Prsteni i polja

Definicija 1 *Neka je R neprazan skup, $a + i \cdot$ binarne operacije skupa R. Uređena trojka $(R, +, \cdot)$ je* ***prsten*** *ako je*

- $(R, +)$ *komutativna grupa;*
- $(R, \cdot)$ *je polugrupa (asocijativan grupoid);*
- *operacija $\cdot$ je distributivna u odnosu na operaciju $+$, tj. za sve $x, y, z \in R$ važe*

  leva distributivnost: $x(y+z) = xy + xz$,

  desna distributivnost: $(y+z)x = yx + zx$.

Definicija 2 *Prsten $(R, +, \cdot)$ je:*

- ***komutativan*** *ako je operacija $\cdot$ komutativna;*
- ***prsten sa jedinicom*** *ako postoji neutralni element za operaciju $\cdot$;*
- ***domen integriteta*** *(ili* ***integralni domen****) ako je komutativan prsten sa jedinicom u kome ne postoje delitelji nule, tj. u kome važi*

$$(a \neq 0 \wedge b \neq 0) \Rightarrow ab \neq 0,$$

  gde je sa 0 označena nula prstena, tj. neutralni element operacije $+$;
- ***polje*** *ako je prsten $(R, +, \cdot)$ u kojem je $(R \setminus \{0\}, \cdot)$ komutativna grupa.*

★ Uobičajeno je da se simbolom 0 označava nula prstena, a simbolom 1 jedinica prstena, ako postoji.

Tvrđenje 1 *Svako polje je domen integriteta. Svaki konačan domen integriteta je i polje, ali za beskonačne to ne mora da važi.*

Zadatak 1 *Koje od sledećih algebarskih struktura su prsteni, domeni integriteta ili polja?*

1. $(\mathbb{N}, +, \cdot)$ 2. $(\mathbb{Z}, +, \cdot)$ 3. $(\{3k \mid k \in \mathbb{Z}\}, +, \cdot)$ 4. $(\mathbb{Q}, +, \cdot)$ 5. $(\mathbb{R} \setminus \{0\}, +, \cdot)$
6. $(\mathbb{C}, +, \cdot)$ 7. $(\mathbb{Z}_6, +, \cdot)$ 8. $(\mathbb{Z}_7, +, \cdot)$ 9. $(\mathbb{Z}_n, +, \cdot)$ 10. $(\mathbb{Z}_6 \setminus \{0\}, +, \cdot)$

Rešenje:

1. nije prsten jer $(\mathbb{N}, +)$ nije grupa;
2. prsten i domen integriteta, nije polje jer $(\mathbb{Z} \setminus \{0\}, \cdot)$ nije grupa;
3. prsten, nije domen interiteta jer nema jedinicu;
4. polje;
5. nije prsten jer $(\mathbb{R} \setminus \{0\}, +)$ nije ni grupoid;
6. polje;
7. komutativan prsten sa jedinicom, nije domen integriteta jer ima delitelje nule;
8. domen integriteta, pa samim tim i polje (jer je konačan, vidi Tvrđenje 1);

9. komutativan prsten sa jedinicom za svako n, polje ako i samo ako je n prost broj;
10. nije prsten jer $(\mathbb{Z}_6 \setminus \{0\}, +)$ nije ni grupoid.

□

★ Komutativan prsten sa jedinicom $(\mathbb{Z}_n, +, \cdot)$ je polje ako i samo ako je n prost broj.

Zadatak 2 *U skupu $\mathbb{Z}^2$ definisane su operacije $\oplus$ i $\star$ sa $\forall (a,b),(c,d) \in \mathbb{Z}^2$*

$$(a,b) \oplus (c,d) = (a+c, b+d) \quad i \quad (a,b) \star (c,d) = (a \cdot c, b \cdot d).$$

(*a*) *Dokazati da je $\left(\mathbb{Z}^2, \oplus, \star\right)$ komutativan prsten sa jedinicom.*

(*b*) *Ispitati da li je $\left(\mathbb{Z}^2, \oplus, \star\right)$ domen integriteta.*

(*c*) *Ispitati da li je $\left(\mathbb{Z}^2, \oplus, \star\right)$ polje.*

Rešenje:

(*a*) Da bi dokazali da je $\left(\mathbb{Z}^2, \oplus, \star\right)$ komutativan prsten sa jedinicom treba da pokažemo:

– $\left(\mathbb{Z}^2, \oplus\right)$ je Abelova grupa.

zatvorenost: Treba pokazati da za svaka dva (a,b) i (c,d) elementa skupa $\mathbb{Z}^2$ važi

$$(a,b) \oplus (c,d) \in \mathbb{Z}^2.$$

Ako su $(a,b),(c,d) \in \mathbb{Z}^2$, to znači da su $a,b,c,d \in \mathbb{Z}$. Pošto važi zatvorenost sabiranja celih brojeva, sledi da su i $a+c, b+d \in \mathbb{Z}$, odakle je $(a,b) \oplus (c,d) = (a+c, b+d) \in \mathbb{Z}^2$.

asocijativnost: Treba pokazati da za svaka tri $(a,b),(c,d)$ i (e,f) elementa skupa $\mathbb{Z}^2$ važi

$$\big((a,b) \oplus (c,d)\big) \oplus (e,f) = (a,b) \oplus \big((c,d) \oplus (e,f)\big).$$

Ovo sledi direktno iz asocijativnosti sabiranja celih brojeva:

$$\begin{aligned} \big((a,b) \oplus (c,d)\big) \oplus (e,f) &= (a+c, b+d) \oplus (e,f) \\ &= ((a+c)+e, (b+d)+f) \\ &= (a+(c+e), b+(d+f)) \\ &= (a,b) \oplus (c+e, d+f) \\ &= (a,b) \oplus \big((c,d) \oplus (e,f)\big). \end{aligned}$$

neutralni element Treba pokazati da postoji $(e_1, e_2) \in \mathbb{Z}^2$ takav da za svaki $(a,b) \in \mathbb{Z}^2$ važi

$$(e_1, e_2) \oplus (a,b) = (a,b) \oplus (e_1, e_2) = (a,b).$$

Po definiciji operacije $\oplus$, poslednje jednakosti su tačne za $e_1 = e_2 = 0$, pa je neutralni element $(e_1, e_2) = (0,0)$.

inverzni elementi: Treba pokazati da za svaki $(a,b) \in \mathbb{Z}^2$ postoji $(a',b') \in \mathbb{Z}^2$ takav da važi

$$(a,b) \oplus (a',b') = (a',b') \oplus (a,b) = (0,0).$$

Rešavanjem poslednje jednačine po a' i b' dobijamo $a' = -a$ i $b' = -b$. Odavde zaključujemo da je za (a,b) inverzni element $(-a,-b)$, koji takođe pripada skupu $\mathbb{Z}^2$ jer iz $a,b \in \mathbb{Z}$ sledi $-a,-b \in \mathbb{Z}$.

komutativnost: Treba pokazati da za svaka dva $(a,b),(c,d) \in \mathbb{Z}^2$ važi

$$(a,b) \oplus (c,d) = (c,d) \oplus (a,b).$$

Ovo sledi direktno iz komutativnosti sabiranja celih brojeva:

$$(a,b) \oplus (c,d) = (a+c, b+d) = (c+a, d+b) = (c,d) \oplus (a,b).$$

– $\left(\mathbb{Z}^2, \star\right)$ je komutativan monoid.

zatvorenost: Za svaka dva $(a,b),(c,d) \in \mathbb{Z}^2$ imamo da važi

$$(a,b) \star (c,d) = (a \cdot c, b \cdot d) \in \mathbb{Z}^2,$$

jer ako su $a,b,c,d \in \mathbb{Z}$ onda su i $a \cdot c, b \cdot d \in \mathbb{Z}$.

asocijativnost: Sledi direktno iz asocijativnosti množenja celih brojeva, a dokaz je analogan dokazu asocijativnosti operacije $\oplus$.

neutralni element: Treba pokazati da postoji $(e',e'') \in \mathbb{Z}^2$ takav da za svaki $(a,b) \in \mathbb{Z}^2$ važi

$$(e',e'') \star (a,b) = (a,b) \star (e',e'') = (a,b).$$

Odavde je neutralni element $(e',e'') = (1,1) \in \mathbb{Z}^2$.

komutativnost: Sledi direktno iz komutativnosti množenja celih brojeva, a dokaz je analogan dokazu komutativnosti operacije $\oplus$.

– distributivnost operacije $\star$ prema $\oplus$. Treba pokazati da za svaka tri $(a,b),(c,d),(e,f) \in \mathbb{Z}^2$ važi

leva distributivnost: $(a,b) \star \big((c,d) \oplus (e,f)\big) = \big((a,b) \star (c,d)\big) \oplus \big((a,b) \star (e,f)\big)$,

desna distributivnost: $\big((c,d) \oplus (e,f)\big) \star (a,b) = \big((c,d) \star (a,b)\big) \oplus \big((e,f) \star (a,b)\big)$.

Leva distributivnost sledi direktno iz leve distributivnosti množenja prema sabiranju celih brojeva:

$$\begin{aligned}
(a,b) \star \big((c,d) \oplus (e,f)\big) &= (a,b) \star (c+e, d+f) \\
&= (a \cdot (c+e), b \cdot (d+f)) \\
&= (ac+ae, bd+bf) \\
&= (ac,bd) \oplus (ae,bf) \\
&= \big((a,b) \star (c,d)\big) \oplus \big((a,b) \star (e,f)\big).
\end{aligned}$$

Desna distributivnost sledi iz leve i komutativnosti operacije $\star$.

(*b*) Da bi $\left(\mathbb{Z}^2, \oplus, \star\right)$ bio domen integriteta potrebno je još da dokažemo da nema delitelje nule, tj. da za svaka dva $(a,b),(c,d) \in \mathbb{Z}^2$ različita od nula elementa $(0,0)$ (neutralnog elementa u odnosu na operaciju $\oplus$) važi $(a,b) \star (c,d) \neq (0,0)$. Ova osobina nije ispunjena, jer, recimo, imamo $(1,0) \star (0,1) = (0,0)$. Dakle, $\left(\mathbb{Z}^2, \oplus, \star\right)$ nije domen integriteta jer ima delitelje nule.

(*c*) Kontrapozicijom Tvrđenja 1 dobijamo da $\left(\mathbb{Z}^2, \oplus, \star\right)$ nije polje jer nije domen integriteta.

□

Zadatak 3 *Koje od sledećih algebarskih struktura su prsteni?*

1. $(\mathbb{N}, +, \cdot)$ 2. $(\mathbb{Z}, +, \cdot)$ 3. $(\mathbb{Z} \setminus \{1\}, +, \cdot)$ 4. $(\mathbb{Q}, +, \cdot)$
5. $(\mathbb{C}, +, \cdot)$ 6. $(\mathbb{C} \setminus \{0\}, +, \cdot)$ 7. $(\mathbb{Z}_4, +, \cdot)$ 8. $(\mathbb{Z}_3, +, \cdot)$
9. $(\mathbb{R}[t], +, \cdot)$ 10. $(\mathbb{R} \setminus \{0\}, \cdot, +)$ 11. $\left(\mathbb{R}^{\mathbb{R}}, +, \circ\right)$

Rešenje:

1. NE: $(\mathbb{N}, +)$ nije grupa; 2. DA; 3. NE: + nije zatvorena, npr. $2 + (-1) = 1$;
4. DA; 5. DA; 6. NE: + nije zatvorena, npr. $1 + (-1) = 0$; 7. DA;
8. DA; 9. DA; 10. NE: ne važi distributivnost + prema $\cdot$;
11. NE: ne važi distributivnost, npr. za $f(x) = \sin x$ i $g(x) = h(x) = x$ imamo

$$\begin{aligned} (f \circ (g + h))(x) &= f(g(x) + h(x)) = \sin 2x \quad \text{i} \\ ((f \circ g) + (f \circ h))(x) &= f(g(x)) + f(h(x)) = 2 \sin x. \end{aligned}$$

□

Zadatak 4 *Koje od sledećih algebarskih struktura su domeni integriteta?*

1. $(\mathbb{Z}, +, \cdot)$ 2. $(\mathbb{Z}, \cdot, +)$ 3. $(\mathbb{Q}^+, +, \cdot)$ 4. $(\mathbb{Z}_3, +, \cdot)$
5. $(\mathbb{Z}_4, +, \cdot)$ 6. $(\mathbb{Z}_4 \setminus \{0\}, +, \cdot)$ 7. $(\mathbb{R}[t], +, \cdot)$ 8. $(\mathbb{Q}, +, \cdot)$
9. $(\{-1, 0, 1\}, +, \cdot)$ 10. $(\mathbb{R}, +, \cdot)$ 11. $(\mathbb{Q} \setminus \{0\}, +, \cdot)$ 12. $((-1, 1), +, \cdot)$
13. $(\mathcal{M}_{2\times 2}, +, \cdot)$,

ako je $\mathcal{M}_{2\times 2}$ *skup svih kvadratnih matrica nad* $\mathbb{R}$ *reda* 2.

Rešenje:

1. DA; 2. NE: $(\mathbb{Z}, \cdot)$ nije grupa; 3. NE: $(\mathbb{Q}^+, +)$ nije grupa; 4. DA;
5. NE: ima delitelje nule $(2 \cdot 2 = 0)$; 6. NE: $(\mathbb{Z}_4 \setminus \{0\}, +)$ nije grupoid;
7. DA; 8. DA; 9. NE: $(\{-1, 0, 1\}, +)$ nije grupoid; 10. DA;
11. NE: $(\mathbb{Q} \setminus \{0\}, +)$ nije grupoid; 12. NE: $((-1, 1), +)$ nije grupoid;
13. NE: ne važi komutativnost.

□

Zadatak 5 *Koje od sledećih algebarskih struktura su komutativni prsteni?*

1. $(\mathbb{Z}, +, \cdot)$ 2. $(\mathbb{Z}_4, +, \cdot)$ 3. $(\mathbb{Q}, +, \cdot)$ 4. $(\mathbb{Z}_3, +, \cdot)$
5. $(\mathbb{N}, +, \cdot)$ 6. $(\mathbb{R}[t], +, \cdot)$ 7. $(\mathbb{R}^+, +, \cdot)$

Rešenje:

1. DA; 2. DA; 3. DA; 4. DA; 5. NE: $(\mathbb{N}, +)$ nije grupa;
6. DA; 7. NE: $(\mathbb{R}^+, +)$ nije grupa.

□

Zadatak 6 *Koje od sledećih algebarskih struktura su polja?*

1. $(\mathbb{Z}_4,+,\cdot)$ 2. $(\mathbb{Z}_4\setminus\{0\},+,\cdot)$ 3. $(\mathbb{Z}_3,+,\cdot)$ 4. $(\mathbb{R}[t],+,\cdot)$
5. $(\mathsf{V},+,\cdot)$ 6. $\left(\{\rho e^{i\theta}\,|\,\rho\in[0,\infty),\theta\in\mathbb{R}\},+,\cdot\right)$ 7. $(\mathbb{R},+,\cdot)$ 8. $(\mathbb{C},+,\cdot)$
9. $(\mathbb{Q},+,\cdot)$ 10. $\left(\{e^{i\theta}\,|\,\theta\in\mathbb{R}\},+,\cdot\right)$

gde je V *skup svih slobodnih vektora.*

Rešenje:

1. NE: nije domen integriteta; 2. NE: nije ni prsten; 3. DA;
4. NE: nema inverzne elemente; 5. NE: operacija $\cdot$ nije binarna operacija skupa V;
6. DA: ovo je polje kompleksnih bojeva; 7. DA; 8. DA; 9. DA;
10. NE: recimo, za $\theta=0$ imamo $e^{i\cdot 0}+e^{i\cdot 0}=2$, a 2 ne pripada datom skupu.

□

Zadatak 7 *Koje od sledećih algebarskih struktura su prsteni, a nisu polja?*

1. $(\mathbb{Z},+,\cdot)$ 2. $(\mathbb{Z}_4,+,\cdot)$ 3. $(\mathbb{Q},+,\cdot)$ 4. $(\mathbb{Z}_3,+,\cdot)$
5. $(\mathbb{N},+,\cdot)$ 6. $(\mathbb{C},+,\cdot)$ 7. $(\mathbb{R}[t],+,\cdot)$ 8. $((0,\infty),+,\cdot)$

Rešenje:

1. DA: domen integriteta i nije polje; 2. DA: prsten i nije domen integriteta (a ni polje);
3. NE: polje; 4. NE: polje; 5. NE: nije prsten; 6. NE: polje;
7. DA: domen integriteta i nije polje; 8. NE: nije prsten. □

Zadatak 8 *U skupu* $\mathbb{R}^2$ *definisane su operacije* $\oplus$ *i* $\otimes$ *sa* $\forall(a,b),(c,d)\in\mathbb{R}^2$

$$(a,b)\oplus(c,d)=(a+c,b+d)\quad i\quad (a,b)\otimes(c,d)=(ac-bd,bc+ad).$$

Dokazati da je $\left(\mathbb{R}^2,\oplus,\otimes\right)$ *polje i da je ono izomorfno polju kompleksnih brojeva* $(\mathbb{C},+,\cdot)$.

Zadatak 9 *Neka je* $\mathbf{A}=(A,+)$ *proizvoljna Abelova (tj. komutativna) grupa, neka je*

$$\mathcal{F}=\{f:A\to A\mid f\text{ je homomorfizam}\},$$

i neka je $\oplus$ *binarna operacija skupa* $\mathcal{F}$ *definisana sa*

$$(f\oplus g)(x)=f(x)+g(x),x\in A,$$

za sve $f,g\in\mathcal{F}$. *Dokazati da je* $\mathbf{F}=(\mathcal{F},\oplus,\circ)$ *prsten sa jedinicom.*

Rešenje: Proveravamo redom aksiome.

(a) $(\mathcal{F},\oplus)$ je Abelova grupa.

zatvorenost: neka je $f,g\in\mathcal{F}$; očigledno je $f\oplus g:A\to A$, a pošto za sve $x,y\in A$ važi

$$\begin{aligned}(f\oplus g)(x+y)&=f(x+y)+g(x+y)\\&=(f(x)+f(y))+(g(x)+g(y))\\&=(f(x)+g(x))+(f(y)+g(y))\\&=(f\oplus g)(x)+(f\oplus g)(y),\end{aligned}$$

sledi da je $f\oplus g$ i homomorfizam grupe A, tj. $f\oplus g\in\mathcal{F}$.

asocijativnost: sledi iz asocijativnosti operacije +; naime, za proizvoljne $f, g, h \in \mathcal{F}$ važi da je za svako $x \in A$

$$\begin{aligned}(f \oplus (g \oplus h))(x) &= f(x) + (g \oplus h)(x) \\ &= f(x) + (g(x) + h(x)) \\ &= (f(x) + g(x)) + h(x) \\ &= (f \oplus g)(x) + h(x) \\ &= ((f \oplus g) \oplus h)(x),\end{aligned}$$

odakle sledi $(f \oplus (g \oplus h)) = ((f \oplus g) \oplus h)$.

neutralni element: je funkcija $\mathbb{O}(x) = 0$, $x \in A$, gde je sa 0 označen neutralni element operacije +. Važi $\mathbb{O} \in \mathcal{F}$ jer $\mathbb{O} : A \to A$ i $\mathbb{O}$ je homomorfizam jer je za sve $x, y \in A$

$$\mathbb{O}(x + y) = 0 = 0 + 0 = \mathbb{O}(x) + \mathbb{O}(y).$$

inverzni elementi: označimo sa $-x$ inverzni element elementa $x \in A$ u grupi $\mathbf{A}$. Za $f \in \mathcal{F}$ je inverzni element funkcija $f' \in \mathcal{F}$ definisana sa $f'(x) = -f(x)$, $x \in A$. Naime, imamo da je

$$(f' \oplus f)(x) = -f(x) \oplus f(x) = 0 = \mathbb{O}(x) = (f \oplus f')(x).$$

Takođe, f' je homomorfizam jer za sve $x, y \in A$ važi

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

komutativnost: sledi iz komutativnosti operacije +. Naime, za proizvoljne $f, g \in \mathcal{F}$ važi da je za svako $x \in A$

$$(f \oplus g)(x) = f(x) + g(x) = g(x) + f(x) = (g \oplus f)(x),$$

odakle sledi $(f \oplus g) = (g \oplus f)$.

(b) $(\mathcal{F}, \circ)$ je monoid (polugrupa sa neutralnim elementom).

zatvorenost: neka je $f, g \in \mathcal{F}$; očigledno je $f \circ g : A \to A$, a pošto za sve $x, y \in A$ važi

$$\begin{aligned}(f \circ g)(x + y) &= f(g(x + y)) \\ &= f(g(x) + g(y)) \\ &= f(g(x)) + f(g(y)) \\ &= (f \circ g)(x) + (f \circ g)(y),\end{aligned}$$

sledi da je $f \circ g$ i homomorfizam grupe A, te sledi $f \circ g \in \mathcal{F}$.

asocijativnost: kompozicija funkcija je uvek asocijativna operacija.

neutralni element: je identička funkcija $i_A \in \mathcal{F}$ skupa A koja jeste homomorfizam jer za sve $x, y \in A$ važi

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

(c) distributivnost: $\circ$ prema $\oplus$.

(l) Za sve $f, g, h \in \mathcal{F}$ i svako $x \in A$ važi

$$\begin{aligned}(f \circ (g \oplus h))(x) &= f((g \oplus h)(x)) \\ &= f(g(x) + h(x)) \\ &= f(g(x)) + f(h(x)) \\ &= (f \circ g)(x) + (f \circ h)(x) \\ &= ((f \circ g) \oplus (f \circ h))(x),\end{aligned}$$

odakle sledi $(f \circ (g \oplus h))x = ((f \circ g) \oplus (f \circ h))$.

(d) Za sve $f, g, h \in \mathcal{F}$ i svako $x \in A$ važi

$$\begin{aligned}((g \oplus h) \circ f)(x) &= (g \oplus h)(f(x)) \\ &= g(f(x)) + h(f(x)) \\ &= (g \circ f)(x) + (h \circ f)(x) \\ &= ((g \circ f) \oplus (h \circ f))(x),\end{aligned}$$

odakle sledi $(g \oplus h) \circ f = (g \circ f) \oplus (g \circ f)$. □