

ALGEBRA 24.3.

6.1. Gauss. obor... když ne〇 prok, ! rozložitelné

$a \parallel p_1^{l_1} \cdots p_n^{l_n}, l_i \geq 1$ \cup invert. ... $\cup \parallel 1$

$$\downarrow u=0$$

Pos. Pro $a, b \in \mathbb{R}$, ne〇:

$$\begin{cases} a \parallel p_1^{k_1} \cdots p_n^{k_n} & 0 \leq k_i, k_i \\ b \parallel p_1^{e_1} \cdots p_n^{e_n} & p_i \neq p_j, p \neq i \neq j \end{cases}$$

$a \parallel p_1^{k_1} \cdots p_n^{k_n}$ ied. rozlož.

$$b \parallel q_1^{m_1} \cdots q_\sigma^{m_\sigma} \parallel p_1^{m_1} q_2^{m_2} \cdots q_\sigma^{m_\sigma}$$

Tedy se stáčí, $q_i \parallel p_j$. Buď

$$\begin{aligned} \text{Takhle } p \text{-padné opadají...} & \quad b \parallel p_1^{m_1} \cdots p_i^{m_i} \underline{q_{i+1}^{m_{i+1}} \cdots} \\ & + q_j \neq p_h, j \geq i+1. \end{aligned}$$

Druhé

$$p_{m+1} = q_{i+1}, p_{m+2} = q_{i+2}, \dots$$

$$a \parallel p_1^{k_1} \cdots p_n^{k_n} \quad \overset{\circ}{\underset{\circ}{\text{P}_{m+1} \ P_{m+2}}} \quad \cdots$$

$$b \parallel p_1^{m_1} \cdots p_i^{m_i} \quad \overset{\circ}{\underset{\circ}{p_{i+1} \cdots p_m \ p_{m+1}}} \quad \overset{\circ}{\underset{\circ}{m_{i+1}}}$$

Důk. 6.2 (délkuost v gaus. oborech). R gaus. obor. Pak

- 1) $\forall a, b \in \mathbb{R}$, neobě 0, existuje NSD(a, b).
- 2) když ied. pvek je prvočísel
- 3) neex. posloupnost $a_1, a_2, a_3, \dots \in \mathbb{R}$: $a_{i+1} | a_i$ & $a_i \nmid a_{i+1}$.

Dl. 1) $b=0 \Rightarrow \text{NSD}(a, b)=a$. Stejně $a \neq 0$.

At' $a, b \neq 0$. Posor. \Rightarrow $a \parallel p_1^{k_1} \cdots p_n^{k_n}$ $p_i \neq p_j$ $i \neq j$
 $b \parallel p_1^{l_1} \cdots p_n^{l_n}$ $k_i, l_i \geq 0$.

c/a. T. 6.1 $\Rightarrow c \parallel p_1^{m_1} \cdots p_n^{m_n}$, kde $0 \leq m_i \leq k_i$.

c/b $\Rightarrow 0 \leq m_i \leq l_i$

Tedy $c/a, b \Rightarrow \underbrace{0 \leq m_i \leq \min(k_i, l_i)}_{\text{řádkověný přeti}\leq} \left\{ \begin{array}{l} = \text{NSD}(a, b) \\ = p_1^{\min(k_1, l_1)} \cdots p_2^{\min(k_2, l_2)} \cdots \end{array} \right.$

2) $p \text{ irred.} \Leftrightarrow p \text{ irr.}$

$\underbrace{a \parallel p_1^{k_1} \cdots}_{p \mid p_1^{k_1+1} \cdots} + b \parallel p_1^{l_1} \cdots \dots \text{ pred. } \overline{p}, \text{ je } k_i \neq 0$
 $\text{nebo } l_i \neq 0$
 $(\text{jinak tam } p_i \text{ nedělit})$

T.6.1 $\Rightarrow \underbrace{P \parallel p_1^{m_1} \cdots p_n^{m_n}}_{0 \leq m_i \leq k_i+l_i}$, kde

Ale $p \text{ irred.} \Rightarrow m_1 = \dots = m_{i-1} = m_{i+1} = \dots = m_n = 0$

$m_i = 1 \quad \& \quad \underbrace{P \parallel p_i^1}$

- $k_i \neq 0 \Rightarrow P \parallel p_i \mid a$ (je $p_i^{k_i}$ neupříjemně v rozdělení)
- $k_i \neq 0 \Rightarrow P \mid b$.

3) $a \parallel p_1^{k_1} \cdots p_n^{k_n}$ irred. rozděl.

Def. $v(a) = k_1 + \dots + k_n$. jednom. irred. rozděl.
 $\Rightarrow v(a)$ je dobré def.

T.6.1: $b \mid a \Rightarrow v(b) \leq v(a)$

Pomocně blla, že $v(b) < v(a)$.

Když $\dots a_{i+1} | a_i | a_{i-1} | \dots | a_2 | a_1$. vlastní díl.
 $\Rightarrow \dots v(a_{i+1}) < v(a_i) < v(a_{i-1}) < \dots < v(a_1)$.

Ale $v(a_i) \in \mathbb{N}_0 \rightarrow$ spor.

v není norma ve $\mathbb{Z}[x]$.

Více v než dobré dělit je abstraktní.

Pi. $\mathbb{Z}[x]$ (je gauss. \rightarrow časné)

... neplatí Béz. věta

$$\text{NSD}(x+1, x-1) = \underbrace{1}_{?} = f(x) \cdot (x+1) + g(x) \cdot (x-1)$$

Dosadím $x=1$: $1 = f(1) \cdot 2 \rightarrow$ spor $\Rightarrow f(1) \in \mathbb{Z}$.

6.2. základní věta aritmetiky

Věta 6.3 (— — — —) je celo.

R je gauss. \Leftrightarrow 1) existuje NSD všech dvojk. parků
 $(\text{kromě } (0,0))$.
 2) neexist. nekompletní pol. vlastních díl.
 $a_1, a_2, a_3 \in R : a_{i+1} | a_i \mid a_i + a_{i+1}$.

\Rightarrow je jasné.

- Dle. existence rovnosti. Bud' $a \neq b$ i $c \neq d$, pak, když jsou všechny redukce vyznáme spoj $\rightarrow 2$). • $a \neq b \Rightarrow a_i = a, a_i \neq b, a_i \neq c, a_i \neq d$ (R).
• Mezi mezijskou redukcí $a_i \neq b$ je nějaký IR. Tedy $a_i \neq b$ je redukce.
 $\Rightarrow a_i = b \cdot c$ pro nějaké $b, c \neq 1$.
Když $b \cdot c$ málo IR, pak by IR měl i a_i -spor.
Takže aspoň jeden z nich málo IR, omečme ho a_{i+1} .
Dostal jsme $a_{i+1} | a_i$, $a_{i+1} \neq 1$, a_{i+1} málo IR.
• Pokračujme, dostaneme $a_{i+1} | a_i | a_{i-1} | \dots$
Zdrobení $a_{i+1} \neq 1$, lze $b \neq a, c \neq a$ (lze $c \neq 1, b \neq 1$)
SPOR $\rightarrow 2$.

Lemma 6.4 R celor., $a, b \in R$, $c \in R$, $c \neq 0$, předpokládejme, že ex. $NSD(a, b)$, $NSD(ca, cb)$.

$$\text{Pal } NSD(ca, cb) = c \cdot NSD(a, b).$$

Dle. viz. skripta.

Lemma 6.5 Bud' R celor., ne běžíme ex. NSD víc dle jeho pořadí.

Pal je každý redukce, pak je prvek prvečnítel.

Dle. Bud' p i ned., $a \neq p | ab$. $A \neq p+a$, $b \neq 0$.

$$NSD(p, a) = 1, \text{ lze } p \text{ i ned.}$$

$$L.6.4 \Rightarrow NSD(pb, ab) = b \cdot NSD(p, a) = b.$$

Zdrobení $p | pb$ a $p | ab$ je lze $NSD \Rightarrow p | b$. \square

Dle. jednoznačnosti rovnosti. Sporem. Než všechny prvky \rightarrow nejednoznačnosti rovnosti vybereme ten, který má nejkratší rozdíl, tedy má minimum. $k_1 + \dots + k_n$.

$$a \parallel p_1^{k_1} \cdots p_n^{k_n} \parallel q_1^{l_1} \cdots q_m^{l_m}$$

\downarrow daný rozdíl IR.

$$p_1 \text{ je ned. \& } p_1 \mid q_1^{l_1} \cdots q_m^{l_m}$$

$$6.5 \Rightarrow p_1 \text{ je prvečnítel. } \Rightarrow p_1 \mid q_i \text{ pro nějaké } i.$$

q_i ned. $\Rightarrow p_1 \parallel q_i$. Mám: $p_1^{k_1-1} \cdots p_n^{k_n} \parallel q_1^{l_1} \cdots q_m^{l_m}$

[opakování používající $p_1 \mid bc \Rightarrow p \mid b \vee p \mid c$]

Ale to jsou
 ze sebe 2 různé IR,
 spor s vypočítanou
 nejkratšího,

7.1 EUKLIDOVSKÉ OBORY

F. EUKLIDŮV + LG. A BÉZOUTOVA ROVNOST

Def. & oboz. & je euklidovský, pokud ne něm ex. euklidovské normy, t. j. zobrazení $v: \mathbb{R} \rightarrow \mathbb{N}_0 \cup \{\infty\}$.

$$v(0) = 0$$

$$1) \text{ Pokud } a/b, b \neq 0, \text{ pak } v(a) \leq v(b).$$

$$2) \forall a, b \in \mathbb{R}, b \neq 0 \exists q, r \in \mathbb{R}: a = bq + r \text{ a } v(r) < v(b).$$

Posor. $b=0 \Leftrightarrow v(b)=0$.

Dk. \Leftarrow At' $v(b)=0, b \neq 0$. Vezmme libovolné $a \in \mathbb{R}$ & rozdělme a po b . $\Rightarrow a = bq + r, 0 \leq v(r) < v(b) = 0$ spor.

Př. • Teleso jsou eukl.: $v(0) = 0, v(a) = 1 \text{ pro } a \neq 0$. (cv.)

• \mathbb{Z} je eukl. ... $v(a) = |\alpha|$.

• $\mathbb{Z}[i]$ je eukl. ... $v(a+bi) = a^2 + b^2$ dokazeli jsme v senci 3.2.

• T teleso, $R = T[x]$. je eukl. obor.

$$v(f) = 1 + \deg f \quad [\text{viz } \deg 0 = -1] \quad (\text{cv.})$$

• $\mathbb{Z}[x]$ není eukl. (ale je gauß.)

Totíž dokázáme, že v eukl. oboru ex. NSD a plati Bézout.

Vidí jsme, že v $\mathbb{Z}[x]$ Bézout neplatí (NSD($x+1, x-1$)).

Euklidův algoritmus. & eukl. obor.

VSTUP: $a, b \in \mathbb{R}, v(a) \geq v(b)$.

VÝSTUP: NSD(a, b), $u, v \in \mathbb{R}$: $\text{NSD}(a, b) = ua + vb$.

$$\bullet a_0 = a \quad u_0 = 1 \quad v_0 = 1$$

$$a_1 = b \quad u_1 = 0 \quad v_1 = 1$$

$$\bullet \text{ Pro } i=1, 2, 3, \dots \text{ dělaj: } \text{ zvol } q, r \text{ t. j. } a_{i-1} = q_i \cdot q + r \quad v(r) < v(a_i)$$

$$\text{Definuj: } a_{i+1} = r, u_{i+1} = u_{i-1} - u_i \cdot q, v_{i+1} = v_{i-1} - v_i \cdot q.$$

Pokud $a_{i+1} = 0$, skončí a vrat' a_i, u_i, v_i .

V.7.1 (soubornost Eukl. algor.), V eukl. oboru \mathbb{R} najde EA pro jehož vstup $a, b \in \mathbb{R}^*$ hodnotu NSD(a, b) a

Bézoutovy koef. $u, v \in \mathbb{R}$ splňující $\text{NSD}(a, b) = ua + vb$.

* a, b ne obě 0.

Dř. řešení, že $v(a_1) > v(a_2) > v(a_3) > \dots$
sledující post. v No.

Ač' sestavil v krok u.

Stáčí dokážet: $\forall i$

$$1) \text{NSD}(a_{i-1}, a_i) = \text{NSD}(a_i, a_{i+1})$$

$$2) a_i = v_i a + v_i b.$$

Při to stáčí? Na m $\text{NSD}(a, b) = \text{NSD}(a_0, a_1) = \text{NSD}(a_1, a_2) = \dots$
 $= \text{NSD}(a_n, a_{n+1}) = a_n.$

A taky $\frac{a_n = v_n a + v_n b}{\text{NSD}(a, b)}$

tedy v_n, v_n fakt jsou Béz. koef.

1, 2 plývou z $a_{i-1} = a_i q + a_{i+1}$.

complete si.
↓

$$1: \text{NSD}(a_{i-1}, a_i) = \text{NSD}(a_i q + a_{i+1}, a_i) = \text{NSD}(a_{i+1}, a_i)$$

2. dokázat se indukci.