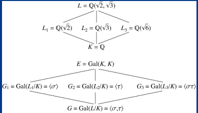

Algebra

Vježbe 7

19.4.2023.

predavač: prof.dr.sc. I.Matić

asistent: dr.sc. Darija Brajković Zorić

PRSTENI - Definicija i osnovni primjeri

Definicija

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>U netrivijalnom je unitalnom prstenu $1 \neq 0$.</u>

Propozicija

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

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

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

Primjer 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 4

Neka je R prsten. Tada je

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

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

<u>prsten polinoma u jednoj varijabli s koeficijentima iz prstena R</u>.

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.

Zadatak 1

Pokažite da je $\mathbb{Z}$, uz binarne 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.

Zadatak 2

Neka su binarne 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) $(\mathbb{Z}, +, \odot)$. □

Potprsteni

Definicija

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

Teorem

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 1

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

Primjer 2

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

Zadatak 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.

Zadatak 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.

Zadatak 3

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

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

Zadatak 4

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

Zadatak 5

Ispitajte je li $\mathbb{Q}$, uz binarne operacije zbrajanja definiranog s

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

i standardnog množenja racionalnih brojeva, prsten.

Zadatak 6

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

Zadatak 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.

Zadatak 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.