PRSTENI I POLJA

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

(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.

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

$$a \cdot b = 0 \Longrightarrow a = 0 \ \vee \ b = 0 \quad \text{ili} \quad a \neq 0 \ \wedge \ b \neq 0 \Longrightarrow a \cdot b \neq 0.$$

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

Svako polje je domen integriteta.

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

U prstenu $(R, +, \cdot)$ za sve $a, b \in R$ važi:

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

Primer:

	prsten	domen integriteta	polje
$(\mathbb{N}, +, \cdot)$	$-$, nema neutralni elemenat	/	/
$(\mathbb{Z}, +, \cdot)$	$+$	$+$	$-$, $(Z \setminus \{0\}, \cdot)$ nema svaki elemenat inverzni
$(\mathbb{Q}, +, \cdot)$	$+$	$+$	$+$
$(\mathbb{R}, +, \cdot)$	$+$	$+$	$+$
$(\mathbb{C}, +, \cdot)$	$+$	$+$	$+$
$(\{3k \mid k \in \mathbb{Z}\}, +, \cdot)$	$+$	$-$, nema jedinicu	$-$, $(\{3k \mid k \in \mathbb{Z}\} \setminus \{0\}, \cdot)$ nema svaki elemenat inverzni

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**.

ZADACI

(1) Ispitati da li je $(\{a,b,c\},+,\cdot)$ prsten, ako su operacije $+$ i $\cdot$ date tablicama

$+$	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

i

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

.

(2) Dokazati da je $(\mathbb{Q},\oplus,\odot)$ polje, ako su operacije $\oplus$ i $\odot$ definisane sa

$$\forall\, a,b\in\mathbb{Q},\ a\oplus b=a+b+1,$$
$$\forall\, a,b\in\mathbb{Q},\ a\odot b=a+b+ab.$$

(3) Neka su na $A=\{(a,1)\mid a\in\mathbb{R}\}$ definisane sledeće binarne operacije:

$$\forall\ (a,1),(b,1)\in A,\ (a,1)\oplus(b,1)=(a+b,1),$$
$$\forall\ (a,1),(b,1)\in A,\ (a,1)\odot(b,1)=(ab+a+b,1).$$

Ispitati da li je $(A,\oplus,\odot)$ prsten.

ZA VEŽBU:
- IZ SKRIPTE Zadatak 7.1, 7.2, 7.6, 7.7;
- 1. Na skupu $A=\{(x,y)\mid x,y\in\mathbb{R}\}$ definisane su operacije

$$\forall\ (a,b),(c,d)\in A,\ (a,b)\oplus(c,d)=(a+c,b+d),$$
$$\forall\ (a,b),(c,d)\in A,\ (a,b)\odot(c,d)=(ac,bd).$$

Dokazati da je $(A,\oplus,\odot)$ komutativan prsten sa jedinicom.