okruh: $(R,+,\cdot)$

$(R,+)$ kom. grupa

$(R,\cdot)$ (kom.) pologrupa s 1

distr. zákon

$a\cdot(b+c) = a\cdot b + a\cdot c$

$(b+c)\cdot a = b\cdot a + c\cdot a$

3 30-12:13

$(\mathbb{Z}_4,+,\cdot)$

$\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$

$[2]_4\cdot[2]_4 = [4]_4 = [0]_4$ (nula $\mathbb{Z}_4$)

dělitelé nuly v $\mathbb{Z}_4$

[R obor integrity: $\forall a,b\in R: a\cdot b = 0 \Rightarrow a=0 \vee b=0$]

$\mathbb{Z}_p$ je OI (integral. domain)

$a\cdot b \equiv 0\ (p) \Leftrightarrow p \mid a\cdot b \Rightarrow p\mid a \vee p\mid b$

$[a]_p = [0]_p$, $a \not\equiv 0 (p)$, $b \equiv 0 (p)$

3 30-12:17

aa1: $0\cdot c = 0$

0 je neutrální v $(R,+)$

$0+0=0 \Rightarrow (0+0)\cdot c = 0\cdot c + 0\cdot c$ (distr.)

$0\cdot c$

$0\cdot c + 0\cdot c = 0\cdot c \quad /+ -(0\cdot c)$

$0\cdot c + (0\cdot c - 0\cdot c) = 0\cdot c + (-(0\cdot c))$

$0\cdot c + 0 = 0$

$0\cdot c = 0$

ad3: dokáže $(-c)\cdot d + (c\cdot d) = 0$ (distr.)

Víme $0\cdot d = 0 \Rightarrow (-c+c)\cdot d = 0 \Rightarrow$

$\Rightarrow (-c)\cdot d + c\cdot d = 0$ □

3 30-12:24

nejednoznačnost podílu

$(\mathbb{Z}_6,+,\cdot)$ $[2]:[2] = ?$

$[2] = [2]\cdot[1]$ $[1]_6 \neq [4]_6$

$[2] = [2]\cdot[4]$

v $\mathbb{Z}_8$ $[4]\cdot[1] = [4] = [4]\cdot[3]$

$= [4]\cdot[5] = [4]\cdot[7]$

3 30-12:34

Inverze v $\mathbb{Z}_p$:

$[a]: [a]\cdot[x] = [1]$

$p \nmid a$ $\quad a\cdot x \equiv 1 \pmod p$

① M. F. V. $a^{p-1} \equiv 1\ (p)$

vhodné $x = a^{p-2}$

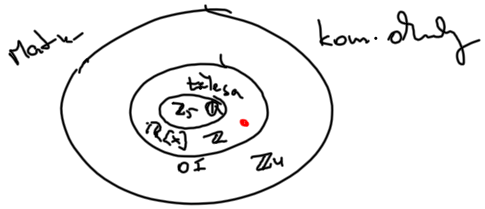
② Bezout: $(a,p)=1 \Rightarrow \exists k,l\in\mathbb{Z}$

$a\cdot k + p\cdot l = 1$

$\Rightarrow a\cdot k \equiv 1 \pmod p$

$x = k$

3 30-12:41



Věta každé těleso je obor integrity

Dk: $a\cdot b = 0 \quad /\cdot a^{-1}$ ($a\neq 0$ je invertibilní)

$a\neq 0$ $(a^{-1}\cdot a)b = a^{-1}\cdot 0$

$b = 1\cdot b = 0 \Rightarrow b = 0 \Rightarrow$ je to OI.

3 30-12:43

Věta

Každý konečný obor integrity je těleso.

Zvolme $a \in R \setminus \{0\}$ pevně

$\varphi_a : R \to R$

$\varphi_a : x \mapsto a \cdot x$

Ukážeme, že φ_a je bijekce, pak ex. $b \in R$:

$\varphi_a(b) = 1 \Leftrightarrow ab = 1 \Rightarrow b = a^{-1}$

φ_a je bijekce, protože φ_a je injekce (komutuje R!)

$(\varphi_a(x) = \varphi_a(y) \Leftrightarrow a \cdot x = a \cdot y \Leftrightarrow a \cdot (x - y) = 0$

$\Downarrow$

$x - y = 0 \Rightarrow x = y)$

3 30-12:53

$\mathbb{Z}_6[x]$ není obor integrity

$[2] \cdot [3] = [0]$

$([2] \cdot x)([3] \cdot x^2) = [0] \cdot x^3 = [0]$

$f(x) \cdot g(x) = 0$ v $R[x]$

$\deg f = k, \deg g = l$

$a_k \cdot b_l$ je koef. u x^{k+l} v součinu $f(x) \cdot g(x)$

$\Rightarrow a_k \cdot b_l = 0 \wedge a_k \neq 0 \neq b_l$ spor

(R je OI)

3 30-13:08

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

$(\mathbb{Q}[x])^\times = \mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$

$(R[[x]])^\times = \{a_0 + a_1 x + \dots ; a_0 \in R^\times\}$

$(R[x])^\times = \{a_0 ; a_0 \in R^\times\}$

$\frac{1}{1-x} = 1 + x + x^2 + \dots$ $\quad 1 - x \notin \mathbb{Z}[x]$, $1 - x \in \mathbb{Z}[[x]]$

$(1-x)(1 + x + x^2 + \dots) = 1$

3 30-13:15

v $\mathbb{Z}$: $6 = 2 \cdot 3 = (-3) \cdot (-2)$

$2 = (-1)(-2)$, $-1 \in \mathbb{Z}^\times$

$3 = (-1)(-3)$, $-1 \in \mathbb{Z}^\times$

v R (obecně v těleso) nejsou žádné ireducibilní prvky

3 30-13:29

$R[\sqrt{-5}] = \{a + b\sqrt{-5} ; a, b \in R\}$

je těleso $\Rightarrow$ OJR (UFD)

$a \neq 0$ nebo $b \neq 0$ (tj. $a + b\sqrt{-5} \neq 0$)

$\frac{1}{a + b\sqrt{-5}} = \frac{a - b\sqrt{-5}}{a^2 + 5b^2} = \frac{a}{a^2 + 5b^2} + \frac{-b}{a^2 + 5b^2}\sqrt{-5}$

$\in R[\sqrt{-5}]$

tj. lib. nenulový prvek $R[\sqrt{-5}]$ má inverzi.

v $\mathbb{Z}[i]$ není 2 ireducibilní

$2 = (1+i)(1-i)$, kde $1+i, 1-i \notin \mathbb{Z}[i]^\times$

3 30-13:45

$\frac{1}{1+i} = \frac{1-i}{1-i^2} = \frac{1-i}{2} = \frac{1}{2} - \frac{1}{2}i$

$\notin \mathbb{Z}[i]$

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

3 30-13:50

$f = x^2$, $g = 3x+1$ nad $\mathbb{Z}[x]$

$q \cdot f = q \cdot g + r$

$q \cdot x^2 = 3x\,(3x+1) - 3x$

$-3x = (-1)(3x+1) + 1$

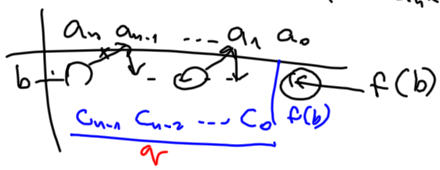
(q) $x^2 = (3x-1)(3x+1) + 1$ $\quad st(1) < st(3x+1)$

$f = x^2$, $g = 3x+1$ $\quad f, g \in \mathbb{R}[x]$

(1) $x^2 = \frac{1}{3}(3x+1) - \frac{1}{3}$

3 30-13:54

Hornerovo schéma $f(x) = a_n x^n + \dots + a_1 x + a_0$



$f = \underbrace{(c_{n-1}x^{n-1} + \dots + c_0)}_{q} \cdot (x-b) + f(b)$

3 30-14:02

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

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

$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 3, 2^4 \equiv 1$

$\mathbb{Z}_7^\times \neq \langle [2] \rangle = \{[1], [2], [4]\}$

$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1, 2^4 \equiv 2, \dots$

$\mathbb{Z}_7^\times = \langle [3] \rangle = \langle [5] \rangle$

3 30-14:11

Dva polynomy nad nekonečným ~~komutativním okruhem~~ tělesem, které zadávají stejné zobrazení $R \to R$, mají rozdíl, jehož kořenem je každý prvek v R. Protože rozdíl polynomů má jen konečný stupeň, pokud není nulový, dokázali jsme tak již dříve uvedené tvrzení:

Věta

Jestliže je R ~~nekonečný okruh~~ (=těleso), pak dva polynomy $f(x)$ a $g(x)$ nad R jsou stejné právě, když jsou stejná příslušná zobrazení f a g.

$\mathbb{Z}_2$: $x^2 + x$ zadává nulové zobrazení

3 30-14:16

$f(x) \in \mathbb{R}[x]$

f má kořen v $\mathbb{R} \Rightarrow f$ je reducibilní

~~$\Leftarrow$~~

Př. $(x^2+1)^2 \in \mathbb{R}[x]$

3 30-14:30

$\sqrt{2} \notin \mathbb{Q}$

SPOREM: $\sqrt{2} = \frac{r}{s}$ $\quad r, s \in \mathbb{Z}$, $s \neq 0$, $(r, s) = 1$

$2s^2 = r^2$

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

$\Rightarrow 2 \mid s^2 \Rightarrow 2 \mid s$ SPOR

GAUSSOVO LEMMA

$f(x) = x^2 - 2 \in \mathbb{Z}[x]$

nemá kořeny v $\mathbb{Z} \Rightarrow$ ireducibilní nad $\mathbb{Z}$

$\Rightarrow$ ireducibilní nad $\mathbb{Q} \Rightarrow$ nemá kořeny v $\mathbb{Q}$

$\Rightarrow \sqrt{2} \notin \mathbb{Q}$ · Anal. pro $\sqrt{a}$, $a \neq a^2$, $a \in \mathbb{Z}$

3 30-14:32

$f(x) = a_n x^n + \dots + a_1 x + a_0 \quad a_i \in \mathbb{Z}$, $a_n \neq 0$

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

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

$r \mid 0 \Rightarrow r \mid a_n r^n + \dots + a_0 s^n \Rightarrow r \mid a_0 s^n \overset{(r,s)=1}{\Longrightarrow} r \mid a_0$

$s \mid 0 \Rightarrow s \mid a_n r^n \Rightarrow s \mid a_n$

3 30-14:38

Př: $x^3 - 3x - 1$ je reducibilní nad $\mathbb{Q}$ $\Rightarrow$ má aspoň 1 lineární faktor $\Rightarrow$ má kořen v $\mathbb{Q}$, neboť je to $\frac{r}{s} \in \mathbb{Q}$

$\Rightarrow r \mid a_0 = -1 \Rightarrow \frac{r}{s} \in \{1, -1\}$, $s \mid a_3 = 1$

nejsou kořeny v $\mathbb{Q}$ $\Rightarrow f(x)$ je ired. nad $\mathbb{Q}$.

Př: $x^3 - 3x - 1 \overset{\text{mod } \mathbb{Z}_2}{=} x^3 + x + 1$ red. $\Rightarrow \dots \Rightarrow$ má kořen v $\mathbb{Z}_2$ to není pravda $\Rightarrow$ je ired.

3 30-14:41

Věta (Eisensteinovo kritérium ireducibility)

Je-li $f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$, přičemž: ex. P prvočíslo

- $p \mid a_0, \dots, a_{n-1}$, $p \nmid a_n$
- $p^2 \nmid a_0$.

Pak je f ireducibilní nad $\mathbb{Z}$ (a tedy i nad $\mathbb{Q}$).

Důk: Sporem $f = g \cdot h = (b_m x^m + \dots + b_0) \cdot (c_k x^k + \dots + c_0)$, $b_i, c_j \in \mathbb{Z}$

$a_0 = b_0 \cdot c_0$

$a_1 = b_0 c_1 + b_1 c_0$

$a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$

$\vdots$

$a_m = a_{m+k} = b_m \cdot c_k$

$p \mid a_0 \Rightarrow p \mid b_0 c_0 \overset{\text{BÚNO}}{\Rightarrow} p \mid b_0$, $p \nmid c_0$

$p \mid a_1 \Rightarrow p \mid b_1 c_0 \Rightarrow p \mid b_1$

$p \mid a_2 \Rightarrow p \mid b_2 c_0 \Rightarrow p \mid b_2$

$\vdots$

$p \mid b_m \Rightarrow p \mid a_{m+k} = a_n$ SPOR

3 30-14:49

Důsledek

Nad okruhem $\mathbb{Z}$ existují ireducibilní polynomy libovolného stupně.

Eisenstein $\Rightarrow x^n + 2$ je ired. $\forall n \in \mathbb{N}$ $p = 2$

3 30-14:49

Polynom nad $\mathbb{Z}$: $f = g \cdot h \rightsquigarrow f \equiv g \cdot h \pmod m$ nad $\mathbb{Z}_m$

$x^3 + 27x^2 - 5x + 97 \mod 3$

$\equiv x^3 + 2x + 1$

Je ireducibilní nad $\mathbb{Z}_3$? Ano, nemá totiž kořen.

$\Rightarrow f(x)$ je ired nad $\mathbb{Z}$

3 30-15:00

$p = 17$:

$f(x) = x^{16} + x^{15} + \dots + x + 1 = \frac{x^{17} - 1}{x - 1}$

$x \leftarrow y + 1$, $y = x - 1$

$f(x) = g(x) \cdot h(x)$

$f(y+1) = g(y+1) \cdot h(y+1)$

$f(y+1) = (y+1)^{16} + (y+1)^{15} + \dots + (y+1) + 1$

$= \frac{(y+1)^{17} - 1}{y + 1 - 1} = \frac{(y+1)^{17} - 1}{y} =$

$= y^{16} + \binom{17}{1} y^{15} + \binom{17}{2} y^{14} + \dots + \binom{17}{16}$

$17 \mid \binom{17}{1}$, $17 \mid \binom{17}{2}$, $17 \mid \binom{17}{16}$

$p \mid \binom{p}{k}$ pro vhodné $p, k = 1, \dots, p-1$

EISEN. $\Rightarrow$ je ired.

3 30-15:06

Věta - dk.

$f(x) = (x-a)^k \cdot g(x)$ $\quad x-a \nmid g(x)$

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

znejme $(x-a)^{k-1} \mid f'(x)$

$(x-a)^k \nmid f'(x) \Leftrightarrow x-a \nmid k \cdot g(x)$

3 30-15:12

(*) $x_1^3 + x_2^3 - x_1^2 x_2 + x_1 x_2^2$ je symetrický

$x_1^2 x_2 - x_1 x_2^2$ NENÍ (záměnou x_1, x_2 se nezmění)

$s_1 = x_1 + x_2$

$s_2 = x_1 \cdot x_2$

$s_1^3 = x_1^3 + 3x_1^2 x_2 + 3x_1 x_2^2 + x_2^3$

$-2s_2 \cdot s_1 = -2(x_1^2 x_2 + x_1 x_2^2) = -2x_1 x_2 (x_1 + x_2)$

$f(x_1, x_2) = g(s_1, s_2) = s_1^3 - 2s_1 s_2$

3 30-15:22

$x^2 + 13x + 7$

Viète:

$x_1 + x_2 = -13 = s_1$

$x_1 \cdot x_2 = 7 = s_2$

$x^2 + ax + b$

$x_1^2 + x_2^2 = -a$ $\quad a = -(x_1^2 + x_2^2) = -(x_1 + x_2)^2 + 2x_1 x_2 = -s_1^2 + 2s_2$

$x_1^2 \cdot x_2^2 = b$ $\quad b = (x_1 x_2)^2 = s_2^2 = 49$

$\Rightarrow a = -169 + 14 = -155$

$x^2 - 155x + 49$

3 30-15:28

$x^2 + cx + d$

$-c = \frac{1}{x_1} + \frac{1}{x_2} = \frac{x_1 + x_2}{x_1 \cdot x_2} = \frac{-13}{7}$

$d = \frac{1}{x_1} \cdot \frac{1}{x_2} = \frac{1}{x_1 x_2} = \frac{1}{7}$

$x^2 + \frac{13}{7}x + \frac{1}{7}$

3 30-15:31