13 Galois a jeho grupy

Řešení
Cvičení 15., 16. nebo 22 května, verze ze dne 7. května 2024.

Cíle cvičení: Jako velký zlatý hřebík našeho algebraického snažení, si zkusíme pro některá rozkladová nadtělesa spočítat jejich Galoisovy grupy. Ačkoli to zpravidla není nijak snadná úloha, síly na to, abychom Galoisovu grupu spočítali aspoň pro rozkladová nadtělesa polynomů malého stupně, máme, neboť víme, že ji můžeme hledat jako podgrupu grupy permutací kořenů daného polynomu.

Úlohy, které bychom určitě měli umět řešit:

V argumentaci cvičení i domácích úkolů můžeme využívat tvrzení 25.2, ačkoli byl jeho důkaz na přednášce jen naznačen.

Úloha 13.1. Je-li U rozkladové nadtěleso polynomu $p = x^3 - 2$ nad tělesem $\mathbb{Q}$, ukažte, že

(a) $U = \mathbb{Q}[\sqrt[3]{2}, e^{\frac{2\pi i}{3}}]$,

(b) $[U : \mathbb{Q}] = 6$,

(c) $\mathrm{Gal}(U/\mathbb{Q}) \cong \mathbf{S}_3$.

Řešení. (a) Snadno uvážíme, že

$$p = x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}e^{\frac{2\pi i}{3}})(x + \sqrt[3]{2}e^{\frac{2\pi i}{3}}),$$

protože navíc $e^{-\frac{2\pi i}{3}} = \overline{e^{-\frac{2\pi i}{3}}} = (e^{\frac{2\pi i}{3}})^{-1}$, vidíme, že

$$U = \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}e^{\frac{2\pi i}{3}}, \sqrt[3]{2}e^{-\frac{2\pi i}{3}}] \subseteq \mathbb{Q}[\sqrt[3]{2}, e^{\frac{2\pi i}{3}}].$$

Dále si všimneme, že $e^{\frac{2\pi i}{3}} = \sqrt[3]{2}e^{\frac{2\pi i}{3}} \cdot (\sqrt[3]{2})^{-1} \in U$, odkud už plyne rovnost $U = \mathbb{Q}[\sqrt[3]{2}, e^{\frac{2\pi i}{3}}]$.

(b) Využijeme-li tvrzení z přednášky a bod (a), víme, že pro každý prvek $\alpha \in U$ platí

$$[U : \mathbb{Q}] = [U : \mathbb{Q}[\alpha]] \cdot [\mathbb{Q}[\alpha] : \mathbb{Q}].$$

Položíme-li $\alpha = \sqrt[3]{2}$, pak

$$[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = \deg m_{\sqrt[3]{2},\mathbb{Q}} = \deg x^3 - 2 = 3$$

a protože minimální polynom prvku $e^{\frac{2\pi i}{3}}$ nad tělesem $\mathbb{Q}[\sqrt[3]{2}]$ dělí polynom $x^3 - 2$ a tudíž i $x^2 + x + 1$, a o lineární polynom se kvůli imaginárním hodnotám nemůže jednat, dostáváme

$$[U : \mathbb{Q}[\sqrt[3]{2}]] = [(Q[\sqrt[3]{2}])[e^{\frac{2\pi i}{3}}] : \mathbb{Q}[\sqrt[3]{2}]] = \deg m_{e^{\frac{2\pi i}{3}}, Q[\sqrt[3]{2}]} = \deg x^2 + x + 1 = 2$$

Tedy $[U : \mathbb{Q}] = [U : \mathbb{Q}[\alpha]] \cdot [\mathbb{Q}[\alpha] : \mathbb{Q}] = 6$.

(c) Protože je polynom $x^3 - 2$ nad tělesem racionálních čísel ireducibilní, plyne z tvrzení 25.2(1) z přednášky, že je grupa $\mathrm{Gal}(U/\mathbb{Q})$ izomorfní podgrupě grupy permutací všech kořenů polynomu $x^3 - 2$ a ta je izomorfní $\mathbb{S}_3$. Snadno nahlédneme (a na přednášce jsme si to rovněž uvědomili), že zobrazení komplexního sdružení $\overline{\mathrm{id}}$ je prvek $\mathrm{Gal}(U/\mathbb{Q})$ řádu 2, což podle Lagrangeovy věty znamená, že 2 dělí řád Galoisovy grupy $\mathrm{Gal}(U/\mathbb{Q})$.

Dále nám za daných předpokladů tvrzení 25.2 z přednášky zaručuje existenci prvku $\varphi \in \mathrm{Gal}(U/\mathbb{Q})$ splňujícího $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}e^{\frac{2\pi i}{3}}$. Protože $\mathrm{id} \neq \varphi \neq \overline{\mathrm{id}}$, vidíme, že $|\mathrm{Gal}(U/\mathbb{Q})| = 6$. Protože je $\mathrm{Gal}(U/\mathbb{Q})$ izomorfní podgrupě $\mathbf{S}_3$, nutně už to znamená, že $\mathrm{Gal}(U/\mathbb{Q}) \cong \mathbf{S}_3$.

Úloha 13.2. Spočítejte Galoisovy grupy $\mathrm{Gal}(U/\mathbb{Q})$ je-li U rozkladové nadtěleso polynomu

(a) $x^4 + 4x^2 + 2$,

(b) $x^4 - 2$.

Řešení. (a) Nejprve snadno najdeme komplexní kořeny $-2 \pm \sqrt{2}$ polynomu $y^2 + 4y + 2$, proto jsou $\pm i\sqrt{2 \pm \sqrt{2}}$ všechny kořeny polynomu $x^4 + 4x^2 + 2$. Dále si všimněme, $\sqrt{2} \in \mathbb{Q}[i\sqrt{2+\sqrt{2}}]$, proto i

$$i\sqrt{2-\sqrt{2}} = \frac{\sqrt{2}}{i\sqrt{2+\sqrt{2}}} \frac{\sqrt{2-\sqrt{2}}}{\sqrt{2-\sqrt{2}}} \in \mathbb{Q}[i\sqrt{2+\sqrt{2}}].$$

To znamená, že $U = \mathbb{Q}[i\sqrt{2+\sqrt{2}}]$ a každý $\mathbb{Q}$-automorfismus tělesa U je tak určen obrazem prvku $i\sqrt{2+\sqrt{2}}$ na kterýkoli kořen $\pm i\sqrt{2 \pm \sqrt{2}}$. Navíc s pomocí Eisensteinova kritéria rychle nahlédneme, že je polynom x^4+4x^2+2 ireducibilní nad tělesem racionálních čísel, což znamená, že $|\operatorname{Gal}(U/\mathbb{Q})| = 4$. Protože podle tvrzení 25.2(1) je Galoisova grupa $\mathrm{Gal}(U/\mathbb{Q})$ iomorfní čtyřprvkové podgrupě grupy $\mathbf{S}_4$, tedy se jedná buď o cyklickou grupu, která je izomorfní $\mathbb{Z}_4$ nebo o grupu izomorfní Kleinově podgrupě $\mathbf{K} = \{\mathrm{id}, (12)(34), (13,(24), (14)(23)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Zbývá tedy rozhodnout, zda $\mathrm{Gal}(U/\mathbb{Q}) \cong \mathbb{Z}_4$ nebo $\mathrm{Gal}(U/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Protože je $\overline{\mathrm{id}}$ opět prvek $\mathrm{Gal}(U/\mathbb{Q})$, stačí si všimnout, že existuje homomorfismus $\varphi \in \mathrm{Gal}(U/\mathbb{Q})$ určený podmínkou $\varphi(i\sqrt{2+\sqrt{2}}) = i\sqrt{2-\sqrt{2}}$ zřejmě splňuje $\varphi(-i\sqrt{2+\sqrt{2}}) = -i\sqrt{2-\sqrt{2}}$, proto jsou automorfismy $\overline{\mathrm{id}}$ a φ různé prvky Galoisovy grupy řádu 2. Takovou vlastnost ovšem určitě žádná cyklická grupa nesplňuje, tudíž $\mathrm{Gal}(U/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(b) Obdobně jako v úloze 13.1 nejprve zjistíme, že $U = \mathbb{Q}[\sqrt[4]{2}, i]$. Protože $\mathbb{Q}[i]$ je rozkladové nadtěleso polynomu x^2+1 na tělesem $\mathbb{Q}$, říká nám lemma 25.5 že $\mathrm{Gal}(U/\mathbb{Q}[i])$ je normální podgrupa $\mathrm{Gal}(U/\mathbb{Q})$ a navíc platí, že

$$\mathrm{Gal}(U/\mathbb{Q})/\operatorname{Gal}(U/\mathbb{Q}[i]) \cong \mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q}).$$

Snadno nyní spočítáme, že je polynom $x^4 - 2$ ireducibilní nad tělesem $\mathbb{Q}[i]$, proto platí, že

$$|\operatorname{Gal}(U/\mathbb{Q}[i])| = 4, \quad \text{dokonce} \quad \mathrm{Gal}(U/\mathbb{Q}[i]) \cong \mathbb{Z}_4,$$

neboť pro automorfismus $\varphi \in \mathrm{Gal}(U/\mathbb{Q}[i])$ určený podmínkou $\varphi(\sqrt[4]{2}) = \sqrt[4]{2}i$, a který existuje podle tvrzení 25.2, platí, že

$$\varphi^2(\sqrt[4]{2}) = \varphi(\sqrt[4]{2}i) = \varphi(\sqrt[4]{2})i = -\sqrt[4]{2}, \quad \varphi^3(\sqrt[4]{2}) = \varphi(-\sqrt[4]{2}) = -\varphi(\sqrt[4]{2}) = -\sqrt[4]{2}i,$$

a pro je φ prvek řádu 4. Nyní zbývá nahlédnout, že se jedná o normální podgrupu indexu 2, a proto $\mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q}) \cong \mathbb{Z}_2$ a následně, že je grupa $\mathrm{Gal}(U/\mathbb{Q})$ nutně izomorfní grupě D_8 symetrií čtverce.

A teď něco pro pro potěšení, protože máme Galoise rádi:

Opět připomeňme značení $\zeta_n = e^{2\pi i/n}$.

Úloha 13.3. Pro $p > 2$ prvočíslo, polynom $\Phi_p = \frac{x^p-1}{x-1} = \sum_{j=0}^{p-1} x^j$ a rozkladové nadtěleso U polynomu Φ_p nad tělesem $\mathbb{Q}$ dokažte, že

(a) $U = \mathbb{Q}[\zeta_p]$,

(b) $[U : \mathbb{Q}] = p - 1$,

(c) $\mathrm{Gal}(U/\mathbb{Q}) \cong \mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$,

Řešení. (a) Protože $x - \zeta_p^a$ jsou pro $a \in \mathbb{Z}_p$ právě všechny odmocniny z jedné polynomu $x^p - 1$, dostáváme, že $\frac{x^p-1}{x-1} = \prod_{a\in\mathbb{Z}_p^*}(x - \zeta_p^a)$. Protože všechny mocniny ζ_p^a už leží v tělese $\mathbb{Q}[\zeta_p]$ jedná se nejen o kořenové nadtěleso, nýbrž i rozkladové nadtěleso polynomu Φ_p nad tělesem $\mathbb{Q}$.

(b) Vzpomeneme-li si, že jsme v 5. sérii v úloha 5.11(c) ukázali, že je polynom Φ_p ireducibilní nad $\mathbb{Q}$ (nebo ireducibilitu znovu dokážeme substitucí $x \to x+1$ a využitím Eisensteinova kritéria), vidíme, že se jedná o minimální polynom prvku ζ_p nad $\mathbb{Q}$, a proto díky (a) a Tvrzení 22.3 dostáváme

$$[U : \mathbb{Q}] = \mathbb{Q}[\zeta_p] = \deg(\Phi_p) = \deg(\sum_{j=0}^{p-1} x^j) = p - 1.$$

(c) Podle tvrzení 25.2(1) a (a) víme, že každý zobrazení kořenu ζ_p na kterýkoli kořen ζ_p^a pro $a \in \mathbb{Z}_p^*$ lze rozšířit na homomorfismus $\rho_a \in \mathrm{Gal}(U/\mathbb{Q})$. Navíc obraz ζ_p už jednoznačně homomorfismus určuje, tedy jsme zkonstruovali bijekci $\mathbb{Z}_p^* \to \mathrm{Gal}(U/\mathbb{Q})$. Zbývá dokázat, že se jedná o grupový homomorfismus. Zvolíme-li $a, b \in \mathbb{Z}_p^*$, pak

$$(\rho_a \circ \rho_b)(\zeta_p) = \rho_a(\rho_b(\zeta_p)) = \rho_a(\zeta_p)^b) = \zeta_p^{ab} = \rho_{ab}(\zeta_p).$$

To znamená, že $\rho_a \circ \rho_b = \rho_{ab}$, a proto je zkonstruovaná bijekce izomorfismus.

Úloha 13.4. Explicitně popište všechny prvky Galoisovy grupy $\mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q})$ z předchozí úlohy. Jak vypadají její prvky řádu 2?

Řešení. Protože umíme pro jednotlivé prvky ρ_a Galoisovy grupy spočítat jejich hodnotu na bázi $(\zeta_p^j \mid j \in \mathbb{Z}_p)$, tedy $f_j(\zeta_p^a) = \zeta_p^{ja}$ a víme, že jde rovněž o lineární zobrazení vektorového prostoru U nad tělesem $\mathbb{Q}$ do sebe, snadno určíme chování f_a na libovolném prvku se souřadnicemi $(t_j)_{j=0}^{p-1}$:

$$f_a(\sum_{j=0}^{p-1} t_j\zeta_p^j) = \sum_{j=0}^{p-1} t_j\zeta_p^{ja}.$$

Prvek řádu dva bude potom díky izomorfismu z předchozí úlohy obrazem jediného prvku řádu dva v grupě $\mathbb{Z}_p^*$, což je $-1 = p - 1$, tedy

$$f_{p-1}(\sum_{j=0}^{p-1} t_j\zeta_p^j) = \sum_{j=0}^{p-1} t_j\zeta_p^{j(p-1)} = \sum_{j=0}^{p-1} t_j\zeta_p^{-j}.$$

Úloha 13.5. Nechť p je prvočíslo, n přirozené číslo a $\mathbb{F}_{p^n}$ konečné těleso řádu p^n, které obsahuje jako podtěleso těleso $\mathbb{F}_p$ řádu p a definujte zobrazení $f_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ předpisem $f_p(a) = a^p$. Dokažte, že

(a) $f_p \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$,

(b) $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle f_p \rangle$ je cyklická grupa řádu n.

(c)* $\{a \in \mathbb{F}_{p^n} \mid f_p^d(a) = a\}$ je podtěleso tělesa $\mathbb{F}_{p^n}$ řádu p^d pro každé $d \mid n$.

Řešení. (a) Nejprve si uvědomíme, že z malé Fermatovy věty plyne, že $f_p(a) = a^p = a$ pro všechny prvky z podtělesa $\mathbb{F}_p \cong \mathbb{Z}_p$. Dále zvolíme $a, b \in \mathbb{F}_{p^n}$ a počítáme:

$$f_p(a \cdot b) = (ab)^p = a^p \cdot b^p = f_p(a) \cdot f_p(b), \quad f(1) = 1^p = 1,$$

$$f_p(a + b) = (a + b)^p = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} = a^p + b^p = f_p(a) + f_p(b),$$

kde jsme využili pozorování, že p dělí $\binom{p}{i}$ pro všechna $i = 1, \ldots, p-1$, a proto jsou všechny členy $\binom{p}{i} a^i b^{p-i}$ v tělese charakteristiky p nulové.

(b) Z přednášky víme, že je multiplikativní grupa $\mathbb{F}_{p^n}^*$ cyklická, tedy v ní najdeme prvek α řádu $p^n - 1$, pro který zřejmě platí, že $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$. Zároveň si snadno uvědomíme, že

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg(m_{\alpha,[\mathbb{F}_p}})$$

pro minimální polynom $m_{\alpha,\mathbb{F}_p}$ prvku α. Tudíž každý automorfismus tělesa $\mathbb{F}_p(\alpha)$ je jednoznačně určen obrazem generátoru α, což musí být rovněž kořen polynomu $m_{\alpha,\mathbb{F}_p}$. Máme tedy nejvýše n prvků Galoisovy grupy $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

Na druhou stranu z předchozí úlohy víme, že $f_p \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ a také f_p^k jsou $\mathbb{F}_p$-automorfismy pro všechna $k \in \mathbb{N}$. Zbývá si uvědomit, že $f_p^n = \mathrm{id}$ a že $f_p^k(\alpha) = \alpha^{p^k}$ jsou různé prvky pro všechna $k = 0, \ldots, n-1$, neboť řád prvku α je $p^n - 1$, což znamená ,že

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \{f_p^k \mid k = 0, \ldots, n-1\} = \langle f_p \rangle$$

je cyklická grupa právě řádu n.

(c) Nejprve uvážíme, že pokud $n = kd$, pak

$$p^n - 1 = (p^d - 1) \sum_{i=0}^{d-1} p^{id},$$

tedy pro $s = \sum_{i=0}^{d-1} p^{ik}$ máme $(p^n - 1) = s(p^d - 1)$, a proto obdobným argumentem dostáváme, že

$$(x^{p^n} - x) = x(x^{p^d - 1} - 1) \sum_{i=0}^{s-1} x^{i(p^d-1)}.$$

Tím jsme dokázali, že polynom $x^{p^d} - x$ dělí polynom $x^{p^n} - x$.

Nyní si všimneme, že za Lagrangeovy věty plyne, že pro každé $u \in \mathbb{F}_{p^n}^*$ platí, že $u^{p^n - 1} = 1$, tudíž jsou všechny prvky tělesa $\mathbb{F}_{p^n}$ kořeny polynomu $x^{p^n} - x$, což nutně znamená, že

$$x^{p^n} - x = \prod_{a \in \mathbb{F}} (x - a).$$

Dále si všimneme, že množina

$$\{a \in \mathbb{F}_{p^n} \mid f_p^d(a) = a\} = \{a \in \mathbb{F}_{p^n} \mid a^{p^d} - a = 0\}$$

obsahuje právě všechny kořeny polynomu $x^{p^d} - x$. Protože tento polynom dělí polynom $x^{p^n} - x$, který se v tělese $\mathbb{F}_{p^n}$ rozkládá na různé kořenové činitele, obsahuje množina právě p^d prvků. Zbývá si všimnout, že je množina opravdu podtělesem, což plyne bezprostředně z (a), kdy jsem dokázali, že je f_p automorfismus.