Úvod do komutativní algebry: cvičení 4

23. listopadu 2023

1. Buď $U \supset T$ rozšíření konečného stupně. Dokaž, že je Galoisovo, právě když $[U : T] = \#\operatorname{Gal}(U/T)$.

Řešení. Položme sérii nerovností:

$$[U : T] \overset{(1)}{\geq} [U : T]_s = \#\left\{T\text{-homomorfismy } U \to \overline{T}\right\} \overset{(2)}{\geq} \#\left\{T\text{-homomorfismy } U \to U\right\} \overset{2.25}{=}$$
$$\overset{2.25}{=} \#\left\{T\text{-automorfismy } U \to U\right\} = \#\operatorname{Gal}(U/T).$$

Jednu z pozdějších rovností obstarává Lemma 2.25 ze skript (můžeme použít, protože konečný stupeň implikuje algebraičnost). V (1) nastává rovnost, právě když je $U \supset T$ separabilní, zatímco v (2) nastává rovnost, právě když je $U \supset T$ normální. Vzhledem k tomu, že už máme dán konečný stupeň rozšíření, Galoisovskost nastane právě tehdy, když je rozšíření i separabilní a normální, tedy právě když nastanou rovnosti v (1) a (2), tedy právě když $[U : T] = \#\operatorname{Gal}(U/T)$.

2. (zachovávání a skládání význačných vlastností) Buďte $V \supset U \supset T$ rozšíření těles. Víš-li, že rozšíření $V \supset T$ má vlastnost X, rozhodni, zda nutně musí i $V \supset U$ či $U \supset T$ mít vlastnost X. Víš-li, že obě $V \supset U$, $U \supset T$ mají vlastnost X, rozhodni, zda ji nutně musí mít i $V \supset T$.

a) $X =$ konečného stupně,
b) $X =$ algebraické,
c) $X =$ separabilní,
d) $X =$ normální,
e) $X =$ Galoisovo.

Řešení.

a) Obě dílčí rozšíření musí být konečného stupně, naopak pokud obě jsou, pak je i $V \supset T$ konečného stupně.
b) Stejně tak jsou obě dílčí rozšíření algebraická a jejich algebraičnost už implikuje algebraičnost $V \supset T$ (viz minulé cvičení).
c) Obě dílčí rozšíření musí být separabilní: $\alpha \in V$ je kořenem separabilního $f \in T[x]$, což je i $\in U[x]$; zato $\beta \in U$ je separabilní nad T čistě z $\beta \in V$. V opačném směru: pro $[V : T] < \infty$ to snadno plyne pomocí stupňů separability. V obecném případě, je-li $\gamma \in V$, pak je separabilní nad U, tedy kořenem jistého $f = a_n x^n + \cdots + a_1 x + a_0 \in U[x]$, takže separabilní nad $T(a_0, \ldots, a_n)$. Víme, že $T(a_0, \ldots, a_n) \supset T$ i $T(\gamma, a_0, \ldots, a_n) \supset T(a_0, \ldots, a_n)$ jsou separabilní a konečných stupňů, takže už je γ separabilní nad T.
d) $V \supset U$ musí být normální (U-homomorfismus je speciálně i T-homomorfismus), $U \supset T$ ne nutně (např. $\mathbb{Q}(\omega, \sqrt[3]{2}) \supset \mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$). Podobně $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ ukazuje, že $V \supset T$ nemusí být normální, i když $V \supset U$ i $U \supset T$ jsou.
e) Jen poskládáme odpovědi z konečného stupně, separability a normálnosti. $V \supset U$ musí být Galoisovo, $U \supset T$ ne nutně, obrácená implikace taky neplatí (stejné protipříklady jako u normality).

3. Rozhodni o následujících rozšířeních, které z význačných vlastností z úlohy **2.** mají a které ne:

a) $\mathbb{C} \supset \mathbb{R}$, b) $\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$, *c) $\mathbb{Z}_p(x) \supset \mathbb{Z}_p$, *d) $\overline{\mathbb{Q}} \supset \mathbb{Q}$.

Řešení.

a) $[\mathbb{C} : \mathbb{R}] = 2$, tedy je to rozšíření konečného stupně, speciálně tak i algebraické. Separabilitu máme zdarma díky charakteristice 0 a normální je třeba díky tomu, že $\mathbb{C}$ je rozkladové nadtěleso polynomu $x^2 + 1$ nad $\mathbb{R}$. Posléze jde i o Galoisovo rozšíření.
b) Stupeň je $3 < \infty$, tedy jde určitě o algebraické rozšíření. Separabilita je zdarma díky charakteristice, avšak rozšíření není normální – polynom $x^3 - 2$ má v rozšíření jeden kořen, ale zbylé dva ne. Posléze tedy rozšíření nemůže být ani Galoisovo.

c) Jako vektorový prostor nad $\mathbb{Z}_p$ má už $\mathbb{Z}_p[x]$ nekonečnou dimenzi, což se může jedině zvětšit přechodem k podílovému tělesu $\mathbb{Z}_p(x)$. Nejedná se tedy o rozšíření konečného stupně. Dále prvek $x \in \mathbb{Z}_p(x)$ není kořenem žádného nenulového polynomu ze $\mathbb{Z}_p[y]$, takže se nejedná o algebraické rozšíření. V důsledku toho ani nemá smysl mluvit o separabilitě nebo normálnosti, tedy ani o Galoisovskosti.

d) Algebraický uzávěr v sobě obsahuje všechna algebraická rozšíření, a ty umíme určitě konstruovat libovolně velká, musí tedy být $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$. (Lze si ale rozmyslet, že dimenze $\overline{\mathbb{Q}}$ jako vektorového prostoru nad $\mathbb{Q}$ je jen spočetná, protože samo $\overline{\mathbb{Q}}$ má jen spočetně mnoho prvků.) Přímo z definice algebraického uzávěru musí jít o algebraické rozšíření. Potom je zadarmo i separabilní, protože charakteristika 0. Normálnosti bude taky platit triviálně: když rozbalíme definici normálnosti, pak v tomhle případě to znamená, zdali každý $\mathbb{Q}$-homomorfismus (T-homomorfismus) $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ (zde myšleno $U \to \overline{T}$) je ve skutečnosti $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ (zde myšleno $U \to U$), což platí naprosto tautologicky. Rozšíření tedy je normální, ale nebude Galoisovo, protože nemá konečný stupeň.

4. Buď $V \supset T$ Galoisovo rozšíření a $V \supset U \supset T$. Dokaž, že $[U : T] = \frac{\#\operatorname{Gal}(V/T)}{\#\operatorname{Gal}(V/U)}$.

Řešení. Podle **2.**d) je i $V \supset U$ Galoisovo rozšíření, takže z **1.** dostaneme

$$\frac{\#\operatorname{Gal}(V/T)}{\#\operatorname{Gal}(V/U)} = \frac{[V : T]}{[V : U]} = [U : T].$$

5. Buď $f \in T[x]$ polynom s rozkladem na navzájem neasociované ireducibilní polynomy $f = f_1 \cdots f_k$. Uvažujme Galoisovu grupu rozkladového nadtělesa f nad T jako grupu permutací na množině kořenů f. Nahlédni, že každá z těchto permutací musí mít alespoň k cyklů.

Řešení. Jelikož jsou jednotlivá f_i navzájem neasociovaná, jejich množiny kořenů A_i jsou navzájem disjunktní (když totiž $\alpha \in A_i \cap A_j$, už to znamená $m_{\alpha,T} \mid f_i, f_j$). Přitom ale víme, že každý T-automorfismus permutuje kořeny stejného ireducibilního polynomu z $T[x]$ jen mezi sebou. Takže každý prvek Gal bude permutovat každé A_i jen uvnitř A_i. V každé A_i se přitom musí vyskytnout alespoň jeden cyklus (je to neprázdná množina), takže celkem půjde o $\geq k$ permutací.

6. (opakování z přednášky) Buď U těleso, $G < \operatorname{Aut}(U)$ podgrupa a $T \subset U$ podtěleso. Potom platí $\operatorname{Gal}(U/\operatorname{Fix}(U, G)) \supset G$ a $\operatorname{Fix}(U, \operatorname{Gal}(U/T)) \supset T$.

Řešení. Po rozbalení definic zjevné: např. $\operatorname{Fix}(U, \operatorname{Gal}(U/T))$ je množina těch prvků $u \in U$, že $\varphi(u) = u$ pro každé $\varphi \in \operatorname{Gal}(U/T)$. Ale prvky Galoisovy grupy nechávají prvky T na místě, tedy $\varphi(t) = t$ pro každé $t \in T$, což už implikuje $T \subset \operatorname{Fix}(U, \operatorname{Gal}(U/T))$.

7. Budiž $U \supset T$ separabilní rozšíření konečného stupně. Nahlédni, že existuje těleso V takové, že $U \subset V$, $[V : T] \leq ([U : T])!$ a rozšíření $V \supset T$ je Galoisovo.

Řešení. Z přednášky je separibilní rozšíření konečného stupně jednoduché, mějme tedy $U = T(\alpha)$. To je kořenové nadtěleso polynomu $m_{\alpha,T}$ nad T, uvažujme tedy také jeho rozkladové nadtěleso, které označíme V. To je určitě nadtěleso U a je normální. Nechť $n = [U : T] = \deg m_{\alpha,T}$. Víme, že $m_{\alpha,T}$ je separabilní, protože α je separabilní nad T, takže $m_{\alpha,T}$ má n různých kořenů $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$. Všechny tyto prvky jsou separabilní nad T, protože mají tentýž (separabilní) polynom. Tedy $V = T(\alpha_1, \ldots, \alpha_n)$ vzniká přidáním několika separabilních prvků, je to tedy separabilní rozšíření T. Dohromady tak už je i konečného stupně (přidali jsme konečně mnoho algebraických prvků), a tedy Galoisovo.

Konečně odhadněme $[V : T]$. To je totéž, co $\#\operatorname{Gal}(V/T)$, ale tato grupa se vnořuje do grupy permutací na množině $\{\alpha_1, \ldots, \alpha_n\}$, kterážto má řád $n!$. Dokonce tedy můžeme říct

$$[V : T] \mid ([U : T])!.$$

8. Podle lemmatu 2.25, je-li $U \supset T$ algebraické rozšíření, pak už musí každý T-homomorfismus $\varphi : U \to U$ být dokonce T-automorfismus. Rozmysli si, že algebraičnost je nutná – pro $T = \mathbb{Z}_p$, $U = T(x)$ (těleso racionálních funkcí) najdi T-homomorfismus $\varphi : U \to U$, který není T-automorfismus.

Řešení. Generický prvek U je tvaru $\frac{f}{g}$, $f, g \in T[x]$, $g \neq 0$. Zaveďme homomorfismus

$$\begin{aligned} \varphi : U &\to U, \\ \frac{f}{g} &\mapsto \frac{f(x^2)}{g(x^2)}, \end{aligned}$$

tedy „místo x píšeme x^2“. Snadno se nahlédne, že toto nezávisí na konkrétním zapsání zlomku $\frac{f}{g}$ a jedná se o homomorfismus (dosazování zachovává operace). Přitom ale evidentně není surjektivní: $x \in U$ nikdy nezapíšeme jako podíl dvou polynomů obsahujících jen sudé mocniny x: v rovnici $f(x^2) = x \cdot g(x^2)$ má levá strana sudý stupeň, zatímco pravá lichý stupeň.

9. Buď T těleso s $\operatorname{char} T \neq 2$ a $a, b \in T$ prvky s $\sqrt{a}, \sqrt{b}, \sqrt{ab} \notin T$. Pak $[T(\sqrt{a}, \sqrt{b}) : T] = 4$.
* Můžeš zkusit dokázat $\operatorname{Gal}(T(\sqrt{a}, \sqrt{b})/T) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Řešení. Uvažujme $T \subset T(\sqrt{a}) \subset T(\sqrt{a}, \sqrt{b})$. Pokaždé rozšiřujeme o odmocninu něčeho, co leží v předchozím tělese, takže každý ze stupňů dvou dílčích rozšíření je buď 2, nebo 1. Abychom ukázali, že oba jsou 2, stačí nahlédnout $\sqrt{a} \notin T$ a $\sqrt{b} \notin T(\sqrt{a})$. První neležení máme hned ze zadání, pro to druhé pro spor předpokládejme, že $\sqrt{b} = u + v\sqrt{a}$ pro nějaká $u, v \in T$. Úpravami pak máme

$$\begin{aligned} \sqrt{b} - v\sqrt{a} &= u, \\ b - 2v\sqrt{ab} + v^2 a &= u^2, \\ 2v\sqrt{ab} &= u^2 - v^2 a - b. \end{aligned}$$

Rozlišme dva případy: pokud $v = 0$, pak jsme vyjádřením $\sqrt{b} = u$ ve skutečnosti měli $\sqrt{b} \in T$, což je spor. V opačném případě $v \neq 0$ a vzhledem k zadané charakteristice $\neq 2$ máme i $2 \neq 0$, takže získáme

$$\sqrt{ab} = \frac{u^2 - v^2 a - b}{2v} \in T,$$

což je opět spor.

Dohromady tak muselo být $\sqrt{b} \notin T(\sqrt{a})$, což už implikuje $[T(\sqrt{a}, \sqrt{b}) : T(\sqrt{a})] = 2$. Tedy $[T(\sqrt{a}, \sqrt{b}) : T] = 2 \cdot 2 = 4$.

10. Rozšíření $U \supset T$ je normální, právě když existuje množina $\mathcal{M} \subset T[x]$ taková, že U je rozkladové nadtěleso množiny $\mathcal{M}$ nad T.

11. * (existence separabilního uzávěru) Buď $U \supset T$ rozšíření těles. Všechny prvky $\alpha \in U$, jež jsou separabilní nad T, tvoří podtěleso U.

Řešení. Položme $V := \{\alpha \in U \mid \alpha \text{ je separabilní nad } T\}$. Chceme jen ukázat, že tahle množina je uzavřená na tělesové operace. Mějme tedy nějaká $\alpha, \beta \in V$. To jsou separabilní prvky nad T, z přednášky tedy víme, že $T(\alpha, \beta) \supset T$ bude separabilní rozšíření. Přitom ale všechny možné operace (součty, součiny, inverzy, ...), co můžeme s α, β vyrobit, budou ležet v $T(\alpha, \beta)$, takže taky budou separabilní, takže budou opět ležet ve V, což jsme chtěli.

12. * Buď p prvočíslo, $U = \mathbb{Z}_p(x, y)$, $T = \mathbb{Z}_p(x^p, y^p)$. Dokaž, že rozšíření $U \supset T$ není jednoduché.

Řešení. Nechť pro spor $U = T(f/g)$, kde $f, g \in \mathbb{Z}_p[x, y]$, $g \neq 0$. Zapišme

$$f = \sum_{i,j \geq 0} c_{ij} x^i y^j,$$

kde koeficienty c_{ij} jsou ze $\mathbb{Z}_p$. V charakteristice p je umocňování na p homomorfismus, takže

$$f^p = \sum_{i,j\geq 0} c_{ij}^p (x^p)^i (y^p)^j \in \mathbb{Z}_p[x^p, y^p].$$

Obdobně $g^p \in \mathbb{Z}_p[x^p, y^p]$, takže $(f/g)^p \in T$. To značí, že $[U : T] \leq p$.

Ukážeme, že stupeň rozšíření je ve skutečnosti větší. Platí, že x má v $T[z]$ minimální polynom $z^p - x^p$ (notačně to může být trochu matoucí, ale je to jen aplikace Eisenstein a Gaussova lemmatu, kterou jsme už několikrát viděli – protože x^p, ač z hlediska notace vypadá rozložitelně, je v $\mathbb{Z}_p[x^p, y^p]$ prvočinitel). Podobně bude mít y nad $T(x)$ minimální polynom $z^p - y^p$, takže dostaneme

$$[U : T] = [T(x, y) : T] = [T(x, y) : T(x)] \cdot [T(x) : T] = p^2,$$

což je spor s $[U : T] \leq p$.