Eukleidův algoritmus & Bézoutovy koeficienty

Připomeňme si rozšířený Eukleidův algoritmus:

- **vstup**: $a, b \in \mathbb{N}, a \geq b$
- **výstup**: $\mathrm{NSD}(a,b)$ a $x, y \in \mathbb{Z}$ taková, že $x \cdot a + y \cdot b = \mathrm{NSD}(a,b)$

krok 1. $i := 1;\quad (a_0, a_1) := (a, b);\quad (x_0, x_1) := (1, 0);\quad (y_0, y_1) := (0, 1);$

krok 2. **while** $(a_i > 0)$ **do**
$\{a_{i+1} := (a_{i-1}) \bmod a_i;\quad q_i := (a_{i-1}) \operatorname{div} a_i;\quad x_{i+1} := x_{i-1} - x_i \cdot q_i;\quad y_{i+1} := y_{i-1} - y_i \cdot q_i;\quad i := i+1;\}$

krok 3. **return** $a_{i-1},\quad x_{i-1},\quad y_{i-1}$.

S pomocí rozšířeného Eukleidova algoritmu můžeme například vyřešit následující úlohy:

1. Najděte $\mathrm{NSD}(37, 10)$ a příslušné Bézoutovy koeficienty. [$1 = 3 \cdot 37 - 11 \cdot 10$; v $\mathbb{Z}_{37}$ tedy platí $10^{-1} = -11 \equiv 26 \pmod{37}$]
2. Najděte $\mathrm{NSD}(1023, 96)$ a příslušné Bézoutovy koeficienty. [$3 = 1023 \cdot (-3) + 96 \cdot 32$]
3. Najděte 27^{-1} v tělese $\mathbb{Z}_{41}$. [38]

$\mathrm{NSD}(a,b) = x \cdot a + y \cdot b$

$\mathrm{NSD}(a,b) = \mathrm{NSD}(a - k\cdot b, b) \quad k \in \mathbb{Z}$

$x \mid a,\ x \mid b \Rightarrow x \mid b \Rightarrow x \mid k\cdot b \Rightarrow x \mid a - k\cdot b$; $x \mid b$

$\boxed{\mathrm{NSD}(a, 0) = a}$

1)

z	x	y
37	1	0
10	0	1
7	1	−3
3	−1	4
1	3	−11
0		

$\mathrm{NSD}(37,10) = \mathrm{NSD}(1,0) = 1$

$37x + 10y = 1 = \mathrm{NSD}(37,10)$

$\forall$ řádek $z = 37x + 10y$

$z_1 = 37x_1 + 10y_1$
$z_2 = 37x_2 + 10y_2 \quad \cdot k$

$z_1 - k\cdot z_2 = 37(x_1 - k\cdot x_2) + 10(y_1 - k y_2)$

$\boxed{1 = 3\cdot \cancel{37} + (-11)\cdot 10}$ $\equiv 0 \bmod 37$

10^{-1} v $\mathbb{Z}_{37}$

$1 \equiv (-11)\cdot 10 \pmod{37}$

$1 \equiv 26 \cdot 10 \pmod{37}$

Okruhy & obory

4. Rozhodněte, zda jsou následující množiny podokruhy tělesa $\mathbb{C}$:
   (a) $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} = S_1 \subseteq \mathbb{R}$
   (b) $\{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Z}\} = S_2$
   (c) $\{a + b\zeta \mid a, b \in \mathbb{Z}\}$, kde $\zeta = e^{\frac{\pi i}{4}}$ S_3

   Je (a) dokonce obor?

$0 \in S$
S uzavřené na $+, -, \cdot$?

a) $(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = a_1a_2 + 2b_1b_2 + (a_1b_2 + b_1a_2)\sqrt{2}$ ✓

b) $0 \in S_2$, "−" ✓, "+": $(a_1 + b_1\sqrt[3]{2}) + (a_2 + b_2\sqrt[3]{2}) =$
$= a_1 + a_2 + (b_1 + b_2)\sqrt[3]{2}$ ✓

"·": $(a_1 + b_1\sqrt[3]{2})(a_2 + b_2\sqrt[3]{2}) =$
$= \underbrace{a_1a_2 + (a_1b_2 + b_1a_2)\sqrt[3]{2}}_{\in S_2} + b_1b_2\underbrace{\sqrt[3]{2}\sqrt[3]{2}}_{=\sqrt[3]{4}}$

$b_1 = b_2 = 1 \Rightarrow \sqrt[3]{4} \in S_2$ ↯ ✗

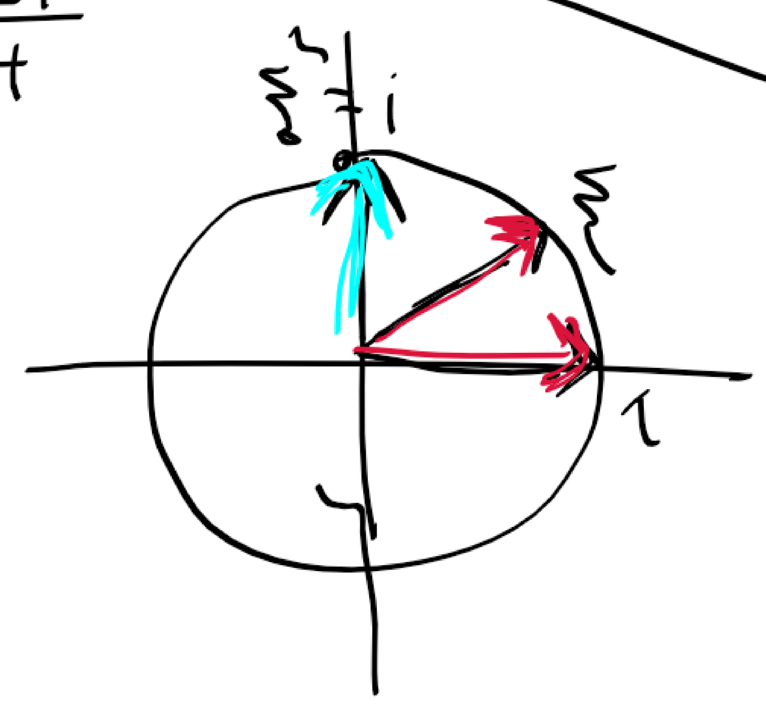
c) $(a_1 + b_1\zeta)(a_2 + b_2\zeta) =$
$= a_1a_2 + (a_1b_2 + b_1a_2)\zeta +$
$+ b_1b_2\zeta^2$

$\zeta^2 \overset{?}{\in} S_3$

$e^{\frac{\pi i}{4}} \cdot e^{\frac{\pi i}{4}} = e^{\frac{\pi i}{2}} = \frac{2\pi i}{4}$

$\ne e^{\frac{2\pi i}{8}}$

$= i$



$i = a + b\zeta$

$1 = (1, 0)$
$\zeta = \left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right)$
$i = (0, 1)$

$a + b\zeta = i$

$a(1, 0) + b\left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right) = (0, 1)$

$a + b\frac{\sqrt{2}}{2} = 0$

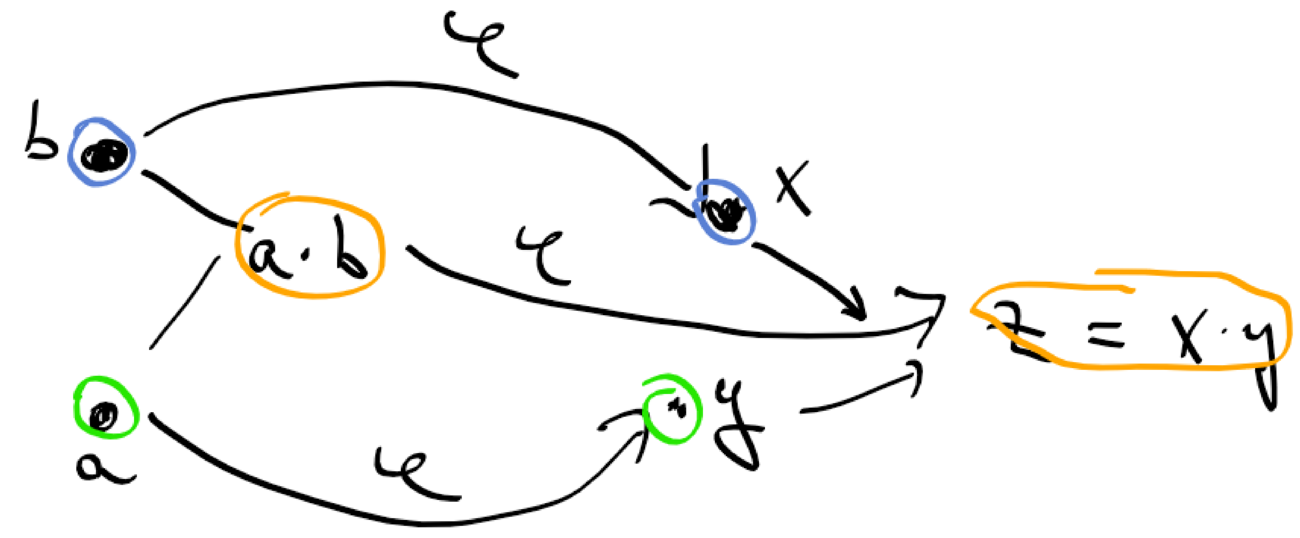
$\Downarrow\ b = 0 \Rightarrow a = 0$, ale $0 \neq 1$

9. Dokažte, že žádné dva z okruhů $\mathbb{Q}$, $\mathbb{Q}[x]$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$ nejsou izomorfní.

S, R okruhy $\quad S \xrightarrow{\varphi} R \quad$ φ … homomorfismus

- $\varphi(a+b) = \varphi(a) + \varphi(b)$
- $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

φ je navíc izomorfismus pokud je φ bijekce



$\cancel{\varphi(0)} = \varphi(0+0) = \cancel{\varphi(0)} + \varphi(0)$

$\boxed{0 = \varphi(0)}$ … pro obecný homomorfismus

φ izomorfismus:

$\exists x$ t.ž. $\varphi(x) = 1$

$\Rightarrow 1 = \varphi(x) = \varphi(x \cdot 1) = \varphi(x) \cdot \varphi(1) = 1 \cdot \varphi(1) = \varphi(1)$

$\Rightarrow \boxed{\varphi(1) = 1}$

$\mathbb{Q}, \mathbb{Q}[x]$: $\nexists$ $x \in \mathbb{Q}[x]$, x nemá inverz v $\mathbb{Q}[x]$

SPOREM:

$\mathbb{Q}[x] \xrightarrow{\varphi} \mathbb{Q}$

$x \longmapsto a \neq 0 \rightsquigarrow \exists b: a \cdot b = 1$

$y \longmapsto b$

$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = a \cdot b = 1$

φ bijekce a $\varphi(1) = 1$ $\Rightarrow x \cdot y = 1$, SPOR s tím, že x nemá inverz

---

$\mathbb{Q}, \mathbb{Q}[\sqrt{2}]$: $\quad \sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, $(\sqrt{2})^2 = 2$

SPOREM:

$\mathbb{Q}[\sqrt{2}] \xrightarrow{\varphi} \mathbb{Q}$

$2 = \sqrt{2} \cdot \sqrt{2}$

$2 = \varphi(2) = \varphi(\sqrt{2} \cdot \sqrt{2}) = \varphi(\sqrt{2}) \cdot \varphi(\sqrt{2}) = a \cdot a$

$\sqrt{2} \xmapsto{\varphi} a$

$a \in \mathbb{Q} \Rightarrow a^2 = 2$ v $\mathbb{Q}$

$a = \pm\sqrt{2} \notin \mathbb{Q}$

SPOR, $\pm\sqrt{2}$ je iracionální

$\varphi(2) = \varphi(1+1) = \varphi(1) + \varphi(1) = 1 + 1 = 2$

$\varphi(3) = \varphi(2+1) = \varphi(2) + \varphi(1) = 2 + 1 = 3$

$\varphi(a) = a$, $a \in \mathbb{Z}$

$\mathbb{Q}, \mathbb{Q}[\sqrt{3}]$: stejně jako předchozí

SPOREM, ať $\varphi: \mathbb{Q}[\sqrt{3}] \to \mathbb{Q}$, potom $3 = \varphi(3) = \varphi(\sqrt{3} \cdot \sqrt{3}) = \varphi(\sqrt{3}) \cdot \varphi(\sqrt{3}) =$
$\qquad \sqrt{3} \longmapsto a \qquad\qquad = a \cdot a$

$\Rightarrow a^2 = 3 \Rightarrow a = \pm\sqrt{3} \Rightarrow$ SPOR, $\pm\sqrt{3}$ je iracionální

8. Dokažte, že žádné dva z okruhů $\mathbb{Q}$, $\mathbb{Q}[x]$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$ nejsou izomorfní.

$\mathbb{Q}[\sqrt{2}], \mathbb{Q}[\sqrt{3}]$: Pro spor ať φ je izomorfismus

$$\varphi: \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{3}]$$
$$\sqrt{2} \mapsto a$$

$$2 = \varphi(2) = \varphi(\sqrt{2}\cdot\sqrt{2}) = \varphi(\sqrt{2})\cdot\varphi(\sqrt{2}) = a\cdot a$$

$a \in \mathbb{Q}[\sqrt{3}] \Rightarrow a = u + v\sqrt{3},\ u, v \in \mathbb{Q}$

$(u + v\sqrt{3})^2 = 2$

součet racionální a iracionální je iracionální

$u^2 + 3v^2 + 2uv\sqrt{3} = 2 \Rightarrow uv = 0$ a $u = 0 \Rightarrow 3v^2 = 2 \Rightarrow v = \pm\sqrt{\frac{2}{3}}$ ...

$v = 0 \Rightarrow u^2 = 2 \Rightarrow u = \pm\sqrt{2}$

ale $\pm\sqrt{\frac{2}{3}}$ i $\pm\sqrt{2}$ jsou iracionální a u, v jsou racionální $\Rightarrow$ SPOR

$\mathbb{Q}[x], \mathbb{Q}[\sqrt{2}]$:

Pro spor ať φ je izomorfismus

$$\varphi: \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[x]$$
$$\sqrt{2} \mapsto a$$

$$2 = \varphi(2) = \varphi(\sqrt{2}\cdot\sqrt{2}) = \varphi(\sqrt{2})\cdot\varphi(\sqrt{2}) = a\cdot a = a^2$$

- a je polynom
- aby $a^2 = 2$, musí být a konstantní polynom

$a \in \mathbb{Q} \Leftarrow$

$a = \pm\sqrt{2}$, SPOR

(obecně pro $f, g \in R[x]$, kde R je obor, platí $\deg(f\cdot g) = \deg(f) + \deg(g)$)

$\mathbb{Q}[x], \mathbb{Q}[\sqrt{3}]$: analogicky jako předchozí