Prsteni i polja

October 25, 2021

ово није скуп реалних бројева

Neka je R neprazan skup, a $+$ i $\cdot$ binarne operacija skupa R. Uređena trojka $(R, +, \cdot)$ je **prsten** ako je ово нису сабирање и множење

1. $(R, +)$ komutativna grupa,
2. $(R, \cdot)$ polugrupa (asocijativan grupoid),
3. operacija $\cdot$ je distributivna u odnosu na operaciju $+$, tj. za svako $x, y, z \in R$ važi

   leva distributivnost: $x \cdot (y + z) = x \cdot y + x \cdot z$,

   desna distributivnost: $(y + z) \cdot x = y \cdot x + z \cdot x$.

Napomena: Ako je operacija $\cdot$ komutativna dovoljno je proveriti samo jednu, npr. levu distributivnost jer iz nje i komutativnosti sledi i desna distributivnost. Inače se moraju proveravati obe distributivnosti.

Neutralni element operacije $+$, ako postoji, naziva se nula prstena i obično se označava sa 0, a neutralni element operacije $\cdot$, ako postoji, naziva se jedinica prstena i obično se označava sa 1.

$(A, *, \circ)$ je prsten ako

1, $(A, *)$ je komutativna grupa

2, $(A, \circ)$ je polugrupa

3, $\forall x, y, z \in A$

$x \circ (y * z) = (x \circ y) * (x \circ z)$

$(y * z) \circ x = (y \circ x) * (z \circ x)$

Prsten $(R, +, \cdot)$ je:

- **prsten sa jedinicom** ako postoji neutralni elemenat multiplikativne operacije $\cdot$;
- **komutativan prsten** ako je operacija $\cdot$ komutativna;
- **domen integriteta** ako je komutativan prsten sa jedinicom (koja mora biti različita od nule prstena) u kome ne postoje delitelji nule, tj. u kome važi

$$a \cdot b = 0 \Longrightarrow a = 0 \lor b = 0 \quad \text{ili} \quad a \neq 0 \land b \neq 0 \Longrightarrow a \cdot b \neq 0.$$

неутрални елементи за операције $+$, $\cdot$

- **polje** ako je $(R \setminus \{0\}, \cdot)$ komutativna grupa. нула прстена

Svako polje je domen integriteta.

Svaki konačan domen integriteta je polje, ali za beskonačne to ne mora da važi.

$(R, \oplus, \odot)$

U prstenu $(R, \oplus, \odot)$ za sve $a, b \in R$ važi:

- $a \odot 0 = 0 \odot a = 0$;
- $(-a) \odot b = a \odot (-b) = -(a \odot b)$;
- $(-a) \odot (-b) = a \odot b$.

0 је неутрални елемент за операцију + није број 0

$+$ није сабирање

$\cdot$ није множење

$(-a)$ - ознака за инверзни елемент елемента a за операцију $+$

① $(\mathbb{Z}, +, \cdot)$

✗ $(\mathbb{Z}, \cdot, +)$

Primer:

	prsten	domen integriteta	polje
$(\mathbb{N}, +, \cdot)$	$-$ nema n.e.	/	/
$(\mathbb{Z}, +, \cdot)$	$+$	$+$	$-$ nema inverzni za $\cdot$
$(\mathbb{Q}, +, \cdot)$	$+$	$+$	$+$
$(\mathbb{R}, +, \cdot)$	$+$	$+$	$+$
$(\mathbb{C}, +, \cdot)$	$+$	$+$	$+$
$(A, +, \cdot)$	$+$	$-$ nema jedinicu	$-$ nema inverzni za $\cdot$

$A = \{3k \mid k \in \mathbb{Z}\}$

$(\mathbb{Z}, +)$ - jeste Abelova grupa

$(\mathbb{Z}, \cdot)$ - jeste polugrupa

$\forall x, y, z \in \mathbb{Z}, \quad x(y+z) = xy + xz$

$(y+z)x = yx + zx$

$(\mathbb{Z}, +, \cdot)$ jeste prsten

$(\mathbb{Z}, +, \cdot)$ je prsten

$(\mathbb{Z} \setminus \{0\}, \cdot)$ je Abelova grupa?

Nema svaki el. $\cdot$ inverzni $2 \cdot \square = 1$?

$\Rightarrow$ nije grupa $\rightarrow$ $(\mathbb{Z}, +, \cdot)$ nije polje

$(\mathbb{Z}, +, \cdot)$ jeste prsten

$\cdot$ je komutativno

$\forall x, y \in \mathbb{Z}, \ x \cdot y = y \cdot x$

1 je neutralni el. za $\cdot$

$x \cdot y = 0 \Rightarrow x = 0 \lor y = 0$

$\Rightarrow$ $(\mathbb{Z}, +, \cdot)$ domen integriteta

$(A,+,\cdot)$, $A=\{3k \mid k\in\mathbb{Z}\}=\{0,\pm3,\pm6,\pm9,\pm12,\dots\}$

I DA LI JE $(A,+,\cdot)$ PRSTEN? ✓ $(A,+,\cdot)$ jeste prsten

1) $(A,+)$ ABELOVA GRUPA? ✓

1° $(A,+)$ - ZATVORENOST? ✓

2° $(A,+)$ ASOCIJATIVNOST? ✓

3° $(A,+)$ LEVI NEUTRALNI EL? ✓

4° $(A,+)$ LEVI INVERZNI EL? ✓

5° $(A,+)$ KOMUTATIVNOST? ✓

$x,y\in A \Rightarrow x=3k_1,\ y=3k_2,\ k_1,k_2\in\mathbb{Z}$

$x+y=3k_1+3k_2=3\cdot(\underbrace{k_1+k_2}_{\in\mathbb{Z}})\in A$

$0\in A?$ $0=3\cdot0\in A$

$x\in A \Rightarrow x=3k,\ k\in\mathbb{Z}$

$0+x=0+3k=3k=x$

0 je neutralni element za +

$x\in A \Rightarrow x=3k,\ k\in\mathbb{Z}$

$\boxed{-3k}+3k=0$?

Samo je ostalo da li $-3k\in A$

$-3k=3\cdot(\underbrace{-k}_{\in\mathbb{Z}})\in A$

2) $(A,\cdot)$ POLUGRUPA?

1) $(A,\cdot)$ - ZATVORENOST? ✓

2) $(A,\cdot)$ ASOCIJATIVNOST? ✓

$x,y\in A \Rightarrow x=3k_1,\ y=3k_2,\ k_1,k_2\in\mathbb{Z}$

$x\cdot y=3k_1\cdot3k_2=3(\underbrace{3k_1\cdot k_2}_{\in\mathbb{Z}})\in A$

3) DISTRIBUTIVNOST ✓

$\forall x,y,z\in A$

$x(y+z)=xy+xz$

$(y+z)x=yx+zx$

II DA LI JE $(A,+,\cdot)$ DOMEN INTEGRITETA?

1) $\cdot$ TREBA DA JE KOMUTATIVNO

2) TREBA DA POSTOJI NEUTRALNI EL. U ODNOSU NA OPERACIJU $\cdot$ ← PROBLEM

$1\notin A$ jer $1\neq3\cdot k,\ k\in\mathbb{Z}$

3) $x\cdot y=0 \Rightarrow x=0 \vee y=0$

$(A,+,\cdot)$ NIJE DI

DA LI JE $(A, +, \cdot)$ POLJE ? nije jer svako polje mora biti DI

Prsten (polje) $\mathcal{R}_1 = (R_1, +, \cdot)$ je **potprsten** (**potpolje**) prstena (polja) $\mathcal{R} = (R, +, \cdot)$ ako je R_1 neprazan podskup od R, a operacije $+$ i $\cdot$ iz R_1 su restrikcije operacija $+$ i $\cdot$ iz R.

Neka su $\mathcal{R}_1 = (R_1, +_1, \cdot_1)$ i $\mathcal{R}_2 = (R_2, +_2, \cdot_2)$ prsteni (polja). Funkcija $f : R_1 \longrightarrow R_2$ je **homomorfizam** iz $\mathcal{R}_1$ u $\mathcal{R}_2$ ako za sve $x, y \in R_1$ važi

$$f(x +_1 y) = f(x) +_2 f(y) \quad \text{i} \quad f(x \cdot_1 y) = f(x) \cdot_2 f(y).$$

Ako je funkcija f još i bijekcija, tada se ona naziva **izomorfizam**.

$$\left.\begin{array}{l} (G, *) \text{ - grupoid} \\ (H, \circ) \text{ - grupoid} \\ \emptyset \neq H \subseteq G \end{array}\right\}$$

$(H, \circ)$ je podgrupoid od $(G, *)$

$(G, *)$, $(H, \circ)$ - grupoidi

$f : G \to H$ - bijekcija

$f(x * y) = f(x) \circ f(y) \quad \forall x, y \in G$

$\Rightarrow f$ izomorfizam