Algebra 2 (NMAG 202)

poznámky k streamu

Jan Šťovíček

18. 5. 2020

Katedra algebry MFF UK

Cardanovy vzorce – obecné triky

- Řekněme, že se snažíme vyřešit v tělese charakteristiky 0 rovnici

$$a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_0 = 0,$$

kde $a_n \neq 0$.

- Pak můžeme vydělit rovnici a_n, tj. BÚNO řešíme

$$x^n + b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \cdots + b_0 = 0.$$

- Dále můžeme provést substituci $y = x + \frac{b_{n-1}}{n}$, tj. BÚNO řešíme

$$y^n + c_{n-2} y^{n-2} + \cdots + c_0 = 0.$$

Řešení kubické rovnice (Tartaglia)

- Řešíme $x^3 + px + q = 0$.
- Všimněme si, že pro libovolné u, v platí

$$(u+v)^3 - 3uv(u+v) - (u^3+v^3) = 0.$$

- Trik: Řešení budeme hledat ve tvaru $x = u + v$. Stačí, aby

$$-3uv = p \qquad \text{a} \qquad -u^3 - v^3 = q.$$

- Konkrétně u^3, v^3 najdeme jako řešení rovnice

$$y^2 + qy - \left(\frac{p}{3}\right)^3 = (y-u^3)(y-v^3) = 0.$$

- Tj. pro $D = (\frac{q}{2})^2 + (\frac{p}{3})^3$ $\left(= \frac{(x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2}{-2^2\cdot 3^3} \right)$ máme

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{D}} \qquad \text{a} \qquad v = -\sqrt[3]{\frac{q}{2} + \sqrt{D}}.$$

- Kořeny $x^3 + px + q$ pak budou

$$x_1 = u + v, \quad x_2 = \zeta_3 u + \zeta_3^2 v, \quad x_3 = \zeta_3^2 u + \zeta_3 v.$$

Řešení kubické rovnice z pohledu Galoisovy teorie

- Řešíme-li $x^3 + px + q = 0$, vezmeme $D = (\frac{q}{2})^2 + (\frac{p}{3})^3$,

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{D}} \qquad \text{a} \qquad v = -\sqrt[3]{\frac{q}{2} + \sqrt{D}}.$$

  a $x_1 = u + v, x_2 = \zeta_3 u + \zeta_3^2 v, x_3 = \zeta_3^2 u + \zeta_3 v$.

- Jsou-li $p, q \in T$, $\mathbb{Q} \leq T \leq \mathbb{C}$, máme rozšíření těles

$$\underbrace{T}_{T_0} \leq \underbrace{T(\sqrt{D})}_{T_1} \leq \underbrace{T(\sqrt{D}, \zeta_3)}_{T_2} \leq \underbrace{T(\sqrt{D}, \zeta_3, u)}_{T_3} \leq \underbrace{T(\sqrt{D}, \zeta_3, u, v)}_{T_4}$$

- Mimo T_3 jde o rozkladová nadtělesa polynomů a T_4 obsahuje x_1, x_2, x_3, tedy i rozkladové nadtěleso S polynomu $x^3 + px + q$.
- V $\mathbf{Gal}(T_4/T)$ máme podgrupy, kromě $\mathbf{Gal}(T_4/T_3)$ normální:

$$\mathbf{Gal}(T_4/T) \geq \mathbf{Gal}(T_4/T_1) \geq \mathbf{Gal}(T_4/T_2) \geq \mathbf{Gal}(T_4/T_3) \geq \{1_{T_4}\}.$$

- Faktorgrupy jsou isomorfní $\mathbf{Gal}(T_i/T_{i-1})$, tedy abelovské. Tj. $\mathbf{Gal}(T_4/T)$ je řešitelná a faktorgrupa $\mathbf{Gal}(S/T)$ také.

Radikálová rozšíření a vyjádřitelnost v radikálech

Definice

1. Rozšíření těles $T \leq S$ je radikálové, pokud existuje rozšíření $S \leq U$ a posloupnost podtěles U,

$$T = T_0 \leq T_1 \leq T_2 \leq \cdots \leq T_k = U$$

   taková, že každé T_i je kořenové nadtěleso polynomu $x^{n_i} - a_i \in T_{i-1}[x]$.

2. Je-li $\mathbb{Q} \leq T \leq \mathbb{C}$, pak prvek $a \in \mathbb{C}$ je vyjádřitelný v radikálech nad T, pokud existuje radikálové rozšíření $\mathbb{Q} \leq T \leq U \leq \mathbb{C}$ takové, že $a \in U$.

3. Je-li $\mathbb{Q} \leq T \leq \mathbb{C}$ a $f \in T[x]$ polynom stupně ≥ 1, pak f je řešitelný v radikálech nad T, pokud každý jeho kořen v $\mathbb{C}$ je vyjádřitelný v radikálech nad T.

Galoisova a Abelova-Ruffiniho věta

Věta (Galoisova)
Buď $\mathbb{Q} \leq T \leq \mathbb{C}$ těleso a $f \in T[x]$ polynom stupně ≥ 1. Pak f je řešitělný v radikálech nad T, právě když $\mathbf{Gal}(f/T)$ je řešitelná grupa.

Důsledek (Abelova-Ruffiniho věta)
Neexistuje vzoreček, který by s pomocí odmocnin a tělesových operací vyjádřil kořeny polynomu stupně ≥ 5 z jeho koeficientů.

Důkaz důsledku pro stupeň 5: Dokonce pro konkrétní polynom $x^5 - 4x + 2 \in \mathbb{Q}[x]$ nelze vyjádřit komplexní kořeny v radikálech z racionálních koeficientů!

Myšlenka důkazu jedné implikace Galoisovy věty

- Buď $f \in T[x]$ řešitelný v radikálech a S jeho rozkladové nadtěleso. Tj. S je radikálové rozšíření a máme:

$$T = T_0 \leq T_1 \leq T_2 \leq \cdots \leq T_k = U, \qquad T \leq S \leq U.$$

- Zvětšíme tělesa T_i na S_i, aby to byla rozkladová nadtělesa polynomů nad T a $\mathbf{Gal}(S_i/S_{i-1})$ byly řešitelné grupy:

$$T = S_0 \leq S_1 \leq S_2 \leq \cdots \leq S_k =: V. \qquad \text{▸ přesný postup}$$

- Pak $\mathbf{Gal}(V/T)$ je také řešitelná, protože máme posloupnost s řešitelnými faktory (vizte důsledek 6.7 z textu o grupách a tvrzení 2.5(3) z textu o Galoisově teorii):

$$\mathbf{Gal}(V/T) \geq \mathbf{Gal}(V/S_1) \geq \cdots \geq \mathbf{Gal}(V/S_k) = \{1_V\}.$$

- Rozkladové nadtěleso S polynomu f je obsaženo v V, proto $\mathbf{Gal}(S/T)$ je faktorgrupa $\mathbf{Gal}(V/T)$, tedy řešitelná.

Důležitá vlastnost rozkladových nadtěles

Lemma 3.3
Buď S rozkladové nadtěleso polynomu $T[x]$ a $g \in T[x]$ nějaký ireducibilní polynom. Má-li g v S kořen, pak už se v S rozkládá na kořenové činitele.

Důkaz:

- Řekněme, že S je rozkladové nadtěleso polynomu $f \in T[x]$ a $a \in S$ kořen g.
- Buď $U \geq S$ rozkladové nadtěleso polynomu $fg \in T[x]$ a $b \in U$ libovolný kořen g. Chceme ukázat, že $b \in S$.
- Máme T-isomorfismus $\varphi_0 \colon T(a) \to T(b)$, který posílá a na b (lemma 2.2). Ten se rozšíří na T-isomorfismus $\varphi \colon U \to U$ (lemma 2.3), tedy prvek $\mathbf{Gal}(U/T)$.
- Jelikož φ permutuje kořeny f (lemma 2.4), máme $\varphi(S) \subseteq S$.
- Speciálně $b = \varphi(a) \in S$.

Úprava radikálových rozšíření, induktivní krok

Lemma 3.4
Buď $\mathbb{Q} \leq T \leq S \leq U \leq \mathbb{C}$ tělesa taková, že

1. S je rozkladové nadtěleso polynomu g nad T a
2. U je kořenové nadtěleso $x^n - a \in S[x]$.

Pak existuje těleso $U \leq V \leq \mathbb{C}$ takové, že V je rozkladové nadtěleso polynomu nad T a $\mathbf{Gal}(V/S)$ je řešitelná.

Důkaz:

- Vezměme minimální polynom $m_{a,T} \in T[x]$. Podle lemmatu 3.3 máme v $S[x]$:

$$m_{a,T}(x) = (x - a_1)(x - a_2) \cdots (x - a_d), \quad \text{kde } a_1 = a.$$

- Položme $f := m_{a,T}(x^n) \in T[x]$; pak máme v $S[x]$:

$$f(x) = (x^n - a_1)(x^n - a_2) \cdots (x^n - a_d).$$

- Za V vezmeme rozkladové nadtěleso polynomu fg nad T.

Úprava radikálových rozšíření, induktivní krok – pokračování

Důkaz lemmatu 3.4 – pokračování:

- Máme $T \leq S \leq V$, kde V je rozkladové nadtěleso polynomu f nad S (a fg nad T), kde v $S[x]$ máme rozklad

$$f(x) = (x^n - a_1)(x^n - a_2)\cdots(x^n - a_d).$$

- Zbývá řešitelnost $\mathbf{Gal}(V/S)$. K tomu uvažme rozkladová nadtělesa V_k polynomů

$$f_k(x) = (x^n - a_1)(x^n - a_2)\cdots(x^n - a_k) \in S[x], \quad (1 \leq k \leq d).$$

- Máme tedy řetězec těles $S \leq V_1 \leq V_2 \leq \cdots \leq V_d = V$, a tedy normálních podgrup (tvrzení 2.5(3))

$$\mathbf{Gal}(V/S) \geq \mathbf{Gal}(V/V_1) \geq \mathbf{Gal}(V/V_2) \geq \cdots \geq \{1_V\}.$$

- Faktory $\mathbf{Gal}(V/V_{i-1})$ / $\mathbf{Gal}(V/V_i) \cong \mathbf{Gal}(V_i/V_{i-1})$ jsou metabelovské (tvrzení 2.6(3)), tedy $\mathbf{Gal}(V/S)$ je řešitelná (důsledek 6.7 z textu o grupách).

Důkaz jedné implikace Galoisovy věty

- Dokončíme ▸ myšlenku důkazu, že řešitelnost $f \in T[x]$ v radikálech implikuje řešitelnost grupy $\mathbf{Gal}(f/T)$.
- Je-li S rozkladové nadtěleso f, máme rozšíření
$$T = T_0 \leq T_1 \leq T_2 \leq \cdots \leq T_k = U, \qquad T \leq S \leq U,$$
kde každé T_i je kořenové nadtěleso $x^{n_i} - a_i \in T_{i-1}[x]$.
- Indukcí sestrojíme nadtělesa $S_i \geq T_i$, rozkladová nad T, aby
$$T = S_0 \leq S_1 \leq S_2 \leq \cdots \leq S_k = V$$
a $\mathbf{Gal}(S_i/S_{i-1})$ byly řešitelné grupy.
- Položíme $S_0 := T$. Máme-li už S_{i-1}, vezmeme U_i kořenové nadtěleso $x^{n_i} - a_i \in S_{i-1}[x]$ a použijeme lemma 3.4 na trojici $T \leq S_{i-1} \leq U_i$. Těleso V ze závěru lemmatu nazveme S_i.
- Zbytek už byl vysvětlen na slidu s ▸ myšlenkou důkazu

Hlavní věta Galoisovy teorie

Opačná implikace Galoisovy věty je založena na:

Věta (hlavní věta Galoisovy teorie)
Buď T těleso char. 0 a U rozkladové nadtěleso polynomu nad T.

1. $\left|\mathbf{Gal}(U/T)\right| = [U : T]$.
2. Máme bijekci (tzv. Galoisovu korespondenci)

$$\begin{aligned} \big\{\text{mezitělesa } T \leq S \leq U\big\} &\leftrightarrow \big\{\text{podgrupy } \mathbf{Gal}(U/T)\big\}, \\ S &\mapsto \mathbf{Gal}(U/S), \\ \big\{a \in U \mid (\forall \varphi \in H)(\varphi(a) = a)\big\} &\leftarrow\!\shortmid H. \end{aligned}$$

3. V bijekci výše je mezitěleso S rozkladové nadtěleso nějakého polynomu nad T, právě když je $\mathbf{Gal}(U/S)$ normální podgrupa $\mathbf{Gal}(U/T)$.

Věta o primitivním prvku

Věta (o primitivním prvku)
Buď T těleso charakteristiky 0 a $U \geq T$ konečné rozšíření. Pak existuje $a \in U$ (tzv. primitivní prvek) takové, že $U = T(a)$.

Důkaz:

- Víme, že $U = T(a_1, \ldots, a_n)$ pro a_i algebraické nad T.
- Stačí ukázat: Jsou-li a, b algebraické nad T, pak $T(a, b) = T(c)$, kde $c = a + tb$ pro vhodné $t \in \mathbb{Z}$.
- Buď U rozkladové nadtěleso $m_{a,T} \cdot m_{b,T}$ nad T a $a = a_1$, $a_2, \ldots, a_m$ kořeny $m_{a,T}$ a $b = b_1, b_2, \ldots, b_n$ kořeny $m_{b,T}$ v U.
- $\mathrm{char}(T) = 0 \implies \exists t \in \mathbb{Z}$, že $a_i + tb_j$ jsou po 2 různé.
- Položme $f := m_a(c - tx) \in T(c)[x]$. Pak $f(b) = 0$, ale $f(b_i) \neq 0$ pro $i > 1$. Tj. $\mathrm{NSD}(f, m_{b,T}) = x - b$ v $T(c)[x]$.
- Speciálně $b, a = c - tb \in T(c)$, a tedy $T(a, b) = T(c)$.

Důkaz rovnosti $\left|\mathbf{Gal}(U/T)\right| = [U : T]$

- Buď U rozkladové nadtěleso polynomu nad T.
- Pak $U = T(a)$ pro nějaké $a \in U$ a podle lemmatu 3.3:

$$m_{a,T} = (x - a_1)(x - a_2)\cdots(x - a_d) \quad \text{v } U[x],$$

  kde $a = a_1$ a $d = \deg m_{a,T} = [U : T]$.
- Pro každé $1 \leq i \leq d$ existuje jednoznačné $\varphi_i \in \mathbf{Gal}(U/T)$ takové, že $\varphi(a) = a_i$ (tvrzení 2.5(2)).
- Na druhou stranu pro každé $\varphi \in \mathbf{Gal}(U/T)$ je $\varphi(a)$ kořenem $m_{a,T}$ (lemma 2.4).
- Tedy $\mathbf{Gal}(U/T) = \{\varphi_1, \ldots, \varphi_d\}$ a

$$\left|\mathbf{Gal}(U/T)\right| = d = [U : T].$$