

Úvod do komutativní algebry: cvičení 3

16. listopadu 2023

1. Bud' α algebraický prvek nad tělesem T . Pak $[T(\alpha) : T] = \deg m_{\alpha, T}$.

Řešení. Bud' $n := \deg m_{\alpha, T}$. Tvrdím, že $1, \alpha, \dots, \alpha^{n-1}$ je báze $T(\alpha)$ jako vektorového prostoru nad T . Že je to generující množina: stačí nagenarovat libovolnou mocninu α^k . Pro $k \leq n-1$ to umíme triviálně. Minimální polynom říká, že $\alpha^n + (\text{nějaká lineární kombinace } 1, \dots, \alpha^{n-1}) = 0$, takže $\alpha^n = \text{nějaká lineární kombinace } 1, \dots, \alpha^{n-1}$, takže každou vyšší mocninu α dovedeme přepsat na lineární kombinaci menších – dostatečným opakováním získáme lineární kombinace $1, \dots, \alpha^{n-1}$. Že je to lineárně nezávislá množina: T -lineární kombinace $1, \dots, \alpha^{n-1}$ je jen hodnota nějakého polynomu stupně $\leq n-1$ v α . Pokud je to netriviální kombinace (ne samé nuly), pak je to nenulový polynom, takže z minimality $m_{\alpha, T}$ nemůže mít α jako kořen.

2. Pro těleso T a polynom $f(x)$ urči všechna možná kořenová nadtělesa pro f nad T , rozkladové nadtěleso pro f nad T , stupně rozšíření všech těchto těles a také jejich Galoisovy grupy nad T :

a) $f(x) = x^2 + 3, T = \mathbb{R}$, b) $f(x) = x^2 - 1, T = \mathbb{Q}$, *c) $f(x) = x^3 - 2, T = \mathbb{Q}$.

Řešení.

- a) Kořeny $x^2 + 3$ jsou $\pm\sqrt{-3}$. Máme $\mathbb{R}(\sqrt{-3}) = \mathbb{R}(-\sqrt{-3}) = \mathbb{C}$, takže $\mathbb{C}$ je kořenové nadtěleso a rovnou i rozkladové nadtěleso. $x^2 + 3$ je kvadratický a nemá v $\mathbb{R}$ kořen, takže je ireducibilní. $\mathbb{C} \supset \mathbb{R}$ pak jako kořenové nadtěleso kvadratického ireducibilního polynomu má stupeň 2. $\text{Gal}(\mathbb{C}/\mathbb{R})$ je dvouprvková: jedním automorfismem je identita, druhým komplexní sdružení $z \mapsto \bar{z}$. Že se jedná o automorfismy: u id je to triviální, u komplexního sdružení víme např. z algebry, že respektuje sčítání i násobení, reálná čísla fixuje a navíc je to bijekce, tedy skutečně je to $\mathbb{R}$ -automorfismus tělesa $\mathbb{C}$. Že další automorfismy neexistují: víme, že v rozšíření stupně 2 se musí Galoisova grupa injektivně vnořovat do S_2 . To je ale dvouprvková grupa, takže víc než dva prvky v $\text{Gal}(\mathbb{C}/\mathbb{R})$ mít nemůžeme.
- b) f má kořeny ± 1 , což jsou oba prvky $\mathbb{Q}$. Kořenovým i rozkladovým nadtělesem je tak pouze $\mathbb{Q}$ samo, stupeň rozšíření je 1 a Galoisova grupa je triviální.
- c) Tato část už je těžší a snáze se bude řešit s pokročilejšími nástroji z přednášky. Tedy bez důkazu: rozkladová nadtělesa jsou tři – $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(e^{\frac{2\pi i}{3}}\sqrt[3]{2})$, $\mathbb{Q}(e^{-\frac{2\pi i}{3}}\sqrt[3]{2})$. Každé je stupně 3 (kořenová rozšíření ireducibilního polynomu stupně 3), ale Galoisovy grupy mají triviální. Rozkladové nadtěleso je $\mathbb{Q}(e^{\frac{2\pi i}{3}}, \sqrt[3]{2})$ a má stupeň šest. Jeho Galoisova grupa je šestiprvková a izomorfní S_3 . Lze ji nagenarovat dvěma prvky, z nichž jeden fixuje $\sqrt[3]{2}$ a komplexně sdružuje $e^{\frac{2\pi i}{3}}$ na $e^{-\frac{2\pi i}{3}}$, zatímco druhý fixuje $e^{\frac{2\pi i}{3}}$ a rotuje $\sqrt[3]{2}$ na $e^{\frac{2\pi i}{3}}\sqrt[3]{2}$.

3. Mějme tělesa $T \subset U \subset V$. Je-li V algebraické nad U a U algebraické nad T , pak je také V algebraické nad T .

Řešení. Nejprve baby verze, když se zároveň jedná o konečná rozšíření (konečné rozšíření je nutně algebraické – viz 5.). Pak prostě můžeme říci, že

$$[V : T] = [V : U] \cdot [U : T]$$

je konečné, tedy $V \supset T$ je algebraické.

Nyní dospělá verze s potenciálně nekonečnými rozšířeními. Berme $\alpha \in V$ a ukažme, že je algebraické nad T . Víme, že je algebraické nad U , takže je kořenem nějakého

$$f = u_n x^n + \dots + u_1 x + u_0 \in U[x].$$

Zjevně je potom tedy α také algebraické nad $T(u_n, \dots, u_1, u_0)$. Pak je $T(\alpha, u_n, \dots, u_0)$ algebraické nad $T(u_n, \dots, u_0)$, což je algebraické nad T (bo je to podtěleso U). Toto jsou už ale určitě konečná rozšíření, takže z baby verze je $T(\alpha, u_n, \dots, u_0)$ algebraické rozšíření T , takže α je algebraické nad T .

4. Bud' $U \supset T$ rozšíření těles a $\alpha \in U$ kořen nějakého separabilního $f \in T[x]$. Potom už je α separabilní nad T .

Řešení. $m_{\alpha,T} \mid f$. Nyní kdyby $m_{\alpha,T}$ měl v $\bar{T}$ násobný kořen, měl by ho dělitelností i f , spor.

5. Rozšíření těles konečného stupně je nutně algebraické.

Řešení. Bud' $[U : T] < \infty$. Pak ale pro každé $a \in U$ máme $T(a) \subset U$, takže

$$[T(a) : T] \leq [U : T] < \infty,$$

což znamená, že a je algebraické nad T .

6. Mějme rozšíření těles $V \supset U \supset T$. Pak $[V : T] = [V : U] \cdot [U : T]$.

Řešení. Bud' $n := [U : T]$, $m := [V : U]$. Dále zvolme $\{u_i\}_{i=1}^n$ bázi U jako vektorového prostoru nad T a $\{v_j\}_{j=1}^m$ bázi V jako vektorového prostoru nad U . Tvrdím, že $\{u_i v_j\}_{\substack{i=1,\dots,n \\ j=1,\dots,m}}$ je báze V jako vektorového prostoru nad T . Že je generující: libovolné $v \in V$ nejdřív vyjádříme jako

$$v = \sum_{j=1}^m \alpha_j \cdot v_j,$$

kde α_j jsou koeficienty náležící U . Každý z nich proto můžeme vyjádřit jako

$$\alpha_j = \sum_{i=1}^n \beta_{i,j} u_i,$$

takže následně máme

$$v = \sum_{i=1}^n \sum_{j=1}^m \beta_{i,j} \cdot u_i v_j.$$

Že je nezávislá: nechť je

$$0 = \sum_{i=1}^n \sum_{j=1}^m \beta_{i,j} \cdot u_i v_j$$

a ukažme, že všechna $\beta_{i,j}$ musí být nulová. V sumě můžeme posbírat $\alpha_j := \sum_{i=1}^n \beta_{i,j} u_i \in U$, pak máme $0 = \sum_{j=1}^m \alpha_j v_j$, což z lineární nezávislosti báze $\{v_j\}$ značí $\alpha_1 = \dots = \alpha_m = 0$. Obdobně pro každé $j = 1, \dots, m$ značí $0 = \sum_{i=1}^n \beta_{i,j} u_i$ díky lineární nezávislosti $\{u_i\}$, že všechna $\beta_{i,j}$ jsou nulová.

7. Bud' $T \subset U$ algebraické rozšíření těles a $U \subset K$ (ne nutně algebraické). Pak K je algebraický uzávěr U , právě když K je algebraický uzávěr T .

Řešení. Být algebraickým uzávěrem tělesa znamená být jeho algebraickým rozšířením a zároveň být algebraicky uzavřený. Algebraická uzavřenost je jen vlastnost tělesa K , která nezávisí na tom, nad kterým menším tělesem se na něj díváme. V důsledku 3. je dále $K \supset T$ algebraické, právě když je $K \supset U$ algebraické.

8. Bud' $\varphi : K \rightarrow R$ homomorfismus okruhů. Připomeň si, že když K je těleso, musí φ být prosté.

Řešení. $\text{Ker } \varphi$ je ideál v K , jenže tělesa mají jen dva ideály (nulový ideál a celé těleso). Přitom z definice okruhového homomorfismu je $\varphi(1_K) = 1_R$, takže $1 \notin \text{Ker } \varphi$, tedy $\text{Ker } \varphi = 0$.

9. Pro těleso T a polynom $f(x)$ urči všechna možná kořenová nadtělesa pro f nad T , rozkladové nadtěleso pro f nad T , stupně rozšíření všech těchto těles a (případně) také jejich Galoisovy grupy nad T :

a) $f(x) = x^2 + 1$, $T = \mathbb{Q}$,

*c) $f(x) = x^2 + 1$, $T = \mathbb{Z}_7$,

b) $f(x) = x^4 - 1$, $T = \mathbb{Q}$,

**d) $f(x) = x^n - 1$, $T = \mathbb{Q}$, $n \in \mathbb{N}$.

Řešení.

- kořenové = rozkladové = $\mathbb{Q}(i)$, $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, $\text{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{\text{id}, (z \mapsto \bar{z})\} \simeq \mathbb{Z}_2$.
- Kořenové může být $\mathbb{Q}(1) = \mathbb{Q}(-1) = \mathbb{Q}$ (stupeň rozšíření 1, Galoisova grupa triviální), nebo $\mathbb{Q}(i) = \mathbb{Q}(-i)$, což už jsme viděli. Rozkladové je $\mathbb{Q}(i)$.
- Kořenové i rozkladové je $\mathbb{Z}_7(i)$. Co to znamená? Prostě k $\mathbb{Z}_7$, kde polynom $x^2 + 1$ neměl kořen, přidáme prvek i , kterému přisoudíme vlastnost $i^2 = -1$. Výsledkem je těleso se $7^2 = 49$ prvky. Stupeň rozšíření je 2, Galoisova grupa dvouprvkové (identita a „komplexní sdružení“ $a + bi \mapsto a - bi$ pro $a, b \in \mathbb{Z}_7$).
- Označme $\zeta_n := e^{\frac{2\pi i}{n}}$. Pak jsou kořenovými nadtělesy všechna $\mathbb{Q}(\zeta_n^j)$. To je vše obsaženo v $\mathbb{Q}(\zeta_n)$, což je tedy rozkladové nadtěleso. (Pro j soudělná s n bude $\mathbb{Q}(\zeta_n^j)$ různé od $\mathbb{Q}(\zeta_n)$, takže pro „hodně složená“ n můžeme dostat spoustu vzájemně neizomorfních kořenových rozšíření.
Určit stupně ve vší obecnosti je těžké: platí (těžká) věta říkající, že minimální polynom ζ_n (tzv. n -tý cyklotomický polynom) má stupeň $\varphi(n)$, z čehož plyne $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. Dokonce potom platí $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

- 10.** Buďte $S \supset T$ tělesa, S algebraicky uzavřené a $U = \{\alpha \in S \mid \alpha \text{ algebraické nad } T\}$. Pak je U algebraický uzávěr T . (tvrzení 2.7 ze skript)

Řešení. Důkaz je ve skriptech...

- 11.** Buďte T, U tělesa charakteristiky 0. Pak $\mathbb{Q} \subset T, U$ a každý homomorfismus $\varphi : T \rightarrow U$ je $\mathbb{Q}$ -homomorfismem. (V charakteristice p má stejnou vlastnost těleso $\mathbb{Z}_p$.)

Řešení. Z definice homomorfismu musí být $\varphi(1) = 1$. Pak dostaneme snadno taky $\varphi(2) = \varphi(1 + 1) = \varphi(1) + \varphi(1) = 1 + 1 = 2$, takto indukcí získáme $\varphi(n) = n$ pro všechna přirozená n . Posléze víme $0 = \varphi(0) = \varphi(n + (-n)) = \varphi(n) + \varphi(-n) = n + \varphi(-n)$, takže nutně $\varphi(-n) = -n$. Tudíž máme $\varphi(n) = n$ pro každé celé číslo n . Pak pro $\frac{p}{q} \in \mathbb{Q}$ podobně získáme

$$p = \varphi(p) = \varphi\left(q \cdot \frac{p}{q}\right) = \varphi(q) \cdot \varphi\left(\frac{p}{q}\right) = q \cdot \varphi\left(\frac{p}{q}\right),$$

takže $\varphi\left(\frac{p}{q}\right) = \frac{p}{q}$. Tedy skutečně φ fixuje všechna racionální čísla.

- 12.** Prvek α je algebraický nad tělesem T , právě když $T(\alpha) = T[\alpha]$.

Řešení. Buď $\beta \in T[\alpha]$ nenulové. Pak má minimální polynom $m_{\beta,T}$ nenulový absolutní člen (jinak by $x \mid m_{\beta,T}$), takže

$$m_{\beta,T}(x) = \sum_{i=0}^n b_i x^i,$$

kde $b_0 \neq 0$. Potom ale můžeme upravit $\frac{1}{\beta} = -\sum_{i=1}^n b_i \beta^{i-1}$. Podobně naopak z vyjádření inverzu získáme zpátky minimální polynom.

- 13.** * Žádné konečné těleso není algebraicky uzavřené.

Řešení. Mějme konečné těleso F a necht' $n := |F|$. Jeho multiplikativní grupa je $(n-1)$ -prvková, z Lagrangeovy věty tak $a^{n-1} = 1$ pro $a \in F \setminus \{0\}$. Z toho už domyslíme, že $a^n = a$ pro každé $a \in F$. Takže polynom $x^n - x$ má za kořen každý prvek F , což ale znamená, že polynom $x^n - x + 1$ nemá v F žádné kořeny – F tak nemůže být algebraicky uzavřené.

- 14.** * Buď p prvočíslo, $T = \mathbb{Z}_p(y)$ a $U = T(\sqrt[p]{y})$. Urči $[U : T]$, $[U : T]_s$ a $\text{Gal}(U/T)$.

Řešení. $\sqrt[p]{y}$ je kořenem $x^p - y$, což je ireducibilní použitím Eisensteinova kritéria nad OHI $\mathbb{Z}_p[y]$ (s výpomocí Gaussova lemmatu se získá i ireducibilita nad $\mathbb{Z}_p(y)$), takže už se jedná o minimální polynom. Rovnou tedy máme $[U : T] = p$. Přitom ale $x^p - y = (x - \sqrt[p]{y})^p$ (v charakteristice p je

umocňování na p homomorfismus), takže tento minimální polynom má je jeden unikátní kořen. Jakýkoliv T -homomorfismus $U \rightarrow \overline{T}$ tedy musí $\sqrt[p]{y}$ poslat znovu na $\sqrt[p]{y}$, což značí, že jediným takovým T -homomorfismem je identita. Tedy $[U : T]_s = 1$. Vzhledem k $[U : T]_s \geq \# \text{Gal}(U/T)$ pak musí Galoisova grupa být triviální.

- 15.** * Algebraický uzávěr nekonečného tělesa T má stejnou mohutnost jako T .