

Algebrie 19.3.

3.2

$$\mathbb{Z}[\sqrt{s}] = \{a + b\sqrt{s} \mid a, b \in \mathbb{Z}\}, \quad s \in \mathbb{Z}, \quad s \neq 0$$

$$v(a + b\sqrt{s}) = |a^2 - b^2s|.$$

Pokud $s < 0$, pak $\mathbb{Z}[\sqrt{s}] \subseteq \mathbb{C}$

$$a^2 + b^2 \cdot (-s) = |a + b\sqrt{s}|^2$$

- $v(\alpha\beta) = v(\alpha)v(\beta)$
- $v(\alpha) = 1 \Leftrightarrow \alpha$ invert.
- $\alpha|\beta$, $\beta+\alpha = 1 \Rightarrow v(\alpha)|v(\beta)$, ale $v(\alpha) \neq v(\beta)$.

Kledečkův invert. prvek: $v \in \mathbb{Z}[i]$. $v(a+bi) = a^2 + b^2$
 $a+bi$ je invert. $\Leftrightarrow a^2 + b^2 = 1 \Leftrightarrow a = \pm 1, b = 0$
 $a = 0, b = \pm 1$

Tedy invert. prvek jsou právě $\pm 1, \pm i$.

$\mathbb{Z}[\sqrt{2}]$. $|a^2 - 2b^2| = 1 \Leftrightarrow a^2 - 2b^2 = \pm 1$ Pellova rovnice
 $a=1, b=1$ je řešení ... $\frac{1+\sqrt{2}}{2}$ je invert.
Pozor. v je invert. $\Rightarrow v^k$ je invert. pro $k \in \mathbb{N}$.
... inverzi je $(v^{-1})^k$.

$\Rightarrow (1+\sqrt{2})^k$ je taky invert.

Víceň řešení \oplus jsou $\pm (1 \pm \sqrt{2})^k$.

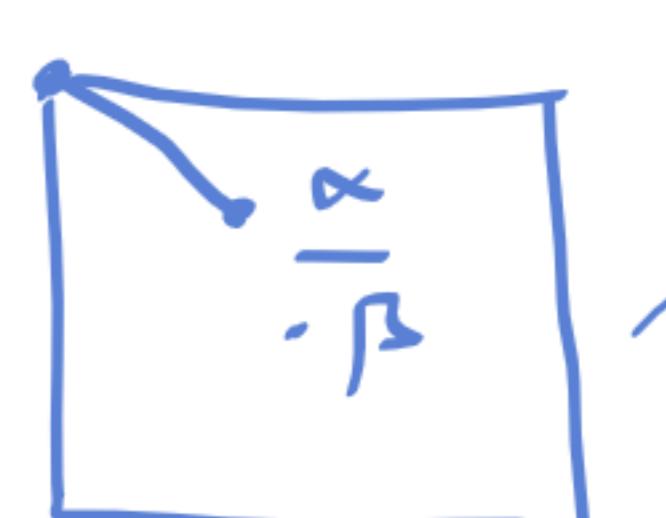
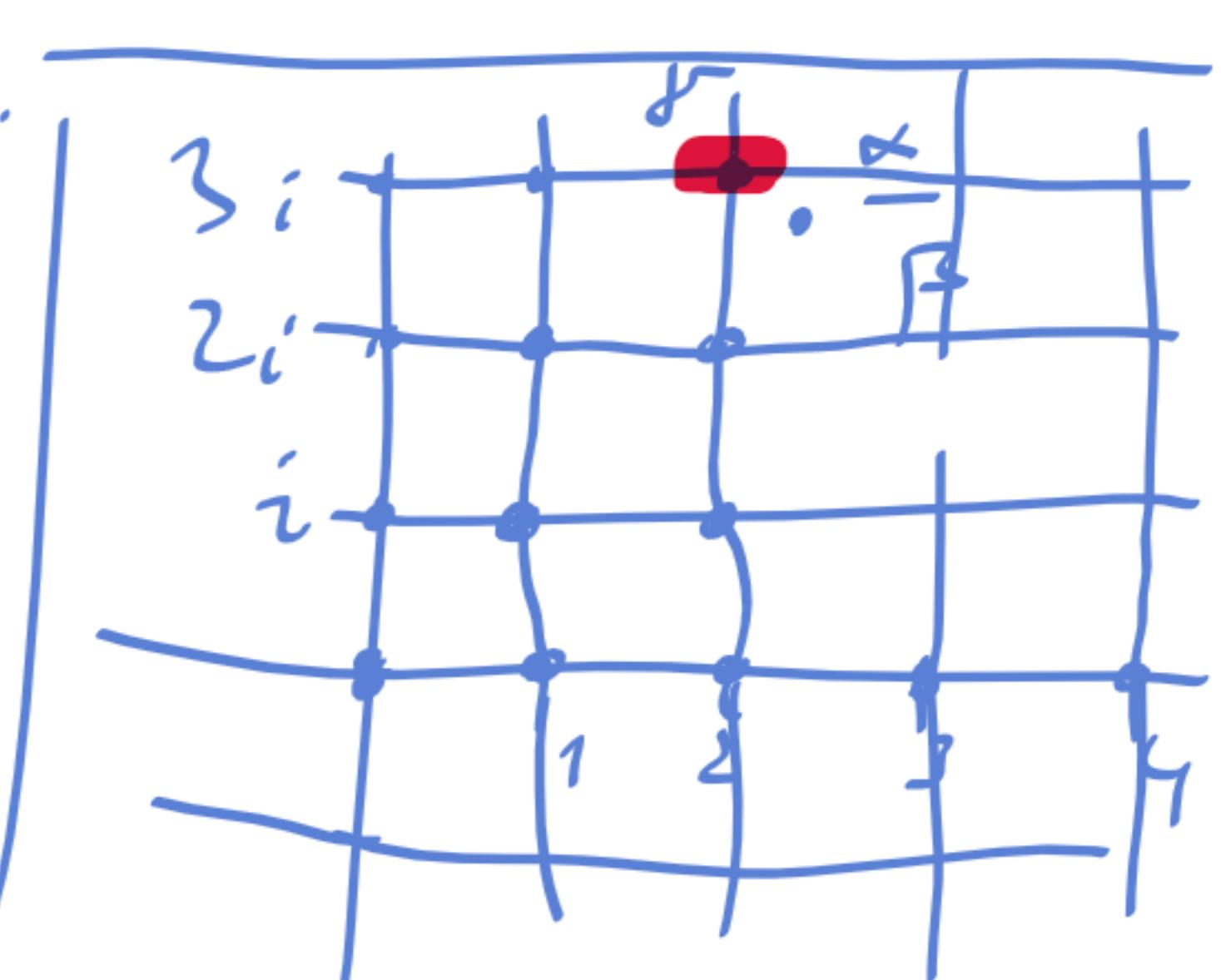
Várovaní v nesplňuje s možnost!

T. 3.4. (dilem! Gaußový důkaz se abystem)

$\forall \alpha, \beta \in \mathbb{Z}[i], \beta \neq 0 \quad \exists \gamma, \delta \in \mathbb{Z}[i]: \alpha = \beta\gamma + \delta \quad \& \quad v(\delta) < v(\beta)$

Dle. $\mathbb{Z}[i] \subseteq \mathbb{C}$. Berme $\frac{\alpha}{\beta} \in \mathbb{C}$. Zvolme $\gamma \in \mathbb{Z}[i]$ jako nejbližší lodek $\frac{\alpha}{\beta}$.
Položme $\delta = \alpha - \beta\gamma$. $\frac{\delta}{\beta} = \frac{\alpha}{\beta} - \gamma \Rightarrow \left| \frac{\delta}{\beta} \right| \leq \frac{\sqrt{2}}{2} \quad \text{zobr.}$
 $\Rightarrow |\delta| \leq \frac{\sqrt{2}}{2} |\beta| < |\beta|$.

Vidíme $v(x) = |x|^2$, a tedy $v(\delta) = |\delta|^2 < |\beta|^2 = v(\beta) \quad \square$.



Stejný dr. funguje: pro $\mathbb{Z}[\sqrt{-2}]$, ale pro $\mathbb{Z}[\sqrt{s}]$, $s < -2$
 \sqrt{s} nefunguje.

Např. taky $\sim \mathbb{Z}[\sqrt{2}]$ jde dělit na zbytem.

5-2 Největší společný dělitel

Rozbor.

Def. Pro $a, b \in \mathbb{R}$ řekneme, že $c \in \mathbb{R}$ je největší spol. děl. a, b ,
znamená $c = \text{NSD}(a, b)$, pokud

1) $c | a, c | b$ (\rightarrow společný děl.)

2) Pokud $d | a, d | b$, pak $d | c$ (největší / spol. děl.)

a, b jsou nezáporné, pokud $\text{NSD}(a, b) \neq 1$.

Anot. $\text{NSD} = c [a/c, b/c \wedge \text{pokud } a/d, b/d, \text{pak } c/d]$

• NSD nemusí ex.

Pří. $\mathbb{Z}[\sqrt{5}]$. $U=4$, $V=2+2\sqrt{5}=2(1+\sqrt{5})$

Par 2, $1+\sqrt{5}$ jsou společnými děliteli. $4 = 2 \cdot 2 = (1+\sqrt{5})(-1+\sqrt{5})$

Ale $\text{NSD}(4, 2+2\sqrt{5})$ neex. (viz scripta).

• NSD nemusí jednoznačný.

Např. v \mathbb{Z} : $\text{NSD}(4, 6)=2$, ale taky $\text{NSD}(4, 6)=-2$.

Pozor. NSD je jednoznačný až ve asociativitě.

a) $\text{NSD}(a, b)=c$, $\text{NSD}(a, c)=d \Rightarrow c \parallel d$

b) $\text{NSD}(a, b)=e$, $e \parallel f \Rightarrow \text{NSD}(a, b)=f$.

$a \parallel b \stackrel{\text{def.}}{\iff} a | b, b | a$
 $\Rightarrow a = b \vee$
pro invert.v

Dl. a) $d | a, d | b$ a c je největší d. $\Rightarrow d | c \quad \left. \begin{array}{l} c \parallel d \\ e | a, c | b \quad d \text{ je největší s.d.} \Rightarrow c | d \end{array} \right\} c \parallel d$.

b) Ověřím 1, 2 z def. NSD pro f.

1) $f | a$? $f | e \wedge e | a \Rightarrow f | a$.

Stejně $f | b$.

2) $\underbrace{d | a, d | b}_{\Downarrow} \stackrel{?}{\Rightarrow} d | f$ $\xleftarrow{\quad \Downarrow \quad}$
 $d | e$. zdroben $e | f$ \square

5-3. Irreducibilní pravky a rovnice

Def. Rozbor. $a \in \mathbb{R} \setminus \{0\}$. $b \in \mathbb{R}$ je vlásný dělitel a , pokud $b | a$
 $a = bt + 1$, $b \neq a$.

Def. $a \neq 0$ je irreducibilní, pokud $a \neq 1$ a a nemá žádný vlásný děl.

Equiv. $a \neq 1$ a $a = bc \Leftrightarrow b \parallel 1$ nebo $c \parallel 1$.

Příklad. V třídě $\mathbb{Z}/d\mathbb{Z}$ jsou i ned. prvky násobkem

bo $a \in \mathbb{Z}$: $a = 0 \text{ nebo } a \parallel 1$.

• \mathbb{Z}^* ... i ned. jenž projevuje $\pm p$ pro $p \in \mathbb{Z}$.

• $\mathbb{Z}[i]$: • $a+bi, b \neq 0$ je i ned. ($\Leftrightarrow |a| \geq 3 \pmod{4}$)

• $a+bi, a \neq 0, b \neq 0$, je i ned. ($\Leftrightarrow a^2+b^2$ je prvočíslo).

Není uplně formální dokázané - viz TČ.

Def. Irreducibilním rozložed prokna je řešení

$a \parallel p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$, kde p_1, \dots, p_n jsou i ned. prvky, $p_i \neq p_j$ pro $i \neq j, k_1, \dots, k_n \in \mathbb{N}$.

Rekneme, že a má jednoznačný i ned. rozložed, pokud má!

rozložed $a \parallel p_1^{k_1} \cdots p_n^{k_n} \parallel q_1^{l_1} \cdots q_m^{l_m}$ jsou 2 i ned. rovnalady, pak

$m=n$ a existuje permutace indexů π (ne $\{1, 2, \dots, n\}$)

$\pm 1 \cdot p_i \parallel q_{\pi(i)}$ a $k_i = l_{\pi(i)}$ pro i .

Například. $12 = 2^2 \cdot 3^1 \parallel 2^2 \cdot (-3)^1 \parallel (-2)^2 \cdot (-3)^1 \parallel 3^1 \cdot (-2)^2$

Příklad. Irreducibilita řešení je obecná!

$\mathbb{Z}[x] \dots 2x^2+2$ není i ned., bo $2x^2+2 = 2 \cdot (x^2+1)$ a x^2+1 je vlastně díl.

$\mathbb{Q}[x] \dots 2x^2+2$ je i ned. ... tedy není $2 \parallel 1$. (není $1=2 \cdot \frac{1}{2}$)

$\mathbb{C}[x] \dots 2x^2+2 \parallel x^2+1 = (x+i)(x-i) \Rightarrow x+i, x-i$ jsou vlastně díl.

Viz příkaz ... tabulka příkladů.

Příklad. $\mathbb{Z}[\sqrt{5}]$... tady $4 = 2^2 = (1+\sqrt{5})(-1+\sqrt{5})$

$\uparrow \quad \uparrow$
2 je i ned. rovnaladý.

$$v(a+6\sqrt{5}) = |a^2-5b^2|$$

Počítej? • 2 je i ned. Předpokládejme, že ne: $2 = \alpha\beta$, $\alpha \neq 1, \beta \neq 1$.

$$\frac{4}{2} = v(2) = v(\alpha\beta) = v(\alpha) \cdot v(\beta) = 2 \cdot 2$$

$$\Rightarrow v(\alpha) = 2, v(\beta) = 2.$$

$$\alpha = a + b\sqrt{5}, \quad |a^2 - 5b^2| = 2 \Leftrightarrow a^2 - 5b^2 = \pm 2 \quad \text{nepřetí pro řešení}$$

Podobně: $\pm 1 + \sqrt{5}$ je taky i ned.

• $2 \neq 1 + \sqrt{5}$, bo $2 + 1 + \sqrt{5} = 1 + \sqrt{5} = 2 \cdot (c + d\sqrt{5})$

$$\text{bo } b^2, a^2 \equiv 0, 1 \pmod{4}$$

$$\Rightarrow a^2 - 5b^2 \equiv a^2 - b^2 \equiv 0, 1, 3 \pmod{4}$$

$$\not\equiv 2 \pmod{4}.$$

5.4. Prvocíničky $\text{P}\text{or. } \left\{ \begin{array}{l} \text{P}\text{říká } a \\ \forall a, b \in \mathbb{R}: \\ p \mid a \cdot b \Rightarrow p \mid a \text{ nebo } p \mid b. \end{array} \right.$

- $\forall \mathbb{Z}$: • každý prvočíslo je prvocíniček.
 - a i red. $\Leftrightarrow a$ je prvocíniček ($\Leftrightarrow \pm a$ je prvočíslo).
- \uparrow neplatí v obecném ohledu

Porovn. P je prvoč. $\Rightarrow P$ je i red.

Dle At' $P = ab$. Pak $p \mid ab \stackrel{\text{prvoč.}}{\Rightarrow} p \mid a \text{ nebo } p \mid b$.
 Zdrovení alp, blp.
 Tedy a, b nerozdělitelné.

$$\Rightarrow \underbrace{p \parallel a}_{\Downarrow b \parallel 1} \text{ nebo } \underbrace{p \parallel b}_{a \parallel 1}.$$

Pi. $\mathbb{Z}[\sqrt{5}]$. 2 je i red., ale $2 \mid (1+\sqrt{5})(-1+\sqrt{5})$ a
 $2 \nmid \pm 1 + \sqrt{5} \Rightarrow 2$ není prvoč.

6. EXISTENCE & DĚLOVÁNÍ (RED. ROZDĚL.)

6.1 Gaußovo skloňování

Def. Obor \mathbb{R} je gaußovo skloňovatelný, pokud $\forall a \in \mathbb{R}, a \neq 0, a \neq 1$, má jednoznačné i red. rozdělení.

Pi. • \mathbb{Z} je gauß.

• $\mathbb{Z}[x]$ je gauß.

• $T[x] =$ obor polynomů nad telesem je gauß.] (časem)

$T[x_1, \dots, x_n] \dots$ gauß.

$\mathbb{Z}[x] \dots$ gauß.

• $\mathbb{Z}[\sqrt{5}]$ není gauß.

• $\mathbb{Z}[\sqrt{s}]$ pro $s = -1, -2, 3$ je gauß.
 typickým není gauß.

Otevřený problém. $\mathbb{Z}[\sqrt{s}]$ je gauß. pro co mnoho s.

[$s < 0$, pak jen kou. mnoho s. gauß.]

$$\boxed{\begin{array}{l} \mathbb{Z}: b \mid 2^3 \cdot 3 \cdot 5^2 \\ \Leftrightarrow b \parallel 2^{l_1} 3^{l_2} 5^{l_3} \\ 0 \leq l_i \leq 3, \dots \end{array}}$$

T.6.1 \mathbb{R} gauß. obor, $a, b \in \mathbb{R}$, $a, b \neq 0$.

At' $a \parallel p_1^{k_1} \cdots p_n^{k_n}$ je i red. rozdělení.

Pak $b/a \Leftrightarrow b \parallel p_1^{l_1} \cdots p_n^{l_n}$, kde
 $0 \leq l_i \leq k_i$ pro i .

[toto nemusí být i red. rozděl., když $k_i = l_i + 1$]

rozsílení def. i red. rozdělení:
 $a \parallel 1$, pak říkáme, že je i red.
 rozdělení a je
 $a \parallel 1 = p_1^{0} \cdots p_n^{0}$ nebo
 $a \parallel 1 \cdots n=0$.

Dr. (⇒) $b \parallel p_1^{e_1} \cdots p_n^{e_n}$. At' $f = r p_1^{e_1} \cdots p_n^{e_n}$, $r \parallel 1$.

a $a = q p_1^{e_1} \cdots p_n^{e_n}$, $q \parallel 1$.

Chceme: $b|a$, tedy $\exists c: a = bc$.

$$c = q^{-1} p_1^{k_1 - e_1} \cdots p_n^{k_n - e_n} \quad \checkmark$$

(⇒) $b|a \Rightarrow a = bc \quad \exists c$.

At' $b \parallel q_1^{s_1} \cdots q_v^{s_v}$, $c \parallel r_1^{t_1} \cdots r_v^{t_v}$ jsou i ned. rovn.

Z kombinace ve výrobeně $b \cdot c$: $bc \parallel q_1^{s'_1} \cdots q_v^{s'_v} \cdot r_1^{t_{1'}} \cdots r_v^{t_{1w}}$

... zde byly z rozkladu c ty r_i , kteří jsou asoc. s něj. q_j .

Mám 2 rozklady $bc = a \parallel p_1^{k_1} \cdots p_n^{k_n}$.

Z jednoznačnosti rozkladu: $q_i = P_{\pi(i)}$ & $s'_i = k_{\pi(i)}$

⇒ $b \parallel p_{\pi(1)}^{s_1} \cdots p_{\pi(v)}^{s_v}$, kde $s_i \leq k_{\pi(i)}$

Také se může doplňovat případně coby $b \parallel p_1^0$. □