$a \sim b$ asociované $:\Leftrightarrow a|b,\ b|a$

$\Leftrightarrow \exists e \in R^\times: a = b\cdot e$

„$\Leftarrow$" $b|a$; $a = b\cdot e \ /\cdot e^{-1}$

$a\cdot e^{-1} = b$

tj. $a|b$

„$\Rightarrow$" $a|b \Rightarrow \exists c \in R: a\cdot c = b$

$b|a \Rightarrow \exists d \in R: a = b\cdot d$

$\Rightarrow a = (a\cdot c)\cdot d = a\cdot(c\cdot d)$

$\Rightarrow 1 = c\cdot d$, tj. $c|1$, $d|1$

$\Rightarrow c, d \in R^\times$

3 20-15:56

$\mathbb{Z}^\times = \{1,-1\}$

$(\mathbb{Z}[i])^\times = \{1, i, -1, -i\}$

$a+bi \in \mathbb{Z}[i]$

kdy $a+bi$ je jednotka v $\mathbb{Z}[i]$?

$$\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}\, i \in \mathbb{Z}[i]$$

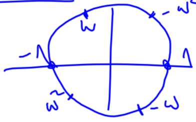
tj. $a^2+b^2 \mid a$, $a^2+b^2 \mid b$

$a,b \in \mathbb{Z}$, $a^2+b^2 \neq 0$ $\Rightarrow a^2+b^2 \mid a \Rightarrow a^2+b^2 = 1$

$\Rightarrow a=\pm 1, b=0$; $a=0, b=\pm 1$

Př: $\mathbb{Z}[\omega]$ má 6 jednotek

$\omega^3 = 1$ $\quad \{1, \omega, \omega^2, -1, -\omega, -\omega^2\}$



3 20-16:13

Jednoznačnost rozkladu:

$$-6 = 2\cdot(-3) = 3\cdot(-2) = (-2)\cdot 3$$

$2 \sim (-2)$

$-3 \sim 3$

rozklad považujeme za „jediný"

3 20-16:22

Dělitelnost a nerozložitelnost | Kořeny a rozklady polynomů | Polynomy více proměnných | Podílová tělesa

Příklad

1. $\mathbb{Z}$, $\mathbb{R}[x]$ jsou obory integrity s jednoznačným rozkladem (ireducibilní prvky v $\mathbb{Z}$ jsou prvočísla a čísla k nim opačná).
2. Každé těleso je obor integrity s jednoznačným rozkladem (kde každý nenulový prvek je jednotka).
3. Např. v okruhu $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5};\ a, b \in \mathbb{Z}\}$ existují dva různé rozklady čísla 6 na nerozložitelné prvky:
$$6 = 2\cdot 3 = (1-\sqrt{-5})(1+\sqrt{-5}).[a]$$

[a] To, že uvedené prvky jsou ireducibilní a že nejsou asociované, je ale třeba trochu „odpracovat".

(3) $\mathbb{R}[\sqrt{-5}]$ je těleso!

$$\frac{1}{a+b\sqrt{-5}} = \frac{a-b\sqrt{-5}}{a^2+5b^2} = \underbrace{\frac{a}{a^2+5b^2}}_{\in\mathbb{R}} - \underbrace{\frac{b}{a^2+5b^2}}_{\in\mathbb{R}}\sqrt{-5} \in \mathbb{R}[\sqrt{-5}]$$

3 20-16:25

$\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ (OJR) UFD

$\mathbb{Z}[\sqrt{-5}]$ není UFD

$\mathbb{Z}[\sqrt{-3}] = \mathbb{Z}[\omega]$ je UFD

3 20-16:28

Př: $\mathbb{Z}[x]$, $f(x) = x^2$, $g(x) = 3x+1$

$a=9$: $9x^2 = (3x+1)\cdot(3x-1)+1$

$-3x$

$+1$ zb.

Př: $\mathbb{Q}[x]$ $\quad x^2 = (3x+1)\cdot\left(\frac{1}{3}x - \frac{1}{9}\right) + \frac{1}{9}$

3 20-16:32

V $\mathbb{Z}[i]$ platí dělení se zbytkem:

$\forall \alpha, \beta \neq 0$ ze $\mathbb{Z}[i]$ ex. $\gamma, \rho \in \mathbb{Z}[i]$

$$\alpha = \beta \cdot \gamma + \rho$$

$(N(\rho) < N(\beta)$ nebo $\rho = 0)$

kde $N(a+bi) = a^2 + b^2$

3 20-16:38

$$f(x) = q(x) \cdot (x - b) + r$$

dosadíme b za x:

$$f(b) = q(b) \cdot (b - b) + r$$

$$f(b) = r$$

3 20-16:44

Horner: $f(x) = a_n x^n + \dots + a_1 x + a_0$

$a_i \in R$

	a_n	a_{n-1}	$\dots$	a_1	a_0
b					
	a_n	$a_n \cdot b + a_{n-1}$	$b(a_n \cdot b + a_{n-1}) + a_{n-2}$	$\dots$	0
	c_{n-1}	$\dots$		c_0	r

$$\underbrace{c_{n-1} \; \dots \; c_0}_{q(x)}$$

$$f(x) = q(x) \cdot (x - b) + r$$

3 20-16:45

$f(x) = x^2 - 1$ nad $\mathbb{Z}_8$

$f(x) = [1]_8 \cdot x^2 - [1]_8$

formálně

$f(b) = 0$ pro $b \in \{[1], [3], [5], [7]\}$

3 20-16:47

Př: $(\mathbb{Z}_5^\times, \cdot)$ je cyklická

$\mathbb{Z}_5^\times = \langle 2 \rangle$

$\{2^1, 2^2, 2^3, 2^4\}$
$\;\; 2, \; 4, \; 3, \; 1 \}$

Př: $(\mathbb{Z}_7^\times, \cdot)$ je cyklická

$\mathbb{Z}_7^\times \neq \langle 2 \rangle$

$\{2^1, 2^2, 2^3, 2^4, 2^5, 2^6$
$\;\; 2, \; 4, \; 1, \; 2, \; 4, \; 1$

$\langle 3 \rangle = \{3^1 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv 1\}$

3 20-16:53

Obecně máme různé polynomy určující totéž polynomiální zobrazení:

nad $\mathbb{Z}_2$: $\left.\begin{array}{l} f \equiv 0 \\ g(x) = x^2 + x \end{array}\right\}$ určují nulové zobrazení

$\left.\begin{array}{l} f(x) = x^4 + 1 \\ g(x) = x + 1 \end{array}\right\}$ určují totéž zobrazení

nad $\mathbb{Z}_3$: $f(x) = x^3 - x$ určuje nulové zobrazení

3 20-16:59

nad $\mathbb{R}$ nemusí mít žádné kořeny

a) x^2+1

b) $(x^2+1)^2$

c) $(x^2+1)(x^2+2)$

3 20-17:09

$3x^3+2x^2+x+1$

je ired. nad $\mathbb{Z}$ $\Rightarrow$ ir. nad $\mathbb{Q}$

$=\left(\frac{3}{2}x+\dots\right)\left(2x^2\dots\right)$

Věta $\sqrt{2}\notin\mathbb{Q}$

x^2-2, ten je ired. nad $\mathbb{Z}$

$(\pm\sqrt{2}\notin\mathbb{Z}) \Rightarrow$ ired. nad $\mathbb{Q}$

Obecněji: $m\in\mathbb{N}$, $m\neq a^2$ pro $a\in\mathbb{Z}$ $\Rightarrow \sqrt{m}\notin\mathbb{Q}$

3 20-17:11

Jinak: sporem ($\sqrt{2}\in\mathbb{Q}$): $\exists\, r,s\in\mathbb{Z}$:

$\sqrt{2}=\frac{r}{s}$ $\quad (r,s)=1$

$s\sqrt{2}=r \quad |^2$

$2s^2=r^2$

$\Rightarrow 2\mid r^2 \Rightarrow 2\mid r \Rightarrow 4\mid r^2$

$\Rightarrow 4\mid 2s^2 \Rightarrow 2\mid s^2 \Rightarrow 2\mid s$ ↯

3 20-17:14

Věta

Má-li polynom $f(x)=a_nx^n+\cdots+a_0\in\mathbb{Z}[x]$ racionální kořen $r/s\in\mathbb{Q}$ v základním tvaru, pak $r\mid a_0$ a $s\mid a_n$.

$\underbrace{f\left(\frac{r}{s}\right)}_{=0}=a_n\cdot\left(\frac{r}{s}\right)^n+\dots+a_1\cdot\frac{r}{s}+a_0 \quad |\cdot s^n$

$0=a_n\cdot r^n+a_{n-1}\cdot r^{n-1}\cdot s+\dots+a_1\cdot r s^{n-1}+a_0 s^n$

$\Rightarrow r\mid a_0\cdot s^n \wedge (r,s)=1 \Rightarrow r\mid a_0$

$\Rightarrow s\mid a_n\cdot r^n \wedge (r,s)=1 \Rightarrow s\mid a_n$

3 20-17:17

$x^3-3x-1\in\mathbb{Q}[x]$ je ireducibilní

$\mathbb{Q}[x]$ je UFD

kdyby se dal rozložit $\Rightarrow \exists$ jeho lineární (st = 1) dělitel $\Rightarrow$ má kořen

ired. nad $\mathbb{Q}$ $\Leftrightarrow$ ired. nad $\mathbb{Z}$

má x^3-3x-1 kořen v $\mathbb{Z}$?

kandidáti ± 1 nevyhovují $\left(\frac{r}{s};\ r\mid a_0,\ s\mid a_n\right)$

3 20-17:21

$\underbrace{x^3-3x-1}_{f(x)}\in\mathbb{Z}_2[x]$

red. $\Rightarrow$ má kořen v $\mathbb{Z}_2$ kořen není splněno

$f([0])=[1]$

$f([1])=[1]$

3 20-17:25

Dk Eisensteinova kritéria

sporem $\exists g,h \in \mathbb{Z}[x]$ $f = g \cdot h$

$g(x) = b_m x^m + \dots + b_1 x + b_0$

$h(x) = c_\ell x^\ell + \dots + c_1 x + c_0$

$n = m + \ell$

$b_i, c_j \in \mathbb{Z}$

$a_0 = b_0 \cdot c_0$ $\quad p \mid b_0 \cdot c_0 \wedge p^2 \nmid b_0 \cdot c_0$

BÚNO: $p \mid b_0 \Rightarrow p \nmid c_0$

$a_1 = b_1 \cdot c_0 + b_0 \cdot c_1$ $\quad p \mid a_1 \wedge p \mid b_0 \Rightarrow$

$a_2 = b_2 \cdot c_0 + b_1 \cdot c_1 + b_0 \cdot c_2$ $\quad p \mid b_1 \cdot c_0 \wedge p \nmid c_0 \Rightarrow p \mid b_1$

$\vdots$

$a_n = b_m \cdot c_\ell$ $\quad$ indukcí: $\forall i: p \mid b_i$ spor

$\Rightarrow p \mid b_m \Rightarrow p \mid a_n$

3 20-17:30

Dělitelnost a nerozložitelnost | Kořeny a rozklady polynomů | Polynomy více proměnných | Podílová tělesa

Poznámka

Užitečná je často také tzv. *lokalizace*, tj. redukce koeficientů modulo zvolené prvočíslo p, příp. posunutí proměnné o konstantu. Např., že polynom $x^3 + 27x^2 + 5x + 97$ je ireducibilní, zjistíme díky redukci (modulo 3). "$f(x)$"

Kdyby $f = g \cdot h$ nad $\mathbb{Z}$

$\Rightarrow f \bmod 3 = (g \bmod 3) \cdot (h \bmod 3)$ nad $\mathbb{Z}_3$

$f \bmod 3$: $x^3 + 2x + 1 \equiv x^3 - x + 1$

nemá kořen v $\mathbb{Z}_3 \Rightarrow$ je ired.

3 20-17:36

Věta

Je-li α kořenem polynomu f nad tělesem násobnosti $k > 1$, je α kořenem f' násobnosti $k - 1$.

$f(x) = (x-\alpha)^k \cdot g(x)$, kde $x - \alpha \nmid g(x)$

$f'(x) = k(x-\alpha)^{k-1} \cdot g(x) + (x-\alpha)^k \cdot g'(x)$

zřejmě $(x-\alpha)^{k-1} \mid f'(x)$

navíc $(x-\alpha)^k \mid f'(x) \Rightarrow x - \alpha \mid g(x)$ ↯

3 20-17:39