

ALGEBRA 7.4.

9.1

• T těleso, $f \equiv v_1 \pmod{m_1}, \dots, f \equiv v_n \pmod{m_n}$

$v_i \in T[x], m_i \in T[x]$ po zvesoud.

$\exists! f \in T[x] \text{ t.ž. } \deg f < \sum \deg m_i.$

$f = g_1 m_1 + v_1 \implies g_1 m_1 + v_1 \equiv v_2 \pmod{m_2}$

$f_1 \equiv m_1^{-1} (v_2 - v_1) \pmod{m_2}$

\bar{m}_1 inverz mod m_2
existuje díky zvesoud: Bézout

• $1 = \text{NSD}(m_1, m_2) = x m_1 + y m_2$
za m_1^{-1} můžeme vzít x , bo
 $1 \equiv x m_1 \pmod{m_2}$

$g_1 = g_2 m_2 + m_1^{-1} (v_2 - v_1)$

Důsledek 9.2 (v.o. interpolaci) T těleso. Máme po n různých bodech

$a_1, \dots, a_n \in T$ a libovolné hodnoty $v_1, \dots, v_n \in T$.

$\exists! f \in T[x], \deg f < n \text{ t.ž. } f(a_i) = v_i \quad \forall i. \textcircled{*}$

Důl. $f \equiv f(a) \pmod{x-a}$ (už bylo, cvičení).

Tedy $\textcircled{*} (\iff) f \equiv v_i \pmod{x-a_i}$. ČZV $\ddot{\smile}$

Lagrangeův interpol. polynom $f = \sum_{i=1}^n \left(v_i \cdot \prod_{j \neq i} \frac{x - a_j}{a_i - a_j} \right)$

Důl. 9.3 (zobrazení ve konečných tel. jsou polynomidlní). T konečné těleso.

Pro $\forall \varphi: T \rightarrow T$ zobrazení $\exists! f \in T[x], \deg f < |T|$

t.ž. $\varphi(a) = f(a)$.

Pozn. ve ukon. tělesech to neplatí: $\left[\begin{array}{l} \text{ved } \mathbb{Q}: \\ \text{zobrazení je } \text{nespoch.} \\ \text{polynom. je } \text{spoch.} \end{array} \right.$

Důl. Interpolují v každém bodě a hodnotu $\varphi(a)$.

9.2 FAKTOROKRUH MODULO POLYNOM



$$\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}, \quad + \left. \begin{array}{l} \text{mod } m \\ - \\ \cdot \end{array} \right\}$$

$$m = m_0 + m_1 \alpha + m_2 \alpha^2 + \dots + m_n \alpha^n$$

$m_n \neq 0$

Def. T těleso. Bud' $m \in T[\alpha]$ polynom stupně $n \geq 1$.

Faktorokruh $T[\alpha]/(m)$ je

- množina všech polynomů z $T[\alpha]$ stupně $< n$

- s standardním $+$, $-$

- a s operací násobení modulo m , čili $f \circ g = f \cdot g \text{ mod } m$

Čili $T[\alpha]/(m) = \left(\{ f \in T[\alpha] \mid \deg f < n \}, +, -, \cdot, 0, 1 \right)$ zbytek po dělení m

Pozor. Jde o komut. okruh s 1:

Axiomy $+$, $-$, 0 : plynou z axiomů pro $T[\alpha]$

Axiomy \cdot se převedou na kongruence mod m :

Pletí: $f \equiv g \pmod{m} \Leftrightarrow f \text{ mod } m = g \text{ mod } m$

- $\frac{f \text{ mod } m}{\text{zbytek po del.}} \equiv \frac{f}{\text{kongruence}} \pmod{m}$

Např. $(f \circ g) \circ h \stackrel{?}{=} f \circ (g \circ h) \stackrel{def}{=} \dots$

$(fg \text{ mod } m) \cdot h \text{ mod } m \stackrel{?}{=} f (gh \text{ mod } m) \text{ mod } m \stackrel{?}{=} \dots$

$(fg)^h \equiv f(gh) \pmod{m}$

což pletí, bo $(fg)h = f(gh)$ (násobení v $T[\alpha]$)

• $f \circ g \in T[\alpha]/(m)$, bo $fg \text{ mod } m$ má stupeň $< n = \deg m$.

Pr. $\mathbb{R}[\alpha]/(\alpha^2+1)$... prvky jsou polynomy $a+b\alpha$.

$= \{ a+b\alpha \mid a, b \in \mathbb{R} \}$

$$(a+b\alpha) + (c+d\alpha) = (a+c) + (b+d)\alpha$$

$$(a+b\alpha) \circ (c+d\alpha) = (ac + (ad+bc)\alpha + bd\alpha^2) \text{ mod } (\alpha^2+1)$$

$$\stackrel{cr}{=} (ac - bd) + (ad+bc)\alpha \in \mathbb{R}[\alpha]/(\alpha^2+1)$$

Máme izom. okruhů $\varphi: \mathbb{R}[\alpha]/(\alpha^2+1) \rightarrow \mathbb{C} = \mathbb{R}[i]$ Ověří se, že

Podobně: $\mathbb{Q}[\alpha]/(\alpha^2+1) \cong \mathbb{Q}[i]$. $[a+b\alpha \mapsto a+bi$ fakt izom.

Pi. Nad tělesem \mathbb{Z}_p (p prvočíslo) zvažme p :

• $\mathbb{Z}_2[x]/(x^2+1)$ má 4 prvky, ale není to obor:

$$(x+1) \odot (x+1) = x^2 + \underbrace{2x}_0 + 1 \pmod{x^2+1} = 0.$$

• $\mathbb{Z}_3[x]/(x^2+1)$ má 9 prvků. Je to těleso (ale není to očiividue!).

T.9.4 (faktor podle irred. polynomu). T těleso, $m \in T[x]$, $\deg m \geq 1$.

NTD E.

1) $T[x]/(m)$ je těleso

2) $T[x]/(m)$ je obor

3) m je ireducibilní polynom v $T[x]$.

Důk. 1) \Rightarrow 2). T. 1.3 ✓

2) \Rightarrow 3). Ať $m = fg$ pro $f, g \in T[x]$, $\deg f, \deg g \geq 1$.

Pak v $T[x]/(m)$ platí $f \odot g = fg \pmod{m} = m \pmod{m} = 0$,
čili $T[x]/(m)$ není obor.

3) \Rightarrow 1). Bud' $f \neq 0$ polynom, $\deg f < \deg m$.

m irreduc., f má menší st. než $m \Rightarrow m, f$ jsou nesoud.

Bézout: $1 = \text{NSD}(f, m) = uf + vm$ pro nějaké $u, v \in T[x]$.

Bud' $\tilde{u} = u \pmod{m}$.

Pak v $T[x]/(m)$ platí: $\tilde{u} \odot f = \tilde{u}f \pmod{m} \equiv uf \equiv 1 \pmod{m}$

Tedy $\tilde{u} \odot f = 1$ v $T[x]/(m)$. Tedy \tilde{u} je inverz. \square

Pak budeme \odot zvažovat jako \cdot .

9.3. KOŘENOVÁ, ROZKLADOVÁ A DĚLITELNÁ TĚLESA

T.9.5 T těleso, $f \in T[x]$, $\deg f \geq 1$. Pak existuje těleso

$S \supseteq T$, ve kterém má f kořen.

• Pro $T = \mathbb{Q}$ se to může zdát triviální: za S jde brát \mathbb{C} .

Triviální to není! To, že každý pol. má v \mathbb{C} kořen, je třeba dokázat!

Důk. Bud' $m = \sum_{i=0}^n a_i x^i \in T[x]$ nějaký irred. dělitel f . (zobledně v. algebr.)

$S = T[x]/(m(x))$. T.9.4 \Rightarrow S je těleso.

$S \supseteq T$ (bo T tam máme jako konst. pol.)

Chceme: $m(x)$ má v S kořen. Jo, a sice $\alpha = \sqrt[n]{m/f}$.

$$m(x) = \sum_{i=0}^n a_i x^i \quad S = T[x] / (m(x)).$$

Dosaďme $\underline{m(x)}$ v S :

$$\begin{aligned} m(x) &= \sum a_i \underbrace{0 \dots 0 \alpha}_{i\text{-krát}} = \sum (a_i x^i \bmod m) \\ &= \underbrace{a_0 \bmod m} + a_1 x \bmod m + \dots + a_{n-1} x^{n-1} \bmod m + a_n x^n \bmod m \\ &= a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + (a_n x^n \bmod m) \\ &= a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + (-a_0 - a_1 x - \dots - a_{n-1} x^{n-1}) \\ &= 0. \quad \checkmark \end{aligned}$$

Pr. $x^3 - 2$ nad $\mathbb{Q} \rightsquigarrow \mathbb{Q}[x] / (x^3 - 2) \cong \mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}(\sqrt[3]{2})$

$x^3 - 2$ nad $\mathbb{Z}_7 \rightsquigarrow \mathbb{Z}_7[x] / (x^3 - 2)$... těleso s 7^3 prvky

Věta 5.6 T těleso, $f \in T[x]$, $\deg f \geq 1$. Pak ex. těleso $S \geq T$, kde x f rozložíme na součin polynomů stupně 1.

Dl. Indukcí podle $\deg f$.

$\deg f = 1 \Rightarrow f = ax + b$ a má kořen $-a^{-1}b \in T$. ($S = T$)

$\deg f > 1$. Podle 5.5 bud' $U \geq T$ t.ž. $f(u) = 0$ pro $u \in U$.

Pak $f = (x - u) \cdot g$ pro nějaké $g \in U[x]$, $\deg g = \deg f - 1$.

IP pro $g \Rightarrow \exists S \geq U$ t.ž. $g = (x - a_1) \dots (x - a_k) \in S[x]$

Pak $f = (x - u)(x - a_1) \dots (x - a_k) \in S[x]$.

A $S \geq U \geq T$, tedy $S \geq T$.

Def. T těleso, $f \in T[x]$, $\deg f \geq 1$.

1) Kořenově udt. těleso f je (libovolné) těleso $S \geq T$, ve kterém ex. $a \in S$ t.ž. $S = T(a)$ a $f(a) = 0$.

2) Rozkladově udt. f

ex. $a_1, \dots, a_n \in S$: $S = T(a_1, \dots, a_n)$ a $f \parallel (x - a_1) \dots (x - a_n) \in S[x]$.

Důl. 5.7 (existence koř., rozkl. udt.) T těleso, $f \in T[x]$, $\deg f \geq 1$

Pak ex. kořenově i rozkladově udt. f nad T .

Dl. 5.5 $\Rightarrow \exists S_0 \geq T$ t.ž. $f(a) = 0$ pro $a \in S_0$. Kořenově udt.

pak je $S = T(a) \leq S_0$.

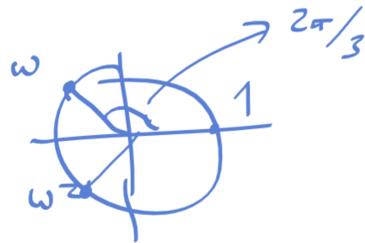
5.6 \Rightarrow rozkl. udt. anal.

Př. • $\mathbb{Q}(\sqrt[3]{2})$ je roz. vedt. $x^3 - 2$ nad \mathbb{Q} .

nemí rozl. vedt.!

$$\text{Bo } x^3 - 2 = (x - \sqrt[3]{2})(x - \omega \sqrt[3]{2})(x - \omega^2 \sqrt[3]{2}),$$

$$\text{kde } \omega = e^{2\pi i/3} \\ = \frac{-1 + i\sqrt{3}}{2}$$



Proč je $\omega \sqrt[3]{2}$ rozl.?

$$(\omega \sqrt[3]{2})^3 - 2 = \omega^3 \cdot 2 - 2 = 1 \cdot 2 - 2 = 0$$

$$\omega^3 = (e^{2\pi i/3})^3 = e^{2\pi i} = 1.$$

Ale $\omega \sqrt[3]{2} \in \mathbb{C} \setminus \mathbb{R}$, tedy $\omega \sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$

Rozl. vedt. $\mathbb{Q}(\sqrt[3]{2}, \omega)$.

• $\mathbb{Q}(i)$ je rozl. vedt. $x^2 + 1$ nad \mathbb{Q} .
" $(x+i)(x-i)$