Algebra

Ivan Prokić

Fakultet tehničkih nauka, Novi Sad

Predavanje 9

Na prethodnom času

- Ciklične grupe
- Homomorfizmi i izomorfizmi
- Kejlijeva teorema o reprezentaciji grupa
- Kongruencije
- Grupa $(\mathbb{Z}_n, +)$ i komutativan monoid $(\mathbb{Z}_n, \cdot)$

Prsten, domen integriteta i polje

Rešavanje jednačina: sa $+$ i $\cdot$

Reši jednačinu $2x + 4 = 3$.

Rešavanje jednačina: sa $+$ i $\cdot$

Reši jednačinu $2x + 4 = 3$.

U kom skupu?

Rešavanje jednačina: sa $+$ i $\cdot$

Reši jednačinu $2x + 4 = 3$. **U kom skupu?**

U $(\mathbb{N}, +, \cdot)$:

$$
\begin{aligned}
2x + 4 &= 3 \\
(2x + 4) + (-4) &= 2 + (-4) && \text{Ovo nije prirodan broj! Probajmo sa celim.} \\
2x &= -1 && \text{Isto kao na prošlom predavanju} \\
2^{-1} \cdot (2 \cdot x) &= 2^{-1}(-1) && \text{Ovo nije ceo broj! Probajmo sa racionalnim.} \\
x &= \frac{-1}{2} && \text{Isto kao na prošlom predavanju}
\end{aligned}
$$

U $(\mathbb{N}, +, \cdot)$ nema rešenja, nema ni u $(\mathbb{Z}, +, \cdot)$, ali u $(\mathbb{Q}, +, \cdot)$ ima i to je $x = \frac{-1}{2}$.

Prsten

Definicija (Prsten)

Neka je $R \neq \emptyset$. *Tada je* $(R, +, \cdot)$ *prsten ako važi*

1. $(R, +)$ *je Abelova grupa;*
2. $(R, \cdot)$ *je polugrupa;*
3. **distributivnost** $\cdot$ **prema** $+$**:** *za sve* $x, y, z \in R$ *važi* $x(y+z) = xy + xz$ *i* $(y+z)x = yx + zx$.

Napomena

Primeti aditivnu i multiplikativnu notaciju: Za prvu operaciju $+$ *pišemo* 0 *za neutralni element i zovemo ga* **nula**, $-x$ *je inverzni od* x, $1x = x$ *i* $(n+1)x = nx + x$, $0x = 0$ *i* $(-n)x = n(-x)$, *pa imamo da važi i* $-(nx) = (-n)x = n(-x)$

Primer

Prsteni su: $(\{0\}, +, \cdot), (\mathbb{Z}, +, \cdot), (\mathbb{Z}_3, +, \cdot), (\mathbb{Z}_4, +, \cdot)$, *a, recimo,* $(\mathbb{N}, +, \cdot)$ *nije prsten.*

Prsten, domen integriteta i polje

Definicija

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

1. **sa jedinicom** *ako postoji neutralni element u odnosu na operaciju* $\cdot$
2. **komutativan** *ako je operacija* $\cdot$ *komutativna*
3. **domen integriteta** *ako je komutativan prsten sa jedinicom bez delitelja nule, tj. za sve* $x, y \in R$ *važi*
$$x \cdot y = 0 \;\Rightarrow\; (x = 0 \vee y = 0)$$
4. **polje** *ako je* $(R \setminus \{0\}, \cdot)$ *Abelova grupa.*

Primeri

Od sledećih struktura zaokruži slovo ispred

prstena:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

domena integriteta:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

polja:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

Primeri

Od sledećih struktura zaokruži slovo ispred

prstena:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

domena integriteta:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

polja:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

Primeri

Od sledećih struktura zaokruži slovo ispred

prstena:

(a) $(\mathbb{N}, +, \cdot)$

(b) $(\mathbb{Z}, +, \cdot)$

(c) $(\mathbb{Z}_3, +, \cdot)$

(d) $(\mathbb{Z}_4, +, \cdot)$

(e) $(\mathbb{Q}, +, \cdot)$

(f) $(\mathbb{R}, +, \cdot)$

domena integriteta:

(a) $(\mathbb{N}, +, \cdot)$

(b) $(\mathbb{Z}, +, \cdot)$

(c) $(\mathbb{Z}_3, +, \cdot)$

(d) $(\mathbb{Z}_4, +, \cdot)$

(e) $(\mathbb{Q}, +, \cdot)$

(f) $(\mathbb{R}, +, \cdot)$

polja:

(a) $(\mathbb{N}, +, \cdot)$

(b) $(\mathbb{Z}, +, \cdot)$

(c) $(\mathbb{Z}_3, +, \cdot)$

(d) $(\mathbb{Z}_4, +, \cdot)$

(e) $(\mathbb{Q}, +, \cdot)$

(f) $(\mathbb{R}, +, \cdot)$

Primeri

Od sledećih struktura zaokruži slovo ispred

prstena:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

domena integriteta:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

polja:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

Primeri

Od sledećih struktura zaokruži slovo ispred

prstena:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

domena integriteta:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

polja:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

Primeri

Od sledećih struktura zaokruži slovo ispred

prstena:

(a) $(\mathbb{N}, +, \cdot)$

(b) $(\mathbb{Z}, +, \cdot)$

(c) $(\mathbb{Z}_3, +, \cdot)$

(d) $(\mathbb{Z}_4, +, \cdot)$

(e) $(\mathbb{Q}, +, \cdot)$

(f) $(\mathbb{R}, +, \cdot)$

domena integriteta:

(a) $(\mathbb{N}, +, \cdot)$

(b) $(\mathbb{Z}, +, \cdot)$

(c) $(\mathbb{Z}_3, +, \cdot)$

(d) $(\mathbb{Z}_4, +, \cdot)$

(e) $(\mathbb{Q}, +, \cdot)$

(f) $(\mathbb{R}, +, \cdot)$

polja:

(a) $(\mathbb{N}, +, \cdot)$

(b) $(\mathbb{Z}, +, \cdot)$

(c) $(\mathbb{Z}_3, +, \cdot)$

(d) $(\mathbb{Z}_4, +, \cdot)$

(e) $(\mathbb{Q}, +, \cdot)$

(f) $(\mathbb{R}, +, \cdot)$

Primeri

Od sledećih struktura zaokruži slovo ispred

prstena:

(a) $(\mathbb{N}, +, \cdot)$

(b) $(\mathbb{Z}, +, \cdot)$

(c) $(\mathbb{Z}_3, +, \cdot)$

(d) $(\mathbb{Z}_4, +, \cdot)$

(e) $(\mathbb{Q}, +, \cdot)$

(f) $(\mathbb{R}, +, \cdot)$

domena integriteta:

(a) $(\mathbb{N}, +, \cdot)$

(b) $(\mathbb{Z}, +, \cdot)$

(c) $(\mathbb{Z}_3, +, \cdot)$

(d) $(\mathbb{Z}_4, +, \cdot)$

(e) $(\mathbb{Q}, +, \cdot)$

(f) $(\mathbb{R}, +, \cdot)$

polja:

(a) $(\mathbb{N}, +, \cdot)$

(b) $(\mathbb{Z}, +, \cdot)$

(c) $(\mathbb{Z}_3, +, \cdot)$

(d) $(\mathbb{Z}_4, +, \cdot)$

(e) $(\mathbb{Q}, +, \cdot)$

(f) $(\mathbb{R}, +, \cdot)$

Primeri

Od sledećih struktura zaokruži slovo ispred

prstena:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

domena integriteta:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

polja:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

Primeri

Od sledećih struktura zaokruži slovo ispred

prstena:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

domena integriteta:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

polja:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

Primeri

Od sledećih struktura zaokruži slovo ispred

prstena:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

domena integriteta:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

polja:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

Primeri

Od sledećih struktura zaokruži slovo ispred

prstena:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

domena integriteta:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

polja:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

Primeri

Od sledećih struktura zaokruži slovo ispred

prstena:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

domena integriteta:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

polja:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

Primeri

Od sledećih struktura zaokruži slovo ispred

prstena:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

domena integriteta:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

polja:

(a) $(\mathbb{N}, +, \cdot)$
(b) $(\mathbb{Z}, +, \cdot)$
(c) $(\mathbb{Z}_3, +, \cdot)$
(d) $(\mathbb{Z}_4, +, \cdot)$
(e) $(\mathbb{Q}, +, \cdot)$
(f) $(\mathbb{R}, +, \cdot)$

Osobine u prstenu

Teorema

U prstenu $(R, +, \cdot)$ *za sve* $x, y \in R$ *važi*

1. $x \cdot 0 = 0 \cdot x = 0$
2. $(-x)y = x(-y) = -(xy)$
3. $(-x)(-y) = xy$

Dokaz

1. $x \cdot 0 = x \cdot 0 + 0 = x \cdot 0 + \big(x \cdot 0 + (-(x \cdot 0))\big) = \big(x \cdot 0 + x \cdot 0\big) + (-(x \cdot 0)) = x \cdot (0 + 0) + (-(x \cdot 0)) = x \cdot 0 + (-(x \cdot 0)) = 0.$ *Drugi deo se dokazuje na isti način.*
2. $(-x)y = (-x)y + 0 = (-x)y + (xy + (-(xy))) = \big((-x)y + xy\big) + (-(xy)) = (-x + x)y + (-(xy)) = 0 \cdot y + (-(xy)) = 0 + (-(xy)) = -(xy).$ *Drugi deo se dokazuje na isti način.*
3. *Na osnovu tvrđenja pod* 2. *sledi* $(-x)(-y) = -(x(-y)) = -(-(xy)) = xy.$

Nula i jednica u prstenu

Teorema

U prstenu sa jedinicom $(R, +, \cdot)$ sa bar dva elementa, jedinica prstena je različita od nule prstena.

Dokaz

Pretpostavimo suprotno, da postoji prsten sa jedinicom $(R, +, \cdot)$ koji ima bar dva elementa kod koga za nulu 0 (neutralni za $+$) i jedinicu 1 (neutralni za $\cdot$) važi $0 = 1$. Tada bi za svako $x \in R$ važilo $x = x \cdot 1 = x \cdot 0 = 0$, pa bi R imao samo jedan element, što je u kontradikciji sa pretpostavkom da R ima bar dva elementa.

Svako polje je domen integriteta

Teorema

Svako polje je i domen integriteta.

Dokaz

Treba samo pokazati da u polju nema delitelja nule, tj. da $(a \neq 0 \wedge b \neq 0) \Rightarrow ab \neq 0$.
Ovo sledi direktno iz činjenice da je u polju $(R \backslash \{0\}, \cdot)$ *(komutativna) grupa.*

Primer

Domeni integriteta koji nisu polja su $(\mathbb{Z}, +, \cdot)$ *i polinomi (radićemo kasnije).*

Svaki konačan domen integriteta je polje

Teorema

Svaki konačan domen integriteta $(R, +, \cdot)$ *je i polje.*

Dokaz

Treba samo pokazati da za sve $x \in R\backslash\{0\}$ *postoji inverzni element* $x^{-1} \in R\backslash\{0\}$. *Neka je* $R = \{x_1, \dots, x_n\}$ *i neka je* $x \in R\backslash\{0\}$. *Posmatrajmo skup* $S = \{xx_1, \dots, xx_n\}$. *Imamo da je* $S \subseteq R$, *jer je* $xx_i \in R$, *zbog zatvorenosti operacije* $\cdot$. *Ako pokažemo da za* $x_i \neq x_j$ *sledi* $xx_i \neq xx_j$, *slediće da* S *ima isti broj elemenata kao i* R, *tj. imaćemo* $S = R$. *Pretpostavimo suprotno, da za* $x_i \neq x_j$ *sledi* $xx_i = xx_j$. *Tada imamo* $xx_i - xx_j = 0$, *tj.* $x(x_i - x_j) = 0$, *odakle sledi* $x = 0$ *ili* $x_i - x_j = 0$, *jer je* $(R, +, \cdot)$ *domen integriteta (nema delitelje nule). Sada smo dobili da je* $x = 0$ *ili* $x_i = x_j$, *što je u suprotnosti sa pretpostavkama* $x \neq 0$ *i* $x_i \neq x_j$. *Sledi* $R = S = \{xx_1, \dots, xx_n\}$, *a pošto je* $(R, +, \cdot)$ *domen integriteta, to je jedan od elemenata iz ovog skupa jedinica prstena. Ako je* $xx_i = 1$, *tada je* $x^{-1} = x_i$, *tj. za svaki* $x \in R\backslash\{0\}$ *postoji inverzni element* $x^{-1} \in R\backslash\{0\}$.

Primeri konačnih prstena: $(\mathbb{Z}_n, +, \cdot)$

Teorema

$(\mathbb{Z}_n, +, \cdot)$ *je komutativan prsten sa jedinicom za svako* $n \in \mathbb{N}$.

Dokaz

- *Pokazujemo da je* $(\mathbb{Z}_n, +)$ *Abelova grupa:*
  1. **Zatvorenost:** *sledi iz definicije sabiranja klasa* $C_x + C_y = C_{x+y}$
  2. **Asocijativnost:** *dokazana kod grupa i kongruencija (pogledati)*
  3. **Neutralni element:** *je* 0, *jer je* $C_x + C_0 = C_0 + C_x = C_x$
  4. **Inverzni elementi:** *za* $k \in \mathbb{Z}_n$ *inverzni je* $n - k$, *jer je* $k + (n-k) = (n-k) + k = 0$
  5. **Komutativnost:** *sledi iz* $C_x + C_y = C_{x+y} = C_{y+x} = C_y + C_x$
- *Pokazujemo da je* $(\mathbb{Z}_n, \cdot)$ *komutativan monoid:*
  1. **Zatvorenost, asocijavitnost, komutativnost:** *se pokazuju isto kao za operaciju* $+$
  2. **Neutralni element:** *je* 1, *jer je* $C_x \cdot C_1 = C_1 \cdot C_x = C_x$
- *Pokazujemo* **distributivnost** $\cdot$ *prema* $+$*: pokazaćemo samo levu, desna će slediti iz leve i komutativnosti*

  $C_x \cdot (C_y + C_z) = C_x \cdot C_{y+z} = C_{x \cdot (y+z)} = C_{xy+xz} = C_{xy} + C_{xz} = (C_x \cdot C_y) + (C_x \cdot C_z)$

Primeri konačnih polja: $(\mathbb{Z}_p, +, \cdot)$

Teorema

$(\mathbb{Z}_p, +, \cdot)$ *jeste polje akko je* p *prost broj.*

Dokaz

$(\Leftarrow)$: *Neka je* p *prost broj. Dokazaćemo samo da* $(\mathbb{Z}_p, +, \cdot)$ *nema delitelje nule (jer će tada biti domen integriteta, a svaki konačan domen integriteta je polje). Pretpostavimo suprotno, da postoje delitelji nule* $x, y \in \mathbb{Z}_p$, *tj.* $x \neq 0$ *i* $y \neq 0$ *i* $xy = 0$. *Odavde imamo da* $p \mid xy$, *a pošto je* p *prost sledi* $p \mid x$ *ili* $p \mid y$ *(ako prost broj deli proizvod mora da deli jednog od činilaca), tj.* $C_x = 0$ *ili* $C_y = 0$, *što je u kontradikciji sa pretpostavkom* $x \neq 0$ *i* $y \neq 0$.

$(\Rightarrow)$: *Neka* $(\mathbb{Z}_p, +, \cdot)$ *jeste polje (tj. domen integriteta). Pokažimo da* p *mora biti prost. Pretpostavimo suprotno, neka je* $p \geq 2$ *složen broj, tj.* $p = x \cdot y$, *za* $1 < x < p$ *i* $1 < y < p$. *Sada važi* $C_x \cdot C_y = C_{x \cdot y} = C_p = C_0$, *pa iz pretpostavke da* $(\mathbb{Z}_p, +, \cdot)$ *jeste polje (nema delitelje nule) imamo* $C_x = 0$ *ili* $C_y = 0$, *odakle* $p \mid x$ *ili* $p \mid y$, *što je u kontradikciji sa pretpostavkom* $1 < x < p$ *i* $1 < y < p$.

Karakteristika polja

Definicija (Karakteristika polja)

Neka je $(F, +, \cdot)$ polje, gde je jedinica e. Ako postoji najmanji prirodan broj n takav da je $ne = e + \ldots + e = 0$, tada je broj n karakteristika polja F. Ako takav n ne postoji, kažemo da je polje karakteristike 0 (ili beskonačne katrakteristike).

Teorema

Karakteristika konačnog polja je prost broj.

Dokaz

Neka je $(F, +, \cdot)$ polje, e jedinica polja i neka je $|F| = m$. Tada znamo da je $me = 0$, pa postoji $p \in \mathbb{N}$ koji je karakteristika polja. Pošto se nula i jedinica moraju razlikovati u prstenu imamo $p > 1$. Pretpostavimo sada suprotno tvrđenju teoreme, da je p složen broj, tj. $p = x \cdot y$, za $1 < x < p$ i $1 < y < p$. Sada važi $pe = (xy)e = (xe)(ye) = 0$, a pošto nemamo delitelje nule (polje) sledi $xe = 0$ ili $ye = 0$, što je u kontradikciji sa pretpostavkom da je p karakteristika polja (najmanji prirodan broj sa osobinom $pe = 0$).

Broj elemenata polja

Primer

Glavni primeri beskonačnih polja su $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ *i* $(\mathbb{C}, +, \cdot)$, *a konačna polja su, recimo,* $(\mathbb{Z}_3, +, \cdot)$ *i* $(\mathbb{Z}_5, +, \cdot)$, *dok* $(\mathbb{Z}_4, +, \cdot)$ *nije polje.*

Napomena

Isopstavlja se da konačna polja mogu imati samo p^n *elemenata, gde je* p *prost broj i* $n \in \mathbb{N}$. *Polja koje imaju* p *elemenata znamo, to su* $(\mathbb{Z}_p, +, \cdot)$. *Za ostala polja, koja imaju* p^n *elemenata, ćemo pokazati kako mogu da se konstruišu pomoću nesvodljivih polinoma nad poljima* $(\mathbb{Z}_p, +, \cdot)$, *ali to ćemo videti tek kad obradimo polinome. Konačna polja se zovu* **polja Galoa** *i označavaju sa* $GF(p^n)$.

Homomorfizam i izomorfizam

Homomorfizam i izomorfizam

Definicija (Homomorfizam i izomorfizam)

Neka su $(R,+,\cdot)$ *i* $(S,\oplus,\odot)$ *prsteni. Funkcija* $f:R\to S$ *je homomorfizam ako za sve* $x,y\in R$ *važi*

$$f(x+y)=f(x)\oplus f(y) \;\; i \;\; f(x\cdot y)=f(x)\odot f(y)$$

Primer

Dokazati da je $(\mathbb{R}^2,\oplus,\odot)$ *polje, ako su operacije definisane sa za svako* $(x_1,y_1),(x_2,y_2),\in\mathbb{R}^2$

$$(x_1,y_1)\oplus(x_2,y_2)=(x_1+x_2,y_1+y_2) \;\; i \;\; (x_1,y_1)\odot(x_2,y_2)=(x_1x_2-y_1y_2,x_1y_2+x_2y_1)$$

Rešenje. Lako se pokazuje da je $f:\mathbb{C}\to\mathbb{R}^2$ definisana sa $f(x+iy)=(x,y)$ izomorfizam iz $(\mathbb{C},+,\cdot)$ u $(\mathbb{R}^2,\oplus,\odot)$. Npr. imamo $f((x_1+iy_1)+(x_2+iy_2))=f((x_1+x_2)+i(y_1+y_2))=(x_1+x_2,y_1+y_2)=(x_1,y_1)\oplus(x_2,y_2)=f(x_1+iy_1)\oplus(x_2+iy_2)$. Kako je $(\mathbb{C},+,\cdot)$ polje, sledi da je i $(\mathbb{R}^2,\oplus,\odot)$ polje.

Potprsten

Potprsten

Definicija (Potprsten)

Kažemo da je $(S,+,\cdot)$ *potprsten prstena* $(R,+,\cdot)$*, ako je* $S \subseteq R$*, operacije na* S *su restrikcije operacija iz* R *i* $(S,+,\cdot)$ *je prsten.*

Primer

Prsten $(\mathbb{Z},+,\cdot)$ *je potprsten prstena* $(\mathbb{Q},+,\cdot)$*, a* $(\{3k \mid k \in \mathbb{Z}\},+,\cdot)$ *je potprsten prstena* $(\mathbb{Z},+,\cdot)$*.*

Kompleksni brojevi

Kompleksni brojevi

Primer

Reši jednačinu $x^2 + 1 = 0$ *u polju* $(\mathbb{R}, +, \cdot)$.

Rešenje. Nema rešenje u tom polju, jer je $x = \pm\sqrt{-1}$, ali zato ima rešenje u polju kompleksnih brojeva.

Definicija (Skup kompleksnih brojeva)

Skup kompleksnih brojeva $\mathbb{C}$ *dat je sa* $\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R} \wedge i^2 = -1\}$.

Posledica

Kompleksni brojevi $z_1 = x_1 + iy_1$ *i* $z_2 = x_2 + iy_2$ *su jednaki akko je* $x_1 = x_2$ *i* $y_1 = y_2$.

Definicija (Operacije na skupu kompleksnih brojeva)

Za sve $z_1 = x_1 + iy_1$ *i* $z_2 = x_2 + iy_2$ *iz skupa* $\mathbb{C}$ *definišemo operacije* $+$ *i* $\cdot$ *sa*

$$z_1 + z_2 = (x_1 + iy_1) + (x_2 + iy_2) = x_1 + x_2 + i(y_1 + y_2)$$

$$z_1 \cdot z_2 = (x_1 + iy_1) \cdot (x_2 + iy_2) = x_1x_2 - y_1y_2 + i(x_1y_2 + x_2y_1)$$

$(\mathbb{C}, +, \cdot)$ je polje (1/2)

- $(\mathbb{C}, +)$ je Abelova grupa:
  1. **Zatvorenost:** ako su $z_1, z_2 \in \mathbb{C}$, tj. $z_1 = x_1 + iy_1$ i $z_2 = x_2 + iy_2$ i $x_1, x_2, y_1, y_2 \in \mathbb{R}$, tada važi $x_1 + x_2, y_1 + y_2 \in \mathbb{R}$. Odatle sledi $z_1 + z_2 = x_1 + x_2 + i(y_1 + y_2) \in \mathbb{C}$
  2. **Asocijativnost:** sledi iz asocijativnosti sabiranja realnih brojeva (ispišite sami)
  3. **Komutativnost:** sledi iz komutativnosti sabiranja realnih brojeva (ispišite sami)
  4. **Neutralni element:** je $0 = 0 + 0i \in \mathbb{C}$
  5. **Inverzni elementi:** za $z \in \mathbb{C}$ i $z = x + iy$ inverzni je $-z = (-x) + i(-y) \in \mathbb{C}$
- Distributivnost $\cdot$ prema $+$: neka su $z_1 = x_1 + iy_1, z_2 = x_2 + iy_2, z_3 = x_3 + iy_3$, tada

$$
\begin{aligned}
z_1(z_2 + z_3) &= (x_1 + iy_1)(x_2 + x_3 + i(y_2 + y_3)) \\
&= x_1(x_2 + x_3) - y_1(y_2 + y_3) + i(x_1(y_2 + y_3) + y_1(x_2 + x_3)) \\
&= x_1x_2 + x_1x_3 - (y_1y_2 + y_1y_3) + i(x_1y_2 + x_1y_3 + y_1x_2 + y_1x_3) \\
&= x_1x_2 - y_1y_2 + i(x_1y_2 + y_1x_2) + x_1x_3 - y_1y_3 + i(+x_1y_3 + y_1x_3) \\
&= z_1z_2 + z_1z_3
\end{aligned}
$$

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

$(\mathbb{C}, +, \cdot)$ je polje (2/2)

Plan: Dokazaćemo da je $(\mathbb{C}, \cdot)$ komutativan monoid i da za sve $z \neq 0$ postoji inverzni element $z^{-1} \neq 0$. Odavde će slediti da je $(\mathbb{C}\backslash\{0\}, \cdot)$ Abelova grupa (npr. zatvorenost: za $z_1, z_2 \in \mathbb{C}\backslash\{0\}$ sledi $z_1 z_2 \in \mathbb{C}\backslash\{0\}$, jer ako je $z_1 z_2 = 0$ i $z_1 \neq 0$, množenjem sa z_1^{-1}, dobijamo $z_2 = 0$).

- $(\mathbb{C}, \cdot)$ je komutativan monoid:
  1. **Zatvorenost:** ako su $z_1, z_2 \in \mathbb{C}$, tj. $z_1 = x_1 + iy_1$ i $z_2 = x_2 + iy_2$ i $x_1, x_2, y_1, y_2 \in \mathbb{R}$, tada važi $x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1 \in \mathbb{R}$. Odatle sledi $z_1 \cdot z_2 = x_1 x_2 - y_1 y_2 + i(x_1 y_2 + x_2 y_1) \in \mathbb{C}$
  2. **Asocijativnost:** sledi iz asocijativnosti sabiranja realnih brojeva (ispišite sami)
  3. **Komutativnost:** sledi iz komutativnosti sabiranja realnih brojeva (ispišite sami)
  4. **Neutralni element:** je $1 = 1 + 0i \in \mathbb{C}$ jer za $z = x + iy$ imamo $z \cdot 1 = x \cdot 1 - y \cdot 0 + i(x \cdot 0 + y \cdot 1) = z$, a $z \cdot 1 = 1 \cdot z$ sledi iz komutativnosti $\cdot$
- **Inverzni elementi u $(\mathbb{C}\backslash\{0\}, \cdot)$:** Za $z = x + iy \in \mathbb{C}\backslash\{0\}$ inverzni je $z^{-1} = \frac{x}{x^2+y^2} + i\frac{-y}{x^2+y^2}$, jer za $z \in \mathbb{C}\backslash\{0\}$, imamo $x, y \in \mathbb{R}$ i $(x, y) \neq (0, 0)$, odakle je $x^2 + y^2 \neq 0$ i $\frac{x}{x^2+y^2} + i\frac{-y}{x^2+y^2} \in \mathbb{C}\backslash\{0\}$, i važi
$$z^{-1} \cdot z = z \cdot z^{-1} = (x + iy)\left(\frac{x}{x^2+y^2} + i\frac{-y}{x^2+y^2}\right) = \frac{x^2+y^2}{x^2+y^2} + i\frac{-xy+yx}{x^2+y^2} = 1$$

Šta smo danas radili

- Prsten, domen integriteta i polje
- Za konačne skupove: domen integriteta $=$ polje
- Konačna polja imaju p^n elemenata
- Homomorfizam i izomorfizam
- Potprsten
- Polje kompleksnih brojeva