e jednotka

$a = e \cdot \underbrace{(e^{-1} \cdot a)} \Rightarrow e \mid a$

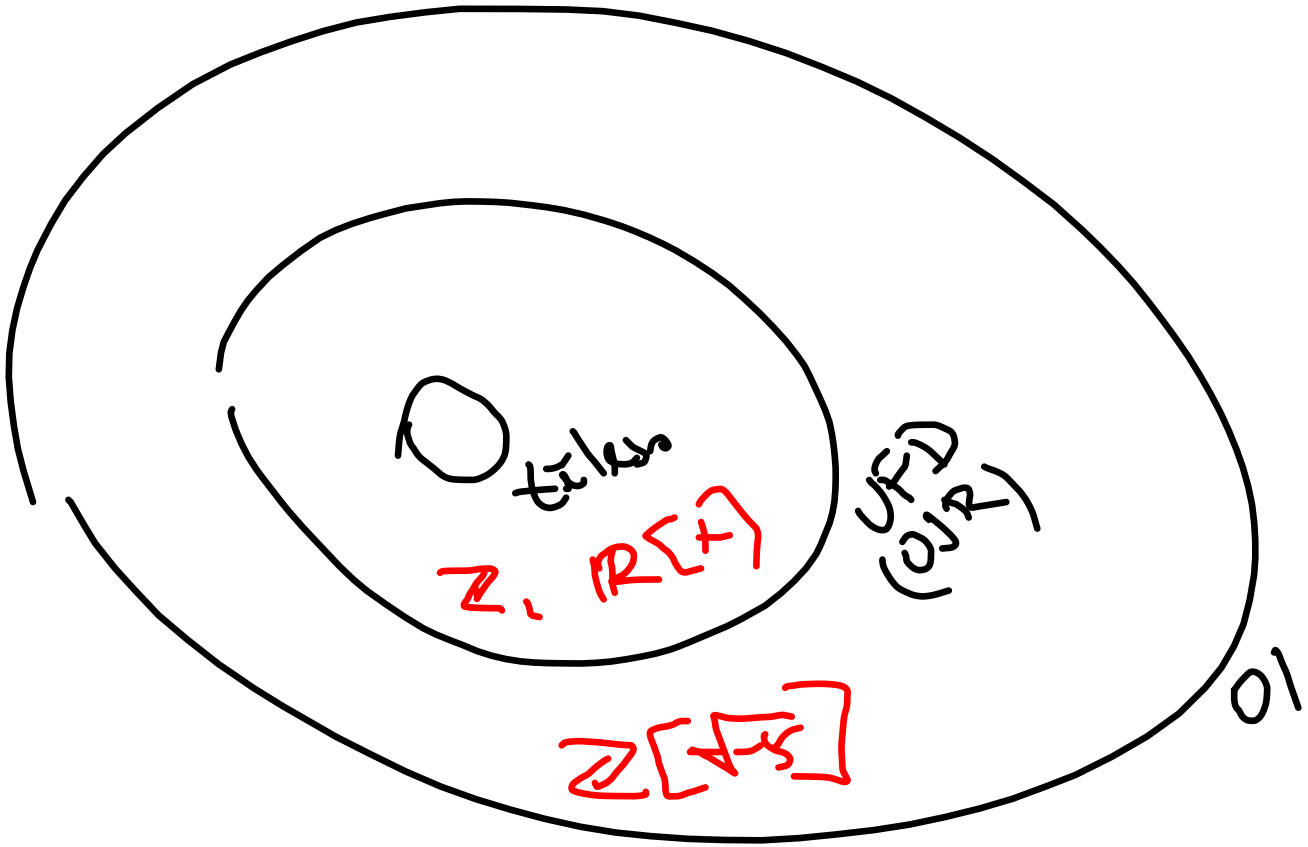
$a \cdot e \sim a$

... asociovaný s a (tj. $a \cdot e \mid a$, $a \mid a \cdot e$)

Př.: jednotky okruhu v $\mathbb{Z}$

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

$2 = (-2) \cdot (-1)$



$\mathbb{Z}[i] = \{a+b\sqrt{-1}; a,b \in \mathbb{Z}\}$ Gaussovy obvody

$$(1+\sqrt{-5})(1-\sqrt{-5}) = 1^2 - (\sqrt{-5})^2 =$$

$$= 1 - (-5) = 6$$

$$5 = (-1)(\sqrt{-5})^2$$

↑ není ireducibilní

$\forall a \in \mathbb{Z}\ \forall b \in \mathbb{Z} \setminus \{0\}$

$\exists q, r \in \mathbb{Z}$ $0 \leq r < |b|$

$a = b \cdot q + r$

~~mad $\mathbb{Z}$~~ ; mad $\mathbb{R}$

$(x^2+1) : (3x+1) \approx \frac{1}{3}x - \frac{1}{9}$

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

$-\frac{1}{3}x+1$

$-(-\frac{1}{3}x-\frac{1}{9})$

$\frac{10}{9}$

$x^2+1 = (3x+1)(\frac{1}{3}x-\frac{1}{9}) + \frac{10}{9} \quad / \cdot 9$

$9x^2+9 = (3x+1)(3x-1)+10$

Příklad Euklidovské obory

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

$$\lambda(a+bi) = a^2 + b^2$$

$\forall \alpha, \beta \in \mathbb{Z}[i] : \beta \neq 0:$

$\exists q, r \in \mathbb{Z}[i]:$

$\alpha = \beta \cdot q + r \quad \wedge$ buď $r = 0$ nebo $\lambda(r) < \lambda(\beta)$

Zajišťuje konec Eukl. alg.

nad $\mathbb{Z}_2$: $f_1 = 0$, $f_2 = x^2 + x$ dávají stejnou funkci (nulovou)

Polynom nad tělesem má nejvýše st f

$(\mathbb{Z}_7, +, \cdot)$

$(\mathbb{Z}_7^\times, \cdot) = \{[1], \ldots, [6]\}$

generátor $2 \times$

$\langle [2] \rangle = \{[2], [4], [1]\}$

$\langle [3] \rangle = \{[3], [2], [6], [4], [5], [1]\}$

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

1 je kořen násobnosti 2

$f, g \in \mathbb{R}[x]$ $|\mathbb{R}| = \infty$

$\mathbb{R}$ těleso

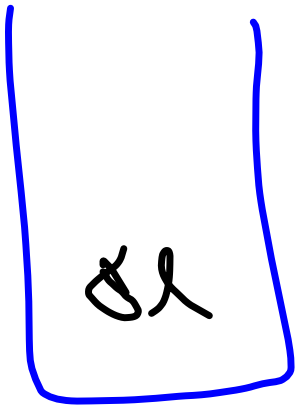
$f - g$ ... nulová polyn. funkce,

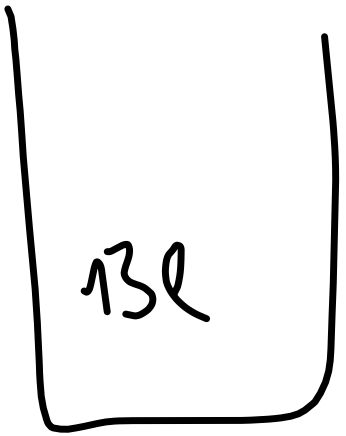
tj. $(f-g)(b) = 0 \quad \forall b \in \mathbb{R}$

$\Rightarrow f - g$ má ∞ kořenů

Př.

Chceme odměřit 2 l





Bez. věta:

$1 = 13a + 5 \cdot b$

$2 = 13(2a) + 5(2b)$

$1 = 3 - 1 \cdot 2 =$

$= 3 - (5 - 3)$

$= -1 \cdot 5 + 2 \cdot 3 =$

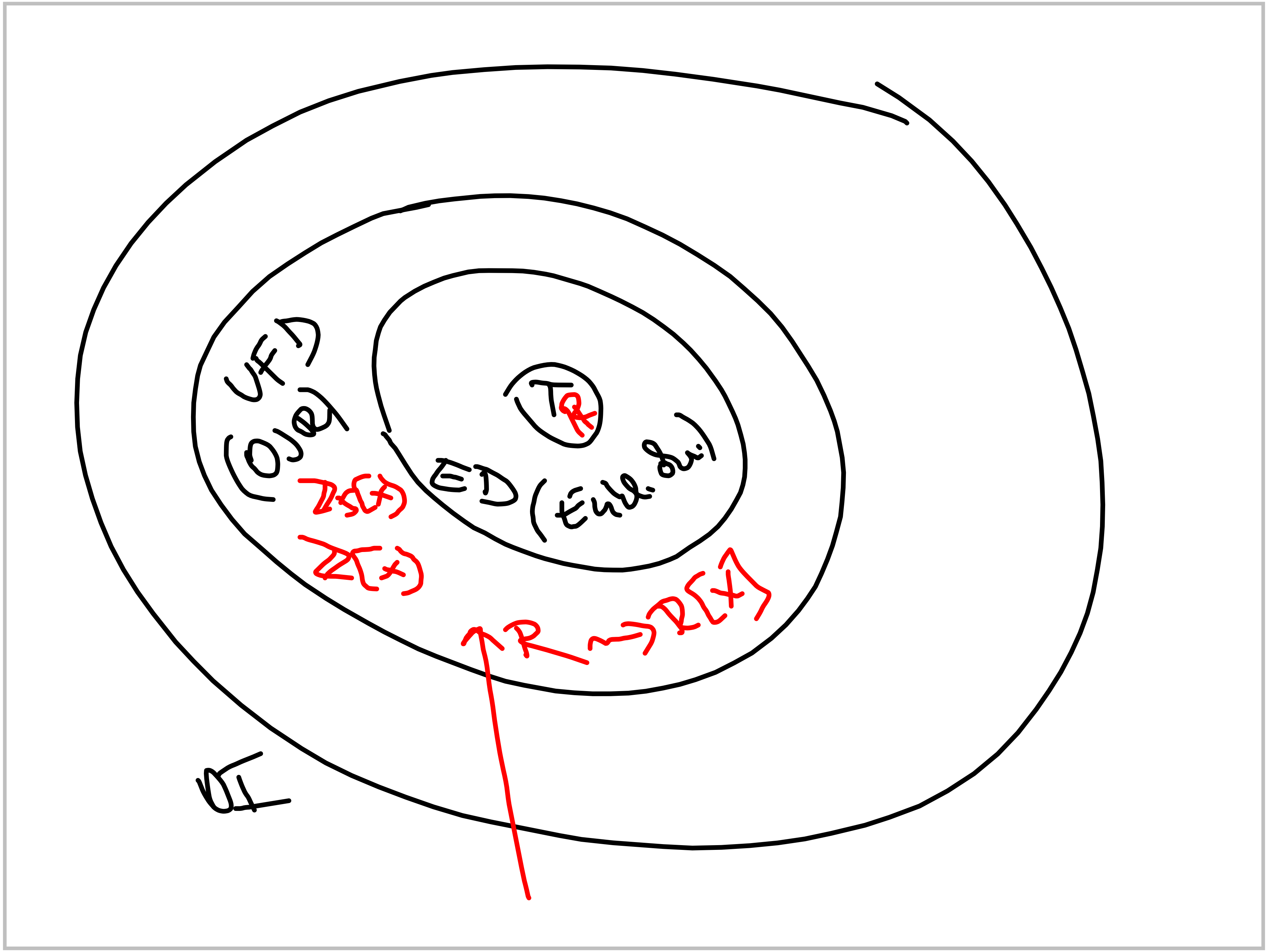
$= -1 \cdot 5 + 2(13 - 2 \cdot 5) = 2 \cdot 13 - 5 \cdot 5$

$13 = 2 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$a = 2 \quad b = -5$


UFD
ED
Z[x]
R → R[x]

x^2+1 ireducibilní nad $\mathbb{R}$

(kdyby šel rozložit $\Rightarrow$ měl by kořeny v $\mathbb{R}$)

nad $\mathbb{C}$: $x^2+1 = (x+i)(x-i)$

---

ireducibilita nad $\mathbb{Z}$

$\Rightarrow$ ireducibilita nad $\mathbb{Q}$

$\sqrt{2} \notin \mathbb{Q}$ $\sqrt{2} \in \mathbb{Q} \Rightarrow x^2-2$ reducib. nad $\mathbb{Q}$

$\Rightarrow$ reducibil nad $\mathbb{Z} \Rightarrow \sqrt{2} \in \mathbb{Z}$

SPOR

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

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

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

$r, s \in \mathbb{Z}$ $(r,s) = 1$

$s \neq 0$

$(r,s) = 1$

$s \mid 0 = a_n r^n + \dots + a_0 s^n \Rightarrow s \mid a_n r^n \Rightarrow s \mid a_n$

$r \mid 0 = \dots \Rightarrow r \mid a_0 s^n \Rightarrow r \mid a_0$

$x^3 - 3x - 1$ je ireducibilní nad $\mathbb{Q}$

SPOREM

rozložitelný $\Rightarrow$ faktor stupně 1

$\Rightarrow$ kořen v $\mathbb{Q}$

možné kořeny: $r \mid 1, \; s \mid 1$

$\frac{r}{s} \in \{\frac{1}{1}, -\frac{1}{1}\}$

Snadno ověříme, že nejsou kořeny

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

p prvočíslo

$$p \mid a_0 \wedge p^2 \nmid a_0$$

$$p \mid a_1, p \mid a_2, \dots, p \mid a_{n-1}, p \nmid a_n$$

Důkaz sporem

$$f(x) = (b_m x^m + \dots + b_0)(c_s x^s + \dots + c_0)$$

$p \mid a_0 = b_0 \cdot c_0 \overset{\text{např.}}{\Rightarrow} p \mid b_0 \wedge p \nmid c_0$

$p \mid a_1 = b_0 c_1 + b_1 c_0 \Rightarrow p \mid b_1 c_0 \Rightarrow p \mid b_1$ atd. $p \mid b_m \Rightarrow p \mid a_n$ spor

nad $\mathbb{C}$: ireducibilní jen lineární

nad $\mathbb{R}$: ireducibilní lineární a kvadratické s diskriminantem < 0

$(\beta \in \mathbb{C} \setminus \mathbb{R}$ kořen $f \in \mathbb{R}[x]$

$(x-\beta)(x-\overline{\beta}) \mid f$

$\uparrow \mathbb{R}[x]$

nad $\mathbb{Z}$ a $\mathbb{Q}$: ireducibilní mohou mít lib. stupeň

$$f = (x-\alpha)^k \cdot f_1 \qquad (x-\alpha) \nmid f_1$$

$$f' = (x-\alpha)^k \cdot f_1' + k(x-\alpha)^{k-1} \cdot f_1$$

zřejmě $(x-\alpha)^{k-1} \mid f'$

snadno $(x-\alpha)^k \nmid f'$

[neboť $(x-\alpha) \nmid k \cdot f_1$]

$$x_1^2 + x_2^2$$

(x_1, x_2 jsou kořeny $f = x^2 + ax + b$

$b = x_1 \cdot x_2 = s_2$

$a = -(x_1 + x_2) = -s_1$)

$$x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1x_2 =$$

$$= s_1^2 - 2s_2$$

pokud

$(M,n) = 1$ $\quad e \cdot d = 1 + k \cdot \varphi(n)$

$$(M^e)^d = M^{e \cdot d} = M^{1+k\cdot\varphi(n)} \equiv$$

$$\equiv M \cdot \left(M^{\varphi(n)}\right)^k \equiv M \pmod{n}$$

$\equiv 1 \pmod{n}$

pokud $(M,n) > 1$, ověří se zvlášť