Ideály okruhu $(R, +, \cdot)$

Definice. Nechť R je okruh. Podmnožina $I \subseteq R$ se nazývá ideál okruhu R, jestliže

- $I \neq \emptyset$;
- $\forall a, b \in I : a + b \in I$;
- $\forall a \in I \ \forall r \in R : a \cdot r,\ r \cdot a \in I$.

Poznámka. Pro libovolný okruh R tvoří $\{0\}$ i R ideály okruhu R. Evidentně jde o nejmenší a největší ideál okruhu R.

Věta 1. Nechť $I \subseteq R$ je ideál okruhu R, pak

- I je podgrupa grupy $(R, +)$;
- $1 \in I$, právě když $I = R$.

Ideál generovaný množinou

Věta 2. *Nechť $S \neq \emptyset$ je libovolná množina taková, že pro každé $s \in S$ je dán ideál I_s okruhu R. Pak $\bigcap_{s \in S} I_s$ je ideál okruhu R.*

Důsledek. *Nechť R je okruh. Systém všech ideálů okruhu R uspořádaný inkluzí je úplný svaz.*

Definice. Nechť R je okruh. Předchozí věta nám umožňuje definovat ideál okruhu R generovaný množinou $M \subseteq R$ jako průnik všech ideálů tuto množinu obsahujících. Je to tedy nejmenší ideál okruhu R obsahující M, značíme jej (M). Je-li $M = \{a_1, \dots, a_n\}$, píšeme místo (M) také $(a_1, \dots, a_n)$.

Věta 3. *Nechť R je komutativní okruh, $a_1, \dots, a_n \in R$. Pak $(a_1, \dots, a_n) = \{r_1 a_1 + \cdots + r_n a_n;\ r_1, \dots, r_n \in R\}$.*

Definice. Nechť R je komutativní okruh, $a \in R$. Ideál $(a) = \{ra;\ r \in R\}$ nazýváme hlavní ideál okruhu R generovaný prvkem a.

Dělitelnost v komutativním okruhu a ideály

Věta 4. *Nechť R je komutativní okruh, $a, b, c \in R$.*

1. $(a) = \{x \in R;\ a \mid x\}$;
2. $(a) \subseteq (b)$, *právě když* $b \mid a$;
3. $(a) = (b)$, *právě když* $a \sim b$;
4. $(a) = R$, *právě když* $a \in R^\times$;
5. $(a) \cap (b) = (c)$, *právě když* c *je nejmenší společný násobek prvků* a, b;
6. $(a, b) = (c)$, *právě když* c *je největší společný dělitel prvků* a, b *a současně je* c *ve tvaru* $c = ra + sb$ *pro vhodné* $r, s \in R$.

Definice. Okruh R se nazývá okruh hlavních ideálů, jestliže

- R je obor integrity;
- každý ideál okruhu R je hlavní.

Příklad. Okruh $\mathbb{Z}$ je okruh hlavních ideálů. Každé těleso je okruh hlavních ideálů. Okruh zbytkových tříd $\mathbb{Z}_m$ je okruh hlavních ideálů, právě když je m prvočíslo.

Věta 5. *Nechť R je netriviální komutativní okruh. Pak R je těleso, právě když R a $\{0\}$ jsou jediné ideály okruhu R.*

Věta 6. *Nechť R je těleso. Pak každý ideál okruhu polynomů $R[x]$ je hlavní.*

Důsledek. *Nechť R je těleso. Pak okruh polynomů $R[x]$ je okruh hlavních ideálů.*

Příklad. Okruh $\mathbb{Z}[x]$ není okruh hlavních ideálů, neboť například ideál $(x, 2)$ není hlavní.

Věta 7. *Nechť $f : R \to S$ je homomorfismus okruhů. Pak platí:*

1. *je-li J ideál okruhu S, pak $f^{-1}(J) = \{x \in R;\ f(x) \in J\}$ je ideál okruhu R;*
2. *jestliže f je surjektivní a I je ideál okruhu R, pak $f(I) = \{f(x); x \in I\}$ je ideál okruhu S.*

Důsledek. *Jádro libovolného homomorfismu okruhů $f : R \to S$ je ideál okruhu R, vždyť $\ker f = f^{-1}(\{0\})$.*