Úvod do komutativní algebry: cvičení 3

3. listopadu 2022

1. Buď α algebraický prvek nad tělesem T. Pak $[T(\alpha) : T] = \deg m_{\alpha,T}$.

Řešení. Buď $n := \deg m_{\alpha,T}$. Tvrdím, že $1, \alpha, \ldots, \alpha^{n-1}$ je báze $T(\alpha)$ jako vektorového prostoru nad T. Že je to generující množina: stačí nagenerovat libovolnou mocninu α^k. Pro $k \leq n-1$ to umíme triviálně. Minimální polynom říká, že $\alpha^n + (\text{nějaká lineární kombinace } 1, \ldots, \alpha^{n-1}) = 0$, takže $\alpha^n =$ nějaká lineární kombinace $1, \ldots, \alpha^{n-1}$, takže každou vyšší mocninu α dovedeme přepsat na lineární kombinaci menších – dostatečným opakování získáme lineární kombinace $1, \ldots, \alpha^{n-1}$. Že je to lineárně nezávislá množina: T-lineární kombinace $1, \ldots, \alpha^{n-1}$ 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. $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ je dvouprvková: jedním automorfismem je identita, druhým komplexní sdružení $z \mapsto \overline{z}$. 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 $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ 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 nagenerovat 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. Buď R gaussovský obor a T jeho podílové těleso. Je-li $u \in T$ celistvé nad R, pak $u \in R$.

Řešení. Bystří si mohou všimnout, že tohle je jen jiná formulace úlohy 3. z prvního DÚ. Využít můžeme cvičení **13**: $x - u$ je monický minimální polynom prvku u, má-li to být polynom z $R[x]$, pak $u \in R$, což jsme přesně chtěli.

4. Urči okruh celistvých prvků v tělese a) $\mathbb{Q}(i)$, b) $\mathbb{Q}(\sqrt{2})$, *c) $\mathbb{Q}(\sqrt{-3})$. (Předpokládej, že už víš **13.**)

Řešení. a) $\mathbb{Z}[i]$, b) $\mathbb{Z}[\sqrt{2}]$, c) $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.

Ukažme a), v ostatních rozebíráme analogicky. Uvažujme $a + bi \in \mathbb{Q}(i)$. Pokud $b = 0$, pak už je samotné $a \in \mathbb{Q}$ celistvé, právě když $a \in \mathbb{Z}$, takže jsme hotovi. Nadále předpokládejme $b \neq 0$. Podle **13.** stačí určit prvky, které jejichž monické minimální polynomy mají prvky ze $\mathbb{Z}$. Minimální polynom $a + bi$ nad $\mathbb{Q}$, kde $b \neq 0$, je určitě kvadratický. Je to navíc jediný monický kvadratický polynom, jehož je $a + bi$ kořenem. Zjevně ale vidíme, že $a + bi$ je kořenem $(x-a)^2 + b^2 = x^2 - 2ax + a^2 + b^2$ – stačí tedy určit, kdy má tento polynom celočíselné koeficienty. K $2a \in \mathbb{Z}$ je buďto $a \in \mathbb{Z}$, nebo $a = \frac{\ell}{2}$ pro liché $\ell \in \mathbb{Z}$:

- Nechť $a \in \mathbb{Z}$. Pak ještě potřebujeme $a^2 + b^2 \in \mathbb{Z}$, což znamená $b^2 \in \mathbb{Z}$. Pokud $b = \frac{p}{q}$ je zlomek v základním tvaru, pak to značí, že $q^2 \mid p^2$. Jenže p, q jsou nesoudělná, takže musí být $q \parallel 1$, BÚNO $q = 1$. To už značí, že $b = p \in \mathbb{Z}$.
- Nechť $a = \frac{\ell}{2}$ a budiž $b = \frac{p}{q}$ v základním tvaru. Pak máme

$$\mathbb{Z} \ni = a^2 + b^2 = \frac{\ell^2}{4} + \frac{p^2}{q^2} = \frac{\ell^2 q^2 + 4p^2}{4q^2}.$$

  Tedy speciálně $4 \mid \ell^2 q^2$, takže q musí být sudé. Buď tedy $q = 2r$, podmínka se přepíše na $\mathbb{Z} \ni \frac{\ell^2 r^2 + p^2}{4r^2}$. Z nesoudělnosti p s $q = 2r$ už je nutně p liché, takže $p^2 \equiv 1 \pmod 4$. Jenže $(\ell r)^2$ dává mod 4 zbytek 0 nebo 1, takže určitě nenastane $\ell^2 q^2 + p^2 \equiv 0 \pmod 4$. To je spor, takže případ $a = \frac{\ell}{2}$ nemůže nastat.

5. 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 **12.**). 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

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

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

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

Řešení. Buď $n := [U : T]$, $m := [V : U]$. 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 $\{u_i v_j\}_{\substack{i=1,\ldots,n \\ j=1,\ldots,m}}$ 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 $\alpha_1 = \cdots = \alpha_m = 0$. Obdobně pro každé $j = 1, \ldots, m$ značí $0 = \sum_{i=1}^n \beta_{i,j} u_i$ díky lineární nezávislosti $\{u_i\}$, že všechna $\beta_{i,j}$ jsou nulová.

7. Buď $T \subset U$ 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 uzavřené. Algebraická uzavřenost je jen vlastnost tělesa K, která nezávisí na tom, nad kterým menším tělesem se na něj díváme. V důsledku **5.** je dále $K \supset T$ algebraické, právě když je $K \supset U$ algebraické.

8. 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...

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) $f(x) = x^2 + 1,\ T = \mathbb{Q}$, b) $f(x) = x^4 - 1,\ T = \mathbb{Q}$,
c) $f(x) = x^2 + 1,\ T = \mathbb{Z}_7$, *d) $f(x) = x^n - 1,\ T = \mathbb{Q},\ n \in \mathbb{N}$.

Řešení.

a) kořenové = rozkladové = $\mathbb{Q}(i)$, $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{\mathrm{id}, (z \mapsto \overline{z})\} \simeq \mathbb{Z}_2$.
b) 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 $\mathbb{Q}(i)$.
c) 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 $a, b \in \mathbb{Z}_7$).
d) 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 $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

10. Buďte T, U tělesa charakteristiky 0. Pak $\mathbb{Q} \subset T, U$ a každý homomorfismus $\varphi : T \to U$ 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.

11. 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.

12. Rozšíření těles konečného stupně je nutně algebraické.

Řešení. Buď $[U : T] < \infty$. 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.

13. Buď T podílové těleso gaussovského oboru R a dále buď $S \supset T$ nadtěleso. Dokaž, že je-li $\alpha \in S$ celistvý prvek nad R, pak má *monický* minimální polynom α nad T koeficienty z R.

Řešení. Buď $f \in R[x]$ monický polynom, jehož je α kořenem (takový existuje z definice celistvosti), a buď $m \in T[x]$ monický minimální polynom α. Z minimality víme, že v $T[x]$ platí $m \mid f$, tedy $f = mg$ pro nějaký $g \in T[x]$. Vedoucí koeficient součin je součin vedoucích koeficientů, takže když jsou m i f monické, musí i g být monický. Buď $p \in R$ libovolný prvočinitel, pak díky vedoucímu koeficientu 1 v m i g máme $c_p(m) \leq 0$, $c_p(g) \leq 0$. Naproti tomu je ale $f \in R[x]$, takže $c_p(f) \geq 0$. Dohromady tak

$$0 \leq c_p(f) = c_p(mg) = c_p(m) + c_p(g) \leq 0 + 0.$$

V nerovnosti nastává rovnost, muselo tedy být $c_p(m) = c_p(g) = c_p(f) = 0$. Speciálně ale $c_p(m) \geq 0$ pro všechna p znamená, že $m \in R[x]$, což jsme chtěli.

14. * Žádné konečné těleso není algebraicky uzavřené.

Řešení. Mějme konečně těleso F a nechť $n := |F|$. 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.

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

16. Ať je obor S konečně generovaný okruh nad R. Pak S je konečně generovaný R-modul, právě když S je celistvý nad R (neboli každý prvek $s \in S$ je celistvý nad R).

17. Pro která $m, n \in \mathbb{Z}$ jsou tělesa $\mathbb{Q}(\sqrt{m})$, $\mathbb{Q}(\sqrt{n})$ $\mathbb{Q}$-izomorfní?