Algebra 2 (NMAG 202)

poznámky k streamu

Jan Šťovíček

4. 5. 2020

Katedra algebry MFF UK

Faktorokruhy – připomenutí

- Je-li $(R, +, -, \cdot, 0_R, 1_R)$ komutativní okruh a I ideál, pak můžeme definovat faktorokruh $(R/I, +, -, \cdot, 0_{R/I}, 1_{R/I})$, kde

$$R/I = \{a + I \mid a \in R\}$$

a

$$\begin{aligned} (a + I) + (b + I) &:= (a + b) + I, & 0_{R/I} &:= 0_R + I, \\ -(a + I) &:= (-a) + I, & 1_{R/I} &:= 1_R + I. \\ (a + I) \cdot (b + I) &:= (a \cdot b) + I. \end{aligned}$$

- Příklady: $\mathbb{Z}/(m)$, $T[x]/(f)$.

Maximální ideály a prvoideály

Definice
Buď $(R, +, -, \cdot, 0, 1)$ komutativní okruh a I ideál.

1. I je prvoideál, pokud $I \lneq R$ a $\forall a, b \in R$,
$$a \cdot b \in I \implies a \in I \text{ nebo } b \in I.$$
Např. pro R obor integrity, $p \in R$ prvočinitel a $I = (p) = \{a \in R \mid p \text{ dělí } a\}$ je I prvoideál.
2. I je maximální, pokud $I \lneq R$ a neexistuje ideál J takový, aby $I \lneq J \lneq R$.

Věta (ve skriptech kap. 23.2)
Buď R komutativních okruh a I ideál.

1. I je prvoideál $\iff$ R/I je obor integrity.
2. I je maximální $\iff$ R/I je těleso.

Speciálně je každý maximální ideál prvoideálem.

Důkaz charakterizace prvoideálů a maximálních ideálů

1.
   - R/I je obor integrity, právě když $\forall a, b \in R$:
   $$(a + I)(b + I) = 0 \implies a + I = 0 \text{ nebo } b + I = 0.$$
   - To se ekvivalentně přeloží na:
   $$ab \in I \implies a \in I \text{ nebo } b \in I.$$
2.
   - Nejprve si všimneme, že ideály R/I jsou přesně tvaru
   $$J/I = \{a + I \mid a \in J\},$$
   kde $J \leq R$ je ideál obsahující I.
   - Víme, že R/I je těleso, právě když R/I je aspoň dvouprvkový a jediné dva ideály jsou $\{0\}$ a R/I.
   - To se ale podle výše uvedeného překládá na to, že
   $$I \lneq R \text{ a neexistuje ideál } I \lneq J \lneq R.$$

Příklady prvoideálů a maximálních ideálů

1.
   - Všechny ideály $\mathbb{Z}$ jsou tvaru $n\mathbb{Z}$, $n \in Z$.
   - Maximální ideály jsou přesně $p\mathbb{Z}$, p prvočíslo.
   - Prvoideály jsou přesně $p\mathbb{Z}$, p prvočíslo nebo $p = 0$.
2. Totéž platí pro OIHI a speciálně pro eukleidovské obory:
   - Všechny ideály R jsou tvaru aR, $a \in R$.
   - Víme: $a \mid b \iff aR \geq bR$.
   - Maximální ideály jsou přesně pR, p ireducibilní.
   - Prvoideály jsou přesně pR, p ireducibilní nebo $p = 0$.
3. Pro obecné Gaussovy obory pozor! Např. $R = T[x, y]$
   - Máme $R/(y) \cong T[x]$ (použijeme 1. větu o isomorfismu na $T[x, y] \to T[x]$, $f \mapsto f(x, 0)$).
     Tj. (y) je prvoideál, ale ne maximální.
   - Dále např. $R/(x, y) \cong T$ (použijeme 1. větu o isomorfismu na $T[x, y] \to T$, $f \mapsto f(0, 0)$).
     Tj. (x, y) je maximální, tedy i prvoideál, ale zase ne hlavní.

Kořenová nadtělesa

Definice
Buď T těleso a $f \in T[x]$ polynom stupně aspoň 1. Pak kořenové nadtěleso polynomu f nad T je tělesové rozšíření $S \geq T$ takové, že

1. Polynom f má kořen $a \in S$ takový, že
2. $S = T(a)$.

Příklady

- Pro $f = x^3 - 2 \in \mathbb{Q}[x]$ máme např. $S = \mathbb{Q}(\sqrt[3]{2})$ nebo $S = \mathbb{Q}(\sqrt[3]{2}e^{\frac{2\pi i}{3}})$.
- Pro $f = (x^3 - 2)(x^2 - 2) \in \mathbb{Q}[x]$ máme např. $S = \mathbb{Q}(\sqrt[3]{2})$ nebo $S = \mathbb{Q}(\sqrt[3]{2}e^{\frac{2\pi i}{3}})$ nebo $S = \mathbb{Q}(\sqrt{2})$.

Kořenová nadtělesa – existence

- Buď T těleso a $f = \sum_{i=0}^{d} c_i x^i \in T[x]$ ireducibilní (tedy nekonstantní) polynom.
- Pozorování: $S = T[x]/(f)$ je tělesové rozšíření T, pokud T ztotožníme s obrazem vnoření

$$T \to T[x]/(f) = S,$$
$$t \mapsto t + (f).$$

- Pozorování: S je kořenové nadtěleso f nad T. Totiž $a := x + (f) \in S$ je kořen f, protože

$$f(a) = \sum_{i=0}^{d} c_i \big(x + (f)\big)^i = \big(\sum_{i=0}^{d} c_i x^i\big) + (f) = f + (f) = 0 + (f).$$

Kořenová nadtělesa – jednoznačnost

- Buď T těleso a $f = \sum_{i=0}^{d} c_i x^i \in T[x]$ ireducibilní (tedy nekonstantní) polynom, BÚNO monický.
- Buď $S \geq T$ nějaké kořenové nadtěleso f nad T, tj. máme $a \in S$ takový, že $f(a) = 0$ a

$$S = T(a) = T[a] = \big\{g(a) \mid g \in T[x]\big\}.$$

- Pak máme surjektivní dosazovací homomorfismus

$$\varphi\colon T[x] \to S, \qquad g \mapsto g(a).$$

- Pozorování: f je minimální polynom a nad T, tj.

$$\mathrm{Ker}(\varphi) = \big\{g \in T[x] \mid g(a) = 0\big\} = f \cdot T[x].$$

- Podle 1. věty o isomorfismu máme isomorfismus těles

$$T[x]/(f) \to S, \qquad g + (f) \mapsto g(a).$$

Kořenová nadtělesa – jednoznačnost, pokračování

Definice
Buď $S_1 \geq T$ a $S_2 \geq T$ dvě rozšíření těles. Isomorfismus těles $\varphi\colon S_1 \to S_2$ se nazývá T-isomorfismus, pokud

$$(\forall t \in T)\big(\varphi(t) = t\big).$$

Věta 2.1(1)
Je-li T těleso a $f \in T[x]$ ireducibilní polynom, pak každá dvě kořenová nadtělesa f nad T jsou T-isomorfní.

Důkaz: Máme-li taková nadtělesa $S_1 = T(a_1)$ a $S_2 = T(a_2)$, kde a_1, a_2 jsou kořeny f, pak máme isomorfismy

$$\begin{array}{ccccc} S_1 & \overset{\cong}{\leftarrow} & T[x]/(f) & \overset{\cong}{\rightarrow} & S_2, \\ g(a_1) & \leftarrow\!\shortmid & g + (f) & \mapsto & g(a_2). \end{array}$$

Příklad: Tělesa $\mathbb{Q}(\sqrt[3]{2})$ a $\mathbb{Q}(\sqrt[3]{2} \cdot e^{\frac{2\pi i}{3}})$ jsou $\mathbb{Q}$-isomorfní.

Rozkladová nadtělesa

Definice
Buď T těleso a $f \in T[x]$ polynom stupně $d \geq 1$. Rozkladovým nadtělesem polynomu f nad T rozumíme minimální rozšíření $S \geq T$, kde se f rozkládá na kořenové činitele, tj.

1. $f \mid\mid (x - a_1) \cdots (x - a_d)$ v $S[x]$ a
2. $S = T(a_1, \ldots, a_d)$.

Věta 2.1(2)
Rozkladové těleso f nad T vždy existuje a je jednoznačné až na T-isomorfismus.

Důkaz:
- Existenci už známe.
- Důkaz jednoznačnosti je technický, plyne přímo z lemmatu 2.3 na přespříštím slidu.

Rozšiřování T-isomorfismů o kořen

Lemma 2.2
Mějme rozšíření $T_1 \geq T$ a $T_2 \geq T$ a T-isomorfismus $\varphi\colon T_1 \to T_2$. Uvažujme ireducibilní polynom $f = \sum_{i=0}^{d} c_i x^i \in T_1[x]$ a označme $\varphi(f) = \sum_{i=0}^{d} \varphi(c_i) x^i \in T_2[x]$.

Je-li $T_1(a)$ kořenové nadtěleso f nad T_1 a $T_2(b)$ kořenové nadtěleso $\varphi(f)$ nad T_2, pak se $\varphi\colon T_1 \to T_2$ dá rozšířit na T-isomorfismus $\psi\colon T_1(a) \to T_2(b)$ takový, že $\psi(a) = b$.

Důkaz: Máme

$$\begin{array}{ccccccc} T_1(a) & \overset{\cong}{\leftarrow} & T_1[x]/(f) & \overset{\cong}{\to} & T_2[x]/\big(\varphi(f)\big) & \overset{\cong}{\to} & T_2(b), \\ g(a) & \leftarrow\!\shortmid & g+(f) & \mapsto & \varphi(g)+\big(\varphi(f)\big) & \mapsto & \varphi(g)(b). \end{array}$$

Rozšiřování T-isomorfismů na rozkladová nadtělesa

Lemma 2.3
Mějme rozšíření $T_1 \geq T$ a $T_2 \geq T$ a T-isomorfismus $\varphi\colon T_1 \to T_2$. Uvažujme $f = \sum_{i=0}^{d} c_i x^i \in T_1[x]$ stupně $d \geq 1$.

Je-li S_1 rozkladové nadtěleso f nad T_1 a $S_2(b)$ rozkladové nadtěleso $\varphi(f)$ nad T_2, pak se $\varphi\colon T_1 \to T_2$ dá rozšířit na T-isomorfismus $\psi\colon S_1 \to S_2$.

Důkaz: Povedeme indukcí podle $d \geq 1$.

- Pro $d = 1$ je $S_1 = T_1$, $S_2 = T_2$ a $\psi = \varphi$.
- Pro $d > 1$ buď $g \mid f$ ireduc. dělitel v $T_1[x]$ a $a \in S_1$ kořen f.
- Pak $\varphi(g)$ je ireduc. dělitel $\varphi(f)$ v $T_2[x]$ a má kořen $b \in S_2$.
- Podle lemmatu 2.2 se φ rozšiřuje na T-isomorfismus $\zeta\colon T_1(a) \to T_2(b)$.
- Použijeme indukční předpoklad na ζ a $f/(x-a) \in T_1(a)[x]$.

Galoisovy grupy

Definice

1. Buď $S \geq T$ rozšíření těles. Pak Galoisova grupa $(\mathbf{Gal}(S/T), \circ, ^{-1}, 1_S)$ tohoto rozšíření je grupa všech T-automorfismů tělesa S s operací skládání. Tj.

   $$\mathbf{Gal}(S/T) = \left\{\varphi\colon S \to S \text{ automorfismus} \mid (\forall t \in T)\big(\varphi(t) = t\big)\right\}$$

2. Je-li T těleso a $f \in T[x]$ polynom stupně $d \geq 1$, pak Galoisova grupa polynomu f nad T se definuje jako

   $$\mathbf{Gal}(f/T) := \mathbf{Gal}(S/T),$$

   kde $S \geq T$ je rozkladové nadtěleso f nad T.

Pozorování: Jsou-li $S_1 \geq T$ a $S_2 \geq T$ rozšíření těles a $\psi\colon S_1 \to S_2$ T-isomorfismus, pak

$$\mathbf{Gal}(S_1/T) \xrightarrow{\cong} \mathbf{Gal}(S_2/T), \qquad \varphi \mapsto \psi\varphi\psi^{-1}.$$

Galoisovy permutují kořeny

Lemma 2.4
Buďte $S \geq T$ rozšíření těles a $\varphi \in \mathbf{Gal}(S/T)$. Je-li $0 \neq f \in T[x]$ a $K \subseteq S$ množina všech kořenů f v S, pak $\varphi|_K$ je permutací množiny K.

Důkaz:

- Rozepíšeme $f = \sum_{i=0}^{d} c_i x^i$. Je-li $a \in K$, pak

$$f\big(\varphi(a)\big) = \sum_{i=0}^{d} c_i \varphi(a)^i = \varphi\Big(\sum_{i=0}^{d} c_i a^i\Big) = \varphi(0) = 0.$$

- Tj. φ se zúží na zobrazení $\varphi|_K \colon K \to K$.
- $\varphi|_K \colon K \to K$ je prosté (protože φ je takové). Protože je K konečná množina, je $\varphi|_K \colon K \to K$ bijekce.