

ALGEBRA 31.3.

1. písemná: 21.4. v 9:00 (ne přednáška!)
cca 30 min.

příklady: sad 1-6. (=po break 14.4.
dowdu' 7.-13.4.)

Ideál. $I \subseteq R \dots$ $a+b, -a \in I$ (pro $a, b \in I$)
 $r \cdot a \in I$ $r \in R$

Hlavní id. $I = a \cdot R = \{ ar \mid r \in R \}$

$a \mid b \Leftrightarrow aR \supseteq bR$

$a \parallel b \Leftrightarrow aR = bR$

OHI. ... \forall ideál je hlavní.

Věta 7.8 Bud' R OHI. Pak R je gaus. a platí v něm
Bez. rovnost.

7.7.7. I, J id. 1) $I \cap J$ ideál
2) $I+J = \{ a+b \mid a \in I, b \in J \}$
3) $I_1 \subseteq I_2 \subseteq \dots$ ideály $\Rightarrow \bigcup_{j=1}^{\infty} I_j$ id.

$aR + bR = \{ ar + bs \mid r, s \in R \}$

Ideál generovaný prvky a_1, a_2, \dots, a_n :

$$a_1R + a_2R + \dots + a_nR = \left\{ \sum_{i=1}^n a_i r_i \mid r_i \in R \right\} \\ = (a_1, \dots, a_n)$$

[Noetherovský stav - \forall id. je kon. gen.]

Důl. v. 7.8 R OHI. Chcun 1) NSD 2) max. vzt. dít. (veta 6.3)

1) $a, b \in R$. Bud' $I = aR + bR \stackrel{\text{OHI}}{=} cR$ pro nějaké $c \in R$.

$aR \subseteq cR \Rightarrow c \mid a$

$bR \subseteq cR \Rightarrow c \mid b$

Bud' $d \mid a, d \mid b \Rightarrow aR \subseteq dR, bR \subseteq dR$.

Ale $aR + bR$ je nejm. id., kt. obsahuje aR, bR (7.7)

$\Rightarrow cR = aR + bR \subseteq dR \Rightarrow d \mid c$ život.

Tedy $c = \text{NSD}(a, b)$. Nauce: $c \in aR + bR \Rightarrow \boxed{c = ar + bs}$ pro něj. $r, s \in R$

2) Pro spor: $\dots a_{i+1} | a_i | a_{i-1} | \dots | a_2 | a_1, a_i \nmid a_{i+1} \forall i.$

$$a_1 R \subsetneq a_2 R \subsetneq a_3 R \subsetneq \dots$$

$$I = \bigcup_{i=1}^{\infty} a_i R \text{ je ideal } \stackrel{OHI}{=} I = bR \exists b \in I.$$

$$I = \bigcup a_i R \ni b \Rightarrow \exists i: b \in a_i R, \exists i: b = a_i r$$

$$\text{Pak } bR \subsetneq a_i R \subsetneq a_{i+1} R \subsetneq \dots \subsetneq I = bR. \text{ SPOR.}$$

Motivace pro idealy: $x^2 + 5 = y^3$
 $\parallel (x + \sqrt{-5})(x - \sqrt{-5}) \quad \vee \mathbb{Z}[\sqrt{-5}].$

Problem: $\mathbb{Z}[\sqrt{-5}]$ není gauss. $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = ABCD$
 $\begin{matrix} \uparrow & \uparrow & \uparrow & \uparrow \\ AB & CD & AC & BD \end{matrix}$

A, B, C, D jsou "ideální prvky".
 A ... se chová jako "NSD $(2, 1 + \sqrt{-5})$ "
 my máme konkrétně ne ideál generovaný $2, 1 + \sqrt{-5}$.

7.3 Hierarchie

eucl. \Rightarrow OHI \Rightarrow gauss. téžto $\left\{ \begin{matrix} \text{viz komut. alg.} \\ \text{Alg. T. 5} \end{matrix} \right.$

obor:	ired. rozl.	NSD	Bézant	eucl. alg.	průhled
eucl.	✓	✓	✓	✓	$\mathbb{Z}, \mathbb{T}, \mathbb{T}[x], \mathbb{Z}[i]$
OHI	✓	✓	✓	x	$\mathbb{Z}\left[\frac{1 + \sqrt{-19}}{2}\right]$ ne eucl.
gauss.	✓	✓	x	x	$\mathbb{Z}[x]$ ne OHI
obecné	x	x	x	x	$\mathbb{Z}[\sqrt{-5}], \mathbb{Z}[\sqrt{5}]$ ne gauss.

8. POLYNOMY NAD GAUSS. OBOREY (BEZ DŮKAZŮ)

$f \in R[x]$ je primitivní, pokud jsou jeho koef. nesoud. a dle: $\forall c \in R: \text{pokud } c \text{ dělí všechny koef. } f, \text{ pak } c \parallel 1.$

Př. $\mathbb{Z}[x] \dots 3x^2 + 2x + 2$ je prim.
 $2x^2 + 2x + 2$ není

Lemma 8.1 (gaussovo lemma). R gauss. obor. f, g prim. pol. v $R[x] \Rightarrow f \cdot g$ je primit.

T. 8.2 R gauss., Q podílové těleso R . (př. $R = \mathbb{Z}, Q = \mathbb{Q}$).

f, g prim. pol. v $R[x]$. Pak

$f|g$ v $R[x] \Leftrightarrow f|g$ v $Q[x]$.

Př. \mathbb{Z}, \mathbb{Q} . $f = 2$ není prim.

$$g = x.$$

$2|x$ v $\mathbb{Z}[x]$, ale $2 \nmid x$ v $\mathbb{Q}[x]$
 $\dots x = 2 \cdot \left(\frac{1}{2}x\right)$

Výhoda: $Q[x]$ je eukl., takže má „rozdělení“.

T. 8.2 převádí dělitelnost v $R[x]$ (složitá) na delit. v $Q[x]$ (snadná).

Značení. $f = \sum_{i=0}^n a_i x^i \in R[x], a_n \neq 0$. (R gauss.)

$c(f) = \text{NSD}(a_0, a_1, \dots, a_n) \in R$... obsah f (content)

[prim. pol. $\Leftrightarrow c(f) = 1$]

$PP(f) = \frac{1}{c(f)} \cdot f$... primitivní část f (primitive part)
 \leftarrow je prim. pol. v $R[x]$.

Věta 8.3. R gauss., Q pod. těleso, $f, g \in R[x]$. Pak

1) $\text{NSD}_{R[x]}(f, g)$ existuje a rovná se $c \cdot h$, kde

$$c = \text{NSD}_R(c(f), c(g)),$$

$h \in R[x]$ je primitivní t.j. $h = \text{NSD}_{Q[x]}(PP(f), PP(g))$.

2) f je ireduc. v $R[x] \Leftrightarrow$

a) $\deg f = 0$ a f je ireduc. v R .

b) $\deg f > 0$, f je primit. a f je ireduc. v $Q[x]$.

Věta 8.4 (Gaussova věta). R gauss. obor $\Rightarrow R[x]$ gauss. obor

Spec. $\mathbb{Z}[x]$ gauss.

$\cdot R$ gauss. $\Rightarrow R[x_1, \dots, x_n]$ gauss. $\Rightarrow R[x_1, x_2, x_3, \dots]$ gauss.

8.2 Reducibilita pol.

T.8.5 (existence rac. kořen). \mathbb{R} gauss. obl., \mathbb{Q} pod. těl.

Ukli: $f = \sum_{i=0}^n a_i x^i \in \mathbb{R}[x]$, $a_n \neq 0$ kořen $\frac{r}{s} \in \mathbb{Q}$ (pro $\text{NSD}(r,s) = 1$)

pak $r \mid a_0$, $s \mid a_n$.

Dů. $0 = f\left(\frac{r}{s}\right) = \sum a_i \left(\frac{r}{s}\right)^i \dots$ přenesolím s^n :

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

$\Rightarrow r \mid a_0 s^n$. (poznámka)

Ale $\text{NSD}(r,s) = 1 \Rightarrow r \mid a_0$.

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

Př. $x^n - p \in \mathbb{Z}[x]$, p prvoc., uvaž. rac. kořen, $\frac{r}{s} \in \mathbb{Q}$

Ale $\sqrt[n]{p}$ je kořen $\Rightarrow \sqrt[n]{p}$ irac.

$\dots r \mid p \Rightarrow r = \pm 1, \pm p$
 $s \mid 1 \Rightarrow s = \pm 1$
 nic z toho nefung.

T.8.6 (Eisensteinovo kritérium) \mathbb{R} obl.

$f = \sum_{i=0}^n a_i x^i \in \mathbb{R}[x]$ primitivní, $a_n \neq 0$.

Polud ex. prvocíteľ $p \in \mathbb{R}$ t.j. $p \mid a_0, p \mid a_1, \dots, p \mid a_{n-1}, p^2 \nmid a_0$,

pak f je ireducibilní. [f prim. $\Rightarrow p \nmid a_n$]

Dů. Pro spor: $f = g \cdot h$, $g = \sum_{i=0}^k b_i x^i$, $h = \sum_{i=0}^l c_i x^i \in \mathbb{R}[x]$
 stupně ≥ 1 .

$$\begin{aligned} a_0 + a_1 x + a_2 x^2 + \dots &= (b_0 + b_1 x + \dots)(c_0 + c_1 x + \dots) \\ &= b_0 c_0 + (b_0 c_1 + b_1 c_0) x + \dots \end{aligned}$$

$\Rightarrow a_0 = b_0 c_0$. $p \mid a_0 = b_0 c_0 \Rightarrow p \mid b_0$ nebo $p \mid c_0$.
 Bůho $p \nmid b_0$.

Pak $p \nmid c_0$, bo $p^2 \nmid a_0$.

\bullet $p \mid a_1 = b_0 c_1 + b_1 c_0$. Zároveň $p \mid b_0 \Rightarrow p \mid b_0 c_1$

$\Rightarrow p \mid b_1 c_0$. $\overset{\text{prvoc.}}{\Rightarrow} p \mid b_1$.

\bullet Pokročijte. Když uvažijte a_i , dostaneme $p \mid b_i$... pro $\forall i \leq n-1$.

\bullet p dělí všechny koef. b_i pro $i \leq k \leq n-1$.

$\Rightarrow p \mid g \mid f$, spor s primitivitou f .

Př. Eisenstein $\Rightarrow x^n \pm a \in \mathbb{Z}[x]$ je irred., pokud existuje prvočíslo p t.ž. $p|a, p^2 \nmid a$.

9. ČZV A INTERPOLACE

Věta 9.1 (ČZV pro polynomy). T těleso.

At' $m_1, m_2, \dots, m_n \in T[x]$ jsou po 2 nesoud. polynomy,
 $d = \sum \deg m_i$.

At' $v_1, \dots, v_n \in T[x]$. Pak $\exists!$ $f \in T[x]$ stupně $< d$ t.ž.
 $f \equiv v_1 \pmod{m_1}, \dots, f \equiv v_n \pmod{m_n}$.

Dě. Jednoznačnost. At' f, g jsou řešení, $\deg f, \deg g < d$.

Čili $f \equiv g \equiv v_i \pmod{m_i} \quad \forall i$.

$\Rightarrow m_i \mid f - g \quad \forall i$.

m_i po 2 nesoud. (a $T[x]$ Gauss.)

$\Rightarrow m_1 \dots m_n \mid f - g$.

Ale $\deg(m_1 \dots m_n) = d$ a $\deg(f - g) < d \Rightarrow f - g = 0$.

Existence. $P_k = \{ f \in T[x] \mid \deg f < k \}$ je vektorový prostor nad T dimenze k , bo $1, x, x^2, \dots, x^{k-1}$ je báze.

$d_i = \deg m_i$.

$\varphi: P_d \longrightarrow P_{d_1} \times \dots \times P_{d_n}$

$f \longmapsto (f \pmod{m_1}, \dots, f \pmod{m_n})$

↑
 zbytky po dělení, mají stupeň $< \deg m_i = d_i$

dobře def. zobrazení.

Nauč: • homom. vekt. prostorů.

• φ prosté. (jednozn.)

• $\dim P_d = d, \dim P_{d_1} \times \dots \times P_{d_n} = d_1 \dots d_n = d$.

Tvrzení z linearity: Prostý hom. mezi vekt. prostory stejné dimenze je bijekce.

$\Rightarrow \varphi$ je bijekce. $\Rightarrow \varphi$ je na.

Tedy pro $\otimes = (v_1 \pmod{m_1}, \dots, v_n \pmod{m_n})$ existuje f t.ž. $\varphi(f) = \otimes$

Takle f řeší kongruence.