

Definice 4.1. Okruhem rozumíme šestici $R = (R, +, -, 0, \cdot, 1)$, kde R je neprázdná množina, na které jsou definovány binární operace $+$, $\cdot$, unární operace $-$ a prvky $0, 1 \in R$ splňující podmínky:

- $(R, +, -, 0)$ je abelovská grupa,
- Asociativita $\forall a, b, c \in R: a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
- Neutrální prvek $\forall a \in R: a \cdot 1 = 1 \cdot a = a$,
- Distributivita $\forall a, b, c \in R: a \cdot (b + c) = a \cdot b + a \cdot c, (b + c) \cdot a = b \cdot a + c \cdot a$.

Definice 4.2. Buď R komutativní okruh. Ideálem rozumíme libovolnou neprázdnou množinu $I \subseteq R$, splňující:

- $a, b \in I$, potom $a + b \in I, -a \in I$,
- $a \in I, r \in R$, potom $r \cdot a \in I$.

Definice 4.3. Buď $R = (R, +, -, 0, \cdot, 1)$ okruh. Podmnožinu $S \subseteq R$ nazveme **podokruhem** okruhu R , pokud S obsahuje jedničku a je uzavřená na operace sčítání, odčítání a násobení. Tedy:

- $1 \in S$,
- $a, b \in S$, potom $a + b \in S, -a \in S$,
- $a, b \in S$, potom $a \cdot b \in S$.

Definice 4.4. Necht' R a S jsou okruhy. Zobrazení $\varphi: R \rightarrow S$ se nazývá **homomorfismus okruhů**, jestliže pro všechna $a, b \in R$ platí:

- $\varphi(a + b) = \varphi(a) + \varphi(b)$,
- $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$,
- $\varphi(1_R) = 1_S$.

Pokud je φ bijekce, nazýváme jej **izomorfismus**.

Definujeme také jádro φ jako: $\ker \varphi = \{a \in R \mid \varphi(a) = 0_S\}$.

Úloha 4.1 (1 bod). Dokažte, že v libovolném okruhu R platí pro všechna $x, y \in R$ rovnost $-x(-y) = xy$.

Úloha 4.2 (1 bod). Najděte v okruhu $\mathbb{Z}_{10}$ ($\{0, 1, \dots, 9\}$ se sčítáním a násobením mod 10) všechny:

- dělitele nuly ($a \in \mathbb{Z}_{10}$ t.ž. $\exists c \in \mathbb{Z}_{10} \setminus \{0\} : ac = 0$),
- invertibilní prvky ($a \in \mathbb{Z}_{10}$ t.ž. $\exists c \in \mathbb{Z}_{10} : ac = 1$).

Úloha 4.3 (3 body). Buď R, S okruhy a $\varphi: R \rightarrow S$ homomorfismus. Dokažte, že

- $\varphi(0_R) = 0_S$,
- $\forall a \in R: \varphi(-a) = -\varphi(a)$,
- φ je prostý $\Leftrightarrow \ker \varphi = \{0_R\}$.

Úloha 4.4 (2 body). Rozhodněte, zda jsou následující zobrazení homomorfismy okruhů (s klasickým $+$, $\cdot$):

- $\varphi: \mathbb{C} \rightarrow \mathbb{C}, \varphi(a + bi) = a - bi$ (komplexní sdružení),
- $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}, \varphi(x) = 2x$.

Úloha 4.5 (3 body). Necht' R je komutativní okruh a $I \subseteq R$. U následujících tvrzení rozhodněte, zda platí. Svou odpověď zdůvodněte.

- I je ideál v $R \rightarrow I$ je podokruh R ,
- I je podokruh $R \rightarrow I$ není ideál v R ,
- pro libovolný prvek $a \in R$ je $aR = \{a \cdot r \mid r \in R\}$ ideál v R .

Bonusová úloha (3 body). Zjistěte poslední cifru čísla 7^{123} a poslední dvě cifry čísla 63^{322} .

Hint. Abyste určili poslední cifru čísla x^n , stačí najít $y \in \{0, 1, \dots, 9\}$, t.ž. $x^n \equiv y \pmod{10}$. K tomu využijte důsledek Lagrangeovy věty, který jsme si říkali na semináři – řád prvku dělí počet prvků grupy, a tedy $\text{prvek} \cdot \text{počet prvků grupy} = \text{identita}$. Grupa, která vás bude zajímat je $\mathbb{Z}_{10}^*$ – operace je násobení mod 10. Její počet prvků jste zjistili v druhé úloze – je to přesně počet invertibilních prvků v okruhu $\mathbb{Z}_{10}$. Dále platí $|\mathbb{Z}_{100}^*| = 40$.