q}$ nije ciklička grupa. ■

Zadatak 1.6.10. Neka je N normalna podgrupa od G takva da je kvocijentna grupa G/N reda n. Dokažite da vrijedi sljedeće:

a) $a^n \in N$ za sve $a \in G$.

b) Ako je $a \in G$ i $a^k \in N$ za $k \in \mathbb{N}$ relativno prost s n, onda je $a \in N$.

Rješenje.

a) Kvocijentna grupa G/N reda je n, pa za svaki $a \in G$ vrijedi $(aN)^n = N$, odnosno $a^n N = N$, iz čega zaključujemo da je $a^n \in N$.

b) Kako je $(k, n) = 1$, postoje cijeli brojevi x, y takvi da je $kx + ny = 1$. Stoga je

$$a = a^{kx+ny} = (a^k)^x \cdot (a^n)^y \in N$$

jer je $a^k \in N$ prema pretpostavci zadatka, a $a^n \in N$ prema a) dijelu zadatka. ■

Zadatak 1.6.11. Ako je $G/Z(G)$ ciklička grupa, dokažite da je tada G Abelova grupa.

Rješenje. Kako je grupa $G/Z(G)$ ciklička, postoji generator $gZ(G)$, $g \in G$, od $G/Z(G)$. Neka su a i b proizvoljni elementi iz G. Tada je $aZ(G) = (gZ(G))^n = g^nZ(G)$ za neki $n \in \mathbb{Z}$ i $bZ(G) = (gZ(G))^m = g^mZ(G)$ za neki $m \in \mathbb{Z}$.

Nadalje, $aZ(G) = g^nZ(G)$ implicira da postoji element $z_1 \in Z(G)$ takav da je $a = g^nz_1$, a $bZ(G) = g^mZ(G)$ implicira da postoji element $z_2 \in Z(G)$ takav da je $b = g^mz_2$. S obzirom da elementi iz centra grupe G komutiraju sa svim elementima grupe G, imamo

$$ab = (g^nz_1)(g^mz_2) = g^ng^mz_1z_2 = g^{n+m}z_1z_2 = g^{m+n}z_2z_1 = g^mg^nz_2z_1 = g^mz_2g^nz_1 = ba.$$

Kako su elementi a i b grupe G bili proizvoljni, pokazali smo da je grupa G Abelova. ■

Napomena 1.6.15. Svaki homomorfizam $\varphi\colon G \to H$, gdje je G ciklička grupa, potpuno je određen djelovanjem na generatoru grupe G.

Promatrajmo sada homomorfizme grupa $\varphi\colon \mathbb{Z}_n \to \mathbb{Z}_m$. Kako je element 1 generator grupe $\mathbb{Z}_n$, prema napomeni 1.6.15 svaki je takav homomorfizam potpuno određen s $\varphi(1)$ i to mora biti neki element $k \in \mathbb{Z}_m$. Može se pokazati da će onda formula $\varphi(x) = kx$ za sve $x \in \mathbb{Z}_n$ definirati homomorfizam grupa ako i samo ako $m \mid kn$.

Posebno, taj će homomorfizam grupa biti izomorfizam grupa ako i samo ako je k generator od $\mathbb{Z}_m$.

Zadatak 1.6.12. Nađite sve homomorfizme grupe $\mathbb{Z}_3$ u grupu $\mathbb{Z}_6$.

Rješenje. Neka je $\varphi\colon \mathbb{Z}_3 \to \mathbb{Z}_6$ homomorfizam grupa. S

$$\varphi(x) = kx \in \mathbb{Z}_6, \;\; k \in \{0, 1, \ldots, 5\},$$

zadan je homomorfizam grupa ako i samo ako $6 \mid k \cdot 3$. Provjerimo redom.

Za $k = 0$ očito $6 \mid 0{\cdot}3$, pa imamo homomorfizam $\varphi_1(x) = 0$ i on je trivijalni homomorfizam. Kada je $k = 1$, $k = 3$ i $k = 5$, očito 6 ne dijeli $3k$ pa u tim slučajevima nemamo homomorfizam. Za $k = 2$ imamo homomorfizam $\varphi_2(x) = 2x$, odnosno $\varphi_2(1) = 2$, $\varphi_2(2) = 4$ i $\varphi_2(0) = 0$ te za $k = 4$ imamo homomorfizam $\varphi_3(x) = 4x$, odnosno $\varphi_3(1) = 4$, $\varphi_3(2) = 2$ i $\varphi_3(0) = 0$. ■

Zadatak 1.6.13. Nađite sve homomorfizme grupe $\mathbb{Z}_3$ u grupu $\mathbb{Z}_2$. □

Zadatak 1.6.14. Odredite $\mathrm{Aut}(\mathbb{Z}_6)$.

Rješenje. Neka je $\varphi\colon \mathbb{Z}_6 \to \mathbb{Z}_6$ homomorfizam grupa. S

$$\varphi(x) = kx \in \mathbb{Z}_6, \;\; k \in \{0, 1, \ldots, 5\},$$

zadan je homomorfizam grupa ako i samo ako $6 \mid k \cdot 6$ i on je izomorfizam grupa ako i samo ako je k generator grupe $\mathbb{Z}_6$, odnosno ako i samo ako je $(k, 6) = 1$. Prema tome, k može biti jednak 1 i 5.

Za $k = 1$ je $\varphi_1(x) = x$, pa se svi elementi grupe $\mathbb{Z}_6$ preslikaju u sebe, odnosno φ_1 jest identiteta preslikavanje. Kada je $k = 5$, $\varphi_2(x) = 5x$, odnosno $\varphi_2(1) = 5$, $\varphi_2(2) = 4$, $\varphi_2(3) = 3$, $\varphi_2(4) = 2$, $\varphi_2(5) = 1$ i $\varphi_2(0) = 0$. ■

Propozicija 1.6.16. *Neka je $\varphi\colon G_1 \to G_2$ izomorfizam grupa.*

a) Za sve elemente a grupe G_1 jest $|a| = |\varphi(a)|$.

b) Ako je grupa G_1 Abelova, onda je i grupa G_2 Abelova.

c) Ako je grupa G_1 ciklička, onda je i grupa G_2 ciklička.

d) Ako je grupa G_1 konačna, onda G_1 i G_2 imaju jednak broj elemenata svakog reda.

Zadatak 1.6.15. Pokažite da je grupa $(\mathbb{Z}_4, +_4)$ izomorfna grupi $(\mathbb{Z}_5^*, \cdot_5)$.

Rješenje. Neka je $\varphi\colon \mathbb{Z}_4 \to \mathbb{Z}_5^*$ homomorfizam grupa. Pogledajmo redove elemenata u danim grupama (naravno, gledamo sve elemente različite od neutralnog elementa). U grupi $\mathbb{Z}_4$ jest $|1| = 4$, $|2| = 2$ i $|3| = 4$, a u grupi $\mathbb{Z}_5^*$ jest $|2| = 4$, $|3| = 4$ i $|4| = 2$.

Kako je φ homomorfizam grupa, znamo da preslikava neutralni element grupe $\mathbb{Z}_4$ u neutralni element grupe $\mathbb{Z}_5^*$, pa je prema tome $\varphi(0) = 1$. Nadalje, stavimo li da je $\varphi(1) = 2$, odnosno da se generator grupe $\mathbb{Z}_4$ preslikao u generator grupe $\mathbb{Z}_5^*$, u grupi $\mathbb{Z}_4$ ostao nam je još jedan element reda 4 i jedan element reda 2, kao i u grupi $\mathbb{Z}_5^*$. Kako izomorfizam čuva red elementa, jasno je da je onda $\varphi(2) = 4$ i $\varphi(3) = 3$.

Uočimo da je homomorfizam s cikličke grupe potpuno određen svojim djelovanjem na generatoru te grupe, pa smo, nakon što smo stavili da je $\varphi(1) = 2$, mogli direktno pokazati da je tada

$$\varphi(2) = \varphi(1 +_4 1) = \varphi(1) \cdot_5 \varphi(1) = 2 \cdot_5 2 = 4$$

i

$$\varphi(3) = \varphi(2 +_4 1) = \varphi(2) \cdot_5 \varphi(1) = 4 \cdot_5 2 = 3.$$

Sada lako vidimo da su grupe $(\mathbb{Z}_4, +_4)$ i $(\mathbb{Z}_5^*, \cdot_5)$ međusobno izomorfne. ■

Zadatak 1.6.16. Pokažite da grupa $(K_4, \cdot)$ nije izomorfna grupi $(A, \cdot_8)$, za $A = \{1, 3, 5, 7\}$.

Rješenje. Pogledajmo redove elemenata u danim grupama. U grupi K_4 jest $|-1| = 2$, $|i| = 4$ i $|-i| = 4$, a u grupi A jest $|3| = 2$, $|5| = 2$ i $|7| = 2$. S obzirom da izomorfizam čuva red elementa, a u grupi K_4 imamo neutralni element, dva elementa reda 4 i jedan element reda 2, dok u grupi A imamo neutralni element i tri elementa reda 2, zaključujemo da ne postoji izomorfizam između grupe K_4 i grupe A.

Posebno, kako je svaka grupa reda 4 izomorfna ili grupi $\mathbb{Z}_4$ ili grupi $\mathbb{Z}_2 \times \mathbb{Z}_2$, pogledamo li redove elemenata u danim grupama, lako vidimo da je grupa K_4 izomorfna grupi $\mathbb{Z}_4$ jer ima neutralni element, dva elementa reda 4 i jedan element reda 2, dok je grupa A izomorfna grupi $\mathbb{Z}_2 \times \mathbb{Z}_2$ jer su svi elementi, različiti od neutralnog elementa, reda 2. Također, grupe K_4 i $\mathbb{Z}_4$ cikličke su, a grupe A i $\mathbb{Z}_2 \times \mathbb{Z}_2$ nisu cikličke grupe. ■

Propozicija 1.6.17. *Cikličke su grupe istog reda međusobno izomorfne.*

Zadatak 1.6.17. Neka je G grupa i neka je indeks od $Z(G)$ u G jednak 4. Dokažite da je tada grupa $G/Z(G)$ izomorfna grupi $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Rješenje. Iz pretpostavke zadatka znamo da je

$$[G\colon Z(G)] = |G/Z(G)| = 4,$$

odnosno kvocijentna je grupa $G/Z(G)$ reda 4, pa je ona izomorfna ili grupi $\mathbb{Z}_4$ ili grupi $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Ako je grupa $G/Z(G)$ ciklička, onda je grupa G Abelova, pa je $G = Z(G)$ i $|G/Z(G)| = 1$, čime smo došli do kontradikcije. Dakle, grupa $G/Z(G)$ nije ciklička. S obzirom da je grupa $\mathbb{Z}_4$ ciklička, a grupa $\mathbb{Z}_2 \times \mathbb{Z}_2$ nije ciklička, zaključujemo da je grupa $G/Z(G)$ izomorfna grupi $\mathbb{Z}_2 \times \mathbb{Z}_2$. ■

Zadatak 1.6.18. Dokažite da nekomutativna grupa G reda pq, gdje su p i q prosti brojevi, ima trivijalan centar. □

Zadatak 1.6.19. Dokažite da grupa $\mathbb{R}^* \times \mathbb{R}^* = \{(a, b)\colon a, b \in \mathbb{R}^*\}$ uz množenje po komponentama nije izomorfna multiplikativnoj grupi $\mathbb{C}^*$.

Rješenje. Pretpostavimo da je $\varphi\colon \mathbb{C}^* \to \mathbb{R}^* \times \mathbb{R}^*$ izomorfizam grupa. Tada φ preslikava neutralni element grupe $\mathbb{C}^*$ u neutralni element grupe $\mathbb{R}^* \times \mathbb{R}^*$, to jest

$$\varphi(1) = (1, 1).$$

Kako je element $i \in \mathbb{C}^*$ reda 4, element $\varphi(i) = (a, b) \in \mathbb{R}^* \times \mathbb{R}^*$ također mora biti reda 4, odnosno $(a, b)^4 = (a^4, b^4) = (1, 1)$. Tada su očito $a, b \in \{1, -1\}$, pa je $(a, b)^2 = (1, 1)$ iz čega slijedi da je element (a, b) reda 1 ili 2, čime smo došli do kontradikcije. Prema tome, ne postoji izomorfizam između grupa $\mathbb{C}^*$ i $\mathbb{R}^* \times \mathbb{R}^*$. Drugim riječima, grupe $\mathbb{C}^*$ i $\mathbb{R}^* \times \mathbb{R}^*$ nisu međusobno izomorfne. ■

1.7 Sylowljevi teoremi

Definicija 1.7.1. Neka je G konačna grupa i neka je p prost broj. Za grupu G kažemo da je $p-$grupa ako je $|G| = p^n$ za neki prirodan broj n. Kažemo da je podgrupa H grupe G $p-$podgrupa od G ako je H $p-$grupa.

Definicija 1.7.2. Podgrupa od G reda p^k za p prost broj, gdje je p^k najveća potencija od p koja dijeli red grupe G, naziva se Sylowljeva $p-$podgrupa od G.

Teorem 1.7.3. *(Cauchy) Neka je G konačna grupa i neka je p prost broj koji dijeli red grupe G. Tada grupa G sadrži podgrupu reda p. Drugim riječima, grupa G sadrži element reda p.*

Teorem 1.7.4. *(Prvi Sylowljev teorem) Neka je G konačna grupa reda $p^n m$, gdje je $n \geq 1$, p prost broj i $(p, m) = 1$. Tada grupa G sadrži podgrupu reda p^i za svaki $1 \leq i \leq n$ i svaka podgrupa od G reda p^i, $i < n$, normalna je u nekoj podgrupi reda p^{i+1}. Posebno, postoji Sylowljeva $p-$podgrupa grupe G.*

Primjer 1.7.1. Grupa $\mathbb{Z}_{12}$ jest reda $12 = 2^2 \cdot 3$, pa Prvi Sylowljev teorem kaže da grupa $\mathbb{Z}_{12}$ mora imati barem jednu podgrupu svakog od sljedećih redova: 2, 4 i 3. Uočimo da Prvi Sylowljev teorem ne govori ništa o postojanju podgrupe reda 6. Nadalje, svaka je podgrupa reda 4 Sylowljeva 2−podgrupa od $\mathbb{Z}_{12}$, a svaka je podgrupa reda 3 Sylowljeva 3−podgrupa od $\mathbb{Z}_{12}$.

Primjer 1.7.2. Grupa $\mathbb{Z}_{18}$ jest reda $18 = 2 \cdot 3^2$. Prvi Sylowljev teorem kaže da grupa $\mathbb{Z}_{18}$ mora imati barem jednu podgrupu svakog od sljedećih redova: 2, 3 i 9. Svaka je podgrupa reda 2 Sylowljeva 2−podgrupa od $\mathbb{Z}_{18}$, a svaka je podgrupa reda 9 Sylowljeva 3−podgrupa od $\mathbb{Z}_{18}$.

Primjer 1.7.3. Pogledajmo podgrupe grupe K_4. Kako je $|K_4| = 4 = 2^2$, prema Lagrangeovom je teoremu $|H| \in \{1, 2, 4\}$. Prvi Sylowljev teorem kaže da grupa K_4 sadrži podgrupe reda 2^i, gdje je $1 \leq i \leq 2$. Dakle, imamo podgrupu $H_1 = \{1\}$ reda 1, 2−podgrupu $H_2 = \{1, -1\}$ reda 2 i Sylowljevu 2−podgrupu $H_3 = K_4$ reda 2^2.

Teorem 1.7.5. *(Drugi Sylowljev teorem) Neka je G konačna grupa i neka je p prost broj koji dijeli red grupe G.*

a) Svaka p−podgrupa grupe G sadržana je u nekoj Sylowljevoj p−podgrupi grupe G.

b) Sve Sylowljeve p−podgrupe grupe G konjugirane su, to jest ako su H i K Sylowljeve p−podgrupe grupe G, onda postoji $a \in G$ takav da je $K = aHa^{-1}$.

Teorem 1.7.6. *(Treći Sylowljev teorem) Neka je G konačna grupa i neka je p prost broj koji dijeli red grupe G. Broj Sylowljevih p−podgrupa od G dijeli red od G i oblika je $kp + 1$ za neki $k \in \mathbb{N}_0$.*

Zadatak 1.7.1. Dokažite da je konačna grupa G p−grupa ako i samo ako je red svakog elementa grupe G potencija broja p.

Rješenje. Neka je G p−grupa, to jest neka postoji $k \in \mathbb{N}$ takav da je $|G| = p^k$. Tada, prema Lagrangeovom teoremu, $|a| = |\langle a \rangle|$ dijeli $|G| = p^k$, pa slijedi da je $|a| = p^l$ za $l \leq k$ za sve $a \in G$ i time smo pokazali nužnost.

Pokažimo sada dovoljnost. Neka je red svakog elementa grupe G potencija broja p i pretpostavimo da grupa G nije p−grupa, to jest pretpostavimo da postoji prost broj $q \neq p$ takav da $q \mid |G|$. Tada, prema Cauchyjevom teoremu, G sadrži element reda q, čime smo došli do kontradikcije, odnosno grupa G jest p−grupa. ■

Zadatak 1.7.2. Neka je N normalna podgrupa od G. Ako su grupe N i G/N p−grupe, dokažite da je tada i G p−grupa.

Rješenje. Kako je N p−grupa, postoji $j \in \mathbb{N}$ takav da je $|x| = p^j$ za $x \in N$, a kako je G/N p−grupa, postoji $k \in \mathbb{N}$ takav da je $|yN| = p^k$ za $yN \in G/N$. Uzmimo proizvoljni $g \in G$. Tada je $(gN)^{p^k} = N$, odnosno $g^{p^k}N = N$, pa vidimo da je $g^{p^k} \in N$. Tada je $(g^{p^k})^{p^j} = e$, odnosno $g^{p^{k+j}} = e$, pa slijedi da $|g| \mid p^{k+j}$. Dakle, postoji $i \in \mathbb{N}$ takav da je $|g| = p^i$ i time smo pokazali da je red svakog elementa grupe G potencija broja p, pa, prema prethodnom zadatku, slijedi da je G p−grupa. ■

Zadatak 1.7.3. Dokažite da ako grupa G ima samo jednu Sylowljevu p−podgrupu H, onda je H normalna podgrupa od G.

Rješenje. Ako je H Sylowljeva p−podgrupa od G, prema Drugom Sylowljevom teoremu slijedi da su sve ostale Sylowljeve podgrupe oblika aHa^{-1} za $a \in G$. Međutim, kako je H jedinstvena, slijedi $aHa^{-1} = H$, odnosno $aH = Ha$ za sve $a \in G$. Dakle, H je normalna podgrupa od G. ■

Zadatak 1.7.4. Dokažite da je svaka podgrupa reda 17 u grupi reda 255 normalna podgrupa.

Rješenje. Prema Trećem Sylowljevom teoremu znamo da je broj Sylowljevih 17−podgrupa oblika $17k+1$ i da

$$17k+1 \mid 255.$$

Kako $17k+1$ za $k>0$ ne dijeli $255 = 3\cdot 5\cdot 17$, slijedi da je $k=0$, odnosno postoji samo jedna Sylowljeva 17−podgrupa, pa je, prema zadatku 1.7.3, ona normalna podgrupa. ■

Zadatak 1.7.5. Ako grupa G reda 56 nema normalnu podgrupu reda 7, odredite koliko je elemenata u grupi G neparnog, a koliko parnog reda.

Rješenje. Neka je G grupa reda 56. Broj je Sylowljevih 7−podgrupa od G oblika $7k+1$ i

$$7k+1 \mid 56.$$

S obzirom da grupa G nema normalnu podgrupu reda 7, slijedi da je $7k+1>1$, odnosno zaključujemo da je $k=1$. Prema tome, grupa G ima osam Sylowljevih 7−podgrupa koje su sve reda 7 i u presjeku svih tih podgrupa nalazi se samo neutralni element. Svi elementi tih podgrupa su, prema Lagrangeovom teoremu, neparnog reda.

Prema tome, imamo $8\cdot 6+1=49$ elemenata neparnog reda. Nadalje, preostali elementi tvore Sylowljevu 2−podgrupu koja je reda 8, odnosno imamo 7 elemenata parnog reda. ■

Definicija 1.7.7. Kažemo da je grupa G prosta ako su jedine njene normalne podgrupe $\{e\}$ i G, odnosno ako G nema netrivijalnih normalnih podgrupa.

Zadatak 1.7.6. Pokažite da grupa reda 12 nije prosta.

Rješenje. Neka je G grupa reda 12. Broj je Sylowljevih 3−podgrupa od G oblika $3k+1$ i

$$3k+1 \mid 12,$$

a to vrijedi za $k=0$ i $k=1$.

Ako je $k=0$, postoji jedinstvena Sylowljeva 3−podgrupa pa je ona normalna.

Pretpostavimo da je $k\neq 0$. Tada imamo četiri Sylowljeve 3−podgrupe koje su sve reda 3, odnosno imamo $4\cdot 2=8$ elemenata reda 3. Preostala 4 elementa tvore grupu reda 4 i to je jedinstvena Sylowljeva 2−podgrupa. Prema zadatku 1.7.3 ona jest normalna podgrupa od G jer je jedinstvena.

Dakle, grupa reda 12 nije prosta. ■

Zadatak 1.7.7. Pokažite da grupa reda 30 nije prosta.

Rješenje. Neka je G grupa reda 30. Broj je Sylowljevih 3−podgrupa od G oblika $3k+1$ i

$$3k+1 \mid 30,$$

što vrijedi za $k=0$ i $k=3$, odnosno imamo jednu ili deset Sylowljevih 3−podgrupa. Dok je broj Sylowljevih 5−podgrupa od G oblika $5k+1$ i

$$5k+1 \mid 30,$$

što vrijedi za $k = 0$ i $k = 1$, odnosno imamo jednu ili šest Sylowljevih 5−podgrupa.

Prema tome, deset Sylowljevih 3−podgrupa daje nam 20 elemenata reda 3, a šest Sylowljevih 5−podgrupa daje nam 24 elementa reda 5, no tada imamo više elemenata negoli je moguće. Dakle, mora postojati ili jedna Sylowljeva 3−podgrupa ili jedna Sylowljeva 5−podgrupa, pa postoji netrivijalna normalna podgrupa, odnosno grupa G nije prosta. ■

Zadatak 1.7.8. Dokažite ili opovrgnite:

(a) Svaka grupa reda 45 ima normalnu podgrupu reda 9.

(b) Grupa reda 40 nema normalnu podgrupu reda 5. □

2

Prsteni

"My [algebraic] methods are really methods of working and thinking; this is why they have crept in everywhere anonymously."
- Emmy Noether

2.1 Definicija i osnovni primjeri

Definicija 2.1.1. Prsten je neprazan skup R na kome su zadane binarne operacije zbrajanja $(a, b) \mapsto a + b$ i množenja $(a, b) \mapsto ab$ za koje vrijedi:

a) Uz zbrajanje je R Abelova grupa. Neutralni element označava se s 0 i zove nula.

b) Uz množenje je R polugrupa.

c) Množenje je i slijeva i zdesna distributivno u odnosu na zbrajanje, to jest za sve a, b, c u R vrijedi
$$a(b + c) = ab + ac \text{ i } (a + b)c = ac + bc.$$

Ako je množenje u prstenu R komutativno, kažemo da je R komutativan prsten.

Kažemo da je R unitalan prsten ili prsten s jedinicom ako je R uz množenje monoid, to jest postoji jedinstveni element $1 \in R$ takav da je $a1 = 1a = a$ za sve $a \in R$ i takav se element

naziva jedinica prstena R. U unitalnom prstenu R jest $1 = 0$ ako i samo ako je R trivijalan prsten, odnosno $R = \{0\}$. U netrivijalnom je unitalnom prstenu $1 \neq 0$.

Propozicija 2.1.2. *Neka su a, b i c elementi prstena R. Vrijedi:*

a) $a0 = 0a = 0$,

b) $a(-b) = (-a)b = -(ab)$,

c) $(-a)(-b) = ab$,

d) $a(b-c) = ab - ac$ *i* $(a-b)c = ac - bc$,

e) ako je R prsten s jedinicom 1, *onda je* $(-1)a = -a$.

Definicija 2.1.3. Neka je R komutativan netrivijalan unitalni prsten. Element $a \in R\backslash\{0\}$, takav da postoji element $b \in R\backslash\{0\}$ sa svojstvom da je $ab = 0$, naziva se djelitelj nule.

Definicija 2.1.4. Komutativan netrivijalan unitalni prsten u kojem nema djelitelja nule naziva se integralna domena.

Primjer 2.1.1. Znamo da je $(\mathbb{Z}, +)$ Abelova grupa te da vrijedi asocijativnost i komutativnost množenja u $\mathbb{Z}$. Također, za sve cijele brojeve vrijedi distributivnost množenja prema zbrajanju. Prema tome, skup $\mathbb{Z}$ jest, uz zbrajanje i množenje, komutativan prsten. Štoviše, postoji neutralni element za množenje, pa je $\mathbb{Z}$ komutativan prsten s jedinicom. Nadalje, u $\mathbb{Z}$ ne postoji djelitelj nule jer kada god je $ab = 0$, slijedi da je $a = 0$ ili $b = 0$, pa je $\mathbb{Z}$ integralna domena.

Primjer 2.1.2. Skup $\mathbb{Z}_m$, uz zbrajanje i množenje modulo m, komutativan je prsten s jedinicom. Kako je $a \cdot_m b = 0$ ako i samo ako je $a \cdot b = k \cdot m$ za neki cijeli broj k i $a, b \in \mathbb{Z}_m$, imamo dva slučaja:

1) Ako je m prost broj, onda $m \mid a$ ili $m \mid b$. No, elementi su a i b iz prstena $\mathbb{Z}_m$, pa je tada $a = 0$ ili $b = 0$, odnosno $\mathbb{Z}_m$ jest integralna domena.

2) Ako je m složen broj, onda je $m = m_1 \cdot m_2$, za $m_1, m_2 \in \mathbb{Z}_m\backslash\{0\}$, pa je $m_1 \cdot_m m_2 = 0$. Prema tome, $\mathbb{Z}_m$ nije integralna domena.

Primjer 2.1.3. Skupovi $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ jesu prsteni.

Primjer 2.1.4. Neka je R prsten. Tada je

$$R[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \colon a_0, a_1, \ldots, a_n \in R,\ n \in \mathbb{N}_0\}$$

prsten uz standardno zbrajanje polinoma i standardno množenje polinoma definirano za f, g iz $R[x]$, $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$ na sljedeći način:

$$(f \cdot g)(x) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k,$$

kojeg zovemo prsten polinoma u jednoj varijabli s koeficijentima iz prstena R.

Ako je R komutativan prsten, onda je i $R[x]$ komutativan prsten, a ako je R netrivijalan unitalni prsten, onda je i $R[x]$ netrivijalan unitalni prsten.

Primjer 2.1.5. Neka su $f, g \in \mathbb{Z}_6[x]$ polinomi definirani s $f(x) = 2 + 4x + 3x^2$ i $g(x) = 2x$. Tada je

$$(f+g)(x) = 2 + 6x + 3x^2 = 2 + 3x^2,$$
$$(f \cdot g)(x) = 4x + 8x^2 + 6x^3 = 4x + 2x^2.$$

Primjer 2.1.6. Skup $2\mathbb{Z}$ komutativan je prsten uz standardno zbrajanje i množenje, ali nije prsten s jedinicom jer $1 \notin 2\mathbb{Z}$. Postoje li u $2\mathbb{Z}$ djelitelji nule?

Primjer 2.1.7. Skup $M(n, R)$ svih matrica $n-$tog reda s koeficijentima iz prstena R tvori prsten uz standardno zbrajanje i množenje matrica kojemu je jedinična matrica I_n jedinica.

Zadatak 2.1.1. Pokažite da je $\mathbb{Z}$, uz operacije zbrajanja i množenja definirane s

$$a \oplus b = a + b + 1 \text{ i } a \odot b = a + b + ab,$$

komutativan prsten. Ukoliko postoji, odredite jedinicu prstena i provjerite postoje li u prstenu $(\mathbb{Z}, \oplus, \odot)$ djelitelji nule te ispitajte ima li svaki element prstena $(\mathbb{Z}, \oplus, \odot)$ multiplikativan inverz.

Rješenje.

- zatvorenost s obzirom na obje operacije vrijedi zbog zatvorenosti zbrajanja i množenja cijelih brojeva
- kako je $(a \oplus b) \oplus c = (a + b + 1) \oplus c = a + b + 1 + c + 1 = a + b + c + 2$ jednako $a \oplus (b \oplus c) = a \oplus (b + c + 1) = a + b + c + 1 + 1 = a + b + c + 2$, zaključujemo da vrijedi asocijativnost zbrajanja
- komutativnost vrijedi za zbrajanje jer je $a \oplus b = a + b + 1 = b + a + 1 = b \oplus a$, kao i za množenje jer je $a \odot b = a + b + ab = b + a + ba = b \odot a$
- iz $a = a \oplus e = a + e + 1$ slijedi da je $e = -1$ desni neutralni element, pa, s obzirom da vrijedi komutativnost zbrajanja, imamo $a = a \oplus e = e \oplus a$ te zaključujemo da je $e = -1 \in \mathbb{Z}$ neutralni element
- iz $-1 = a \oplus b = a + b + 1$ zaključujemo da je $b = -a - 2$ desni inverzni element od a, pa, jer vrijedi komutativnost zbrajanja, imamo $e = a \oplus b = b \oplus a$ te zaključujemo da je $b = -a - 2 \in \mathbb{Z}$ inverzni element od $a \in \mathbb{Z}$
- kako je $(a \odot b) \odot c = (a + b + ab) \odot c = a + b + ab + c + ac + bc + abc$ jednako $a \odot (b \odot c) = a \odot (b + c + bc) = a + b + c + bc + ab + ac + abc$, zaključujemo da vrijedi asocijativnost množenja
- jer je

  $$(a \oplus b) \odot c = (a + b + 1) \odot c = a + b + 1 + c + ac + bc + c = a + b + 2c + ac + bc + 1$$

  jednako

  $$a \odot c \oplus b \odot c = (a + c + ac) \oplus (b + c + bc) = a + c + ac + b + c + bc + 1 = a + b + 2c + ac + bc + 1,$$

zaključujemo da vrijedi distributivnost zdesna, pa, s obzirom da vrijedi komutativnost množenja, vrijedi i distributivnost slijeva

Dakle, $\mathbb{Z}$ je uz zbrajanje Abelova grupa, uz množenje komutativna polugrupa i vrijedi distributivnost slijeva i zdesna, odnosno $(\mathbb{Z}, \oplus, \odot)$ jest komutativan prsten.

Da bi element $e \in \mathbb{Z}$ bio jedinica prstena, mora vrijediti $a \odot e = a$ za sve $a \in \mathbb{Z}$, odnosno $a + e + ae = a$, pa lako zaključimo da je $e = 0 \in \mathbb{Z}$ jedinica prstena.

Provjerimo postoje li u prstenu $(\mathbb{Z}, \oplus, \odot)$ djelitelji nule. Mora vrijediti $a \odot b = -1$, jer je -1 nula u danom prstenu, za $a \neq -1$ i $b \neq -1$. Tada je $a + b + ab = -1$, odnosno $b = \frac{-1-a}{1+a} = -1$. Prema tome, ne postoje djelitelji nule u danom prstenu.

Da bi element $a \in \mathbb{Z}$ imao multiplikativan inverz, mora vrijediti $a \odot b = 0$ jer je 0 jedinica u danom prstenu, pa lako vidimo da je $b = \frac{-a}{1+a}$ za $a \neq -1$, ali kako je b cijeli broj, očito nema svaki element prstena $(\mathbb{Z}, \oplus, \odot)$ multiplikativan inverz. ■

Zadatak 2.1.2. Neka su operacije $\oplus$ i $\odot$ definirane kao u prethodnom zadatku, a $+$ i $\cdot$ standardne binarne operacije zbrajanja i množenja cijelih brojeva. Provjerite jesu li sljedeće strukture prsteni:

a) $(\mathbb{Z}, \oplus, \cdot)$,

b) $(\mathbb{Z}, +, \odot)$. □

2.2 Potprsteni

Definicija 2.2.1. Potprsten prstena R jest podskup S od R koji je i sam prsten u odnosu na operacije od R.

Teorem 2.2.2. *Neprazan podskup S prstena R jest potprsten prstena R ako za sve $a, b \in S$ vrijedi $a - b \in S$ i $ab \in S$.*

Ako je R netrivijalan prsten s jedinicom 1 i S potprsten od R, onda se S naziva unitalan ako je $1 \in S$.

Primjer 2.2.1. $\{0\}$ i R potprsteni su svakog prstena R.

Primjer 2.2.2. Za svaki $n \in \mathbb{N}$ jest $n\mathbb{Z}$ potprsten od $\mathbb{Z}$.

Zadatak 2.2.1. Pokažite da je skup $S = \{x + y\sqrt[3]{3} + z\sqrt[3]{9} \colon x, y, z \in \mathbb{Q}\}$ prsten uz standardne binarne operacije zbrajanja i množenja realnih brojeva.

Rješenje. Skup S podskup je skupa realnih brojeva i on je neprazan jer je, primjerice, $0 \in S$. Pokažimo da je S potprsten od $\mathbb{R}$. Uzmimo proizvoljne elemente A, B iz S. Tada je $A = x_1 + y_1\sqrt[3]{3} + z_1\sqrt[3]{9}$ i $B = x_2 + y_2\sqrt[3]{3} + z_2\sqrt[3]{9}$, pa je

$$A - B = x_1 - x_2 + (y_1 - y_2)\sqrt[3]{3} + (z_1 - z_2)\sqrt[3]{9} \in S,$$

$$A \cdot B = x_1x_2 + 3y_1z_2 + 3y_2z_1 + (x_1y_2 + x_2y_1 + 3z_1z_2)\sqrt[3]{3} + (x_1z_2 + y_1y_2 + x_2z_1)\sqrt[3]{9} \in S.$$

Dakle, S je potprsten od $\mathbb{R}$, iz čega zaključujemo da je $(S,+,\cdot)$ prsten.

Uočimo da je S komutativan prsten jer je $\mathbb{R}$ komutativan prsten te s obzirom da $\mathbb{R}$ nema djelitelja nule, nema ih niti S. Također, kako je 1 jedinica prstena $\mathbb{R}$ i $1 \in S$, zaključujemo da je S prsten s jedinicom. Prema tome, S je integralna domena. ■

Zadatak 2.2.2. Pokažite da je skup

$$S = \left\{ \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} : z, w \in \mathbb{C} \right\}$$

prsten uz standardne binarne operacije zbrajanja i množenja matrica.

Rješenje. Očito je skup S podskup od $M(2,\mathbb{C})$ i on je neprazan jer je, primjerice, jedinična matrica drugog reda $I \in S$. Uzmimo proizvoljne $A, B \in S$. Tada je

$$A = \begin{bmatrix} z_1 & w_1 \\ -\overline{w_1} & \overline{z_1} \end{bmatrix} \text{ i } B = \begin{bmatrix} z_2 & w_2 \\ -\overline{w_2} & \overline{z_2} \end{bmatrix},$$

pa je

$$A - B = \begin{bmatrix} z_1 - z_2 & w_1 - w_2 \\ -\overline{w_1} - (-\overline{w_2}) & \overline{z_1} - \overline{z_2} \end{bmatrix} = \begin{bmatrix} z_1 - z_2 & w_1 - w_2 \\ -\overline{(w_1 - w_2)} & \overline{z_1 - z_2} \end{bmatrix} \in S$$

te

$$AB = \begin{bmatrix} z_1 z_2 - w_1\overline{w_2} & z_1 w_2 + w_1\overline{z_2} \\ -\overline{w_1} z_2 - \overline{z_1} w_2 & -\overline{w_1} w_2 + \overline{z_1} z_2 \end{bmatrix} = \begin{bmatrix} z_1 z_2 - w_1\overline{w_2} & w_1\overline{z_2} + z_1 w_2 \\ -\overline{(w_1\overline{z_2} + z_1 w_2)} & \overline{z_1 z_2 - w_1\overline{w_2}} \end{bmatrix} \in S.$$

Prema tome, S je potprsten od $M(2,\mathbb{C})$, odnosno $(S,+,\cdot)$ jest prsten. ■

Zadatak 2.2.3. Pokažite da je skup $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ prsten uz standardne binarne operacije zbrajanja i množenja kompleksnih brojeva.

Prsten $\mathbb{Z}[i]$ naziva se prsten Gaussovih cijelih brojeva.

Rješenje. Skup $\mathbb{Z}[i]$ očito je podskup od $\mathbb{C}$ i on je neprazan jer je, primjerice, $0 + 0i \in \mathbb{Z}[i]$. Uzmimo proizvoljne $z_1, z_2 \in \mathbb{Z}[i]$. Tada je $z_1 = a_1 + b_1 i$ i $z_2 = a_2 + b_2 i$, pa je

$$z_1 - z_2 = a_1 - a_2 + (b_1 - b_2)i \in \mathbb{Z}[i],$$

$$z_1 \cdot z_2 = a_1 a_2 - b_1 b_2 + (a_1 b_2 + a_2 b_1)i \in \mathbb{Z}[i].$$

Dakle, $\mathbb{Z}[i]$ potprsten je od $\mathbb{C}$, odnosno $\mathbb{Z}[i]$ jest prsten.

Posebno, uočimo da je $\mathbb{Z}[i]$ komutativan netrivijalan unitalni prsten i da u $\mathbb{Z}[i]$ ne postoje djelitelji nule, pa je $\mathbb{Z}[i]$ integralna domena. ■

Zadatak 2.2.4. Pokažite da skup $S = \{m + n\sqrt{2} + k\sqrt{3} : m, n, k \in \mathbb{Z}\}$ nije prsten uz standardne binarne operacije zbrajanja i množenja realnih brojeva.

Rješenje. Dovoljno je pronaći jedan kontraprimjer. Kako $\sqrt{2} \cdot \sqrt{3}$ nije u S, slijedi da skup S nije prsten. ■

Zadatak 2.2.5. Ispitajte je li $\mathbb{Q}$, uz operacije zbrajanja definiranog s

$$a \oplus b = a + b + 3$$

i standardnog množenja racionalnih brojeva, prsten.

Rješenje.

- ▷ vrijedi zatvorenost zbrajanja zbog zatvorenosti zbrajanja racionalnih brojeva, također očito vrijedi zatvorenost množenja racionalnih brojeva
- ▷ komutativnost vrijedi za zbrajanje jer je $a \oplus b = a + b + 3 = b + a + 3 = b \oplus a$, a očito vrijedi komutativnosti množenja racionalnih brojeva
- ▷ kako je

  $$(a \oplus b) \oplus c = (a + b + 3) \oplus c = a + b + 3 + c + 3 = a + b + c + 6$$

  jednako

  $$a \oplus (b \oplus c) = a \oplus (b + c + 3) = a + b + c + 3 + 3 = a + b + c + 6,$$

  zaključujemo da vrijedi asocijativnost zbrajanja
- ▷ iz $a = a \oplus e = a + e + 3$ slijedi da je $e = -3$ desni neutralni element, pa, s obzirom da vrijedi komutativnost zbrajanja, imamo $a = a \oplus e = e \oplus a$ te zaključujemo da je $e = -3 \in \mathbb{Q}$ nula
- ▷ iz $-3 = a \oplus b = a + b + 3$ zaključujemo da je $b = -a - 6$ desni inverzni element od a, pa, s obzirom da vrijedi komutativnost zbrajanja, imamo $e = a \oplus b = b \oplus a$ te zaključujemo da je $b = -a - 6 \in \mathbb{Q}$ suprotni element od $a \in \mathbb{Q}$
- ▷ asocijativnost množenja racionalnih brojeva očito vrijedi
- ▷ jer

  $$(a \oplus b) \cdot c = (a + b + 3) \cdot c = a \cdot c + b \cdot c + 3 \cdot c$$

  nije jednako

  $$a \cdot c \oplus b \cdot c = a \cdot c + b \cdot c + 3,$$

  zaključujemo da množenje nije zdesna distributivno u odnosu na zbrajanje

Dakle, $\mathbb{Q}$ je uz zbrajanje Abelova grupa, uz množenje polugrupa, ali množenje nije zdesna distributivno u odnosu na zbrajanje pa $(\mathbb{Q}, \oplus, \cdot)$ nije prsten. ■

Zadatak 2.2.6. Ispitajte je li skup $S = \{n2^m \colon n \in \mathbb{Z}, m \in \mathbb{N}\}$ prsten uz standardne binarne operacije zbrajanja i množenja cijelih brojeva. □

Zadatak 2.2.7. Pokažite da je skup $\mathbb{Q}^4$ uz binarne operacije zbrajanja po komponentama i množenja definiranog s

$$(a, b, c, d) \cdot (e, f, g, h) = (ae + bg, af + bh, ce + dg, cf + dh)$$

unitalan prsten.

Rješenje. Pokažite za vježbu da je $(\mathbb{Q}^4, +, \cdot)$ prsten. Da bi element $(e, f, g, h) \in \mathbb{Q}^4$ bio desna jedinica prstena $\mathbb{Q}^4$, mora vrijediti

$$(a, b, c, d) \cdot (e, f, g, h) = (a, b, c, d), \ \ \forall (a, b, c, d) \in \mathbb{Q}^4.$$

Dakle, tražimo sve racionalne brojeve e, f, g, h takve da je

$$ae + bg = a, \ \ af + bh = b, \ \ ce + dg = c, \ \ cf + dh = d.$$

Pomnožimo li prvu jednakost s d i oduzmemo li od nje treću jednakost prethodno pomnoženu s b, dobijemo $ade + bdg - bce - bdg = ad - bc$, odnosno $(ad - bc)e = ad - bc$, iz čega slijedi da je $e = 1$. Uvrstimo li to u prvu jednakost, dobijemo da je $g = 0$. Nadalje, pomnožimo li sada drugu jednakost s c i oduzmemo li od nje četvrtu jednakost prethodno pomnoženu s a, dobijemo $acf + bch - acf - adh = bc - ad$, odnosno $(bc - ad)h = bc - ad$, pa je $h = 1$. Uvrstimo li to u drugu jednakost, vidimo da je $f = 0$. Prema tome, desna je jedinica $(1, 0, 0, 1)$. Kako je $(1, 0, 0, 1) \cdot (a, b, c, d) = (a, b, c, d)$, zaključujemo da je $(1, 0, 0, 1)$ i lijeva jedinica. Stoga je $(1, 0, 0, 1)$ jedinica prstena $\mathbb{Q}^4$, odnosno $\mathbb{Q}^4$ jest unitalan prsten. ■

Zadatak 2.2.8. Pokažite da je skup $S = \{(a, b, -b, a) \colon a, b \in \mathbb{Q}\}$ uz binarne operacije zbrajanja po komponentama i množenja definiranog s

$$(a, b, -b, a) \cdot (c, d, -d, c) = (ac - bd, ad + bc, -ad - bc, ac - bd)$$

potprsten prstena iz prethodnog zadatka.

Rješenje. Primijetimo najprije da je operacija množenja jednaka operaciji množenja definiranoj u prethodnom zadatku. Kako je u prethodnom zadatku množenje definirano s

$$(a, b, c, d) \cdot (e, f, g, h) = (ae + bg, af + bh, ce + dg, cf + dh)$$

za elemente $(a, b, -b, a), (c, d, -d, c)$ iz skupa S, imamo

$$(a, b, -b, a) \cdot (c, d, -d, c) = (ac - bd, ad + bc, -ad - bc, ac - bd),$$

pa vidimo da je množenje na skupu S definirano na isti način kao množenje u prethodnom zadatku.

Nadalje, skup S neprazan je jer je, primjerice, $(0, 0, 0, 0) \in S$ i očito je S podskup od $\mathbb{Q}^4$. Uzmimo sada proizvoljne elemente X, Y iz S. Tada je $X = (a, b, -b, a)$ i $Y = (c, d, -d, c)$, pa je

$$X - Y = (a - c, b - d, -b - (-d), a - c) = (a - c, b - d, -(b - d), a - c) \in S,$$

$$X \cdot Y = (ac - bd, ad + bc, -(ad + bc), ac - bd) \in S.$$

Dakle, S je potprsten prstena iz prethodnog zadatka. ■

Zadatak 2.2.9. Neka je R prsten i S netrivijalan unitalni potprsten od R. Dokažite da ako R nema jedinicu, onda R ima djelitelje nule.

Rješenje. Potprsten S od R ima jedinicu pa postoji $e \in S$ takav da je $es = se = s$ za sve elemente $s \in S$. Ako prsten R nema jedinicu, onda postoji element $r \in R$ takav da je $er \neq r$ ili $re \neq r$. Pretpostavimo da je $er \neq r$. Prema pretpostavci je onda $r \in R \backslash S$. Tada je $er = x$, za $x \neq r$, pa je

$$e(x - r) = ex - er = eer - er \overset{e \in S}{=} er - er = 0.$$

Kako su elementi $e, x - r$ u R različiti od 0, slijedi da R ima djeljitelje nule. Analogno vrijedi kada je $re \neq r$. ■

Definicija 2.2.3. Kažemo da je element r prstena R idempotentan ako vrijedi $r^2 = r$.

Zadatak 2.2.10. Neka je R komutativan netrivijalan prsten s jedinicom 1 i $r \in R$. Dokažite da je prsten $Rr = \{ar : a \in R\}$ potprsten od R. Zatim, ukoliko je svaki element u prstenu R idempotentan, pokažite da je tada $r = 1r \in Rr$ jedinica prstena Rr.

Rješenje. Kako u prstenu R vrijedi zatvorenost množenja, očito je skup Rr podskup od R. Prsten R netrivijalan je unitalni prsten, pa je $1r \in Rr$, odnosno Rr jest neprazan skup. Uzmimo sada proizvoljne $x, y \in Rr$. Tada je $x = ar$ i $y = br$, pa je

$$x - y = (a - b)r \in Rr,$$

$$xy = (ar)(br) \overset{asoc.}{=} (arb)r \in Rr.$$

Dakle, Rr jest potprsten od R.

Pokažimo sada da je $r = 1r \in Rr$ jedinica prstena Rr. Neka je $x \in Rr$. Tada je $x = ar$, za $a \in R$. Jer je svaki element u prstenu R idempotentan, vrijedi

$$xr = (ar)(1r) = ar^2 = ar = x,$$

pa iz komutativnosti prstena R slijedi da je $x = xr = rx$ te zaključujemo da je $r = 1r \in Rr$ jedinica prstena Rr. ■

Zadatak 2.2.11. Neka je svaki element prstena R idempotentan. Dokažite sljedeće tvrdnje:

a) Za svaki element $r \in R$ vrijedi $r = -r$.

b) Prsten R jest komutativan.

Rješenje.

a) Neka je $r \in R$. Kako je svaki element prstena R idempotentan, vrijedi

$$(-r)^2 = (-r)(-r) = r^2 = r.$$

S druge strane, $(-r)^2 = -r$ jer je $-r \in R$, a svaki je element prstena R idempotentan. Prema tome, $r = -r$.

b) Uzmimo proizvoljne $a, b \in R$. Kako je svaki element prstena R idempotentan, vrijedi

$$(a + b)^2 = (a + b)(a + b) = a^2 + ab + ba + b^2 = a + ab + ba + b.$$

S druge strane, $(a + b)^2 = a + b$ jer je $(a + b) \in R$, a svaki je element prstena R idempotentan. Dakle, vrijedi

$$a + ab + ba + b = a + b,$$

odnosno $ab = -ba$. Kako je element $ba \in R$, prema a) je dijelu zadatka $ba = -ba$, pa imamo $ab = ba$. Prema tome, prsten R jest komutativan. ■

Zadatak 2.2.12. Neka je R komutativan netrivijalan prsten s jedinicom 1. Ako je svaki element prstena R idempotentan, pokažite da je tada element $1 - r$ idempotentan. □

Zadatak 2.2.13. Pokažite da je skup $\mathbb{Z}_5[i] = \{a + bi \colon a, b \in \mathbb{Z}_5\}$ prsten. Postoje li u $\mathbb{Z}_5[i]$ djelitelji nule te postoji li idempotentni element različit od 0 i 1? Je li $\mathbb{Z}_5[i]$ integralna domena? □

Neka je R prsten i S neprazan podskup od R. Presjek svih potprstena od R koji sadrže S naziva se prsten generiran skupom S i označava se sa $[S]$. Prsten generiran skupom S najmanji je potprsten od R koji sadrži skup S.

Zadatak 2.2.14. Odredite potprsten prstena $\mathbb{C}$ generiran skupom:

a) $\{\sqrt{2}\}$,

b) $\{i, \sqrt{3}\}$,

c) $\{5, i, 1 + i\}$.

Rješenje.

a) Označimo s $P = [\{\sqrt{2}\}]$. Kako vrijedi zatvorenost zbrajanja u prstenu P, vidimo da su elementi $m\sqrt{2}$ za $m \in \mathbb{N}$ u P, no kako u prstenu P postoje njihovi suprotni elementi, zaključujemo da je $m\sqrt{2} \in P$ za $m \in \mathbb{Z}$. Nadalje, zbog zatvorenosti s obzirom na množenje, lako se pokaže da je $2m\sqrt{2} \in P$ za $m \in \mathbb{Z}$ i $2n \in P$ za $n \in \mathbb{Z}$. Definirajmo

$$K = \{2n + m\sqrt{2} \colon m, n \in \mathbb{Z}\}$$

i pokažimo da je $P = K$.

Najprije pokažimo da je K prsten. Očito je K podskup od $\mathbb{C}$ i neprazan. Uzmimo proizvoljne $a, b \in K$. Tada je $a = 2n_1 + m_1\sqrt{2}$ i $b = 2n_2 + m_2\sqrt{2}$, pa je

$$a - b = 2(n_1 - n_2) + (m_1 - m_2)\sqrt{2} \in K,$$

$$a \cdot b = 2(2n_1n_2 + m_1m_2) + (2n_1m_2 + 2n_2m_1)\sqrt{2} \in K.$$

Prema tome, K je potprsten od $\mathbb{C}$, odnosno on je prsten. Isto tako, K je očito podskup od P, pa s obzirom da je P najmanji potprsten od $\mathbb{C}$ koji sadrži skup $\{\sqrt{2}\}$, slijedi da je $K = P$.

b) Za vježbu.

c) Označimo s $P = [\{5, i, 1 + i\}]$. Lako se pokaže da su elementi m i $mi \in P$ za $m \in \mathbb{Z}$. Definirajmo $K = \mathbb{Z}[i]$. Pokazali smo ranije da je $\mathbb{Z}[i]$ potprsten od $\mathbb{C}$, odnosno da je on prsten i $\mathbb{Z}[i]$ očito je podskup od P, pa s obzirom da je P najmanji potprsten od $\mathbb{C}$ koji sadrži skup $\{5, i, 1 + i\}$, zaključujemo da je $K = P$. ■

2.3 Homomorfizmi prstena

Definicija 2.3.1. Neka su R i S prsteni. Preslikavanje $\varphi\colon R \to S$ zove se homomorfizam prstena ako vrijedi

$$\varphi(a+b) = \varphi(a) + \varphi(b) \text{ i } \varphi(ab) = \varphi(a)\varphi(b) \text{ za sve } a, b \in R.$$

Homomorfizam prstena koji je injekcija nazivamo monomorfizam prstena, a homomorfizam prstena koji je surjekcija nazivamo epimorfizam prstena.

Homomorfizam prstena koji je bijekcija nazivamo izomorfizam prstena. Ako postoji izomorfizam prstena $\varphi\colon R \to S$, kažemo da je prsten R izomorfan prstenu S. Inverzno preslikavanje izomorfizma prstena izomorfizam je prstena i kompozicija $\psi \circ \varphi\colon R \to T$ izomorfizama prstena $\varphi\colon R \to S$ i $\psi\colon S \to T$ izomorfizam je prstena. Prema tome, biti izomorfan relacija je ekvivalencije.

Propozicija 2.3.2. *Neka je $\varphi\colon R \to S$ homomorfizam prstena. Tada vrijedi:*

a) $\varphi(0) = 0$,

b) $\varphi(-r) = -\varphi(r)$ *za sve* $r \in R$.

Propozicija 2.3.3. *Neka je $\varphi\colon R \to S$ homomorfizam prstena. Tada je slika*

$$Im\,\varphi = \{\varphi(r)\colon r \in R\}$$

homomorfizma φ potprsten od S, a jezgra

$$Ker\,\varphi = \{r \in R\colon \varphi(r) = 0\}$$

homomorfizma φ potprsten od R.

Ako je R netrivijalan prsten s jedinicom 1_R i S netrivijalan prsten s jedinicom 1_S, onda se homomorfizam prstena $\varphi\colon R \to S$ zove unitalan ako je $\varphi(1_R) = 1_S$.

Neka je $\varphi\colon R \to S$ homomorfizam prstena. Ako prsten R ima jedinicu 1, $S \neq \{0\}$ i preslikavanje φ jest surjekcija, onda je $\varphi(1)$ jedinica od S.

Propozicija 2.3.4. *Homomorfizam prstena $\varphi\colon R \to S$ monomorfizam je ako i samo ako je $Ker\,\varphi = \{0\}$.*

Zadatak 2.3.1. Pokažite da je skup $n\mathbb{Z}$ za $n \in \mathbb{N}$, uz standardno zbrajanje i množenje definirano s

$$a * b = \frac{ab}{n},$$

prsten izomorfan prstenu $(\mathbb{Z}, +, \cdot)$.

Rješenje. Pokažite za vježbu da je $(n\mathbb{Z}, +, *)$ prsten. Definirajmo preslikavanje $\varphi\colon n\mathbb{Z} \to \mathbb{Z}$ s

$$\varphi(a) = \tfrac{a}{n}.$$

Lako se pokaže da je preslikavanje φ dobro definirano. Uzmimo proizvoljne $a, b \in n\mathbb{Z}$ i imamo

$$\varphi(a+b) = \tfrac{a+b}{n} = \tfrac{a}{n} + \tfrac{b}{n} = \varphi(a) + \varphi(b),$$

$$\varphi(a * b) = \varphi\left(\tfrac{ab}{n}\right) = \tfrac{\frac{ab}{n}}{n} = \tfrac{ab}{n^2} = \tfrac{a}{n} \cdot \tfrac{b}{n} = \varphi(a) \cdot \varphi(b).$$

Prema tome, preslikavanje $\varphi\colon n\mathbb{Z} \to \mathbb{Z}$ homomorfizam je prstena.

Kako $\varphi(a) = \varphi(b)$, odnosno $\frac{a}{n} = \frac{b}{n}$ implicira $a = b$, zaključujemo da je preslikavanje φ monomorfizam prstena. Nadalje, pokažimo sada da je preslikavanje φ surjekcija. Neka je $z \in \mathbb{Z}$. Tražimo element u $n\mathbb{Z}$ koji će se preslikati u z. Kako je $\varphi(nz) = \frac{nz}{n} = z$ i $nz \in n\mathbb{Z}$, očito je preslikavanje φ epimorfizam prstena.

Prema tome, preslikavanje φ izomorfizam je prstena. ■

Zadatak 2.3.2. Dokažite da prsteni $2\mathbb{Z}$ i $3\mathbb{Z}$ nisu izomorfni.

Rješenje. Pretpostavimo suprotno, to jest pretpostavimo da postoji izomorfizam prstena $\varphi\colon 2\mathbb{Z} \to 3\mathbb{Z}$. Uočimo da za neki cijeli broj n imamo $\varphi(2) = 3n$. Kako je prema pretpostavci preslikavanje φ homomorfizam prstena, vrijedi

$$\varphi(4) = \varphi(2+2) = \varphi(2) + \varphi(2) = 3n + 3n = 6n,$$

kao i

$$\varphi(4) = \varphi(2 \cdot 2) = \varphi(2) \cdot \varphi(2) = 3n \cdot 3n = 9n^2.$$

Prema tome, $6n = 9n^2$, a to vrijedi ako i samo ako je $n = 0$ ili $n = \frac{2}{3}$. Kako je n cijeli broj, očito je $n \neq \frac{2}{3}$. Dakle, imamo $n = 0$, ali u tom slučaju preslikavanje φ nije bijekcija, čime smo došli do kontradikcije. Prema tome, ne postoji izomorfizam između prstena $2\mathbb{Z}$ i $3\mathbb{Z}$, odnosno prsteni $2\mathbb{Z}$ i $3\mathbb{Z}$ nisu izomorfni. ■

Definicija 2.3.5. Karakteristika prstena R najmanji je prirodan broj n takav da je $nr = 0$, za sve $r \in R$, ukoliko takav n postoji. Ako ne postoji takav prirodan broj, kažemo da je R prsten karakteristike 0. Karakteristiku prstena R označavamo s $\operatorname{char} R$.

Primjer 2.3.1. Prsten $(\mathbb{Z}_m, +_m, \cdot_m)$ prsten je karakteristike m, a prsten $(\mathbb{Z}, +, \cdot)$ prsten je karakteristike 0.

Zadatak 2.3.3. Neka je p prost broj i R komutativan netrivijalan unitalni prsten karakteristike p. Pokažite da je preslikavanje

$$r \mapsto r^p$$

homomorfizam prstena R u R. To preslikavanje nazivamo Frobeniusov homomorfizam.

Rješenje. Neka su a i b elementi prstena R. Tada iz asocijativnosti i komutativnosti prstena R slijedi

$$(ab)^p = (ab)(ab)\cdots(ab) = a^p \cdot b^p.$$

Nadalje, imamo

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}.$$

Uočimo da je za $1 \leq k \leq p-1$

$$\binom{p}{k} = \frac{p!}{k!(p-k)!},$$

gdje je brojnik djeljiv brojem p, a nazivnik nije. Prema tome, slijedi da p dijeli $\binom{p}{k}$. Kako je R prsten karakteristike p, za svaki element r prstena R vrijedi $pr = 0$, pa vidimo da su svi članovi u gornjoj sumi jednaki 0, odnosno $(a+b)^p = a^p + b^p$.

Time smo pokazali da je dano preslikavanje homomorfizam prstena. ■

Zadatak 2.3.4.

a) Dokažite da je prsten kompleksnih brojeva $\mathbb{C}$ izomorfan prstenu

$$R = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}.$$

b) Skupovi $R = \{x + y\sqrt{2} \colon x, y \in \mathbb{Z}\}$ i $S = \{v + w\sqrt{10} \colon v, w \in \mathbb{Q}\}$ prsteni su uz standardno zbrajanje i množenje realnih brojeva. Dokažite da prsteni R i S nisu međusobno izomorfni. □

2.4 Ideali

Definicija 2.4.1. Aditivna podgrupa I prstena R zove se lijevi ideal u prstenu R ako vrijedi

$$a \in I, \ \ r \in R \Rightarrow ra \in I,$$

a desni ideal ako vrijedi

$$a \in I, \ \ r \in R \Rightarrow ar \in I.$$

Ako je I i lijevi i desni ideal u prstenu R, nazivamo ga ideal ili obostrani ideal u prstenu R.

Napomena 2.4.2. U komutativnom je prstenu svaki ideal obostrani ideal.

Teorem 2.4.3. *Neprazan podskup I prstena R jest ideal u R ako je*

a) $a - b \in I$ za sve $a, b \in I$,

b) ra i ar su u I za sve $a \in I$ i $r \in R$.

Primjer 2.4.1. Za svaki prsten R su $\{0\}$ i R ideali u R. Ideal $\{0\}$ nazivamo trivijalan ideal u prstenu R.

Primjer 2.4.2. Pokazali smo ranije da su $\langle 0 \rangle$, $\mathbb{Z}_6$, $\langle 2 \rangle$ i $\langle 3 \rangle$ sve aditivne podgrupe od $\mathbb{Z}_6$. Direktnom se provjerom lako pokaže da su one ideali u komutativnom prstenu $\mathbb{Z}_6$.

Lema 2.4.4. *Neka je R netrivijalan prsten s jedinicom 1 i I ideal u R. Tada je $1 \in I$ ako i samo ako je $R = I$.*

Zadatak 2.4.1. Pokažite da je skup

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{R} \right\}$$

prsten uz standardno zbrajanje i množenje matrica te ispitajte je li

$$I = \left\{ \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix} : x \in \mathbb{R} \right\}$$

ideal u R.

Rješenje. Kako je R očito podskup prstena $M(2, \mathbb{R})$, ispitajmo je li R potprsten od $M(2, \mathbb{R})$. Skup R neprazan je jer je, primjerice, jedinična matrica drugog reda element iz R. Uzmimo proizvoljne matrice $A, B \in R$. Tada je

$$A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}, \ B = \begin{bmatrix} d & e \\ 0 & f \end{bmatrix},$$

pa imamo

$$A - B = \begin{bmatrix} a-d & b-e \\ 0 & c-f \end{bmatrix} \in R \text{ i } AB = \begin{bmatrix} ad & ae+bf \\ 0 & cf \end{bmatrix} \in R.$$

Prema tome, R je potprsten od $M(2, \mathbb{R})$, odnosno R je prsten.

Pokažimo sada da je I ideal u prstenu R. Očito je I podskup od R i I je neprazan jer je, primjerice, nulmatrica drugog reda u I. Nadalje, I je aditivna podgrupa od R jer za proizvoljne $X, Y \in I$,

$$X = \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix} \text{ i } Y = \begin{bmatrix} 0 & y \\ 0 & 0 \end{bmatrix}$$

vrijedi

$$X - Y = \begin{bmatrix} 0 & x-y \\ 0 & 0 \end{bmatrix} \in I.$$

Uzmimo sada prozvoljne matrice $A \in R$ i $X \in I$. Tada je

$$A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \text{ i } X = \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix},$$

pa je

$$AX = \begin{bmatrix} 0 & ax \\ 0 & 0 \end{bmatrix} \in I \text{ i } XA = \begin{bmatrix} 0 & xc \\ 0 & 0 \end{bmatrix} \in I.$$

Time smo pokazali da je I ideal u prstenu R. ■

Napomena 2.4.5. Uočimo kako činjenica je li neki skup ideal ovisi i o prstenu u kojem ga promatramo. Pokažite za vježbu da I iz prethodnog zadatka nije ideal u prstenu $M(2, \mathbb{R})$.

Zadatak 2.4.2. Pokažite da je skup R svih donjetrokutastih matrica iz prstena $M(2,\mathbb{Z})$ prsten uz standardno zbrajanje i množenje matrica i ispitajte jesu li

$$I = \left\{ \begin{bmatrix} 0 & 0 \\ x & y \end{bmatrix} : x, y \in \mathbb{Z} \right\} \text{ i } J = \left\{ \begin{bmatrix} z & 0 \\ 0 & z \end{bmatrix} : z \in \mathbb{Z} \right\}$$

ideali u prstenu R.

Rješenje. Za vježbu pokažite da je R prsten te ispitajte je li I ideal u R. Povjerimo je li skup J ideal u prstenu R. Očito je J podskup od R i on je neprazan jer je, primjerice, nulmatrica drugog reda u J. Nadalje, J je aditivna podgrupa od R jer za proizvoljne $X, Y \in J$,

$$X = \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} \text{ i } Y = \begin{bmatrix} y & 0 \\ 0 & y \end{bmatrix}$$

vrijedi

$$X - Y = \begin{bmatrix} x-y & 0 \\ 0 & x-y \end{bmatrix} \in J.$$

Uzmimo sada matrice $A = \begin{bmatrix} a & 0 \\ b & c \end{bmatrix} \in R$, gdje je $b \neq 0$, i $X = \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} \in J$, gdje je $x \neq 0$. Tada

$$AX = \begin{bmatrix} ax & 0 \\ bx & cx \end{bmatrix} \notin J.$$

Prema tome, J nije ideal u prstenu R. ■

Zadatak 2.4.3. Ispitajte je li skup $I = \{(x-1)p(x) \colon p(x) \in \mathbb{Q}[x]\}$ ideal u komutativnom prstenu $(\mathbb{Q}[x], +, \cdot)$.

Rješenje. Skup I očito je neprazan podskup komutativnog prstena $\mathbb{Q}[x]$. Kako za proizvoljne polinome $p(x), q(x) \in \mathbb{Q}[x]$ imamo $p(x) - q(x) \in \mathbb{Q}[x]$, vidimo da je

$$(x-1)p(x) - (x-1)q(x) = (x-1)[p(x) - q(x)] \in I,$$

pa je I aditivna podgrupa od $\mathbb{Q}[x]$. Nadalje, za elemente $(x-1)p(x) \in I$ i $q(x) \in \mathbb{Q}[x]$ jest

$$(x-1)p(x) \cdot q(x) \in I$$

jer je $p(x) \cdot q(x) \in \mathbb{Q}[x]$, pa zaključujemo da je I ideal u prstenu $\mathbb{Q}[x]$. ■

Neka je S neprazan podskup prstena R. Presjek svih ideala u R koji sadrže S naziva se ideal generiran skupom S i označava se sa (S).

Primjer 2.4.3. Neka je R komutativan netrivijalan unitalni prsten i neka su $a_1, a_2, \ldots, a_n$ elementi iz R. Tada je

$$I = (a_1, a_2, \ldots, a_n) = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n \colon r_i \in R\}$$

ideal u R kojeg nazivamo ideal generiran s $a_1, a_2, \ldots, a_n$.

Definicija 2.4.6. Za ideal kažemo da je glavni ukoliko je generiran jednim elementom.

Teorem 2.4.7. *Neka je R prsten i $a \in R$. Tada vrijedi sljedeće:*

a) $(a) = \{ra + as + ma + \sum_{i=1}^{n} r_i a s_i \colon r, s, r_i, s_i \in R, m \in \mathbb{Z}, n \in \mathbb{N}\}$.

b) Ako je R netrivijalan unitalni prsten, onda je $(a) = \{\sum_{i=1}^{n} r_i a s_i \colon r_i, s_i \in R, n \in \mathbb{N}\}$.

c) Ako je R komutativan prsten, onda je $(a) = \{ra + ma \colon r \in R, m \in \mathbb{Z}\}$.

d) Ako je R komutativan netrivijalan unitalni prsten, onda je $(a) = Ra = aR$.

Definicija 2.4.8. Kažemo da je prsten R prsten glavnih ideala ukoliko je svaki ideal u R glavni. Ako je R i integralna domena, onda za R kažemo da je domena glavnih ideala.

Zadatak 2.4.4. Pokažite da je $\mathbb{Z}$ domena glavnih ideala.

Rješenje. Neka je I proizvoljan ideal u prstenu $\mathbb{Z}$. Kako je ideal I aditivna podgrupa od $\mathbb{Z}$, iz leme 1.6.3 slijedi da je $I = (m) = m\mathbb{Z}$ za $m \in \mathbb{N}_0$. Prsten $\mathbb{Z}$ komutativan je i za svaki cijeli broj n je $n(ma) = m(na) \in m\mathbb{Z}$, gdje je $ma \in m\mathbb{Z}$. Prema tome, $\mathbb{Z}$ je prsten glavnih ideala.

Ranije smo pokazali da je $\mathbb{Z}$ integralna domena pa zaključujemo da je $\mathbb{Z}$ domena glavnih ideala. ■

2.5 Polja

Definicija 2.5.1. Tijelo ili prsten s dijeljenjem netrivijalan je unitalni prsten takav da je svaki element različit od nule invertibilan.

Definicija 2.5.2. Komutativno tijelo nazivamo polje.

Napomena 2.5.3. Svako je polje integralna domena.

Primjer 2.5.1. Skup $\mathbb{Z}$ nije polje.

Primjer 2.5.2. Skupovi $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ jesu polja.

Teorem 2.5.4. *Neka su a, b, c elementi integralne domene R. Ako je $a \neq 0$ i $ab = ac$, onda je $b = c$.*

Zadatak 2.5.1. Dokažite da je svaka konačna integralna domena polje.

Rješenje. Neka je R konačna integralna domena s jedinicom 1 te neka je r nenul element od R. Treba pokazati da element r ima multiplikativan inverz. Ako je $r = 1$, onda je on sam sebi inverz, pa možemo pretpostaviti da je $r \neq 1$. Promotrimo niz $r, r^2, r^3, \ldots$ elemenata integralne domene R. Kako je R konačna inegralna domena, postoje prirodni brojevi m i n takvi da je $m > n$ i $r^m = r^n$. Zapišemo li $m = n + k$ za $k \geq 1$, imamo

$$r^n = r^m = r^{n+k} = r^n \cdot r^k.$$

Nadalje, R je integralna domena i r je nenul element od R, pa indukcijom dobijemo $r^n \neq 0$ za svaki $n \in \mathbb{N}$. Sada imamo

$$r^n = r^n \cdot 1 = r^n \cdot r^k,$$

iz čega slijedi da je $r^k = 1$. Konačno,

$$1 = r^k = r \cdot r^{k-1},$$

odnosno r^{k-1} multiplikativan je inverz od r. Time smo pokazali da je svaka konačna integralna domena polje. ■

2.6 Kvocijentni prsteni

Neka je I ideal u prstenu R. Tada je skup

$$R/I = \{r + I : r \in R\}$$

uz operaciju $(a+I)+(b+I) = a+b+I$ za $a, b \in R$ kvocijentna grupa. Definirajmo operaciju množenja na R/I na sljedeći način:

$$(a + I)(b + I) = ab + I \text{ za } a, b \in R.$$

S tako definiranim operacijama, R/I prsten je kojeg nazivamo kvocijentni prsten prstena R po idealu I.

Nula u kvocijentnom prstenu R/I jest $0 + I = I$.

Napomena 2.6.1. Ako je R prsten s jedinicom 1 i $I \neq R$ ideal u R, onda je R/I prsten s jedinicom $1 + I$.

Primjer 2.6.1. $\mathbb{Z}/6\mathbb{Z}$ jest kvocijentni prsten. Pogledajmo kako zbrajamo i množimo elemente danog kvocijentnog prstena. Uzmimo, primjerice, elemente $2 + 6\mathbb{Z}$ i $5 + 6\mathbb{Z}$. Tada je

$$(2 + 6\mathbb{Z}) + (5 + 6\mathbb{Z}) = 7 + 6\mathbb{Z} = 1 + 6 + 6\mathbb{Z} = 1 + 6\mathbb{Z},$$

$$(2 + 6\mathbb{Z})(5 + 6\mathbb{Z}) = 10 + 6\mathbb{Z} = 4 + 6 + 6\mathbb{Z} = 4 + 6\mathbb{Z}.$$

Zadatak 2.6.1. Neka je $I = (x^2 + 2x + 2)$ ideal u prstenu $\mathbb{Z}_5[x]$. Ispitajte je li $2x + 3 + I$ djelitelj nule u prstenu $\mathbb{Z}_5[x]/I$.

Rješenje. Dijeljenjem polinoma $x^2 + 2x + 2$ polinomom $2x + 3$ u prstenu $\mathbb{Z}_5[x]$ dobijemo da je

$$x^2 + 2x + 2 = (2x + 3)(3x + 4).$$

Kako su $2x + 3 + I$ i $3x + 4 + I$ nenul elementi prstena $\mathbb{Z}_5[x]/I$ čiji je umnožak nula u tom prstenu, zaključujemo da je element $2x + 3 + I$ djelitelj nule u prstenu $\mathbb{Z}_5[x]/I$. ■

Zadatak 2.6.2. Neka je R prsten i I ideal u R. Dokažite da je kvocijentni prsten R/I komutativan ako i samo ako je $rs - sr \in I$ za sve $r, s \in R$. □

Teorem 2.6.2. *Neka je $\varphi\colon R \to S$ homomorfizam prstena.*

a) Jezgra $Ker\,\varphi = I$ preslikavanja φ ideal je u prstenu R.

b) Preslikavanje $\Phi\colon R/I \to Im\,\varphi$ definirano s

$$\Phi(r+I) = \varphi(r) \;\; za\; r \in R$$

izomorfizam je kvocijentnog prstena na prsten $Im\,\varphi$.

Napomena 2.6.3. Dio b) teorema 2.6.2 naziva se Prvi teorem o izomorfizmu za prstene.

Zadatak 2.6.3. Dokažite da je kvocijentni prsten $\mathbb{R}[x]/(x^2+1)$ izomorfan prstenu $\mathbb{C}$.

Rješenje. Označimo ideal (x^2+1) s I. Uočimo najprije da je

$$I = \{f(x)(x^2+1)\colon f(x) \in \mathbb{R}[x]\}.$$

Prema tome,

$$\mathbb{R}[x]/I = \{g(x) + I\colon g(x) \in \mathbb{R}[x]\}.$$

Kako je polinom $g(x) \in \mathbb{R}[x]$, možemo ga zapisati u obliku $g(x) = q(x)(x^2+1) + r(x)$, gdje su $q(x), r(x) \in \mathbb{R}[x]$, pa je $r(x) = 0$ ili je stupanj od $r(x)$ manji od 2, odnosno $r(x) = a + bx$ za neke $a, b \in \mathbb{R}$. Tada je

$$g(x) + I = q(x)(x^2+1) + r(x) + I = r(x) + I.$$

Dakle, $\mathbb{R}[x]/I = \{a + bx + I\colon a, b \in \mathbb{R}\}$.

Definirajmo preslikavanje $\varphi\colon \mathbb{R}[x]/I \to \mathbb{C}$ s

$$\varphi(a + bx + I) = a + bi.$$

Lako se pokaže da je ono dobro definirano. Pokažimo najprije da je preslikavanje φ homomorfizam prstena. Uzmimo proizvoljne elemente A, A' iz $\mathbb{R}[x]/I$. Tada je $A = a + bx + I$ i $A' = a' + b'x + I$, pa je

$$\varphi(A + A') = \varphi(a + a' + (b+b')x + I) = a + a' + (b+b')i = \varphi(A) + \varphi(A').$$

Nadalje,

$$A \cdot A' = (a+bx)(a'+b'x) + I = aa' + ab'x + a'bx + bb'x^2 + I = (aa' - bb') + (ab' + a'b)x + I$$

jer je $x^2 + 1 + I = 0 + I$, odnosno $x^2 + I = -1 + I$, pa imamo

$$\begin{aligned}\varphi(A \cdot A') &= \varphi((aa' - bb') + (ab' + a'b)x + I)\\ &= (aa' - bb') + (ab' + a'b)i\\ &= (a + bi)(a' + b'i)\\ &= \varphi(A) \cdot \varphi(A').\end{aligned}$$

Prema tome, preslikavanje φ homomorfizam je prstena.

Pokažimo sada da je preslikavanje φ surjekcija. Neka je $a + bi \in \mathbb{C}$. Tražimo element iz $\mathbb{R}[x]/I$ koji će se preslikati u $a+bi$. Očito za $a+bx+I \in \mathbb{R}[x]/I$ imamo $\varphi(a+bx+I) = a+bi$.

Nadalje, kako iz $\varphi(a+bx+I)=\varphi(a'+b'x+I)$, odnosno iz $a+bi=a'+b'i$ slijedi da je $a=a'$ i $b=b'$, vidimo da je $a+bx+I=a'+b'x+I$, pa zaključujemo da je preslikavanje φ injekcija.

Dakle, preslikavanje φ izomorfizam je prstena. Drugim riječima, kvocijentni prsten $\mathbb{R}[x]/I$ i prsten $\mathbb{C}$ jesu izomorfni. ■

Zadatak 2.6.4. Neka je I skup svih polinoma iz $\mathbb{Z}[x]$ kojima je suma koeficijenata jednaka 0. Dokažite da je prsten $\mathbb{Z}[x]/I$ izomorfan prstenu $\mathbb{Z}$.

Rješenje. Definirajmo preslikavanje $\varphi\colon \mathbb{Z}[x]\to\mathbb{Z}$ s

$$\varphi(f(x))=f(1).$$

Lako se pokaže da je preslikavanje φ dobro definirano. Neka su $f(x),g(x)\in\mathbb{Z}[x]$. Preslikavanje φ homomorfizam je prstena jer je

$$\varphi(f(x)+g(x))=(f+g)(1)=f(1)+g(1)=\varphi(f(x))+\varphi(g(x)),$$

$$\varphi(f(x)g(x))=(fg)(1)=f(1)g(1)=\varphi(f(x))\varphi(g(x)).$$

Nadalje,

$$\operatorname{Ker}\varphi=\{f(x)\in\mathbb{Z}[x]\colon \varphi(f(x))=f(1)=0\}=I$$

i za svaki element $z\in\mathbb{Z}$ slika je konstantnog polinoma $f(x)=z$ upravo z, pa je preslikavanje φ surjekcija, odnosno $\operatorname{Im}\varphi=\mathbb{Z}$. Sada je, prema Prvom teoremu o izomorfizmu za prstene, prsten $\mathbb{Z}[x]/I$ izomorfan prstenu $\mathbb{Z}$. ■

2.7 Prosti i maksimalni ideali

Neka je R u ovom odjeljku komutativan netrivijalan unitalni prsten.

Napomena 2.7.1. Ideal I u prstenu R pravi je ideal ako je $I\neq R$.

Definicija 2.7.2. Kažemo da je pravi ideal I u prstenu R prost ako iz $ab\in I$ slijedi da je ili $a\in I$ ili $b\in I$.

Definicija 2.7.3. Kažemo da je pravi ideal I u prstenu R maksimalan ako u R ne postoji ideal J takav da je $I\subsetneq J\subsetneq R$.

Primjer 2.7.1. Uočimo da je (0) prost ideal u $\mathbb{Z}$, kao i u svakoj integralnoj domeni, jer za $ab\in(0)$ slijedi da je $a\in(0)$ ili $b\in(0)$, ali (0) nije maksimalan ideal u $\mathbb{Z}$ jer je $(0)\subsetneq(2)\subsetneq\mathbb{Z}$.

Primjer 2.7.2. Ideal (2) prost je i maksimalan ideal u $\mathbb{Z}$. Pokažite to za vježbu.

Primjer 2.7.3. Uočimo da (4) nije prost ideal u $\mathbb{Z}$ jer je $4=2\cdot2$ i očito je $4=2\cdot2\in(4)$, ali $2\notin(4)$. Također, (4) nije maksimalan ideal u $\mathbb{Z}$ jer $(4)\subsetneq(2)\subsetneq\mathbb{Z}$.

Primjer 2.7.4. Trivijalan ideal i $(p)=p\mathbb{Z}$, gdje je p prost broj, prosti su ideali u prstenu $\mathbb{Z}$. Ideal (p) i maksimalan je ideal u prstenu $\mathbb{Z}$.

Primjer 2.7.5. Ideal (x^2+1) nije prost ideal u prstenu $\mathbb{Z}_2[x]$ jer u tom prstenu vrijedi

$$(x+1)^2 = x^2 + 2x + 1 = x^2 + 1$$

i ideal (x^2+1) očito sadrži x^2+1, ali ne sadrži $x+1$.

Zadatak 2.7.1. Neka je R komutativan netrivijalan unitalni prsten.

a) Ako je I ideal u R, dokažite da je tada $I + aR$ ideal u R za svaki $a \notin I$.

b) Dokažite da je pravi ideal I maksimalan u R ako i samo ako za svaki $a \notin I$ postoji $a' \in R$ takav da je $1 + aa' \in I$.

Rješenje.

a) Za vježbu.

b) Pokažimo najprije nužnost. Pretpostavimo da je I maksimalan ideal u R. Tada ne postoji ideal J u R takav da je $I \subsetneq J \subsetneq R$. Kako je $I + aR$ ideal u R za $a \notin I$, slijedi da je $I + aR \neq I$, pa je, prema pretpostavci, $I + aR = R$. Nadalje, s obzirom da je R unitalan prsten, postoje elementi $x \in I$ i $r \in R$ takvi da je $x + ar = 1$. No, tada je $x = 1 - ar$ pa označimo li r s $-a' \in R$, slijedi da je $x = 1 + aa' \in I$, što je trebalo dokazati.

   Pretpostavimo sada da za element $a \notin I$ postoji element $a' \in R$ takav da je $1 + aa' \in I$. Tada je $1 \in I + aR$ jer je $aa' \in aR$, pa kako je $I + aR$ ideal u R, slijedi da je $I + aR = R$. Treba pokazati da je I maksimalan ideal u R. Pretpostavimo da postoji ideal J u R takav da je $I \subsetneq J \subsetneq R$. Tada za $a \notin I$, ali $a \in J$, vrijedi $I + aR \subseteq J$, iz čega slijedi da je $J = R$. Dakle, I je maksimalan ideal u R i time smo pokazali dovoljnost. ■

Zadatak 2.7.2. Dan je skup

$$I = \{f(x) \in \mathbb{Z}[x] \colon f(0) = 0\}.$$

Pokažite da je I ideal u $\mathbb{Z}[x]$. Nakon toga, dokažite da je I glavni ideal te da je I prost ideal u $\mathbb{Z}[x]$. □

Propozicija 2.7.4. *Neka su R i S međusobno izomorfni netrivijalni komutativni unitalni prsteni.*

a) Ako je R integralna domena, onda je i S integralna domena.

b) Ako je R polje, onda je i S polje.

Propozicija 2.7.5. *Neka je I pravi ideal u R. Tada postoji maksimalan ideal u R koji sadrži ideal I.*

Teorem 2.7.6. *Ideal I u prstenu R prost je ako i samo ako je kvocijentni prsten R/I integralna domena.*

Primjer 2.7.6. Kvocijentni je prsten $\mathbb{Z}/m\mathbb{Z}$ integralna domena ako i samo ako je m prost broj. Prema tome, ideal $(m) = m\mathbb{Z}$ prost je ideal u prstenu $\mathbb{Z}$ ako i samo ako je m prost broj.

Teorem 2.7.7. *Ideal I u prstenu R maksimalan je ako i samo ako je kvocijentni prsten R/I polje.*

Primjer 2.7.7. Pokazali smo ranije da je kvocijentni prsten $\mathbb{R}[x]/(x^2+1)$ izomorfan prstenu $\mathbb{C}$. Kako je $\mathbb{C}$ polje, slijedi da je (x^2+1) maksimalan ideal u prstenu $\mathbb{R}[x]$.

Primjer 2.7.8. Kvocijentni je prsten $\mathbb{Z}/m\mathbb{Z}$ polje ako i samo ako je m prost broj. Prema tome, ideal $(m) = m\mathbb{Z}$ maksimalan je ideal u prstenu $\mathbb{Z}$ ako i samo ako je m prost broj.

Teorem 2.7.8. *Svaki je maksimalan ideal I u R prost.*

Zadatak 2.7.3. Ispitajte je li (x^2+4) prost i maksimalan ideal u prstenu $\mathbb{C}[x]$.

Rješenje. Kako je x^2+4, koji je sadržan u idealu (x^2+4), produkt polinoma $x+2i$ i $x-2i$, koji nisu sadržani u idealu (x^2+4), zaključujemo da ideal (x^2+4) nije prost ideal u $\mathbb{C}[x]$. Prema teoremu 2.7.8, ideal (x^2+4) nije maksimalan ideal u $\mathbb{C}[x]$. ■

Teorem 2.7.9. *R je polje ako i samo ako ne postoji netrivijalan pravi ideal u R.*

Zadatak 2.7.4. Neka je F polje, R komutativan unitalni prsten i $\varphi\colon F \to R$ homomorfizam prstena. Dokažite da je tada ili $\varphi(F) = \{0\}$ ili je $\varphi(F)$ polje.

Rješenje. Znamo da je jezgra $\operatorname{Ker}\varphi$ preslikavanja φ ideal u F te da su jedini ideali u polju trivijalan ideal i cijelo polje. Prema tome, $\operatorname{Ker}\varphi = \{0\}$ ili $\operatorname{Ker}\varphi = F$.

Ako je $\operatorname{Ker}\varphi = F$, onda je $\varphi(F) = \{0\}$, a ako je $\operatorname{Ker}\varphi = \{0\}$, onda je preslikavanje φ injekcija, pa je $\varphi(F)$ izomorfno F, odnosno $\varphi(F)$ jest polje. ■

Propozicija 2.7.10. *Neka je R domena glavnih ideala. Tada je svaki prost netrivijalan ideal u R maksimalan u R.*

Zadatak 2.7.5. Ako je R konačan komutativan unitalni prsten, dokažite da je tada svaki prost ideal u R maksimalan ideal u R.

Rješenje. Pretpostavimo da je I prost ideal u R. Tada je kvocijentni prsten R/I integralna domena. Kako je R konačan prsten, slijedi da je kvocijentni prsten R/I konačan. Nadalje, pokazali smo ranije da je svaka konačna integralna domena polje pa je, prema tome, R/I polje, a onda slijedi da je ideal I maksimalan u R . ■

Zadatak 2.7.6. Dan je komutativan unitalni prsten

$$R = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} : a, b \in \mathbb{Z} \right\}$$

i homomorfizam prstena $\varphi\colon R \to \mathbb{Z}$ definiran s

$$\varphi\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix} \right) = a - b.$$

Odredite jezgru od φ te provjerite je li prsten $R/\operatorname{Ker}\varphi$ izomorfan prstenu $\mathbb{Z}$. Je li $\operatorname{Ker}\varphi$ prost ideal u R? Je li $\operatorname{Ker}\varphi$ maksimalan ideal u R? □

2.8 Faktorizacija u prstenima polinoma

Definicija 2.8.1. Neka je R integralna domena. Kažemo da je polinom $f \in R[x]$, koji nije ni nul polinom ni invertibilan element u $R[x]$, ireducibilan nad R ako kada god f izrazimo kao produkt

$$f(x) = g(x)h(x), \;\; g, h \in R[x],$$

slijedi da je g ili h invertibilan element u $R[x]$. Za nenul neinvertibilan element od $R[x]$ koji nije ireducibilan nad R kažemo da je reducibilan nad R.

Napomena 2.8.2. U slučaju da je integralna domena R polje, primijetimo da je nekonstantan polinom $f \in R[x]$ ireducibilan nad R ako i samo ako se f ne može zapisati kao produkt dvaju polinoma nižeg stupnja.

Teorem 2.8.3. *Ako je R integralna domena, onda je $R[x]$ integralna domena.*

Propozicija 2.8.4. *Neka je F polje, $\alpha \in F$ i $f \in F[x]$. Tada je element α nultočka polinoma f ako i samo ako $x - \alpha$ dijeli f.*

Teorem 2.8.5. *Neka je F polje. Ako je $f \in F[x]$ i ako je stupanj polinoma f jednak 2 ili 3, onda je f reducibilan nad F ako i samo ako f ima nultočku u F.*

Primjer 2.8.1. Neka je $f(x) = x^2 + 1$. Koristeći teorem 2.8.5, kako je

$$x^2 + 1 = (x + i)(x - i),$$

zaključujemo da je polinom f reducibilan nad $\mathbb{C}$. Također, uočimo da polinom f nema racionalnu nultočku pa je, prema teoremu 2.8.5, ireducibilan nad $\mathbb{Q}$.

Zadatak 2.8.1. Ispitajte jesu li sljedeći polinomi ireducibilni nad poljem $\mathbb{Z}_5$ i, ukoliko jesu, zapišite ih kao produkt odgovarajućih polinoma:

a) $f_1(x) = x^3 + x + 1$,

b) $f_2(x) = 2x^3 + 3x^2 + 2x + 3$.

Rješenje.

a) Direktnom se provjerom lako pokaže da niti jedan element iz $\mathbb{Z}_5$ nije nultočka polinoma f_1 pa, prema teoremu 2.8.5, zaključujemo da je polinom f_1 ireducibilan nad $\mathbb{Z}_5$.

b) Polinom f_2 očito je reducibilan nad $\mathbb{Z}_5$ prema teoremu 2.8.5, jer mu je 1 nultočka. Podijelimo li polinom f_2 polinomom $x - 1$, dobijemo da je

$$f_2(x) = (x - 1)(2x^2 + 2). \qquad \blacksquare$$

Napomena 2.8.6. Neka je R integralna domena. Jedini elementi u $R[x]$ koji su invertibilni u $R[x]$ jesu oni konstantni polinomi koji su invertibilni u R.

Primjer 2.8.2. Neka je $f(x) = 2x^2 + 4$. Kako je

$$2x^2 + 4 = 2(x^2 + 2),$$

zaključujemo da je polinom f reducibilan nad $\mathbb{Z}$ jer ni 2 ni $x^2 + 2$ nisu invertibilni elementi u $\mathbb{Z}[x]$, a ireducibilan u $\mathbb{Q}[x]$ i u $\mathbb{R}[x]$. Također, uočimo da je polinom f reducibilan nad $\mathbb{C}$.

Propozicija 2.8.7. *Neka je* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ *i neka je* $\alpha = \frac{b}{d} \in \mathbb{Q}$, *gdje su* $b \in \mathbb{Z}$, $d \in \mathbb{N}$ *i* $(b, d) = 1$, *nultočka polinoma* f. *Tada* b *dijeli* a_0, *a* d *dijeli* a_n. *Ako je polinom* f *normiran, onda je* $\alpha \in \mathbb{Z}$ *i dijeli* a_0.

Definicija 2.8.8. Sadržaj nenul polinoma $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ najveći je zajednički djelitelj od $a_n, a_{n-1}, \ldots, a_0$ i označavamo ga s $c(f)$. Kažemo da je polinom s cjelobrojnim koeficijentima primitivan ako je sadržaja 1.

Teorem 2.8.9. *Neka je* f *nekonstantan polinom u* $\mathbb{Z}[x]$.

a) Ako je f *reducibilan nad* $\mathbb{Q}$, *onda je reducibilan i nad* $\mathbb{Z}$.

b) Neka je f *primitivan polinom. Polinom* f *ireducibilan je nad* $\mathbb{Z}$ *ako i samo ako je ireducibilan nad* $\mathbb{Q}$.

Teorem 2.8.10. *(Eisensteinov kriterij) Neka je* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. *Ako postoji prost broj* p *takav da*

$$p \nmid a_n, \;\; p \mid a_{n-1}, \ldots, p \mid a_0 \;\; i \;\; p^2 \nmid a_0,$$

onda je polinom f *ireducibilan nad* $\mathbb{Q}$.

Primjer 2.8.3. Neka je $f(x) = 2x^5 - 5x^4 + 5$. Kako prost broj 5 ne dijeli 2 niti 5^2 dijeli 5, a 5 dijeli -5 i 5, prema Eisensteinovom je kriteriju polinom f ireducibilan nad $\mathbb{Q}$. Sada, jer je f primitivan polinom, iz teorema 2.8.9 slijedi da je polinom f ireducibilan i nad $\mathbb{Z}$.

Zadatak 2.8.2. Ispitajte je li polinom $f(x) = x^2 + x - 1$ ireducibilan nad $\mathbb{Q}$ i nad $\mathbb{R}$.

Rješenje. Prema teoremu 2.8.5 dovoljno je provjeriti ima li polinom f nultočke u odgovarajućim poljima. Tražimo najprije racionalne nultočke danog polinoma. Jedini su kandidati za nultočke 1 i -1 jer su to jedini djelitelji slobodnog člana. No, kako je $f(1) \neq 0$ i $f(-1) \neq 0$, zaključujemo da je polinom f ireducibilan nad $\mathbb{Q}$. Realne su nultočke danog polinoma

$$\tfrac{-1+\sqrt{5}}{2} \;\text{ i }\; \tfrac{-1-\sqrt{5}}{2},$$

pa zaključujemo da je polinom f reducibilan nad $\mathbb{R}$. ■

Zadatak 2.8.3. Ispitajte je li polinom $f(x) = x^3 + x^2 + x + 1$ ireducibilan nad $\mathbb{Q}$.

Rješenje. Kako je $f(x) = x^3 + x^2 + x + 1 = x^2(x+1) + x + 1 = (x+1)(x^2+1)$, zaključujemo da je polinom f reducibilan nad $\mathbb{Q}$. ■

Zadatak 2.8.4. Ispitajte jesu li sljedeći polinomi ireducibilni nad $\mathbb{Z}$:

a) $f_1(x) = x^2 + 4x + 2$,

b) $f_2(x) = x^3 - x^2 - 4$,

c) $f_3(x) = x^4 - 10x^2 + 1$,

d) $f_4(x) = x^3 - 3x^2 + 6x + 3$,

e) $f_5(x) = x^{50} + 14x - 56$.

Rješenje.

a) Polinom f_1 ireducibilan je nad $\mathbb{Q}$ prema Eisensteinovom kriteriju jer 2 ne dijeli 1 niti 4 dijeli 2, ali 2 dijeli 4 i 2. Kako je f_1 primitivan i ireducibilan nad $\mathbb{Q}$, iz teorema 2.8.9 slijedi da je polinom f_1 ireducibilan nad $\mathbb{Z}$.

b) Eisensteinov nam kriterij očito ne daje odgovor, pa pronađimo cjelobrojne nultočke polinoma f_2. Jedini su kandidati za nultočke 1, -1, 2, -2, 4 i -4 jer su to svi djelitelji slobodnog člana. Direktnom se provjerom lako vidi da je $f(2) = 0$, odnosno da je 2 nultočka polinoma f_2. Podijelimo li polinom f_2 s polinomom $x - 2$, vidimo da je

$$f_2(x) = (x^2 + x + 2)(x - 2).$$

Prema tome, polinom f_2 reducibilan je nad $\mathbb{Z}$ jer ni $x^2 + x + 2$ ni $x - 2$ nisu invertibilni elementi u $\mathbb{Z}[x]$.

c) Vidimo da nam Eisensteinov kriterij ne daje odgovor. Jedini su kandidati za cjelobrojne nultočke 1 i -1, no direktnom provjerom lako vidimo da ni 1 ni -1 nije nultočka polinoma f_3.

Nadalje, kako je polinom f_3 stupnja 4, pitamo se postoje li cijeli brojevi a, b, c, d takvi da je $f_3(x) = (x^2 + ax + b)(x^2 + cx + d)$, odnosno

$$x^4 - 10x^2 + 1 = x^4 + (c + a)x^3 + (d + ac + b)x^2 + (ad + bc)x + bd.$$

Sada iz jednakosti polinoma slijedi da je:

$$c + a = 0, \;\; d + ac + b = -10, \;\; ad + bc = 0 \;\text{ i }\; bd = 1.$$

Iskoristimo li najprije da je $bd = 1$, vidimo da imamo dva slučaja:

1) Ako je $b = 1$, onda je $d = 1$. Uvrstimo li to u $d + ac + b = -10$, dobijemo da je $ac = -12$. Kako je $a = -c$, što vidimo iz prve jednadžbe, slijedi da je $c^2 = 12$ i očito c nije cijeli broj, čime smo došli do kontradikcije.
2) Ako je $b = -1$, onda je $d = -1$. Analogno kao u prvom slučaju dobijemo da je $c^2 = -8$, pa smo i u tom slučaju došli do kontradikcije.

Sada lako možemo zaključiti da je polinom f_3 ireducibilan nad $\mathbb{Z}$.

d) Za vježbu.

e) Kako prost broj 7 očito dijeli 14 i -56, a ne dijeli 1 niti 49 dijeli -56, prema Eisensteinovom kriteriju slijedi da je primitivni polinom f_5 ireducibilan nad $\mathbb{Q}$. Sada, koristeći teorem 2.8.9, možemo zaključiti da je polinom f_5 ireducibilan nad $\mathbb{Z}$. ■

Zadatak 2.8.5. Ispitajte jesu li sljedeći polinomi ireducibilni nad $\mathbb{Z}$:

a) $f_1(x) = x^7 + 11x^3 - 33x + 22$,

b) $f_2(x) = x^3 - 7x^2 + 3x + 3$. □

Zadatak 2.8.6. Pokažite da je polinom

$$f(x) = \frac{2}{9}x^5 + \frac{5}{3}x^4 + x^3 + \frac{1}{3}$$

ireducibilan nad $\mathbb{Q}$.

Rješenje. Neka je

$$h(x) = 9f(x) = 2x^5 + 15x^4 + 9x^3 + 3.$$

Tada je polinom f ireducibilan nad $\mathbb{Q}$ ako i samo ako je polinom h ireducibilan nad $\mathbb{Z}$. Prema Eisensteinovom kriteriju za prost broj 3 slijedi da je polinom h ireducibilan nad $\mathbb{Q}$ jer 3 ne dijeli 2 niti 9 dijeli 3, ali 3 dijeli 15, 9 i 3. S obzirom da je on primitivan, očito je ireducibilan i nad $\mathbb{Z}$. Prema tome, polinom f ireducibilan je nad $\mathbb{Q}$. ■

Napomena 2.8.11. Ako je $f \in \mathbb{Q}[x]$ i $a \in \mathbb{Q}$, onda je $f(x)$ ireducibilan nad $\mathbb{Q}$ ako i samo ako je $f(x + a)$ ireducibilan nad $\mathbb{Q}$.

Zadatak 2.8.7. Ispitajte je li polinom $f(x) = x^4 + x^3 + x^2 + x + 1$ ireducibilan nad $\mathbb{Q}$.

Rješenje. Eisensteinov kriterij ne daje odgovor, ali možemo promatrati polinom $f(x + 1)$. Kako je

$$f(x+1) = (x+1)^4 + (x+1)^3 + (x+1)^2 + x + 1 + 1 = x^4 + 5x^3 + 10x^2 + 10x + 5,$$

prema Eisensteinovom kriteriju, za prost broj 5 slijedi da je polinom $f(x + 1)$ ireducibilan nad $\mathbb{Q}$ jer 5 ne dijeli 1 niti 25 dijeli 5, ali 5 dijeli 5 i 10. Sada možemo zaključiti da je, prema napomeni 2.8.11, i polinom $f(x)$ ireducibilan nad $\mathbb{Q}$. ■

Zadatak 2.8.8. Pokažite da je polinom $f(x) = x^4 + 1$ ireducibilan nad $\mathbb{Q}$, a reducibilan nad $\mathbb{R}$.

Rješenje. Polinom $f(x + 1) = x^4 + 4x^3 + 6x^2 + 4x + 2$ ireducibilan je nad $\mathbb{Q}$ prema Eisensteinovom kriteriju za $p = 2$ jer 2 dijeli $4, 6$ i 2, ali ne dijeli 1 niti 4 dijeli 2, pa slijedi da je i polinom $f(x)$ ireducibilan nad $\mathbb{Q}$. Nadalje, kako je

$$f(x) = x^4 + 1 = x^4 + 2x^2 + 1 - 2x^2 = (x^2+1)^2 - (\sqrt{2}x)^2 = (x^2 + 1 - \sqrt{2}x)(x^2 + 1 + \sqrt{2}x),$$

zaključujemo da je polinom $f(x)$ reducibilan nad $\mathbb{R}$ jer se može zapisati kao produkt dvaju polinoma nižeg stupnja. ■

Zadatak 2.8.9.

(a) Pokažite da je polinom $f(x) = x^2 + 8x - 2$ ireducibilan nad $\mathbb{Q}$. Je li dani polinom ireducibilan nad $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$?

(b) Je li polinom $g(x) = x^4 - 5x^2 + 2$ ireducibilan u $\mathbb{Z}[x]$?

(c) Je li polinom $h(x) = x^2 + x + 4$ ireducibilan nad $\mathbb{Z}_{11}$? □

3

Proširenja polja

"Good, he did not have enough imagination to become a mathematician."
- David Hilbert

3.1 Osnovni pojmovi

Definicija 3.1.1. Neka je K polje. Ako je L polje takvo da je $K \subseteq L$, kažemo da je L proširenje polja K.

Polje L možemo promatrati kao vektorski prostor nad poljem K. Ako je taj prostor konačnodimenzionalan, kažemo da je L konačno proširenje polja K, a prirodan broj $\dim_K L$ nazivamo stupanj proširenja i označavamo s $[L : K]$. Ukoliko proširenje L polja K nije konačno, pišemo $[L : K] = \infty$.

Primjer 3.1.1. Polje $\mathbb{C}$ konačno je proširenje polja $\mathbb{R}$.

Primjer 3.1.2. Polje $\mathbb{C}$ nije konačno proširenje polja $\mathbb{Q}$, to jest $[\mathbb{C} : \mathbb{Q}] = \infty$.

Teorem 3.1.2. *Neka je K polje i neka je f nekonstantan polinom u $K[x]$. Tada postoji proširenje L polja K u kojem polinom f ima nultočku.*

Primjer 3.1.3. Neka je $f(x) = x^2 + 1 \in \mathbb{R}[x]$. Polinom f očito nema nultočku u polju $\mathbb{R}$, ali za $i \in \mathbb{C}$ vrijedi $f(i) = 0$, odnosno polinom f ima nultočku u proširenju $\mathbb{C}$ polja $\mathbb{R}$.

Neka je L proširenje polja K i $\alpha \in L$. Najmanji potprsten od L koji sadrži K i α označavamo s $K[\alpha]$. Vrijedi

$$K[\alpha] = \{f(\alpha) \colon f \in K[x]\}.$$

Nadalje, s $K(\alpha)$ označavamo najmanje potpolje od L koje sadrži K i α.

Definicija 3.1.3. Neka je L proširenje polja K. Za element $\alpha \in L$ kažemo da je algebarski nad K ako postoji nekonstantan polinom f u $K[x]$ takav da je $f(\alpha) = 0$. Ako element α nije algebarski nad K, kažemo da je transcendentan nad K.

Definicija 3.1.4. Ako je svaki element $\alpha \in L$ algebarski nad K, kažemo da je L algebarsko proširenje polja K.

Primjer 3.1.4. Polinom $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ nema racionalnih nultočki. Kako je očito $f(\sqrt{2}) = 0$ i $\sqrt{2}$ je element proširenja $\mathbb{R}$ polja $\mathbb{Q}$, zaključujemo da je element $\sqrt{2} \in \mathbb{R}$ algebarski nad $\mathbb{Q}$.

Primjer 3.1.5. Elementi $\pi, e \in \mathbb{R}$ transcendentni su nad $\mathbb{Q}$. Dakle, polje $\mathbb{R}$ nije algebarsko proširenje polja $\mathbb{Q}$.

Napomena 3.1.5. Polje $\mathbb{C}$ algebarsko je proširenje polja $\mathbb{R}$.

Zadatak 3.1.1. Ispitajte jesu li sljedeći elementi algebarski nad poljem $\mathbb{Q}$:

a) $\sqrt[3]{2}$,

b) π^2.

Rješenje.

a) Očito je $\sqrt[3]{2} \in \mathbb{R}$ nultočka polinoma

$$f(x) = x^3 - 2 \in \mathbb{Q}[x],$$

pa je prema tome $\sqrt[3]{2}$ algebarski nad $\mathbb{Q}$.

b) Pretpostavimo da postoji polinom f u $\mathbb{Q}[x]$ takav da je $f(\pi^2) = 0$. Definirajmo polinom $g(x) = f(x^2)$. Tada je $g \in \mathbb{Q}[x]$ i vrijedi

$$f(\pi^2) = g(\pi) = 0,$$

pa slijedi da je element $\pi \in \mathbb{R}$ algebarski nad $\mathbb{Q}$, čime smo došli do kontradikcije jer znamo da je element π transcendentan nad $\mathbb{Q}$. Prema tome, element π^2 transcendentan je nad $\mathbb{Q}$. ■

Zadatak 3.1.2.

a) Ispitajte jesu li $\alpha = \sqrt{2 + \sqrt{3}}$ i $\beta = \dfrac{-1 + i\sqrt{3}}{2}$ algebarski nad poljem $\mathbb{Q}$.

b) Neka je L proširenje polja K i neka je $a \in L$ algebarski nad K, a $t \in L$ transcendentan nad K. Pokažite da je tada $a + t$ transcendentan nad K. □

Neka je $\alpha \in L$ algebarski nad K. Tada je

$$I = \{f \in K[x] \colon f(\alpha) = 0\}$$

ideal u prstenu $K[x]$.

Teorem 3.1.6. *Ako je K polje, onda je $K[x]$ domena glavnih ideala.*

Kako je $K[x]$ domena glavnih ideala, ideal I glavni je ideal, pa postoji jedinstven normirani polinom μ_α u $K[x]$ takav da je $I = (\mu_\alpha)$. Polinom μ_α zove se minimalni polinom elementa $\alpha \in L$ algebarskog nad K.

Propozicija 3.1.7. *Minimalni polinom μ_α elementa α iz L algebarskog nad K ima sljedeća svojstva:*

a) Ako je $f \in K[x]$ takav da je $f(\alpha) = 0$, onda je polinom f djeljiv s polinomom μ_α u $K[x]$.

b) Polinom μ_α ima najmanji stupanj među svim nekonstantnim polinomima iz $K[x]$ kojima je α nultočka.

c) Polinom μ_α jedini je normiran ireducibilni polinom u $K[x]$ kojemu je α nultočka.

Teorem 3.1.8. *Neka je L proširenje polja K, element α iz L algebarski nad K i μ_α minimalni polinom od α nad K stupnja m. Tada je*

$$K(\alpha) = K[\alpha] = \{f(\alpha) \colon f \in K[x],\ \deg f \leq m-1\}.$$

Nadalje, skup $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ je baza vektorskog prostora $K(\alpha)$ nad K, odnosno

$$[K(\alpha) : K] = m = \deg \mu_\alpha.$$

Primjer 3.1.6. Lako se pokaže da je polinom $f(x) = x^2 + 1$ minimalni polinom od $i \in \mathbb{C}$ nad $\mathbb{R}$. Prema tome, polje $\mathbb{C}$ proširenje je stupnja 2 polja $\mathbb{R}$ i baza od $\mathbb{C}$ nad $\mathbb{R}$ jest $\{1, i\}$.

Zadatak 3.1.3. Nađite minimalni polinom μ_α u $\mathbb{Q}[x]$ i bazu od $\mathbb{Q}(\alpha)$ nad $\mathbb{Q}$ za

a) $\alpha = \sqrt[3]{3} + 1$,

b) $\alpha = \sqrt{2 + \sqrt[3]{2}}$.

Rješenje.

a) Očito je $\alpha - 1 = \sqrt[3]{3}$ pa je $\alpha^3 - 3\alpha^2 + 3\alpha - 4 = 0$. Sada vidimo da je α nultočka normiranog polinoma

$$f(x) = x^3 - 3x^2 + 3x - 4.$$

Provjerimo je li polinom f ireducibilan nad $\mathbb{Q}$. Eisensteinov kriterij ne daje odgovor, a jedini su kandidati za racionalne nultočke 1, -1, 2, -2, 4 i -4 jer su to jedini djelitelji slobodnog člana. Međutim, direktnom provjerom lako vidimo da polinom f nema racionalnih nultočaka pa, koristeći teorem 2.8.5, zaključujemo da je polinom f ireducibilan nad $\mathbb{Q}$. Prema tome, polinom $f = \mu_\alpha$ minimalni je polinom od α nad $\mathbb{Q}$ i on je očito stupnja 3, pa je $\{1, \alpha, \alpha^2\}$ baza od $\mathbb{Q}(\alpha)$ nad $\mathbb{Q}$.

b) Kako je $\alpha^2 = 2 + \sqrt[3]{2}$, slijedi da je $(\alpha^2 - 2)^3 = 2$, pa je $\alpha^6 - 6\alpha^4 + 12\alpha^2 - 10 = 0$. Tada je α nultočka normiranog polinoma

$$f(x) = x^6 - 6x^4 + 12x^2 - 10$$

koji je, prema Eisensteinovom kriteriju za $p = 2$, ireducibilan nad $\mathbb{Q}$ jer 2 ne dijeli 1 niti 4 dijeli 10, ali 2 dijeli -6, 12 i -10. Dakle, polinom $f = \mu_\alpha$ minimalni je polinom od α nad $\mathbb{Q}$ i baza od $\mathbb{Q}(\alpha)$ nad $\mathbb{Q}$ jest $\{1, \alpha, \alpha^2, \ldots, \alpha^5\}$. ■

Neka je L proširenje polja K i $S \subseteq L$. Tada s $K(S)$ označavamo najmanje potpolje od L koje sadrži K i S. Ako je $S = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq L$, onda pišemo $K(S) = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Definicija 3.1.9. Za polje L kažemo da je konačno generirano proširenje polja K ako postoje $n \in \mathbb{N}$ i $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ takvi da je

$$L = K(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Teorem 3.1.10. *Proširenje L polja K konačno je ako i samo ako je algebarsko i konačno generirano.*

Definicija 3.1.11. Proširenje polja K oblika $K(\alpha)$ naziva se jednostavno proširenje od K.

Primjer 3.1.7. Polje $\mathbb{Q}(\sqrt{2})$ jednostavno je proširenje polja $\mathbb{Q}$.

Napomena 3.1.12. Neka je L proširenje polja K i neka su a i b elementi od L. Tada je

$$K(a, b) = K(a)(b) = K(b)(a).$$

Primjer 3.1.8. Polje $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3})(\sqrt{5})$ jednostavno je proširenje polja $\mathbb{Q}(\sqrt{3})$.

Zadatak 3.1.4. Pokažite da je proširenje $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ polja $\mathbb{Q}$ jednostavno i nađite bazu za njega.

Rješenje. Treba pronaći $\alpha \in \mathbb{Q}(\sqrt{3}, \sqrt{5})$ takav da je $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Pretpostavimo da je $\alpha = \sqrt{3} + \sqrt{5}$. Očito je

$$\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5})$$

i treba pokazati da je $\mathbb{Q}(\sqrt{3}, \sqrt{5}) \subseteq \mathbb{Q}(\alpha)$, odnosno da je $\sqrt{3} \in \mathbb{Q}(\alpha)$ i da je $\sqrt{5} \in \mathbb{Q}(\alpha)$. Kako je $\mathbb{Q}(\alpha)$ polje, očigledno je $\alpha^{-1} \in \mathbb{Q}(\alpha)$, odnosno

$$\alpha^{-1} = \frac{1}{\sqrt{3} + \sqrt{5}} = \frac{1}{\sqrt{3} + \sqrt{5}} \cdot \frac{\sqrt{3} - \sqrt{5}}{\sqrt{3} - \sqrt{5}} = \frac{\sqrt{3} - \sqrt{5}}{3 - 5} = \frac{-1}{2}(\sqrt{3} - \sqrt{5}) \in \mathbb{Q}(\alpha).$$

Dakle, $-2\alpha^{-1} = \sqrt{3} - \sqrt{5}$. Zbrojimo li sada $-2\alpha^{-1}$ i α, dobijemo da je $2\sqrt{3} = \alpha - 2\alpha^{-1}$, pa kako su α i $2\alpha^{-1}$ elementi polja $\mathbb{Q}(\alpha)$, zaključujemo da je $2\sqrt{3}$ element polja $\mathbb{Q}(\alpha)$, odnosno $\sqrt{3}$ je element polja $\mathbb{Q}(\alpha)$.

Analogno se pokaže da je $\sqrt{5}$ element polja $\mathbb{Q}(\alpha)$. Prema tome,

$$\mathbb{Q}(\sqrt{3}, \sqrt{5}) \subseteq \mathbb{Q}(\alpha).$$

Time smo pokazali da je

$$\mathbb{Q}(\sqrt{3},\sqrt{5}) = \mathbb{Q}(\sqrt{3}+\sqrt{5}),$$

odnosno da je proširenje $\mathbb{Q}(\sqrt{3},\sqrt{5})$ polja $\mathbb{Q}$ jednostavno.

Pronađimo sada minimalni polinom od $\alpha \in \mathbb{Q}(\sqrt{3},\sqrt{5})$ algebarskog nad $\mathbb{Q}$. Očito je $\alpha - \sqrt{3} = \sqrt{5}$ pa je $\alpha^2 - 2\sqrt{3}\alpha + 3 = 5$, odnosno $\alpha^2 - 2 = 2\sqrt{3}\alpha$. Tada je $\alpha^4 - 16\alpha^2 + 4 = 0$ i vidimo da je α nultočka normiranog polinoma

$$f(x) = x^4 - 16x^2 + 4.$$

Provjerimo je li polinom f ireducibilan nad $\mathbb{Q}$. Eisensteinov kriterij ne daje odgovor, a jedini su kandidati za racionalne nultočke 1, -1, 2, -2, 4 i -4. Direktnom provjerom lako vidimo da polinom f nema racionalnih nultočaka pa zaključujemo da polinom f nema linearan član u rastavu. S obzirom da je polinom f stupnja 4, pitamo se postoje li cijeli brojevi a, b, c, d takvi da je $f(x) = (x^2 + ax + b)(x^2 + cx + d)$. Analogno kao ranije, pokaže se da ne postoje takvi cijeli brojevi. Sada lako možemo zaključiti da je polinom f ireducibilan nad $\mathbb{Q}$. Prema tome, polinom $f = \mu_\alpha$ minimalni je polinom od α nad $\mathbb{Q}$, a kako je on očito stupnja 4, skup $\{1, \alpha, \alpha^2, \alpha^3\}$ baza je od $\mathbb{Q}(\alpha)$ nad $\mathbb{Q}$. ■

Zadatak 3.1.5. Pokažite da je proširenje $\mathbb{Q}(\sqrt{3},\sqrt{21})$ polja $\mathbb{Q}(\sqrt{7})$ jednostavno i odredite stupanj proširenja polja $\mathbb{Q}(\sqrt{3},\sqrt{21})$ nad poljem $\mathbb{Q}(\sqrt{7})$. □

Teorem 3.1.13. *Neka su $K \subseteq L \subseteq M$ polja. Neka je $\{\alpha_i : i \in I\}$ baza vektorskog prostora L nad poljem K i neka je $\{\beta_j : j \in J\}$ baza vektorskog prostora M nad poljem L. Tada je*

$$\{\alpha_i\beta_j : i \in I, j \in J\}$$

baza vektorskog prostora M nad poljem K.

Teorem 3.1.14. *Neka su $K \subseteq L \subseteq M$ polja. Tada je*

$$[M : K] = [M : L] \cdot [L : K].$$

Pri tome je $\infty \cdot n = n \cdot \infty = \infty \cdot \infty = \infty$ za $n \in \mathbb{N}$. Drugim riječima, proširenje M polja K konačno je ako i samo ako su proširenja M od L i L od K konačna i tada je stupanj $[M : K]$ jednak umnošku stupnjeva $[M : L]$ i $[L : K]$.

Zadatak 3.1.6. Koristeći činjenicu

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3}),$$

odredite stupanj proširenja $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}]$ i nađite bazu od $\mathbb{Q}(\sqrt{2},\sqrt{3})$ nad $\mathbb{Q}$.

Rješenje. Prema teoremu 3.1.14 slijedi da je

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}].$$

Odredimo najprije stupanj proširenja $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$. To je stupanj minimalnog polinoma od $\alpha = \sqrt{2} \in \mathbb{Q}(\sqrt{2})$ algebarskog nad $\mathbb{Q}$. Očito je $\alpha^2 = 2$ pa vidimo da je α nultočka normiranog polinoma

$$f(x) = x^2 - 2$$

koji je, prema Eisensteinovom kriteriju za $p = 2$, ireducibilan nad $\mathbb{Q}$. Prema tome, $f = \mu_\alpha$ minimalni je polinom od α nad $\mathbb{Q}$ pa je stupanj proširenja

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2,$$

a baza od $\mathbb{Q}(\sqrt{2})$ nad $\mathbb{Q}$ jest $\{1, \sqrt{2}\}$.

Da bismo odredili stupanj $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$, uzmimo $\beta = \sqrt{3}$. Očito je β nultočka normiranog polinoma

$$g(x) = x^2 - 3.$$

Treba pokazati da je polinom g ireducibilan nad $\mathbb{Q}(\sqrt{2})$. Pretpostavimo da je g reducibilan nad $\mathbb{Q}(\sqrt{2})$, odnosno pretpostavimo da $g(x) = (x - \sqrt{3})(x + \sqrt{3})$. Tada je $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Prema tome, postoje racionalni brojevi a i b takvi da je $\sqrt{3} = a + b\sqrt{2}$. Tada je

$$3 = a^2 + 2ab\sqrt{2} + 2b^2.$$

Kako je $\{1, \sqrt{2}\}$ baza za $\mathbb{Q}(\sqrt{2})$ nad $\mathbb{Q}$, očito je $3 - a^2 - 2b^2 = 0$ i $2ab = 0$. Iz $2ab = 0$ vidimo da je $a = 0$ ili $b = 0$. Ako je $a = 0$, onda je $b^2 = \frac{3}{2}$, što ne može biti jer je b racionalan broj, a ako je $b = 0$, onda je $a^2 = 3$, što ne može biti jer je a racionalan broj. Prema tome, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Time smo pokazali da je polinom $g(x) = x^2 - 3$ ireducibilan nad $\mathbb{Q}(\sqrt{2})$, odnosno $g = \mu_\beta$ minimalni je polinom od $\beta = \sqrt{3}$ nad $\mathbb{Q}(\sqrt{2})$. Dakle, stupanj proširenja

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$$

i baza od $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ nad $\mathbb{Q}(\sqrt{2})$ jest $\{1, \sqrt{3}\}$.

Sada vidimo da je stupanj proširenja

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4,$$

a baza od $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ nad $\mathbb{Q}$ jest $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. ■

Zadatak 3.1.7. Neka je α nultočka polinoma $f(x) = x^3 + x + 3$. Ispitajte je li polinom $p(x) = x^2 - 2$ reducibilan nad $\mathbb{Q}(\alpha)$.

Rješenje. Ranije smo pokazali da je $p(x) = x^2 - 2$ minimalni polinom od $\sqrt{2}$ nad $\mathbb{Q}$, pa je, prema tome, stupanj proširenja od $\mathbb{Q}(\sqrt{2})$ nad $\mathbb{Q}$ jednak 2. Pretpostavimo sada da je polinom p reducibilan nad $\mathbb{Q}(\alpha)$. Tada iz

$$p(x) = (x - \sqrt{2})(x + \sqrt{2})$$

slijedi da je $\sqrt{2} \in \mathbb{Q}(\alpha)$. Dakle, vrijedi

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\alpha),$$

pa iz teorema 3.1.14 slijedi da je

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}].$$

Nadalje, polinom f normiran je i ireducibilan nad $\mathbb{Q}$ jer nema racionalnih nultočki i trećeg je stupnja, pa je on minimalni polinom od α nad $\mathbb{Q}$. Prema tome, stupanj je proširenja od $\mathbb{Q}(\alpha)$ nad $\mathbb{Q}$ jednak 3. Sada vidimo da je

$$[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] = \tfrac{3}{2},$$

što ne može biti jer je stupanj proširenja prirodan broj. Dakle, polinom p ireducibilan je nad $\mathbb{Q}(\alpha)$. ■

Zadatak 3.1.8. Odredite stupanj proširenja

$$[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})]$$

i minimalni polinom elementa $\sqrt[6]{2}$ nad $\mathbb{Q}(\sqrt{2})$.

Rješenje. Najprije uočimo da je $x^6 - 2$ minimalni polinom od $\sqrt[6]{2}$ algebarskog nad $\mathbb{Q}$, pa je stupanj proširenja

$$[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6.$$

Nadalje, kako je $\sqrt{2} = (\sqrt[6]{2})^3 \in \mathbb{Q}(\sqrt[6]{2})$, očito je

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[6]{2}),$$

pa iz teorema 3.1.14 slijedi da je

$$[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}],$$

odnosno da je

$$[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})] = 3$$

jer je stupanj proširenja $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, što je ranije pokazano. Sada možemo zaključiti da je stupanj minimalnog polinoma od $\sqrt[6]{2}$ algebarskog nad $\mathbb{Q}(\sqrt{2})$ jednak 3. Lako se pokaže da je

$$\mu_{\sqrt[6]{2}}(x) = x^3 - \sqrt{2}$$

traženi minimalni polinom. ■

Zadatak 3.1.9. Odredite stupanj proširenja polja $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3})$ nad poljem $\mathbb{Q}$.

Rješenje. Kako je $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3})$, očito je

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}) : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}].$$

Također, kako je $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{3}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3})$, očito je

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}) : \mathbb{Q}(\sqrt[4]{3})] \cdot [\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}].$$

Nadalje, lako se pokaže da je stupanj proširenja $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, a stupanj proširenja $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 4$. Prema tome, 3 dijeli $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}) : \mathbb{Q}]$ i 4 dijeli $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}) : \mathbb{Q}]$, odnosno stupanj proširenja $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}) : \mathbb{Q}]$ veći je ili jednak 12.

S druge strane, stupanj proširenja

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}) : \mathbb{Q}(\sqrt[3]{2})]$$

najviše je 4 jer je $\sqrt[4]{3}$ nultočka polinoma $x^4 - 3 \in \mathbb{Q}(\sqrt[3]{2})[x]$, a iz ranijih svojstava minimalnog polinoma slijedi da je minimalni polinom od $\sqrt[4]{3}$ nad $\mathbb{Q}(\sqrt[3]{2})$ stupnja manjeg ili jednakog 4. Dakle,

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}) : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \leq 4 \cdot 3 = 12.$$

Sada možemo zaključiti da je stupanj proširenja $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}) : \mathbb{Q}] = 12$. ■

Zadatak 3.1.10. Odredite stupanj proširenja

$$[\mathbb{Q}(\sqrt[7]{16}+3\sqrt[7]{8})\colon \mathbb{Q}]$$

i nađite jednu bazu za $\mathbb{Q}(\sqrt[7]{16}+3\sqrt[7]{8})$ nad $\mathbb{Q}$. □

Zadatak 3.1.11. Neka je L konačno proširenje polja K. Pretpostavimo da je $[L:K]=p$, gdje je p prost broj. Ako je $\alpha \in L$ i $\alpha \notin K$, dokažite da je $L=K(\alpha)$.

Rješenje. Odmah vidimo da je $K(\alpha)$ potpolje od L koje sadrži K, odnosno imamo

$$K \subseteq K(\alpha) \subseteq L,$$

pa iz teorema 3.1.14 slijedi da je

$$[L:K]=[L:K(\alpha)]\cdot[K(\alpha):K].$$

Iz pretpostavke zadatka znamo da je stupanj proširenja $[L:K]=p$, gdje je p prost broj, pa je $[L:K(\alpha)]=1$ ili $[K(\alpha):K]=1$ jer su stupnjevi proširenja prirodni brojevi.

Ako je $[K(\alpha):K]=1$, onda je $K(\alpha)=K$. Očito polje $K(\alpha)$ sadrži element α, pa iz $K(\alpha)=K$ slijedi da i K sadrži element α, čime smo došli do kontradikcije jer $\alpha \notin K$. Dakle, mora biti $[L:K(\alpha)]=1$, odnosno $L=K(\alpha)$. ■

Zadatak 3.1.12. Polinom $f(x)=x^3-x-1$ ireducibilan je nad $\mathbb{Q}$. Neka je $\alpha \in \mathbb{C}$ nultočka danog polinoma i neka je $\beta \in \mathbb{Q}(\alpha)$, ali $\beta \notin \mathbb{Q}$. Pokažite da je tada $\mathbb{Q}(\beta)=\mathbb{Q}(\alpha)$. □

Zadatak 3.1.13. Neka su $\alpha, \beta \in L$, gdje je L proširenje polja K, te neka su f i g iz $K[x]$ ireducibilni normirani polinomi nad poljem K. Ako je α nultočka polinoma f i β nultočka polinoma g, pokažite da je f ireducibilan nad $K(\beta)$ ako i samo ako je g ireducibilan nad $K(\alpha)$.

Rješenje. Neka je stupanj polinoma f jednak n, a stupanj polinoma g jednak m. Pretpostavimo da je polinom f ireducibilan nad $K(\beta)$. Tada je $[K(\alpha,\beta):K(\beta)]=n$. Kako je

$$K \subseteq K(\beta) \subseteq K(\alpha,\beta),$$

iz teorema 3.1.14 slijedi da je

$$[K(\alpha,\beta):K]=[K(\alpha,\beta):K(\beta)]\cdot[K(\beta):K],$$

odnosno $[K(\alpha,\beta):K]=nm$.

Također,

$$K \subseteq K(\alpha) \subseteq K(\alpha,\beta),$$

pa iz teorema 3.1.14 slijedi da je

$$[K(\alpha,\beta):K]=[K(\alpha,\beta):K(\alpha)]\cdot[K(\alpha):K].$$

Sada možemo zaključiti da je $[K(\alpha,\beta):K(\alpha)]=m=\deg \mu_\beta$, pa iz svojstava minimalnog polinoma slijedi da je polinom g ireducibilan nad $K(\alpha)$.

Obrat se pokaže analogno. ■

3.2 Polja cijepanja

Definicija 3.2.1. Neka je K polje i $f \in K[x]$ nekonstantan polinom. Kažemo da se polinom f cijepa nad proširenjem L polja K ako postoji $a \in K$ i $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ takvi da je

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Ako je pri tome $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, kažemo da je proširenje L polje cijepanja polinoma f nad poljem K.

Primjer 3.2.1. Polinom $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ cijepa se nad $\mathbb{R}$. Polje cijepanja polinoma f nad $\mathbb{Q}$ jest

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \colon a, b \in \mathbb{Q}\}.$$

Primjer 3.2.2. Polinom $f(x) = x^2 + 1 \in \mathbb{Q}[x]$ cijepa se nad $\mathbb{C}$. Polje

$$\mathbb{Q}(i) = \{a + bi \colon a, b \in \mathbb{Q}\}$$

polje je cijepanja polinoma f nad $\mathbb{Q}$.

Teorem 3.2.2. *Neka je K polje i $f \in K[x]$ nekonstantan polinom. Tada postoji polje cijepanja polinoma f nad K. Štoviše, ako su L_1 i L_2 polja cijepanja polinoma f nad K, onda postoji izomorfizam polja $\varphi \colon L_1 \to L_2$ takav da je $\varphi(x) = x$ za sve $x \in K$.*

3.3 Algebarski zatvarač

Definicija 3.3.1. Proširenje L polja K naziva se algebarski zatvarač polja K ako je to proširenje algebarsko nad K i ako je polje L algebarski zatvoreno, odnosno ako svaki nekonstantan polinom u $L[x]$ ima nultočku u L.

Primjer 3.3.1. Polje $\mathbb{C}$ algebarski je zatvarač polja $\mathbb{R}$.

Teorem 3.3.2. *Svako polje K ima algebarski zatvarač. Ako su L_1 i L_2 algebarski zatvarači od K, onda postoji izomorfizam polja $\varphi \colon L_1 \to L_2$ takav da je $\varphi(x) = x$ za sve $x \in K$.*

Propozicija 3.3.3. *Neka je L algebarsko proširenje polja K. Ako se svaki nekonstantan polinom $f \in K[x]$ cijepa nad L, onda je polje L algebarski zatvoreno.*

Zadatak 3.3.1. Dokažite da konačno polje nije algebarski zatvoreno.

Rješenje. Neka je K konačno polje. Tada je $K = \{a_1, a_2, \ldots, a_n\}$. Definirajmo polinom

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_n) + a_1, \text{ gdje je } a_1 \neq 0.$$

Tada je $f(a_i) = a_1$ za svaki $i \in \{1, 2, \ldots, n\}$. Prema tome, kako nekonstantan polinom u $K[x]$ nema nultočku u K, slijedi da polje K nije algebarski zatvoreno. ■

3.4 Izomorfizmi polja

Neka su K i L polja. Izomorfizam je polja K na polje L bijekcija $\varphi\colon K \to L$ takva da je

$$\varphi(a+b) = \varphi(a) + \varphi(b) \text{ i } \varphi(ab) = \varphi(a)\varphi(b) \text{ za sve } a, b \in K.$$

Lema 3.4.1. *Ako su K i L polja, svaki je netrivijalni homomorfizam prstena $\varphi\colon K \to L$ unitalan monomorfizam.*

Napomena 3.4.2. Jedini je automorfizam polja racionalnih brojeva identiteta.

Zadatak 3.4.1. Dokažite da polja $\mathbb{Q}(\sqrt{2})$ i $\mathbb{Q}(\sqrt{3})$ nisu izomorfna.

Rješenje. Pretpostavimo suprotno, odnosno pretpostavimo da postoji izomorfizam

$$\varphi\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3}).$$

Koristeći lemu 3.4.1, vidimo da je $\varphi(1) = 1$. Lako se pokaže da je onda $\varphi(x) = x$ za sve racionalne brojeve x. Kako je preslikavanje φ homomorfizam, za $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ vrijedi

$$\varphi(a + b\sqrt{2}) = \varphi(a) + \varphi(b)\varphi(\sqrt{2}) = a + b \cdot \varphi(\sqrt{2}).$$

Prema tome, treba odrediti $\varphi(\sqrt{2})$. Očito je $\varphi(\sqrt{2}) \in \mathbb{Q}(\sqrt{3})$, pa postoje racionalni brojevi x i y takvi da je $\varphi(\sqrt{2}) = x + y\sqrt{3}$. Kako je

$$(\varphi(\sqrt{2}))^2 = \varphi(\sqrt{2}) \cdot \varphi(\sqrt{2}) = \varphi((\sqrt{2})^2) = \varphi(2) = 2,$$

imamo $(x + y\sqrt{3})^2 = 2$, odnosno

$$x^2 + 2xy\sqrt{3} + 3y^2 = 2.$$

S obzirom da je $\{1, \sqrt{3}\}$ baza od $\mathbb{Q}(\sqrt{3})$ nad $\mathbb{Q}$, slijedi da je $x^2 + 3y^2 = 2$ i $2xy = 0$. Iz $2xy = 0$ vidimo da je ili $x = 0$ ili $y = 0$.

Ako je $x = 0$, onda je $3y^2 = 2$, pa dolazimo do kontradikcije jer je y racionalan broj, a ako je $y = 0$, onda je $x^2 = 2$, čime dolazimo do kontradikcije jer je x racionalan broj. Prema tome, ne postoji izomorfizam između $\mathbb{Q}(\sqrt{2})$ i $\mathbb{Q}(\sqrt{3})$. ■

Zadatak 3.4.2. Dokažite da su polja $\mathbb{Q}(\alpha)$ i $\mathbb{Q}(\beta)$ izomorfna, ako je α nultočka polinoma $f(x) = x^2 - 2$, a β nultočka polinoma $g(x) = x^2 - 4x + 2$.

Rješenje. Polinomi f i g normirani su i ireducibilni nad $\mathbb{Q}$ prema Eisensteinovom kriteriju za prost broj 2. Prema tome, polinom $f = \mu_\alpha$ minimalni je polinom od α nad $\mathbb{Q}$ i baza od $\mathbb{Q}(\alpha)$ nad $\mathbb{Q}$ jest $\{1, \alpha\}$, a polinom $g = \mu_\beta$ minimalni je polinom od β nad $\mathbb{Q}$ i baza od $\mathbb{Q}(\beta)$ nad $\mathbb{Q}$ jest $\{1, \beta\}$. Dakle,

$$\mathbb{Q}(\alpha) = \{a + b\alpha\colon a, b \in \mathbb{Q}\},$$
$$\mathbb{Q}(\beta) = \{x + y\beta\colon x, y \in \mathbb{Q}\}.$$

Odredimo izomorfizam $\varphi\colon \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$. Kako je preslikavanje φ homomorfizam, analogno kao u prethodnom zadatku, vidimo da je

$$\varphi(a + b\alpha) = a + b \cdot \varphi(\alpha).$$

Trebamo odrediti $\varphi(\alpha) \in \mathbb{Q}(\beta)$. Znamo da je $\varphi(\alpha) = x + y\beta$ za racionalne brojeve x i y. Tada je $\varphi(\alpha^2) = (x + y\beta)^2$. Kako je α nultočka polinoma f, očito je $\alpha^2 - 2 = 0$, odnosno $\alpha^2 = 2$, pa je, prema tome, $\varphi(\alpha^2) = \varphi(2) = 2$.

Sada je $2 = (x + y\beta)^2$, odnosno

$$2 = x^2 + 2xy\beta + y^2\beta^2.$$

Kako je β nultočka polinoma g, očito je $\beta^2 - 4\beta + 2 = 0$, pa je $\beta^2 = 4\beta - 2$. Dakle, vrijedi

$$2 = x^2 + 2xy\beta + y^2(4\beta - 2).$$

S obzirom da je $\{1, \beta\}$ baza od $\mathbb{Q}(\beta)$ nad $\mathbb{Q}$, vidimo da je

$$2 = x^2 - 2y^2,$$

$$0 = 2xy + 4y^2 = 2y(x + 2y).$$

Sada iz $2y(x + 2y) = 0$ slijedi da je ili $y = 0$ ili $x + 2y = 0$.

Ako je $y = 0$, onda je $x^2 = 2$, što ne može biti jer je x racionalan broj, a ako je $x + 2y = 0$, odnosno $x = -2y$, onda je $2y^2 = 2$, pa je $y = 1$ i $x = -2$ ili $y = -1$ i $x = 2$. Dakle,

$$\varphi(\alpha) = -2 + \beta \text{ ili } \varphi(\alpha) = 2 - \beta. \qquad \blacksquare$$

3.5 Galoisova grupa proširenja

Neka je K polje. Automorfizam polja K izomorfizam je polja K na samog sebe. Skup svih automorfizama polja K označavat ćemo s $\mathrm{Aut}(K)$ i $\mathrm{Aut}(K)$ grupa je s obzirom na kompoziciju. Također, $\mathrm{Aut}(K)$ podgrupa je grupe permutacija skupa K.

Neka je L proširenje polja K. Automorfizam $\sigma \in \mathrm{Aut}(L)$ za kojeg vrijedi $\sigma(a) = a$, za sve $a \in K$, nazivamo K-automorfizam polja L. Skup svih K-automorfizama polja L označavamo s $\mathrm{Aut}_K(L)$ i $\mathrm{Aut}_K(L)$ podgrupa je od $\mathrm{Aut}(L)$. Grupa $\mathrm{Aut}_K(L)$ naziva se Galoisova grupa proširenja L polja K i obično se označava s $\mathrm{Gal}(L/K)$, $\mathrm{Gal}(L, K)$, $G(L/K)$ ili $G(L, K)$.

Zadatak 3.5.1. Odredite sve automorfizme polja $\mathbb{Q}(\sqrt{2})$.

Rješenje. Neka je $\sigma\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ izomorfizam polja. Kako je $\sigma(x) = x$ za sve $x \in \mathbb{Q}$ i preslikavanje σ homomorfizam polja, imamo

$$\sigma(a + b\sqrt{2}) = a + b \cdot \sigma(\sqrt{2}).$$

Dakle, trebamo odrediti $\sigma(\sqrt{2})$. Pokazali smo ranije da je $(\sigma(\sqrt{2}))^2 = \sigma(2) = 2$. Tada je $\sigma(\sqrt{2}) = \sqrt{2}$ ili je $\sigma(\sqrt{2}) = -\sqrt{2}$. Prema tome, imamo preslikavanje

$$\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$$

i preslikavanje

$$\sigma_2(a+b\sqrt{2}) = a - b\sqrt{2}.$$

Očito je $\sigma_1 = \mathrm{id}$ automorfizam od $\mathbb{Q}(\sqrt{2})$. Uvjerimo se da je i σ_2 automorfizam od $\mathbb{Q}(\sqrt{2})$. Pokažimo najprije da je preslikavanje σ_2 homomorfizam. Uzmimo proizvoljne $A, A' \in \mathbb{Q}(\sqrt{2})$. Tada je $A = a + b\sqrt{2}$ i $A' = a' + b'\sqrt{2}$ i vrijedi

$$\sigma_2(A+A') = a + a' - (b+b')\sqrt{2} = a - b\sqrt{2} + a' - b'\sqrt{2} = \sigma_2(A) + \sigma_2(A').$$

Nadalje,

$$\sigma_2(AA') = \sigma_2(aa' + 2bb' + (ab' + a'b)\sqrt{2}) = aa' + 2bb' - (ab' + a'b)\sqrt{2},$$

a s druge je strane

$$\sigma_2(A)\sigma_2(A') = (a - b\sqrt{2})(a' - b'\sqrt{2}) = aa' + 2bb' - (ab' + a'b)\sqrt{2}$$

i vidimo da je $\sigma_2(AA') = \sigma_2(A)\sigma_2(A')$. Time smo pokazali da je preslikavanje σ_2 homomorfizam polja.

Kako $\sigma_2(A) = \sigma_2(A')$, odnosno $a - b\sqrt{2} = a' - b'\sqrt{2}$ implicira da je $a = a'$ i $b = b'$, pa je $A = A'$, zaključujemo da je preslikavanje σ_2 injekcija.

Da bismo pokazali da je preslikavanje σ_2 surjekcija, uzmimo element $a + b\sqrt{2}$ iz $\mathbb{Q}(\sqrt{2})$ i pronađimo element X iz $\mathbb{Q}(\sqrt{2})$ takav da je $\sigma_2(X) = a + b\sqrt{2}$. Očito za $X = a - b\sqrt{2}$ imamo $\sigma_2(a - b\sqrt{2}) = a + b\sqrt{2}$ i $X = a - b\sqrt{2}$ jest u $\mathbb{Q}(\sqrt{2})$. Prema tome, preslikavanje σ_2 jest surjekcija.

Time smo pokazali da je i preslikavanje σ_2 automorfizam polja $\mathbb{Q}(\sqrt{2})$.

Dakle, Galoisova je grupa proširenja

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) = \{\mathrm{id}, \sigma_2\}. \qquad \blacksquare$$

Zadatak 3.5.2. Odredite Galoisovu grupu proširenja $\mathbb{Q}(\sqrt[3]{2})$ polja $\mathbb{Q}$.

Rješenje. Očito je $\mu_{\sqrt[3]{2}}(x) = x^3 - 2$ minimalni polinom od $\sqrt[3]{2}$ nad $\mathbb{Q}$ jer mu je $\sqrt[3]{2}$ nultočka, normiran je i ireducibilan nad $\mathbb{Q}$ prema Eisensteinovom kriteriju za prost broj 2. Prema tome, baza od $\mathbb{Q}(\sqrt[3]{2})$ nad $\mathbb{Q}$ jest $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$.

Neka je $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$. Tada je $\sigma(x) = x$ za sve $x \in \mathbb{Q}$ i

$$\sigma(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2) = a + b \cdot \sigma(\sqrt[3]{2}) + c \cdot (\sigma(\sqrt[3]{2}))^2.$$

Dakle, trebamo odrediti $\sigma(\sqrt[3]{2})$. Vidimo da je

$$(\sigma(\sqrt[3]{2}))^3 = \sigma(2) = 2,$$

odnosno $\sigma(\sqrt[3]{2})$ nultočka je polinoma $\mu_{\sqrt[3]{2}}(x) = x^3 - 2$. Kako je $\sqrt[3]{2}$ jedina realna nultočka polinoma $\mu_{\sqrt[3]{2}}$, a očito je $\sigma(\sqrt[3]{2}) \in \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, zaključujemo da je $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$, odnosno $\sigma = \mathrm{id}$ i to je automorfizam polja $\mathbb{Q}(\sqrt[3]{2})$. Prema tome, Galoisova je grupa proširenja

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{id}\}. \qquad \blacksquare$$

Zadatak 3.5.3. Odredite $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$.

Rješenje. Znamo da je polje $\mathbb{C}$ proširenje stupnja 2 polja $\mathbb{R}$ i da je baza od $\mathbb{C}$ nad $\mathbb{R}$ jednaka $\{1, i\}$. Prema tome,

$$\mathbb{C} = \mathbb{R}(i) = \{a + bi \colon a, b \in \mathbb{R}\}.$$

Neka je $\sigma \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$. Tada je $\sigma(r) = r$ za sve realne brojeve r i

$$\sigma(a + bi) = a + b \cdot \sigma(i)$$

jer je σ homomorfizam polja. Nadalje, kako je

$$(\sigma(i))^2 = \sigma(i^2) = \sigma(-1) = -1,$$

očito je $\sigma(i) = i$ ili je $\sigma(i) = -i$. Dakle, imamo dva preslikavanja, $\sigma_1 = \mathrm{id}$ koje je očito automorfizam od $\mathbb{C}$ i $\sigma_2(a + bi) = a - bi$.

Analogno kao ranije, lako se pokaže da je preslikavanje σ_2 zaista automorfizam od $\mathbb{C}$. Stoga je

$$\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \sigma_2\}.$$ ■

Zadatak 3.5.4. Odredite Galoisovu grupu proširenja $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ polja $\mathbb{Q}$.

Rješenje. Ranije je pokazano da je skup

$$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$$

baza od $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ nad $\mathbb{Q}$. Neka je $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))$. Tada je $\sigma(x) = x$ za sve racionalne brojeve x, a kako je preslikavanje σ homomorfizam polja, slijedi da je

$$\sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b \cdot \sigma(\sqrt{2}) + c \cdot \sigma(\sqrt{3}) + d \cdot \sigma(\sqrt{6}).$$

Nadalje, kako je $\sigma(\sqrt{6}) = \sigma(\sqrt{2})\sigma(\sqrt{3})$, vidimo da je potrebno odrediti $\sigma(\sqrt{2})$ i $\sigma(\sqrt{3})$. Ranije je pokazano da je $(\sigma(\sqrt{2}))^2 = 2$, pa je $\sigma(\sqrt{2}) = \pm\sqrt{2}$, a analogno je $\sigma(\sqrt{3}) = \pm\sqrt{3}$. Prema tome, imamo najviše 4 automorfizma od $\mathbb{Q}(\sqrt{2}, \sqrt{3})$:

σ_1	σ_2	σ_3	σ_4
$\sqrt{2} \mapsto \sqrt{2}$	$\sqrt{2} \mapsto \sqrt{2}$	$\sqrt{2} \mapsto -\sqrt{2}$	$\sqrt{2} \mapsto -\sqrt{2}$
$\sqrt{3} \mapsto \sqrt{3}$	$\sqrt{3} \mapsto -\sqrt{3}$	$\sqrt{3} \mapsto \sqrt{3}$	$\sqrt{3} \mapsto -\sqrt{3}$.

Očito je $\sigma_1 = \mathrm{id}$ automorfizam od $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Lako se pokaže da su i σ_2, σ_3 te σ_4 zaista automorfizmi polja $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Stoga je

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{\mathrm{id}, \sigma_2, \sigma_3, \sigma_4\}.$$ ■

3.6 Separabilna i normalna proširenja

Definicija 3.6.1. Neka je K polje, $f \in K[x]$ nekonstantan polinom i L polje cijepanja polinoma f nad poljem K. Kažemo da je f separabilan polinom ako su sve nultočke od f u L jednostruke, odnosno ako je

$$f(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),\ a \in K,\ \alpha_1, \alpha_2, \ldots, \alpha_n \in L,\ \alpha_i \neq \alpha_j \text{ za } i \neq j.$$

Definicija 3.6.2. Neka je L proširenje polja K i $\alpha \in L$. Kažemo da je element α separabilan nad K ako je α algebarski nad K i ako je njegov minimalni polinom $\mu_\alpha \in K[x]$ separabilan.

Definicija 3.6.3. Kažemo da je L separabilno proširenje polja K ako je svaki element iz L separabilan nad K.

Napomena 3.6.4. Neka je K polje karakteristike 0. Tada je svako algebarsko proširenje polja K separabilno.

Primjer 3.6.1. Polje $\mathbb{Q}(\sqrt{2})$ algebarsko je proširenje polja $\mathbb{Q}$. Kako je $\mathbb{Q}$ polje karakteristike 0, slijedi da je polje $\mathbb{Q}(\sqrt{2})$ separabilno proširenje polja $\mathbb{Q}$.

Definicija 3.6.5. Konačno separabilno proširenje L polja K naziva se normalno proširenje polja K ako je L polje cijepanja nekog polinoma $f \in K[x]$ nad K.

Propozicija 3.6.6. *Neka je L konačno separabilno proširenje polja K. Tada su sljedeće tvrdnje međusobno ekvivalentne:*

a) L je normalno proširenje polja K.

b) Ako je $f \in K[x]$ ireducibilan polinom koji ima nultočku u polju L, onda se f cijepa nad poljem L.

c) $|\,Aut_K(L)| = [L : K]$.

d) Vrijedi $K = L^{Aut_K(L)} = \{x \in L \colon \sigma(x) = x,\ za\ sve\ \sigma \in Aut_K(L)\}$.

Primjer 3.6.2. Polje $\mathbb{Q}(\sqrt{2})$ normalno je proširenje od $\mathbb{Q}$.

Primjer 3.6.3. Polje $\mathbb{Q}(\sqrt[3]{2})$ nije normalno proširenje od $\mathbb{Q}$ jer polinom $x^3 - 2$ osim realne nultočke $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})$ ima i dvije nultočke koje nisu realne.

Definicija 3.6.7. Galoisova grupa polinoma $f \in K[x]$ nad poljem K grupa je $\mathrm{Aut}_K(L)$, gdje je L polje cijepanja polinoma f nad poljem K.

Zadatak 3.6.1. Odredite Galoisovu grupu polinoma $f(x) = x^4 + 1$ nad poljem $\mathbb{Q}$.

Rješenje. Kako su

$$x_{1,2} = \frac{-\sqrt{2} \pm i\sqrt{2}}{2} \text{ i } x_{3,4} = \frac{\sqrt{2} \pm i\sqrt{2}}{2}$$

nultočke polinoma f, vidimo da je

$$\mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}(i, \sqrt{2})$$

polje cijepanja polinoma f nad poljem $\mathbb{Q}$. Također, polje $\mathbb{Q}(i,\sqrt{2})$ konačno je separabilno proširenje polja $\mathbb{Q}$ prema teoremu 3.1.10 i napomeni 3.6.4. Prema tome, $\mathbb{Q}(i,\sqrt{2})$ normalno je proširenje polja $\mathbb{Q}$ i iz propozicije 3.6.6 slijedi da je

$$|\operatorname{Gal}(\mathbb{Q}(i,\sqrt{2})/\mathbb{Q})| = |\operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(i,\sqrt{2}))| = [\mathbb{Q}(i,\sqrt{2}):\mathbb{Q}].$$

Odredimo stupanj proširenja $[\mathbb{Q}(i,\sqrt{2}):\mathbb{Q}]$. Kako je

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(i,\sqrt{2}),$$

imamo

$$[\mathbb{Q}(i,\sqrt{2}):\mathbb{Q}] = [\mathbb{Q}(i,\sqrt{2}):\mathbb{Q}(\sqrt{2})]\cdot[\mathbb{Q}(\sqrt{2}):\mathbb{Q}].$$

Ranije je pokazano da je stupanj proširenja $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ i da je baza od $\mathbb{Q}(\sqrt{2})$ nad $\mathbb{Q}$ jednaka $\{1,\sqrt{2}\}$. Da bismo odredili stupanj proširenja $[\mathbb{Q}(i,\sqrt{2}):\mathbb{Q}(\sqrt{2})]$, uzmimo $\alpha = i$ i uočimo da je α nultočka normiranog polinoma

$$g(x) = x^2 + 1.$$

Pretpostavimo da je polinom g reducibilan nad $\mathbb{Q}(\sqrt{2})$. Tada je $g(x) = (x-i)(x+i)$ i $i \in \mathbb{Q}(\sqrt{2})$, a očito $i \notin \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$. Time smo pokazali da je polinom $g(x) = x^2+1$ ireducibilan nad $\mathbb{Q}(\sqrt{2})$, odnosno $g = \mu_\alpha$ je minimalni polinom od $\alpha = i$ nad $\mathbb{Q}(\sqrt{2})$. Dakle, stupanj proširenja

$$[\mathbb{Q}(i,\sqrt{2}):\mathbb{Q}(\sqrt{2})] = 2$$

i baza od $\mathbb{Q}(i,\sqrt{2})$ nad $\mathbb{Q}(\sqrt{2})$ jest $\{1,i\}$.

Sada vidimo da je stupanj proširenja $[\mathbb{Q}(i,\sqrt{2}):\mathbb{Q}] = 4$, odnosno

$$|\operatorname{Gal}(\mathbb{Q}(i,\sqrt{2})/\mathbb{Q})| = 4,$$

i baza od $\mathbb{Q}(i,\sqrt{2})$ nad $\mathbb{Q}$ jest

$$\{1, i, \sqrt{2}, i\sqrt{2}\}.$$

Neka je $\sigma \in \operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(i,\sqrt{2}))$. Tada je $\sigma(x) = x$, za sve racionalne brojeve x, a kako je σ homomorfizam polja, vrijedi

$$\sigma(a + bi + c\sqrt{2} + di\sqrt{2}) = a + b\cdot\sigma(i) + c\cdot\sigma(\sqrt{2}) + d\cdot\sigma(i)\sigma(\sqrt{2}).$$

Vidimo da treba odrediti $\sigma(\sqrt{2})$ i $\sigma(i)$. Ranije je pokazano da je $\sigma(\sqrt{2}) = \pm\sqrt{2}$ i $\sigma(i) = \pm i$. Prema tome,

$$\operatorname{Gal}(\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\},$$

gdje su

σ_1	σ_2	σ_3	σ_4
$\sqrt{2} \mapsto \sqrt{2}$	$\sqrt{2} \mapsto \sqrt{2}$	$\sqrt{2} \mapsto -\sqrt{2}$	$\sqrt{2} \mapsto -\sqrt{2}$
$i \mapsto i$	$i \mapsto -i$	$i \mapsto i$	$i \mapsto -i.$

■

Zadatak 3.6.2. Odredite Galoisovu grupu polinoma $f(x) = x^4 - 2$ nad poljem $\mathbb{Q}$.

Rješenje. Nultočke od f jesu $x_{1,2} = \pm\sqrt[4]{2}$ i $x_{3,4} = \pm i\sqrt[4]{2}$, pa je polje cijepanja polinoma f nad poljem $\mathbb{Q}$ jednako

$$\mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i).$$

Također, $\mathbb{Q}(\sqrt[4]{2}, i)$ konačno je separabilno proširenje polja $\mathbb{Q}$. Dakle, proširenje $\mathbb{Q}(\sqrt[4]{2}, i)$ polja $\mathbb{Q}$ normalno je i iz propozicije 3.6.6 slijedi da je

$$|\operatorname{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})| = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}].$$

Odredimo stupanj proširenja $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}]$. Kako je

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}, i),$$

vrijedi

$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}].$$

Lako vidimo da je polinom $\mu_\alpha(x) = x^4 - 2$ minimalni polinom od $\alpha = \sqrt[4]{2}$ nad $\mathbb{Q}$, pa je stupanj proširenja

$$[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$$

i baza od $\mathbb{Q}(\sqrt[4]{2})$ nad $\mathbb{Q}$ jest $\{1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}\}$.

Odredimo sada stupanj proširenja $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})]$. Neka je $\beta = i$ i β je nultočka normiranog polinoma $g(x) = x^2 + 1$. Polinom g ireducibilan je nad $\mathbb{Q}(\sqrt[4]{2})$ jer bi u suprotnom u polju $\mathbb{Q}(\sqrt[4]{2})$ vrijedilo $g(x) = (x - i)(x + i)$ i $i \in \mathbb{Q}(\sqrt[4]{2})$, a očito $i \notin \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$. Dakle, $g = \mu_\beta$ minimalni je polinom od $\beta = i$ nad $\mathbb{Q}(\sqrt[4]{2})$ i stupanj je proširenja

$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2,$$

a baza od $\mathbb{Q}(\sqrt[4]{2}, i)$ nad $\mathbb{Q}(\sqrt[4]{2})$ jest $\{1, i\}$.

Sada vidimo da je

$$|\operatorname{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})| = 8$$

i baza od $\mathbb{Q}(\sqrt[4]{2}, i)$ nad $\mathbb{Q}$ jest

$$\{1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}, i, i\sqrt[4]{2}, i\sqrt[4]{4}, i\sqrt[4]{8}\}.$$

Nadalje, uočimo da su $\sigma \in \operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}, i))$ određeni sa $\sigma(\sqrt[4]{2})$ i $\sigma(i)$. Kako je

$$(\sigma(\sqrt[4]{2}))^4 = \sigma(2) = 2,$$

očito je $\sigma(\sqrt[4]{2})$ neka od nultočki polinoma $x^4 - 2$, pa vidimo da je

$$\sigma(\sqrt[4]{2}) \in \{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\},$$

a ranije je pokazano da je $\sigma(i) = \pm i$. Prema tome,

$$\operatorname{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_8\},$$

gdje su

$$\sigma_1 = \begin{cases} \sqrt[4]{2} \mapsto \sqrt[4]{2} \\ i \mapsto i, \end{cases} \quad \sigma_2 = \begin{cases} \sqrt[4]{2} \mapsto \sqrt[4]{2} \\ i \mapsto -i, \end{cases} \quad \sigma_3 = \begin{cases} \sqrt[4]{2} \mapsto -\sqrt[4]{2} \\ i \mapsto i, \end{cases} \quad \sigma_4 = \begin{cases} \sqrt[4]{2} \mapsto -\sqrt[4]{2} \\ i \mapsto -i, \end{cases}$$

$$\sigma_5 = \begin{cases} \sqrt[4]{2} \mapsto i\sqrt[4]{2} \\ i \mapsto i, \end{cases} \quad \sigma_6 = \begin{cases} \sqrt[4]{2} \mapsto i\sqrt[4]{2} \\ i \mapsto -i, \end{cases} \quad \sigma_7 = \begin{cases} \sqrt[4]{2} \mapsto -i\sqrt[4]{2} \\ i \mapsto i, \end{cases} \quad \sigma_8 = \begin{cases} \sqrt[4]{2} \mapsto -i\sqrt[4]{2} \\ i \mapsto -i. \end{cases}$$

■

Zadatak 3.6.3. Odredite Galoisovu grupu polinoma $f(x) = x^4 + 4x^2 + 2$ nad poljem $\mathbb{Q}$.

Rješenje. Uočimo najprije da je normirani polinom f ireducibilan nad $\mathbb{Q}$ prema Eisensteinovom kriteriju za prost broj 2.

Vidimo da je $f(x) = (x^2+2)^2 - 2$, odnosno da je $f(x) = 0$ ako i samo ako je $x^2+2 = \pm\sqrt{2}$. Prema tome, nultočke polinoma f jesu

$$x_{1,2} = \pm\sqrt{-2+\sqrt{2}} \in \mathbb{C} \text{ i } x_{3,4} = \pm\sqrt{-2-\sqrt{2}} \in \mathbb{C},$$

pa je polje cijepanja polinoma f nad poljem $\mathbb{Q}$ jednako

$$\mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}\left(\sqrt{-2+\sqrt{2}}, \sqrt{-2-\sqrt{2}}\right) = \mathbb{Q}\left(\sqrt{-2+\sqrt{2}}, \sqrt{2}\right)$$

jer je

$$\sqrt{-2+\sqrt{2}} \cdot \sqrt{-2-\sqrt{2}} \in \mathbb{Q}\left(\sqrt{-2+\sqrt{2}}, \sqrt{-2-\sqrt{2}}\right).$$

Također, $\mathbb{Q}\left(\sqrt{-2+\sqrt{2}}, \sqrt{2}\right)$ konačno je separabilno proširenje polja $\mathbb{Q}$. Prema tome, vidimo da je $\mathbb{Q}\left(\sqrt{-2+\sqrt{2}}, \sqrt{2}\right)$ normalno proširenje polja $\mathbb{Q}$ i iz propozicije 3.6.6 slijedi da je i

$$\left|\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{-2+\sqrt{2}}, \sqrt{2}\right) \Big/ \mathbb{Q}\right)\right| = \left[\mathbb{Q}\left(\sqrt{-2+\sqrt{2}}, \sqrt{2}\right) : \mathbb{Q}\right].$$

Radi jednostavnosti, označimo $L = \mathbb{Q}\left(\sqrt{-2+\sqrt{2}}, \sqrt{2}\right)$. Kako je

$$\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{-2+\sqrt{2}}\right) \subseteq L,$$

vrijedi

$$[L : \mathbb{Q}] = \left[L : \mathbb{Q}\left(\sqrt{-2+\sqrt{2}}\right)\right] \cdot \left[\mathbb{Q}\left(\sqrt{-2+\sqrt{2}}\right) : \mathbb{Q}\right].$$

Odredimo najprije stupanj proširenja $\left[\mathbb{Q}\left(\sqrt{-2+\sqrt{2}}\right) : \mathbb{Q}\right]$. Očito je polinom $f = \mu_\alpha$ minimalni polinom od $\alpha = \sqrt{-2+\sqrt{2}}$ nad $\mathbb{Q}$, pa je stupanj proširenja

$$\left[\mathbb{Q}\left(\sqrt{-2+\sqrt{2}}\right) : \mathbb{Q}\right] = 4$$

i baza od $\mathbb{Q}\left(\sqrt{-2+\sqrt{2}}\right)$ nad $\mathbb{Q}$ jest $\{1, \alpha, \alpha^2, \alpha^3\}$.

Da bismo odredili stupanj proširenja $\left[L : \mathbb{Q}\left(\sqrt{-2+\sqrt{2}}\right)\right]$, uzmimo $\beta = \sqrt{2}$ i β je nultočka normiranog polinoma

$$g(x) = x^2 - 2.$$

Pretpostavimo da je polinom g reducibilan nad $\mathbb{Q}\left(\sqrt{-2+\sqrt{2}}\right)$. Kako su u polju cijepanja polinoma g nad poljem racionalnih brojeva $\sqrt{2}$ i $-\sqrt{2}$ jedine nultočke od g, slijedi da je tada i $\sqrt{2} \in \mathbb{Q}\left(\sqrt{-2+\sqrt{2}}\right)$. Dakle, postoje racionalni brojevi a, b, c, d takvi da je

$$\sqrt{2} = a + b \cdot \sqrt{-2+\sqrt{2}} + c \cdot \left(\sqrt{-2+\sqrt{2}}\right)^2 + d \cdot \left(\sqrt{-2+\sqrt{2}}\right)^3.$$

Tada je $b+d(-2+\sqrt{2}) = 0$ i $a+c(-2+\sqrt{2}) = \sqrt{2}$. Uočimo da je $b = d = 0$ te da je $a-2c = 0$ i $c = 1$, iz čega slijedi da je $a = 2$. Dakle,

$$\sqrt{2} = 2 + \left(\sqrt{-2+\sqrt{2}}\right)^2 \in \mathbb{Q}\left(\sqrt{-2+\sqrt{2}}\right),$$

pa zaključujemo da je polinom g reducibilan nad $\mathbb{Q}\left(\sqrt{-2+\sqrt{2}}\right)$. Tada je stupanj proširenja

$$\left[L : \mathbb{Q}\left(\sqrt{-2+\sqrt{2}}\right)\right] = 1.$$

Sada je očito

$$|\operatorname{Gal}(L/\mathbb{Q})| = 4$$

i baza od L nad $\mathbb{Q}$ je

$$\{1, \alpha, \alpha^2, \alpha^3\}.$$

Analogno kao ranije, lako vidimo da je potrebno odrediti

$$\sigma\left(\sqrt{-2+\sqrt{2}}\right) = \sigma(\alpha).$$

Kako vrijedi

$$0 = \sigma(0) = \sigma(\alpha^4 + 4\alpha^2 + 2) = (\sigma(\alpha))^4 + 4(\sigma(\alpha))^2 + 2,$$

vidimo da je $\sigma(\alpha)$ nultočka polinoma f. Prema tome,

$$\operatorname{Gal}(L/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\},$$

gdje su

$$\sigma_1 = \left\{ \sqrt{-2+\sqrt{2}} \mapsto \sqrt{-2+\sqrt{2}}, \quad \sigma_2 = \left\{ \sqrt{-2+\sqrt{2}} \mapsto -\sqrt{-2+\sqrt{2}}, \right.\right.$$
$$\sigma_3 = \left\{ \sqrt{-2+\sqrt{2}} \mapsto \sqrt{-2-\sqrt{2}}, \quad \sigma_4 = \left\{ \sqrt{-2+\sqrt{2}} \mapsto -\sqrt{-2-\sqrt{2}}. \right.\right.$$

■

Zadatak 3.6.4. Odredite Galoisovu grupu polinoma $f(x) = x^4 + 6x^2 + 6$ nad poljem $\mathbb{Q}$.

Rješenje. Za vježbu. Uočite da je

$$\mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}\left(\sqrt{-3+\sqrt{3}}, \sqrt{-3-\sqrt{3}}\right) = \mathbb{Q}\left(\sqrt{-3+\sqrt{3}}, \sqrt{2}\right)$$

polje cijepanja polinoma f nad poljem $\mathbb{Q}$ te da je

$$\left[\mathbb{Q}\left(\sqrt{-3+\sqrt{3}}\right) : \mathbb{Q}\right] = 4,$$

a

$$\left[\mathbb{Q}\left(\sqrt{-3+\sqrt{3}}, \sqrt{2}\right) : \mathbb{Q}\left(\sqrt{-3+\sqrt{3}}\right)\right] = 2,$$

pa je

$$\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{-3+\sqrt{3}}, \sqrt{2}\right) \Big/ \mathbb{Q}\right) = \left[\mathbb{Q}\left(\sqrt{-3+\sqrt{3}}, \sqrt{2}\right) : \mathbb{Q}\right] = 2 \cdot 4 = 8. \qquad \square$$

Zadatak 3.6.5. Odredite Galoisovu grupu polinoma $f(x) = x^4 - 4x^2 + 10$ nad $\mathbb{Q}$. $\square$

Literatura

[1] P. Aluffi: *Algebra: Chapter 0*; American Mathematical Society, 2009

[2] J. A. Beachy, W. D. Blair: *Abstract algebra*; Waveland Press, Inc., 2006

[3] D. S. Dummit, R. M. Foote: *Abstract algebra*; John Wiley and Sons, Inc., 2004

[4] J. B. Fraleigh, V. Katz: *A first course in abstract algebra*; Pearson, 2003

[5] J. Gallian: *Contemporary abstract algebra*; Brooks/Cole, Cengage Learning, 2010

[6] L. Gilbert, J. Gilbert: *Elements of modern algebra*; Brooks/Cole, Cengage Learning, 2009

[7] T. W. Hungerford: *Algebra*; Springer-Verlag, 2003

[8] H. Kraljević: *Algebra, skripta*; Sveučilište J.J. Strossmayera u Osijeku, Odjel za matematiku, 2007

[9] S. Lang: *Algebra*; Springer-Verlag, 2005

[10] I. Matić: *Uvod u teoriju brojeva*; Sveučilište J.J. Strossmayera u Osijeku, Odjel za matematiku, 2015