Algebra 2 (NMAG 202)

poznámky k streamu

Jan Šťovíček

11. 5. 2020

Katedra algebry MFF UK

Galoisovy grupy – připomenutí

Definice

1. Buď $S \geq T$ rozšíření těles. Pak Galoisova grupa $(\mathbf{Gal}(S/T), \circ, ^{-1}, 1_S)$ tohoto rozšíření je grupa všech T-automorfismů tělesa S s operací skládání. Tj.

   $$\mathbf{Gal}(S/T) = \left\{ \varphi \colon S \to S \text{ automorfismus} \mid (\forall t \in T)\big(\varphi(t) = t\big) \right\}$$

2. Je-li T těleso a $f \in T[x]$ polynom stupně $d \geq 1$, pak Galoisova grupa polynomu f nad T se definuje jako

   $$\mathbf{Gal}(f/T) := \mathbf{Gal}(S/T),$$

   kde $S \geq T$ je rozkladové nadtěleso f nad T.

Galoisovy permutují kořeny

Lemma 2.4
Buďte $S \geq T$ rozšíření těles a $\varphi \in \mathbf{Gal}(S/T)$. Je-li $0 \neq f \in T[x]$ a $K \subseteq S$ množina všech kořenů f v S, pak $\varphi|_K$ je permutací množiny K.

Důkaz:

- Rozepíšeme $f = \sum_{i=0}^{d} c_i x^i$. Je-li $a \in K$, pak

$$f\big(\varphi(a)\big) = \sum_{i=0}^{d} c_i \varphi(a)^i = \varphi\Big(\sum_{i=0}^{d} c_i a^i\Big) = \varphi(0) = 0.$$

- Tj. φ se zúží na zobrazení $\varphi|_K \colon K \to K$.
- $\varphi|_K \colon K \to K$ je prosté (protože φ je takové). Protože je K konečná množina, je $\varphi|_K \colon K \to K$ bijekce.

Galoisova grupa polynomu je podmnožinou permutační grupy

Tvrzení 2.5, část 1.
Buď T těleso, $f \in T[x]$ polynom stupně aspoň 1 a S rozkladové nadtěleso f nad T. Je-li m počet různých kořenů f v $S \setminus T$, pak se $\mathbf{Gal}(S/T)$ vnořuje do permutační grupy S_m.

Důkaz:

- Buď $K = \{a_1, \ldots, a_m\}$ kořeny f v $S \setminus T$.
- Pro každé $\varphi \in \mathbf{Gal}(S/T)$ je podle posledního lemmatu $\varphi|_K$ permutace K, což nám dává homomorfismus grup

$$\mathbf{Gal}(S/T) \to S_K, \qquad \varphi \mapsto \varphi|_K.$$

- Jelikož navíc $S = T(a_1, \ldots, a_m) = T[a_1, \ldots, a_m]$, je prvek $\varphi \in \mathbf{Gal}(S/T)$ určen hodnotami $\varphi(a_1), \varphi(a_2), \ldots, \varphi(a_m)$.
- Zobrazení, které přiřadí prvku $\varphi \in \mathbf{Gal}(S/T)$ permutaci $K = \{a_1, a_2, \ldots, a_m\}$, je tedy prosté.

Tranzitivita akce na kořenech

Tvrzení 2.5, část 2.
Buď T těleso, $f \in T[x]$ ireducibilní polynom a S rozkladové nadtěleso f nad T. Pak pro každé dva kořeny $a, b \in S$ polynomu S existuje $\varphi \in \mathbf{Gal}(S/T)$ takové, že $\varphi(a) = b$.

Důkaz:

- Máme T-isomorfismus $\varphi_0 \colon T(a) \to T(b)$, který posílá a na b (podívejte se na důkaz věty 2.1 nebo na lemma 2.2 z minula).
- Těleso S je rozkladové nadtěleso polynomu f nad T, tím spíš i polynomu f nad $T(a)$ i $T(b)$.
- $\varphi_0 \colon T(a) \to T(b)$ se tedy rozšíří na T-isomorfismus $\varphi \colon S \to S$ podle lemmatu 2.3 z minula.

Galoisova grupa násobného rozšíření

Tvrzení 2.5, část 3.
Buď $T \leq S \leq U$ rozšíření těles a předpokládejme, že S i U jsou rozkladová nadtělesa nějakých polynomů z $T[x]$.
Pak $\mathbf{Gal}(S/T)$ je isomorfní faktorgrupě $\mathbf{Gal}(U/T)$ podle normální podgrupy $\mathbf{Gal}(U/S)$.

Důkaz:

- Z předpokladu $S = T(a_1, \ldots, a_n)$, kde a_i jsou všechny kořeny nějakého polynomu $f \in T[x]$.
- Je-li $\varphi \in \mathbf{Gal}(U/T)$, pak φ permutuje $a_1, \ldots, a_n$ (lemma 2.4).
- Speciálně $\varphi(S) = S$. Máme tedy následující homomorfismus grup, na který použijeme 1. větu o iso:

$$\Phi \colon \mathbf{Gal}(U/T) \to \mathbf{Gal}(S/T), \qquad \varphi \mapsto \varphi|_S.$$

- Pak $\mathrm{Ker}(\Phi) = \mathbf{Gal}(U/S)$ přímo z definice a Φ je na z lemmatu 2.3.

Galoisova grupa $x^n - 1$

Tvrzení 2.6, část 1.
Buď $\mathbb{Q} \leq T \leq \mathbb{C}$ a $n \geq 1$. Pak $\mathbf{Gal}(x^n - 1/T)$ je abelovská grupa.

Důkaz:

- Ukážeme, že $\mathbf{Gal}(x^n - 1/T)$ je isomorfní podgrupě $\mathbb{Z}_n^*$.
- Označíme-li $\zeta_n = e^{\frac{2\pi i}{n}}$, pak rozkladové těleso $x^n - 1$ nad T je $S = T(\zeta_n)$.
- Je-li $\varphi \in \mathbf{Gal}(S/T)$, pak $\varphi(\zeta_n) = \zeta_n^k$ pro $k \in \mathbb{Z}_n^*$ (jinak by $\varphi(\zeta_n)^m = 1$ pro nějaké $0 < m < n$, a tedy i $\zeta_n^m = 1$, spor!)
- To nám dá prosté zobrazení $\Phi\colon \mathbf{Gal}(S/T) \to \mathbb{Z}_n^*$.
- Jde o grupový homomorfismus: Jsou-li $\varphi, \psi \in \mathbf{Gal}(S/T)$ a $\varphi(\zeta_n) = \zeta_n^k$, $\psi(\zeta_n) = \zeta_n^\ell$, pak

$$\varphi \circ \psi(\zeta_n) = \varphi(\zeta_n^\ell) = \varphi(\zeta_n)^\ell = (\zeta_n^k)^\ell = \zeta_n^{k\ell}.$$

Galoisova grupa $x^n - a$, máme-li odmocniny z 1

Tvrzení 2.6, část 2.
Buď $\mathbb{Q} \leq T \leq \mathbb{C}$ a $n \geq 1$ a $a \in T$. Je-li $e^{\frac{2\pi i}{n}} \in T$, pak
Gal$(x^n - a/T)$ je abelovská grupa.

Důkaz:

- Ukážeme, že **Gal**$(x^n - a/T)$ je isomorfní podgrupě $\mathbb{Z}_n$.
- Označme b nějaký komplexní kořen $x^n - a$ a $\zeta_n = e^{\frac{2\pi i}{n}}$.
- Pak kořeny $x^n - a$ v $\mathbb{C}$ jsou $b \cdot \zeta_n^k$, $0 \leq k \leq n-1$.
  Rozkladové nadtěleso $x^n - a$ nad T je tedy $T(b)$.
- Je-li $\varphi \in$ **Gal**(S/T), pak $\varphi(b) = b \cdot \zeta_n^k$ pro $k \in \mathbb{Z}_n$.
  To nám dá prosté zobrazení $\Phi\colon$ **Gal**$(S/T) \to \mathbb{Z}_n$.
- Jde o grupový homomorfismus: Jsou-li $\varphi, \psi \in$ **Gal**(S/T) a
  $\varphi(b) = b \cdot \zeta_n^k$, $\psi(b) = b \cdot \zeta_n^\ell$, pak

  $$\varphi\circ\psi(\zeta_n) = \varphi(b\cdot\zeta_n^\ell) = \varphi(b)\cdot\varphi(\zeta_n^\ell) = \varphi(b)\cdot\zeta_n^\ell = b\cdot\zeta_n^k\cdot\zeta_n^\ell = b\cdot\zeta_n^{k+\ell}.$$

Galoisova grupa $x^n - a$ obecně

Tvrzení 2.6, část 3.
Buď $\mathbb{Q} \leq T \leq \mathbb{C}$ a $n \geq 1$ a $a \in T$. Pak $\mathbf{Gal}(x^n - a/T)$ je metabelovská grupa.

Důkaz:

- Označme b nějaký komplexní kořen $x^n - a$ a $\zeta_n = e^{\frac{2\pi i}{n}}$.
- Pak rozkladové nadtěleso $x^n - a$ nad T je obecně $U = T(\zeta_n, b)$ a máme rozšíření těles

$$T \leq T(\zeta_n) \leq U.$$

- Položíme-li $S = T(\zeta_n)$, podle předchozích částí jsou $\mathbf{Gal}(S/T)$ i $\mathbf{Gal}(U/S)$ abelovské.
- Důkaz dokončíme pomocí Tvrzení 2.5, části 3:

$$\mathbf{Gal}(S/T) \cong \mathbf{Gal}(U/T) \,/\, \mathbf{Gal}(U/S).$$

Polynom s (neřešitelnou) Galoisovou grupou S_5

Tvrzení 2.7
Buď p prvočíslo a $f \in \mathbb{Q}[x]$ ireducibilní polynom stupně p, který má $p-2$ reálných a 2 komplexní kořeny (např. $f = x^5 - 4x + 2$ pro $p = 5$). Pak $\mathbf{Gal}(f/\mathbb{Q}) \cong S_p$.

Důkaz:

- Buď $a_1, a_2 \in \mathbb{C} \setminus \mathbb{R}$ a $a_3, \ldots, a_p \in \mathbb{R}$ kořeny f a $S = \mathbb{Q}(a_1, \ldots, a_p)$ rozkladové nadtěleso.
- Víme: $\mathbf{Gal}(S/\mathbb{Q})$ se vnoří do grupy permutací na $\{a_1, \ldots, a_p\}$.
- Ukážeme, že obraz obsahuje transpozici a p-cyklus—pak už obsahuje celou S_p (příklad pod tvrz. 2.4 v textu o grupách)!
- Transpozice: Komplexní sdružování se zúží na S.
- Cyklus: Působení $\mathbf{Gal}(S/\mathbb{Q})$ má (jedinou) p-prvkovou orbitu (Tvrzení 2.5, část 2.) Tedy p dělí řád $\mathbf{Gal}(S/\mathbb{Q})$ (Lagrange). Nakonec $\mathbf{Gal}(S/\mathbb{Q})$ musí obsahovat prvek řádu p (Cauchy).