

Okruhy a ideály

10. októbra 2024

Okruhy

Definícia

Nech R je množina, $+$ a $\cdot$ sú binárne operácie na tejto množine. Potom $(R, +, \cdot)$ voláme *okruh*, ak platí:

- (i) $(R, +)$ je komutatívna grupa.
- (ii) Operácia $\cdot$ je asociatívna, t.j. platí:

$$(\forall x, y, z \in R)(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

- (iii) Platia distributívne zákony:

$$(\forall x, y, z \in R)x \cdot (y + z) = x \cdot y + x \cdot z$$

$$(\forall x, y, z \in R)(y + z) \cdot x = y \cdot x + z \cdot x$$

Okruhy

- (i) $(R, +)$ je komutatívna grupa.
- (ii) Operácia $\cdot$ je asociatívna, t.j. platí:

$$(\forall x, y, z \in R)(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

- (iii) Platia distributívne zákony:

$$(\forall x, y, z \in R)x \cdot (y + z) = x \cdot y + x \cdot z$$

$$(\forall x, y, z \in R)(y + z) \cdot x = y \cdot x + z \cdot x$$

Označenie pri operácii $+$:

- ▶ neutrálny prvok označujeme 0;
- ▶ inverzný prvok označujeme $-x$.

Okruhy

$$(\forall x, y \in R) x + y = y + x$$

$$(\forall x, y, z \in R) (x + y) + z = x + (y + z)$$

$$(\exists 0 \in R) (\forall x \in R) x + 0 = 0 + x = x$$

$$(\forall x \in R) (\exists y \in R) x + y = y + x = 0$$

$$(\forall x, y, z \in R) (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

$$(\forall x, y, z \in R) x \cdot (y + z) = x \cdot y + x \cdot z$$

$$(\forall x, y, z \in R) (y + z) \cdot x = y \cdot x + z \cdot x$$

Okruhy

Definícia

Okruh $(R, +, \cdot)$ sa nazýva *komutatívny okruh*, ak operácia $\cdot$ je komutatívna.

$$(\forall x, y \in R) x \cdot y = y \cdot x$$

Okruh $(R, +, \cdot)$ nazývame *okruh s jednotkou*, ak existuje neutrálny prvok na násobenie, ktorý je navyše rôzny od nuly. Ak takýto prvok existuje, budeme ho označovať 1.

$$(\exists 1 \in R \setminus \{0\})(\forall x \in R) 1 \cdot x = x \cdot 1 = x$$

Okruhy

Definícia

Nech $(R, +, \cdot)$ je okruh. Hovoríme, že R je *okruh bez deliteľov nuly*, ak z $a \cdot b = 0$ vyplýva $a = 0$ alebo $b = 0$.

$$(\forall a, b \in R)(a \cdot b = 0 \Rightarrow a = 0 \vee b = 0)$$

Okruh $(R, +, \cdot)$ nazývame *obor integrity*, ak je to komutatívny okruh s jednotkou bez deliteľov nuly.

Pole

Definícia

Nech F je ľubovoľná množina, $+$ a $\cdot$ sú binárne operácie na množine F . Trojicu $(F, +, \cdot)$ nazveme *pole*, ak je to komutatívny okruh s jednotkou na navyše pre ľubovoľný $a \in F \setminus \{0\}$ existuje inverzný prvok vzhľadom na násobenie.

$$(\forall a \in F \setminus \{0\})(\exists b \in F)a \cdot b = 1$$

Příklady okruhů

- ▶ $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ s obvyklým sčítáním a násobením
- ▶ matice 2×2 (resp. $n \times n$)

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

Příklady okruhů

$$(\mathcal{P}(X), \Delta, \cap)$$

$$A \Delta B = (A \setminus B) \cup (B \setminus A)$$

$$A \cap B = \{x; (x \in A) \wedge (x \in B)\}$$

Príklady okruhov

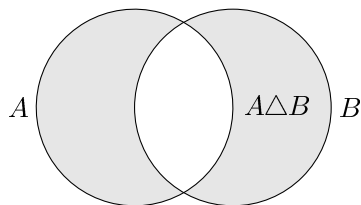


Figure: Vennov diagram pre symetrickú diferenciu $A \Delta B$

Podokruh

Definícia

Nech $(R, +, \cdot)$ je okruh a $S \subseteq R$. Hovoríme, že S je *podokruh* okruhu R , ak:

- (i) $S \neq \emptyset$
- (ii) Pre ľubovoľné $x, y \in S$ platí aj $x - y \in S$.
- (iii) Pre ľubovoľné $x, y \in S$ platí aj $x \cdot y \in S$.

Homomorfizmus a izomorfizmus

Definícia

Nech $R_{1,2}$ sú okruhy a $f: R_1 \rightarrow R_2$ je zobrazenie. Hovoríme, že $f: R_1 \rightarrow R_2$ je *homomorfizmus* ak pre ľubovoľné $x_{1,2} \in R_1$ platí:

$$f(x_1 + x_2) = f(x_1) + f(x_2)$$

$$f(x_1 \cdot x_2) = f(x_1) \cdot f(x_2)$$

Definícia

Ak $f: R_1 \rightarrow R_2$ je homomorfizmus a súčasne to je bijekcia, tak hovoríme, že f je *izomorfizmus*.

Okruhy $R_{1,2}$ nazývame *izomorfné*, ak existuje izomorfizmus $R_1 \rightarrow R_2$. Označujeme $R_1 \cong R_2$.

Podokruh

Definícia

Nech $(R, +, \cdot)$ je okruh a $S \subseteq R$. Hovoríme, že S je *podokruh* okruhu R , ak:

- (i) $S \neq \emptyset$
- (ii) Pre ľubovoľné $x, y \in S$ platí aj $x - y \in S$.
- (iii) Pre ľubovoľné $x, y \in S$ platí aj $x \cdot y \in S$.

Ideály

Definícia

Nech R je okruh a $I \subseteq R$. Hovoríme, že I je *ideál* v R ak $I \neq \emptyset$ a súčasne platí:

- (i) Pre ľubovoľné $a, b \in I$ aj $a - b \in I$.
- (ii) Pre ľubovoľné $a \in I$ a $r \in R$ platí aj $ar, ra \in I$.

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

Ideály

- (i) Pre ľubovoľné $a, b \in I$ aj $a - b \in I$.
- (ii) Pre ľubovoľné $a \in I$ a $r \in R$ platí aj $ar, ra \in I$.
 - ▶ $(I, +)$ je podgrupa $(R, +)$
 - ▶ Ideál = podokruh, ale navyše vyžadujeme uzavretosť na násobenie ľubovoľným prvkom.

Ideály

- ▶ $\{0\}$ a R sú ideály v R .
- ▶ Ak F je pole, tak jedinými ideálmi sú $\{0\}$ a F .

Hlavný ideál

Nech R je komutatívny okruh s jednotkou a $a \in R$.

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

$$ax_1 - ax_2 = a(x_1 - x_2)$$

$$(ax)r = a(xr)$$

Jadro homomorfizmu

Tvrdenie

*Nech R, R' sú okruhy a $f: R \rightarrow R'$ je homomorfizmus okruhov.
Potom množina*

$$\text{Ker } f = \{x \in R; f(x) = 0\}$$

je ideál v R . Túto množinu nazývame jadro homomorfizmu f .
 $f(a) = f(b) = 0$

$$f(a - b) = f(a) - f(b) = 0 - 0 = 0.$$

$$f(ax) = f(a) \cdot f(x) = 0 \cdot f(x) = 0,$$

$$f(xa) = f(x) \cdot f(a) = f(x) \cdot 0 = 0.$$