

Euklidovské okruhy

14. apríla 2025

Euklidovské okruhy

Definícia

Obor integrity R sa nazýva *euklidovský okruh*, ak existuje funkcia $N: R \setminus \{0\} \rightarrow \mathbb{N}$ taká, že pre ľubovoľné $a, b \in R$, $b \neq 0$ existujú $q, r \in R$ také, že $a = qb + r$ a buď $r = 0$ alebo $N(r) < N(b)$. Funkciu N budeme nazývať *norma*.

$$q = ab + r \quad \text{a} \quad N(r) < N(b)$$

Euklidovské okruhy

$$q = ab + r \quad a \quad N(r) < N(b)$$

- ▶ $\mathbb{Z}$ a $F[x]$ sú euklidovské okruhy.
- ▶ V $\mathbb{Z}$ aj v $F[x]$ platí veta o delení so zvyškom.
- ▶ Norma v $\mathbb{Z}$ je $N(a) = |a|$.
- ▶ Norma v $F[x]$ je stupeň polynómu.

Euklidovské okruhy

Lema

Ak R je euklidovský okruh, $u \neq 0$ a $N(u) = 0$, tak u je deliteľ jednotky.

Okruhy hlavných ideálov

Definícia

Ak R je obor integrity, hovoríme, že R je okruh hlavných ideálov, ak každý ideál v R je hlavný, t.j. ak je tvaru

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

pre nejaké $a \in R$.

Okruhy hlavných ideálov

Tvrdenie

Každý euklidovský okruh je okruh hlavných ideálov.

Plán:

- ▶ Zoberme prvok $b \in I \setminus \{0\}$ s najmenšou normou.
- ▶ Ukážme $I = (b)$.

Okruhy hlavných ideálov

- ▶ Každý euklidovský okruh je okruh hlavných ideálov.
- ▶ Špeciálne $\mathbb{Z}$ a $F[x]$ sú OHI.

Okruhy hlavných ideálov

Okruh $\mathbb{Z}[x]$ nie je OHI.

$$(2, x) = \{a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]; a_0 \in 2\mathbb{Z}, a_i \in \mathbb{Z} \text{ pre } i \geq 1\}$$

Okruhy hlavných ideálov

Tvrdenie

Ak $I = (m)$, $I \neq \{0\}$, je prvoideál v OHI R , tak I je maximálny.

OHI a deliteľnosť

$$a \mid b \Leftrightarrow b \in (a) \Leftrightarrow (b) \subseteq (a)$$

$$a \sim b \Leftrightarrow (a) = (b)$$

OHI a deliteľnosť

- ▶ $(a_1, \dots, a_n)$ označuje najmenší ideál obsahujúci všetky prvky $a_1, \dots, a_n$.

$$(a_1, \dots, a_n) = \left\{ \sum_{i=1}^n x_i a_i; x_i \in R \right\}$$

- ▶ Špeciálne máme:

$$(a, b) = \{ax + by; x, y \in R\}.$$

Najväčší spoločný deliteľ

Definícia

Najväčší spoločný deliteľ prvkov $a, b \in R$ je taký prvok $c \in R$, že

- (i) $c \mid a, c \mid b$,
 - (ii) pre ľubovoľný prvok $d \in R$ taký, že $d \mid a$ a $d \mid b$ platí aj $d \mid c$.
- Označujeme ho $\gcd(a, b)$.

Je určený jednoznačne až na asociovanosť.

Najväčší spoločný deliteľ

Lema

Ak R je obor integrity a $a, b \in R$, tak

$$\gcd(a, b) = \gcd(a + bx, b)$$

pre ľubovoľné $x \in R$.

Bézoutova identita v OHI

Tvrdenie (Bézoutova identita)

Ak R je okruh hlavných ideálov, tak pre ľubovoľné $a, b \in R$ existuje v R najväčší spoločný deliteľ $c = \gcd(a, b)$.

Navyše, existujú také $x, y \in R$, že

$$c = xa + yb.$$

OHI a deliteľnosť

Dôsledok

Nech R je okruh hlavných ideálov, $a, b, c \in R$, $a, b \neq 0$. Ak $\gcd(a, b) = 1$ a $a \mid bc$, tak $a \mid c$.

$$\gcd(a, b) = 1 \quad \wedge \quad a \mid bc \quad \Rightarrow \quad a \mid c$$

Ireducibilné prvky

Definícia

Prvok $a \neq 0$ okruhu R sa nazýva *ireducibilný*, ak a je nenulový, nie je to deliteľ jednotky a ak z rovnosti $a = bc$ vyplýva, že niektorý z prvkov b , c je deliteľ jednotky v R .

- ▶ V $\mathbb{Z}$ sú čísla $\pm p$, kde p je prvočíslo.
- ▶ V $F[x]$ sú to ireducibilné polynómy.

Okruh s jednoznačným rozkladom

Definícia

Okruh s jednoznačným rozkladom (alebo tiež *Gaussov okruh*) je obor integrity, v ktorom pre každý prvok $x \in R$, ktorý je nenulový a nie je deliteľom jednotky, existuje rozklad

$$x = p_1 \dots p_k$$

na súčin ireducibilných prvkov a navyše je tento rozklad jednoznačný až na asociovanosť a poradie.

Ireducibilné prvky a prvoideály

Tvrdenie

Ak ideál (p) v obore integrity R je vlastný prvoideál a $p \neq 0$, tak p je ireducibilný v R .

Tvrdenie

Ak p je ireducibilný prvok v OHI R , tak (p) je prvoideál.

Dôsledok

V OHI pre ľubovoľný ireducibilný prvok p platí implikácia

$$p \mid ab \quad \Rightarrow \quad p \mid a \vee p \mid b.$$

Jednoznačný rozklad v OHI

$$p \mid ab \quad \Rightarrow \quad p \mid a \vee p \mid b$$

Tvrdenie

Každý okruh hlavných ideálov je okruhom s jednoznačným rozkladom.