Úvod do komutativní algebry: cvičení 5

24. listopadu 2022

Počítání Galoisových grup, Galoisova korespondence

Na tomto cvičení pro nás *určit* Galoisovu grupu znamená najít nějakou „známou“ grupu, které je izomorfní, a rozmyslet si, jak jednotlivé automorfismy působí. Známe grupy jsou třeba $\mathbb{Z}_n$, D_{2n}, S_n nebo součiny známých grup.

Řeš na klidně na přeskáčku – nestrav celé cvičení na jednom typu úlohy! Úlohy s * jsou těžší.

1. Buď U rozkladové nadtěleso polynomu f nad tělesem T. Urči U, $[U : T]$, bázi U jako vektorového prostoru nad tělesem T a $\mathrm{Gal}(U/T)$. Rozhodni, zda jde o Galoisovo rozšíření, a pokud ano, urči také všechna tělesa V, $U \supset V \supset T$, jestliže

a) $f = x^2 - 5$, $T = \mathbb{Q}$,
b) $f = x^3 - 2$, $T = \mathbb{Q}$,
c) $f = x^3 - 2$, $T = \mathbb{Q}(e^{2\pi i/3})$,
d) $f = (x^2 - 3)(x^2 - 5)$, $T = \mathbb{Q}$,
e) $f = x^{12} - 1$, $T = \mathbb{Q}$,
f) $f = x^{20} - 1$, $T = \mathbb{Q}(i)$,
g) $f = x^3 + x^2 - 2x - 1$, $T = \mathbb{Q}$,
h) * $f = x^4 + 5x^2 + 5$, $T = \mathbb{Q}$,
i) * $f = x^5 + x^3 - 2x^2 - 2$, $T = \mathbb{Q}$.

2. Pro rozšíření těles $U \supset T$ urči U, $[U : T]$, bázi U jako vektorového prostoru nad tělesem T a $\mathrm{Gal}(U/T)$. Rozhodni, zda jde o Galoisovo rozšíření, a pokud ano, urči také všechna tělesa V, $U \supset V \supset T$, jestliže

a) $U = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, $T = \mathbb{Q}$,
b) $U = \mathbb{Q}(\sqrt[3]{3})$, $T = \mathbb{Q}$,
c) $U = \mathbb{Q}(\sqrt{2}, e^{2\pi i/3})$, $T = \mathbb{Q}$,
d) * $U = \mathbb{Q}\left(\sqrt{1 + \sqrt{2}}\right)$, $T = \mathbb{Q}$.

3. Buď U rozkladové nadtěleso polynomu f nad tělesem T. Urči U, $[U : T]$, bázi U jako vektorového prostoru nad tělesem T a $\mathrm{Gal}(U/T)$. Rozhodni, zda jde o Galoisovo rozšíření, a pokud ano, urči také všechna tělesa V, $U \supset V \supset T$, jestliže

a) $f = x^3 - 5$, $T = \mathbb{Z}_7$,
b) $f = x^4 - 3$, $T = \mathbb{Z}_5$,
c) * $f = x^{p^2} - x$, $T = \mathbb{Z}_p$.

4. Buď U rozkladové nadtěleso polynomu $x^n - 1$ nad $\mathbb{Q}$.

a) Pokud víš, že $[U : \mathbb{Q}] = \varphi(n)$, nahlédni $\mathrm{Gal}(U/\mathbb{Q}) \simeq \mathbb{Z}_n^\times$.
b) * Je-li $n = p$ prvočíslo, dokaž, že skutečně $[U : \mathbb{Q}] = p - 1$.

5. Mějme tělesa $V \supset U \supset T$ taková, že jak $V \supset T$, tak $U \supset T$ jsou normální rozšíření. Pak $\mathrm{Gal}(V/U) \triangleleft \mathrm{Gal}(V/T)$ a $\mathrm{Gal}(V/T)/\mathrm{Gal}(V/U) \simeq \mathrm{Gal}(U/T)$.

6. Mějme rozšíření $U \supset \mathbb{Q}$ konečného stupně, které ale není normální. Zamysli se, jestli přesto nedovedeme *nějak* pomocí Galoisovy korespondence najít všechna tělesa V, $U \supset V \supset \mathbb{Q}$. Obecněji uvažuj totéž pro rozšíření $U \supset T$, jež je separabilní a konečného stupně, ale není normální.

7. * Doplň a zopakuj si důkaz věty 2.29 ze skript: jsou-li $a_1, \ldots, a_n \in \mathbb{Q}$ taková, že pro všechny neprázdné $I \subset \{1, \ldots, n\}$ platí $\prod_{i \in I} \sqrt{a_i} \notin \mathbb{Q}$, pak je $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n}) \supset \mathbb{Q}$ Galoisovo rozšíření stupně 2^n s Galoisovou grupou izomorfní $\mathbb{Z}_2^n$.

Hinty:

3. a), b) Jaké má $\mathbb{Z}_7/\mathbb{Z}_5$ třetí/čtvrté odmocniny z jedničky? c) Trik: množina kořenů je uzavřená na sčítání i násobení.

4. b) Ber $f = \frac{x^p - 1}{x - 1}$, přesubstituuj na $f(x+1)$ a zamysli se, jaká znáš kritéria ireducibility.

6. Nestačí se na všechno podívat uvnitř většího rozšíření, které je Galoisovo?

7. Stupeň rozšíření dokazuj indukcí s pomocí lemmatu: je-li T těleso s charakteristikou $\neq 2$ a $\sqrt{a}, \sqrt{b}, \sqrt{ab} \notin T$, pak $[T(\sqrt{a}, \sqrt{b}) : T] = 4$. Indukční předpoklad chceš v indukčním kroku použít vícekrát!