Deliteľnosť, rozklad na ireducibilné polynómy

7. apríla 2025

Deliteľnosť

Deliteľnosť

Lema

Nech R je obor integrity, $a, b \in R$. Ak platí $ab = a$ pre $a \neq 0$, tak $b = 1$.

$$ab = a$$
$$a(b-1) = 0$$

Deliteľnosť

Deliteľnosť

Definícia

Nech R je obor integrity. Hovoríme, že a *delí* b, označujeme $a \mid b$, ak existuje $c \in R$ také, že $b = ca$.

- $3 \mid 9$, $3 \nmid 7$ v $\mathbb{Z}$
- $3 \mid \pm 9$ v $\mathbb{Z}$
- $x - 1 \mid x^2 - 1$ v $\mathbb{R}[x]$

Deliteľnosť

Deliteľnosť

Lema

Nech R je obor integrity. Potom pre ľubovoľné $a, b, c, d \in R$, $a_i, r_i \in R$ platí

(i) $a \mid a$

(ii) $a \mid b \wedge b \mid c \Rightarrow a \mid c$

(iii) $a \mid b \wedge c \mid d \Rightarrow ac \mid bd$

(iv) $a \mid 0,\ 1 \mid a$

(v) $0 \mid a \Leftrightarrow a = 0$

(vi) $ac \mid bc \wedge c \neq 0 \Rightarrow a \mid b$

(vii) $a \mid a_i$ *pre* $i = 1, \ldots n \Rightarrow a \mid a_1 r_1 + \cdots + a_n r_n$

Deliteľnosť

Asociovanosť

Definícia

Ak $a, b \in R$, kde R je obor integrity, hovoríme, že prvky a a b sú *asociované,* označujeme $a \sim b$, ak $a \mid b$ a súčasne $b \mid a$

$$a \mid b \ \wedge \ b \mid a \Leftrightarrow a \sim b$$

Lema

Nech R je obor integrity. Pre ľubovoľné $a, b, c, d \in R$ platí

(i) $a \sim b \wedge b \sim c \Rightarrow a \sim c$

(ii) $a \sim a$

(iii) $a \sim b \Rightarrow b \sim a$

(iv) $a \sim b \wedge c \sim d \Rightarrow ac \sim bd$

Deliteľnosť

Delitele jednotky

Definícia

Ak okruh R má jednotku a $ab = 1$, hovoríme, že a je *deliteľ jednotky.* Množinu všetkých deliteľov jednotky budeme označovať $U(R)$.

- ± 1 v $\mathbb{Z}$
- nenulové konštantné polynómy v $F[x]$

Deliteľnosť

Asociovanosť a delitele jednotky

Tvrdenie

Nech R je obor integrity. Potom

(i) *Delitele jednotky s operáciou násobenia tvoria grupu, t.j. $(U(R), \cdot)$ je grupa.*

(ii) *$a \sim b$ práve vtedy, keď existuje deliteľ jednotky u taký, že $a = bu$.*

Euklidovské okruhy

Veta o delení so zvyškom

- V okruhu $F[x]$:

$$f(x) = q(x) \cdot g(x) + r(x) \qquad \text{a} \qquad \operatorname{st} r(x) < \operatorname{st} g(x).$$

- V okruhu Z:

$$a = qb + r \qquad \text{a} \qquad |r| < |b|.$$

Euklidovské okruhy

Euklidovské okruhy

Definícia

Obor integrity R sa nazýva *euklidovský okruh,* ak existuje funkcia $N\colon R \setminus \{0\} \to \mathbb{N}$ 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.*

- V literatúre sa vyskytuje aj podmienka $N(a) \leq N(ab)$.
- $\mathbb{Z}$ a $F[x]$ sú euklidovské okruhy.

Euklidovské okruhy

Euklidovské okruhy

Lema

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

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.

Euklidov algoritmus

Lema

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

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

pre ľubovoľné $x \in R$. Uvedenú rovnosť treba chápať tak, že ak existuje jedna strana (ľavá alebo pravá), potom existuje aj druhá strana a spĺňa uvedenú rovnosť.

Euklidov algoritmus

$$a = q \cdot b + r \qquad \Rightarrow \qquad \gcd(a, b) = \gcd(b, r)$$

Vypočet n.s.d: opakovaným delením so zvyškom.

Euklidov algoritmus

$$
\begin{aligned}
a &= q_1 \cdot b + r_1 && N(r_1) < N(b) \\
b &= q_2 \cdot r_1 + r_2 && N(r_2) < N(r_1) \\
r_1 &= q_3 \cdot r_2 + r_3 && N(r_3) < N(r_2) \\
&\vdots && \vdots \\
r_{l-2} &= q_l \cdot r_{l-1} + r_l && N(r_l) < N(r_{l-1}) \\
r_{l-1} &= q_{l+1} \cdot r_l && \text{zvyšok } 0
\end{aligned}
$$

Euklidov algoritmus

$$
\begin{aligned}
a &= q_1 \cdot b + r_1 & r_1 &= a - q_1 . b \\
b &= q_2 \cdot r_1 + r_2 & r_2 &= b - q_2 . r_1 = (1 + q_1 q_2) b - q_2 a \\
r_1 &= q_3 \cdot r_2 + r_3 & r_3 &= r_2 - q_3 . r_2 = \cdots = x_3 a + y_3 b \\
&\vdots & &\vdots \\
r_{l-2} &= q_l \cdot r_{l-1} + r_l & r_l &= r_{l-2} - q_l . r_{l-1} = \cdots = x_l a + y_l b \\
r_{l-1} &= q_{l+1} \cdot r_l
\end{aligned}
$$

Najväčší spoločný deliteľ

Tvrdenie

Ak R je okruh $\mathbb{Z}$ alebo $F[x]$, 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

$$c = xa + yb.$$

Dôsledok

Nech R je okruh $\mathbb{Z}$ alebo $F[x]$, $a, b, c \in R$, $a, b \neq 0$. Ak $\gcd(a, b) = 1$ ($\gcd(a, b) \sim 1$) a $a \mid bc$, tak $a \mid c$.

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

Euklidov algoritmus

$$89 = 5 \cdot 16 + 9$$
$$16 = 1 \cdot 9 + 7$$
$$9 = 1 \cdot 7 + 2$$
$$7 = 3 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

$$9 = 89 - 5 \cdot 16$$
$$7 = 16 - 9 = 6 \cdot 16 - 89$$
$$2 = 9 - 7 = 2 \cdot 89 - 11 \cdot 16$$
$$1 = 7 - 3 \cdot 2 = 39 \cdot 16 - 7 \cdot 89$$

$$1 = 39 \cdot 16 - 7 \cdot 89.$$

Euklidov algoritmus

89	1	0	
16	0	1	
9	1	-5	1r-5*2r
7	-1	6	2r-3r
2	2	-11	3r-4r
1	-7	39	4r-3*5r

Rozklad polynómu na ireducibilné polynómy

Ireducibilné prvky

Definícia

Prvok $a \neq 0$ obore integrity 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 okruhu $\mathbb{Z}$ sú to $\pm p$, kde p je prvočíslo.
- V okruhu $F[x]$ to je definícia *ireducibilného polynómu.*

Rozklad polynómu na 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.

Rozklad polynómu na ireducibilné polynómy

Ireducibilné prvky a $p \mid ab$

Dôsledok

Nech R je okruh $\mathbb{Z}$ alebo $F[x]$. Pre ľubovoľný ireducibilný prvok $p \in R$ platí implikácia

$$p \mid ab \qquad \Rightarrow \qquad p \mid a \vee p \mid b,$$

a všeobecnejšie,

$$p \mid a_1 \dots a_n \qquad \Rightarrow \qquad (\exists i \in \{1, \dots, n\})\ p \mid a_i.$$

Rozklad polynómu na ireducibilné polynómy

Existencia a jednoznačnosť rozkladu

Tvrdenie

Každý okruh typu $F[x]$ (a aj okruh $\mathbb{Z}$) je okruhom s jednoznačným rozkladom.