

ALGEBRA 2.6.

25. (NE)ŘEŠITELNOST POLYONOMU V RADIKÁLECH

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

ODNOVNUTÍ

$$\bullet \ ax^2 + bx + c = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

- 3. stupně ~1530 Tartaglia ... Cardanovy r.v. 1545
- 4. st. ... Ferraria

≥ 5. stupně?

Ruffini 1799 nesplý

Abel 1823 důkaz

Galois ~1830 lepišť teorie

Def. $T \subseteq U$, $a \in U$. a je ujednáitelný v radikálech ve T ,
polnud ex. řešení v $T = T_0 \subseteq T_1 \subseteq \dots \subseteq T_q \subseteq U$ t.z.

$$\bullet a \in T_q$$

• $\forall i$, T_i je rozložové nedt. užitelné pol. $x^{n_i} - a_i \in T_{i-1}[x]$
přidělum vš. kořeny $x^{n_i} - a_i$, když jsou užitelné
odmocniny $\sqrt[n_i]{a_i}$.

Př. $a = \frac{\sqrt[5]{7} + \sqrt{2}}{i+1}$

$$T = T_0 = \mathbb{Q}$$

$$U = \mathbb{C}$$

$$T_1 \dots x^2 + 1$$

$$T_2 \dots x^2 - 2$$

$$T_3 \dots x^3 - 7$$

$$T_4 \dots x^5 - (\sqrt[3]{7} + \sqrt{2})$$

Def. T těleso, $f \in T[x]$. f je řešitelný v radikálech nedt.,
polnud ex. $T = T_0 \subseteq T_1 \subseteq \dots \subseteq T_q$ t.z.

• $\forall i$, T_i je rozlož. nedt. užitelné pol. $x^{n_i} - a_i \in T_{i-1}[x]$

• f je rozložitelný v T_q ve lineárními i maticemi, iili
rozlož. nedt. f je obsažen v T_q .

Př. St. 1 ... $T_1 = T_0$. $ax+b$

$$\underline{T = \mathbb{Q}}$$

St. 2. $T_1 = \text{rozlož. nedt. } x^2 - (b^2 - 4ac) = \mathbb{Q}(\sqrt{b^2 - 4ac})$

$$\text{St.3} \quad \text{Rjedno } x^3 + bx + c. \quad D = c^2 + \frac{b^3}{27}$$

$$\xi = e^{\frac{2\pi i}{3}}$$

Koreny jsou $\xi^2 \sqrt[3]{\frac{-c + \sqrt{D}}{2}} - \xi^{-2} \sqrt[3]{\frac{c + \sqrt{D}}{2}}, \quad \varrho = 0, 1, 2.$

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{D}) \leq \mathbb{Q}(\xi, \omega)$$

$$x^2 - D \quad ; \quad x^3 - \frac{-c + \sqrt{D}}{2}$$

V.25.1 (Galoisova veta) T tiblo čer. 0, $f \in T[x]$, $\deg f \geq 1$.

Polyynom f je řešitelný v redile'ch ned $T \Leftrightarrow$

$\text{Gal}(f/T)$ je řešitelné' grupa.

Přípon. f je rosl. nedt. $S \geq T$.

$$\text{Gal}(f/T) = \text{Gal}(S/T) = \left\{ \varphi: S \rightarrow S \mid \begin{array}{l} \\ \text{T-autom.} \end{array} \right\}$$

- T.24.5 $\Rightarrow \text{Gal}(f/T) \hookrightarrow S_n$ (kde $n = \deg f$)
- S_2, S_3, S_4 řešitelné' gr.; Bodgr. řešit. gr. je řešitelná
 $\Rightarrow \deg f \leq 4$, pak f je řešitelný.

Důsled. 25.2. \nexists polyynom. stupně ≤ 5 je řešitelný v red.

• Naopak jsme videli (zkuš 19.3), že grupy S_n , $n \geq 5$, nejsou řešitelné. Tedy pokud nejdeme f , $\deg f = 5$

+ž. $\text{Gal}(f/\mathbb{Q}) \cong S_5$, pak tento pol. je neřešitelný.

T. 24.8 \exists prvočíslo, $f \in \mathbb{Q}[x]$ irreduc. pol., $\deg f = p$,

+ž. f má $p-2$ reálných a 2 komplexních nezáhlavých kořenů. Pak $\text{Gal}(f/\mathbb{Q}) \cong S_p$.

Dl. Bud \cup rosl. nedt. f ned \mathbb{Q} . T.24.5(1) \Rightarrow

$\text{Gal}(V/\mathbb{Q}) \cong H \leq S_p$. [pokdy H j,ou síténí φ ne]
 [rovný f]

Chci: H obsahuje transponaci a p -cyklos.

CV: Pok $H = S_p$.

- f má $p-2$ reáln., 2 imagin. koř. $\Rightarrow Q \subseteq U \subseteq \mathbb{C}$
- Na \mathbb{C} méně \mathbb{Q} -autom. = komplexní jazyk.
- Vražíme již sítě U , $\overline{\omega}$ je \mathbb{Q} -autom. U .
- f fixuje reálné kořeny a prolesuje mezi nimi 2 imagin. kořeny
- Tedy \mathbb{P} je permutace na kořenech je transpose.
- H působí na možné kořeny f .
- T. 24.5(2) \Rightarrow působení H je transitiční (neboli má jen 1 orbitu)
- Ta má velikost p (\leq počet kořenů f).
- T. 18.3 $\Rightarrow p = \text{velikost orbity } |\mathcal{O}_H|$
- V. 18.6 $\Rightarrow H$ obsahuje pár sítí P ... to je právě hledaný p -cyklus :-)
- H obsahuje transp. & p -cyklus $\Rightarrow H = S_p$.
- $\text{Ri. } f = x^5 - 4x + 2 \dots$ irreducibilní dílčí Eisensteinova pro 2 .
Kořeny? $f' = 5x^4 - 4 \dots f' = 0 \dots$ má 2 reálné
 $\Rightarrow f$ má pět reálných koř.
 \Rightarrow zahrnuje 2 imagin.
- $\text{Tvrz. } \Rightarrow \text{Gal}(f/\mathbb{Q}) \cong S_5$.
- Disk. 25.3 (Abelova-Buffalova věta) Existují osmdesátí pětirozšího st. ≥ 5 , které mají reálné a nezáporné kořeny.
- Dl. S_5 nemá reálné, $\exists f : \text{Gal}(f/\mathbb{Q}) \cong S_5$.
- 25.1 $\Rightarrow f$ nemá reálné.
- Zbyla dle Galoisova větu 25.1, a to jenom
 $\text{"Gal nemá reál."} \Rightarrow f \text{ nemá reál.}"$
- Myslím: $\mathbb{Q} = T_0 \leq T_1 \leq \dots \leq T_k + \sum T_i$ nosil. nedl. $x^n - a$,
- $\text{Gal}(T_k/\mathbb{Q}) \geq \text{Gal}(T_k/T_1) \geq \dots \geq \text{Gal}(T_k/T_1) = \{1\}$
- faktorgroup $\text{Gal}(T_k/T_1) / \text{Gal}(T_k/T_{k+1}) \cong \text{Gal}(T_{k+1}/T_1)$

L. 25.4 S rovn. nedt. nějakeho pol. f ued tělesu T ,
 $g \in T[x]$ irreducibilní pol. Polud g me' v S nejsou
 par x tam rovnéde' ne lin. činitel.

Dr. NEČKOVSKÝ. $U =$ rovn. nedt. polyg. fg.

Bud' a rovn. g v tělesu S .

b rovn. g v U .

Jednoznacnost rovn. nedt. $\Rightarrow \exists \varphi \in \text{Gal}(U/T) + \bar{z}$.

$$\varphi(a) = b.$$

φ permutuje břez polygonum f ($v U$) (+.24.1);

ty jenži' $S \Rightarrow \varphi(S) \subseteq S$. Par b = $\varphi(a) \in S$ ✓

L. 25.5 T těleso char. 0, $T \leq S \leq U$, kde

S = rovn. nedt. nějakeho pol. f ued T

$U = \underbrace{\dots}_{n} x^n - a \in S[x]$ nad S .

Pak \exists rovník $U \leq V + \bar{z}$.

- $V =$ rovn. nedt. nějakeho pol. nad T

- $\text{Gal}(V/S)$ je řešitelná grupa.

Připomímk. +.24.7: $\text{Gal}(U/S)$ je řešit. (bo metabel.)

Dr. Blahos $U \leq \mathbb{C}$.

$$g = m_{a,T}(x^n) \in T[x].$$

$V =$ rovn. nedt. fg nad T
 $\cong \mathbb{C}$.

$$\boxed{\begin{aligned} m_{a,T}(x) &= (x-a)(x-a_2)\dots(x-a_m) \\ g &= (x^n - a)(x^n - a_2)\dots \end{aligned}}$$

- $U \leq V$: bo $x-a \mid m_{a,T}$ v $S[x] \Rightarrow$

$$x^n - a \mid m_{a,T}(x^n) = g$$

$\Rightarrow x^n - a$ se ve V rovnéde' ne lin. činitel

$\Rightarrow U \leq V$.

- $m_{a,T}$ je iredu, me' rovn. v S . L. 25.4 $\Rightarrow m_{a,T}$ ze v S rovnéde' ne lin. čin.

$$m_{a,T} = (x-a_1) \dots (x-a_m) \Rightarrow g = (x^n - a_1) \dots (x^n - a_m)$$

(nepř. $a = a_1$)

$$g = (x^n - a_1) \cdots (x^n - a_m) \in S[x].$$

Chci: $\text{Gal}(V/S)$ je řešit.

$$S = S_0 \leq S_1 \leq \cdots \leq S_m = V.$$

$$S_i = \text{rostl. nedf. } x^n - a_i \text{ nad } S_{i-1}.$$

$$= \text{rostl. nedf. } (x^n - a_1) \cdots (x^n - a_i) \text{ nad } S$$

$$\text{Gal}(V/S) \geq \text{Gal}(V/S_1) \geq \cdots \geq \text{Gal}(V/S_m) = \{\text{id}\}$$

Vídejme S_i jenž je rostl. nedf. nad $S \Rightarrow$ jde pouze + 24.5(3)
a máme $\text{Gal}(V/S_i) \leq \text{Gal}(V/S)$ a

$$\text{Gal}(V/S_i) / \text{Gal}(V/S_{i+1}) \cong \text{Gal}(S_{i+1}/S_i)$$

Dísl. 19.5 $\Rightarrow \text{Gal}(V/S)$ je řešit. řešitelné podle 24.7. \square

Dr. polohu Galoisov r. 25.1 f řešitelný $\Rightarrow \text{Gal}(f/T)$ je řešit.

$$\text{Náme } T = T_0 \leq T_1 \leq \cdots \leq T_\ell \quad +.2.$$

$$T_i = \text{rostl. nedf. } x^{n_i} - a_i \in T_{i-1}[x]$$

$$\text{a } W \leq T_\ell, \text{ kde } W = \text{rostl. nedf. } f \text{ nad } T.$$

Chci: $\text{Gal}(f/T) = \text{Gal}(W/T)$ je řešitelné!

• Vypočíme $T = U_0 = V_0 \leq U_1 \leq V_1 \leq \cdots \leq U_\ell \leq V_\ell \quad +.2.$

$$\cdot U_i = \text{rostl. nedf. } x^{n_i} - a_i \text{ nad telosem } V_{i-1} \quad a$$

• $V_i = \text{telos } V$ z lemmatu 25.5 aplikovaného na $T \leq V_{i-1} \leq U_i$.

• $V_i = \text{rostl. nedf. } \bar{u} \text{ jehož pol. nad } T \text{ & } \text{Gal}(V_i/V_{i-1}) \text{ je řešit.}$

1) $\text{Gal}(V_\ell/T)$ je řešit. dílčí postup.

$$T = V_0 \leq V_1 \leq \cdots \leq V_\ell$$

$$\text{Gal}(V_\ell/T) \geq \text{Gal}(V_\ell/V_1) \geq \cdots \geq \text{Gal}(V_\ell/V_\ell)$$

podobně jako v dr. 25.5.

2) $\text{Gal}(W/T)$ je řešit. náme $T \leq W \leq V_\ell$

$$24.5(3) : \text{Gal}(W/T) \cong \text{Gal}(V_\ell/T) / \text{Gal}(V_\ell/W)$$

19.8: faktor $\text{Gal}(W/T)$ je řešitelné gropy $\text{Gal}(V_\ell/T)$ je řešit.