

Okruhy (a súvisiace pojmy)

22. apríla 2024

Okruhy

Definícia

Trojicu $(R, +, \cdot)$ nazývame *okruh* ak $+$ a \cdot sú binárne operácie na množine R také, že

- (i) $(R, +)$ je komutatívna grupa,
- (ii) operácia \cdot je asociatívna,

$$(\forall a, b, c \in R) \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

- (iii) pre operácie $+$ a \cdot platia *distributívne zákony*

$$(\forall a, b, c \in R) \quad a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(\forall a, b, c \in R) \quad (b + c) \cdot a = b \cdot a + c \cdot a$$

Okruhy

Neutrálny prvok operácie $+$ budeme označovať 0 . Podobne ako sme to robili pre polia, inverzný prvok k prvku a vzhľadom na operáciu $+$ budeme označovať $-a$. Označenie $b - a$ bude znamenať $b + (-a)$.

- ▶ komutatívny okruh = ak operácia \cdot je komutatívna;
- ▶ okruh s jednotkou = ak existuje neutrálny prvok $1 \neq 0$ pre \cdot .
- ▶ $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_n, \oplus, \odot)$ sú komutatívne okruhy s jednotkou.
- ▶ $(2\mathbb{Z}, +, \cdot)$, komutatívny okruh, nemá jednotku.

Okruhy

Lema

Nech $(R, +, \cdot)$ je okruh, $a, b \in R$. Potom platí

$$0a = a0 = 0$$

$$a(-b) = -ab = (-a)b$$

$$(-a)(-b) = ab$$

Súčin okruhov

$$(R_1 \times R_2, +, \cdot)$$

$$(a, b) + (a', b') = (a + a', b + b'),$$

$$(a, b)(a', b') = (aa', bb').$$

$$\prod_{i \in M} R_i = \{f: M \rightarrow \bigcup_{i \in M} R_i \mid (\forall i \in M)(f(i) \in R_i)\}$$

$$(f + g)(i) = f(i) + g(i)$$

$$(f \cdot g)(i) = f(i) \cdot g(i)$$

Špeciálny prípad: R^M ak $R_i = R$ pre všetky $i \in M$.

Zobrazenia $M \rightarrow R$

$$R^M = \{f: M \rightarrow R\}$$

$$(f + g)(i) = f(i) + g(i)$$

$$(f \cdot g)(i) = f(i) \cdot g(i)$$

Matice

$(M_{n,n}(F), +, \cdot)$ – príklad nekomutatívneho okruhu (pre $n \geq 2$)

Podokruhy

Definícia

Nech $(R, +, \cdot)$ je okruh a $S \subseteq R$ je neprázdna podmnožina množiny R . Hovoríme, že S je *podokruh* okruhu R , ak pre ľubovoľné $a, b \in S$ platí $a - b \in S$, $ab \in S$.

$$a, b \in S \quad \Rightarrow \quad a - b \in S, ab \in S$$

Tvrdenie

Nech $(R, +, \cdot)$ je okruh a $S \subseteq R$, $S \neq \emptyset$. Množina S je podokruh okruhu $(R, +, \cdot)$ práve vtedy, keď S s operáciami $+$ a \cdot zúženými na množinu S tvorí okruh.

Príklady podokruhov

- ▶ $2\mathbb{Z}$ v $(\mathbb{Z}, +, \cdot)$
- ▶ $\mathbb{Z} \times \{0\}$, $\{0\} \times \mathbb{Z}$ aj $\{(x, x); x \in \mathbb{Z}\}$ v $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$
- ▶ $C(0, 1)$ v $(\mathbb{R}^{(0,1)}, +, \cdot)$

Delitele nuly

Definícia

Ak v okruhu $(R, +, \cdot)$ neexistujú prvky a, b také, že $a, b \neq 0$ a

$$ab = 0,$$

tak hovoríme, že R je *okruh bez deliteľov nuly* (alebo tiež, že R nemá delitele nuly).

Ak $(R, +, \cdot)$ je komutatívny okruh s jednotkou bez deliteľov nuly, hovoríme, že $(R, +, \cdot)$ je *obor integrity*.

- ▶ \mathbb{Z} je obor integrity
- ▶ $\mathbb{Z} \times \mathbb{Z}$ má delitele nuly

Tvrdenie

Nech R je okruh bez deliteľov nuly a $a, b, c \in R$. Ak $a \neq 0$ a platí $ab = ac$, tak $b = c$.

Teleso, pole

Definícia

Okruh R s jednotkou nazývame *telesom*, ak ku každému nenulovému prvku $a \in R \setminus \{0\}$ existuje inverzný prvok vzhľadom na násobenie, t.j.

$$(\forall a \in R \setminus \{0\})(\exists b \in R) \quad ab = ba = 1$$

Komutatívne teleso voláme *pole*.

Tvrdenie

Každé teleso je okruh bez deliteľov nuly.

Každé pole je oborom integrity.

kvaternióny = príklad telesa, ktoré nie je poľom

Homomorfizmus okruhov

Definícia

Nech $(R, +, \cdot)$, $(S, +, \cdot)$ sú okruhy. Zobrazenie $f: R \rightarrow S$ nazývame *homomorfizmus*, ak platí

$$\begin{aligned}f(a + b) &= f(a) + f(b), \\f(ab) &= f(a)f(b).\end{aligned}$$

- ▶ epimorfizmus = surjektívny homomorfizmus
- ▶ monomorfizmus = injektívny homomorfizmus
- ▶ izomorfizmus = bijektívny homomorfizmus
- ▶ $R \cong S$ = okruhy R a S sú izomorfné

Homomorfizmus okruhov

Tvrdenie

Zloženie homomorfizmov je homomorfizmus. Zloženie izomorfizmov je izomorfizmus.

$$\begin{aligned}g(f(a + b)) &= g(f(a) + f(b)) = g(f(a)) + g(f(b)), \\g(f(ab)) &= g(f(a)f(b)) = g(f(a))g(f(b)).\end{aligned}$$

Homomorfizmus okruhov

Tvrdenie

Zloženie homomorfizmov je homomorfizmus. Zloženie izomorfizmov je izomorfizmus.

Príklad

Jednoduché príklady homomorfizmov:

$$f: \mathbb{Z} \rightarrow \mathbb{Z}_n, f: k \mapsto k \bmod n$$

$$g: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, g: (a, b) \mapsto a$$

$$h: \mathbb{C} \rightarrow \mathbb{C}, h: a + bi \mapsto a - bi$$

Matice rotácií

$$S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix}; a, b \in \mathbb{R} \right\}$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix},$$

Homomorfizmus $f: S \rightarrow \mathbb{C}$:

$$f: \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a + bi$$