13 Galois a jeho grupy

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

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

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

(b) $x^4 - 2$.

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

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?

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 $d \mid n$.