

Okruhy

31. marca 2025

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

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

$$\begin{aligned}(a, b) + (a', b') &= (a + a', b + b'), \\ (a, b)(a', b') &= (aa', bb').\end{aligned}$$

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

$$\begin{aligned}(f + g)(i) &= f(i) + g(i) \\ (f \cdot g)(i) &= f(i) \cdot g(i)\end{aligned}$$

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 $i \in M$.

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.

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

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

Ideál

Definícia

Nech R je okruh. Neprázdna podmnožina $I \subseteq R$ je *ideál* v okruhu R , ak platí

$$\begin{aligned}(\forall a, b \in I) \quad & a - b \in I \\ (\forall a \in I)(\forall r \in R) \quad & ar \in I, ra \in I\end{aligned}$$

t.j. ak je táto množina uzavretá vzhľadom na sčítovanie (prvkov z I) a násobenie ľubovoľným prvkom z R .

ideál = podokruh je uzavretý vzhľadom na násobenie všetkými prvkami z R .

Príklady ideálov

- ▶ $\{0\}$, R v ľubovoľnom okruhu R ;
- ▶ $k\mathbb{Z} = \{kz; z \in \mathbb{Z}\}$ v $(\mathbb{Z}, +, \cdot)$;
- ▶ $R_1 \times \{0\}$ v $R_1 \times R_2$

Hlavné ideály

Definícia

Ak R je komutatívny okruh s jednotkou a $a \in R$, tak množina

$$(a) = \{ax; x \in R\}$$

je ideálom v R . Ideály takéhoto tvaru voláme *hlavné ideály*.

Ideály v poliach

Lema

Nech R je okruh s jednotkou a I je ideál v R . Potom $I = R$ práve vtedy, keď $1 \in I$.

Dôsledok

Ak R je pole, tak jediné ideály v R sú $\{0\}$ a R .

Jadro homomorfizmu

Lema

Ak $\varphi: R \rightarrow S$ je homomorfizmus okruhov, tak jeho jadro $\text{Ker } \varphi$ je ideál v R .

Faktorový okruh

Veta

Nech $(R, +, \cdot)$ je ľubovoľný okruh a I je ideál v R . Ak na prvkoch faktorovej grupy $(R, +)$ podľa podgrupy I

$$R/I = \{a + I; a \in R\}$$

definujeme binárnu operáciu $\cdot$ ako

$$(a + I) \cdot (b + I) = (a \cdot b) + I,$$

tak je táto binárna operácia dobre definovaná a $(R/I, +, \cdot)$ je okruh. Tento okruh voláme faktorový okruh R podľa I .

Ak je okruh R komutatívny, tak aj R/I je komutatívny. Ak R je okruh s jednotkou a $I \neq R$, tak $1 + I$ je jednotka faktorového okruhu R/I .

Faktorový okruh

$$a + I = b + I \quad \Leftrightarrow \quad a - b \in I$$

$$(a + I) \cdot (b + I) = (a \cdot b) + I$$

Faktorový okruh

$$a + I = b + I \quad \Leftrightarrow \quad a - b \in I$$

$$(a + I) \cdot (b + I) = (a \cdot b) + I$$

$$\left. \begin{array}{l} a - a' \in I \\ b - b' \in I \end{array} \right\} \Rightarrow \begin{array}{l} ab - a'b' = \\ a(b - b') + (a - a')b' \in I \end{array}$$

Faktorový okruh

$$(a + I)((b + I)(c + I)) = a(bc) + I$$

$$((a + I)(b + I))(c + I) = (ab)c + I$$

$$(a + I)((b + I) + (c + I)) = a(b + c) + I$$

$$(ab + I) + (ac + I) = (ab + ac) + I$$

Faktorový okruh

$$(a + I)(1 + I) = a + I$$

$$(1 + I)(a + I) = a + I$$

$$(a + I)(b + I) = ab + I$$

$$(b + I)(a + I) = ba + I$$

Veta o izomorfizme

Veta (Veta o izomorfizme)

Ak $f: R \rightarrow R'$ je homomorfizmus okruhov, tak $\text{Ker } f$ je ideál v okruhu R a faktorový okruh $R/\text{Ker } f$ je izomorfný s podokruhom $\text{Im } f$ okruhu R' .

Kanonický homomorfizmus

Kanonický homomorfizmus: $\varphi: R \rightarrow R/I$

$$\varphi: a \mapsto a + I$$

- ▶ $I = \text{Ker } \varphi$.
- ▶ ideály = jadrá homomorfizmov

Prvoideál

Definícia

Ideál I v okruhu R sa nazýva prvoideál, ak pre ľubovoľné $a, b \in R$ také, že $a \cdot b \in I$ aspoň jeden z prvkov a, b patrí do I čiže ak platí

$$a \cdot b \in I \quad \Rightarrow \quad a \in I \vee b \in I.$$

Napríklad: (p) v $\mathbb{Z}$, kde p je prvočíslo.

Prvoideály a faktorizácia

Veta

Nech R je komutatívny okruh s jednotkou a I je ideál v R . Potom faktorový okruh R/I je oborom integrity práve vtedy, keď I je vlastný prvoideál.

Príklady: $\mathbb{Z}/(3) \cong \mathbb{Z}_3$, $\mathbb{Z}/(4) \cong \mathbb{Z}_4$

Prvoideály a faktorizácia

Veta

Nech R je komutatívny okruh s jednotkou a I je ideál v R . Potom faktorový okruh R/I je oborom integrity práve vtedy, keď I je vlastný prvoideál.

$$\begin{aligned} ab + I = 0 + I &\Leftrightarrow a + I = 0 + I \vee b + I = 0 + I \\ ab \in I &\Leftrightarrow a \in I \vee b \in I \end{aligned}$$

Maximálny ideál

Definícia

Ideál I v okruhu R nazývame *maximálny*, ak $I \neq R$ a súčasne pre každý ideál J s vlastnosťou $I \subseteq J \subseteq R$ platí $I = J$ alebo $J = R$.

Inak: Maximálny prvok množiny vlastných ideálov (usporiadanej inklúziou).

Maximálne ideály a faktorizácia

Veta

Nech R je komutatívny okruh s jednotkou a I je ideál v R . Potom faktorový okruh R/I je pole práve vtedy, keď I je maximálny ideál.

Dôsledok

V komutatívnom okruhu s jednotkou je každý maximálny ideál prvoideál.