Algebra 2 (NMAG 202)

poznámky k streamu

Jan Šťovíček

27. 4. 2020

Katedra algebry MFF UK

Řešitelné grupy – připomenutí

Definice
Grupa G se nazývá řešitelná, pokud existuje řetězec normálních podgrup

$$\{1\} = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_k = G$$

takový, že každá faktorgrupa N_i/N_{i-1}, $1 \leq i \leq k$, je abelovská.

Věta 6.6
Buď G grupa.

1. Je-li G řešitelná a H její pogrupa, pak je H řešitelná.
2. Je-li G řešitelná a N její normální podgrupa, pak je G/N řešitelná.
3. Pokud G obsahuje normální podgrupu N takovou, že jsou N i G/N řešitelné, pak je G řešitelná.

Podgrupa řešitelné grupy je řešitelná

- Buď G řešitelná grupa a

$$\{1\} = N_0 \leq N_1 \leq \cdots \leq N_k = G$$

posloupnost normálních podgrup s abelovskými faktory.

- Je-li $H \leq G$, pak ukážeme, že posloupnost

$$\{1\} = N_0 \cap H \leq N_1 \cap H \leq \cdots \leq N_k \cap H = H$$

svědčí pro řešitelnost H.

- Máme totiž podle 3. věty o iso:

$$\begin{aligned}(N_i \cap H)/(N_{i-1} \cap H) &= (N_i \cap H)/\big((N_i \cap H) \cap N_{i-1}\big) \\ &\cong (N_i \cap H)N_{i-1}/N_{i-1} \\ &\leq N_i/N_{i-1}\end{aligned}$$

- $(N_i \cap H)/(N_{i-1} \cap H)$ je tedy isomorfní podgrupě N_i/N_{i-1}, a proto abelovská.

Faktorgrupa řešitelné grupy je řešitelná

- Buď G řešitelná a $\{1\} = N_0 \leq N_1 \leq \cdots \leq N_k = G$.
- Je-li $K \trianglelefteq G$, pro řešitelnost G/K bude svědčit

$$\{1\} = N_0K/K \leq N_1K/K \leq \cdots \leq N_kK/K = G/K.$$

- Použijeme postupně 2., 3. a 2. větu o iso:

$$\begin{aligned}(N_iK/K)/(N_{i-1}K/K) &\cong N_iK/N_{i-1}K \\ &= N_i(N_{i-1}K)/N_{i-1}K \\ &\cong N_i/(N_i \cap N_{i-1}K) \\ &\cong \big(N_i/N_{i-1}\big) \,/\, \big((N_i \cap N_{i-1}K)/N_{i-1}\big).\end{aligned}$$

- $(N_iK/K)/(N_{i-1}K/K)$ je tedy isomorfní faktorgrupě N_i/N_{i-1}, a proto abelovská.

Rozšíření řešitelných grup je řešitelné

- Buď $N \trianglelefteq G$, a předpokládejme, že N i G/N řešitelné a svědčí proto posloupnosti

$$\{1\} = L_0/N \leq L_1/N \leq L_2/N \leq \cdots \leq L_r/N = G/N,$$

$$\{1\} = K_0 \leq K_1 \leq K_2 \leq \cdots \leq K_s = N$$

- Speciálně tedy $K_i \trianglelefteq N$, $L_j \trianglelefteq G$,

$$N = L_0 \leq L_1 \leq L_2 \leq \cdots \leq L_r = G$$

  a podle 3. věty o iso jsou L_j/L_{j-1} abelovské.
- Můžeme tedy použít spojenou posloupnost

$$\{1\} = K_0 \leq K_1 \cdots \leq K_s = L_0 \leq L_1 \leq \cdots \leq L_r = G?$$

- Obecně NE, protože

$$K_i \trianglelefteq N \trianglelefteq G \implies K_i \trianglelefteq G!$$

Rozšíření řešitelných – pokračování pro zvídavé

- Musíme nahradit $\{1\} = K_0 \leq \cdots \leq K_{s-2} \leq K_{s-1} \leq K_s = N$ lepší posloupností svědčící pro řešitelnost N.
- Použijeme tzv. derivovanou podgrupu

$$N' = \langle aba^{-1}b^{-1} \mid a, b \in N \rangle_N \leq N.$$

- Pak $N' \trianglelefteq G$, protože pro $g \in G$ a $a, b \in N$ platí

$$g(aba^{-1}b^{-1})g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gag^{-1})^{-1} \in N.$$

- Dále $N' \leq K_{s-1}$, protože K_s/K_{s-1} je abelovská.
- Tj. pro řešitelnost N svědčí i posloupnost

$$\{1\} = K_0 \cap N' \leq \cdots \leq K_{s-2} \cap N' \leq N' \leq N$$

a navíc $N' \trianglelefteq G$.

- Dál pokračujeme indukcí podle s.

Faktorokruhy

- Začneme s komutativním okruhem $(R, +, -, \cdot, 0_R, 1_R)$ a relací ekvivalence $\sim$ na R.
- Chtěli bychom definovat okruh $(R/\sim, +, -, \cdot, 0_{R/\sim}, 1_{R/\sim})$, kde

$$\begin{aligned} [a]_\sim + [b]_\sim &:= [a+b]_\sim, & 0_{R/\sim} &:= [0_R]_\sim, \\ -[a]_\sim &:= [-a]_\sim, & 1_{R/\sim} &:= [1_R]_\sim. \\ [a]_\sim \cdot [b]_\sim &:= [a \cdot b]_\sim, \end{aligned}$$

- Aby byly, musí podobně jako u grup platit

$$\begin{aligned} a_1 \sim a_2 \quad \& \quad b_1 \sim b_2 &\implies a_1 + b_1 \sim a_2 + b_2, \\ &\implies a_1 \cdot b_1 \sim a_2 \cdot b_2, \\ a \sim b &\implies -a \sim -b. \end{aligned}$$

- Relace ekvivalence na R, která toto splňuje, se opět říká kongruence. Pak $R/\sim$ s operacemi výše je automaticky okruh.

Kongruence okruhů versus ideály

Buď $(R, +, -, \cdot, 0, 1)$ komutativní okruh a $\sim$ kongruence na R.

Pozorování: $I := [0]_\sim$ je ideál R.

- $0 \in [0]_\sim$,
- $a, b \sim 0 \implies a + b \sim 0 + 0 = 0$ a $-a \sim -0 = 0$.
- $a \sim 0$ & $u \in R \implies a \cdot u \sim 0 \cdot u = 0$.

Pozorování: Bloky $\sim$ jsou přesně tvaru $a + I$, $a \in R$, tj.

$$(R/\sim) = \{a + I \mid a \in R\}.$$

- Máme totiž $a \sim b \Leftrightarrow a - b \in I \Leftrightarrow a + I = b + I$.

Kongruence okruhů versus ideály – pokračování

Tvrzení
Buď $(R, +, -, \cdot, 0, 1)$ komutativní okruh. Pak existuje bijekce mezi

1. kongruencemi na R a
2. ideály $I \leq R$.

Důkaz:

- Je-li $\sim$ kongruence, položíme $I := [0]_\sim$.
- Je-li naopak $I \leq R$ ideál, definujeme relaci ekvivalence

$$a \sim_I b \quad \text{pokud} \quad a - b \in I \quad (\Leftrightarrow a + I = b + I).$$

- To je kongruence, neboť z $a_1 - a_2 \in I$ a $b_1 - b_2 \in I$ plyne

$$(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in I.$$

$$\begin{aligned} a_1 b_1 - a_2 b_2 &= a_1 b_1 - a_1 b_2 + a_1 b_2 - a_2 b_2 \\ &= a_1(b_1 - b_2) + (a_1 - a_2) b_2 \in I. \end{aligned}$$

$$(-a_1) - (-a_2) = -(a_1 - a_2) \in I$$

- Nakonec si všimněme, že $[0]_{\sim_I} = I$.

Příklady

- Je-li $R = \mathbb{Z}$ a $I = (m) = m\mathbb{Z}$, $m \geq 1$, pak

$$\mathbb{Z}_m \cong \mathbb{Z}/(m) = \{0 + (m), 1 + (m), \ldots, m - 1 + (m)\}.$$

- Je-li $R = T[x]$ a $I = (f) = f \cdot T[x]$ pro $f \in T[x]$ stupně $d \geq 1$, pak

$$T[x]/(f) = \{g + (f) \mid \deg g < d\}.$$

- $R/\{0\} \cong R$ a $R/R \cong \{0\}$. Je-li R těleso, pak toto jsou všechny faktorokruhy!

- Naopak, pokud R je aspoň dvouprvkový a jediné ideály jsou $\{0\}$ a R, pak R je těleso. Je-li totiž $0 \neq a \in R$, pak $aR = R \ni 1$. Tj. $ab = 1$ pro nějaké $b \in R$.

Homomorfismy okruhů

Definice
Zobrazení $\varphi\colon R \to S$ okruhů s jednotkou je homomorfismus, pokud $\forall a, b \in R$:

$$\varphi(a+b) = \varphi(a) + \varphi(b), \qquad \varphi(0) = 0,$$
$$\varphi(-a) = -\varphi(a), \qquad \varphi(1) = 1.$$
$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b),$$

Je-li $\varphi\colon R \to S$ homomorfismus, pak definujeme

$$\mathrm{Ker}(\varphi) = \{a \in R \mid \varphi(a) = 0\}, \qquad \text{jádro } \varphi,$$
$$\mathrm{Im}(\varphi) = \{\varphi(a) \mid a \in R\}, \qquad \text{obraz } \varphi.$$

Základní fakta o homomorfismech okruhů

Lemma

1. Zobrazení $\varphi\colon R \to S$ je homomorfismus, právě když $\forall a, b$:

   $$\varphi(a+b) = \varphi(a)+\varphi(b), \quad \varphi(a\cdot b) = \varphi(a)\cdot\varphi(b), \quad \text{a} \quad \varphi(1) = 1.$$

2. Je-li φ homomorfismus, pak $\mathrm{Ker}(\varphi)$ je ideál v R a $\mathrm{Im}(\varphi)$ je podokruh (s jednotkou!) okruhu S.
3. Homomorfismus φ je prostý, právě když $\mathrm{Ker}(\varphi) = \{0\}$.

Důkaz:

- 1. a 3. plynou z toho, že $(R, +, -, 0)$ a $(S, +, -, 0)$ jsou abelovské grupy a okruhový homomorfismus je vždy homomorfismus mezi těmito grupami.
- U 2. je $\mathrm{Ker}(\varphi)$ podgrupa $(R, +, -, 0)$ a pro $a \in \mathrm{Ker}(\varphi)$ a $u \in R$ platí

  $$\varphi(a \cdot u) = \varphi(a) \cdot \varphi(u) = 0 \cdot \varphi(u) = 0 \in S.$$

První věta o isomorfismu pro okruhy

Věta (ve skriptech věta 23.1 a důsl. 23.2)
Buď $\varphi\colon R \to S$ homomorfismus komutativních okruhů.

1. Je-li $I \leq R$ ideál obsažený v $\mathrm{Ker}(\varphi)$, pak je zobrazení
$$R/I \to S$$
$$a + I \mapsto \varphi(a)$$
dobře definovaný homomorfismus komutativních okruhů.
2. $R/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$ jakožto okruhy.

Důkaz:

1. $a + I = b + I \iff a - b \in I \implies$
$\varphi(a - b) = 0 \iff \varphi(a) - \varphi(b) = 0 \iff \varphi(a) = \varphi(b)$.
2. Použijeme předchozí pro $I = \mathrm{Ker}(\varphi)$. Pak máme okruhový homomorfismus $R/\mathrm{Ker}(\varphi) \to \mathrm{Im}(\varphi)$, $a + \mathrm{Ker}(\varphi) \mapsto \varphi(a)$.
Ten je zřejmě na a je prostý, protože
$\varphi(a) = \varphi(b) \iff a - b \in \mathrm{Ker}(\varphi) \iff a + \mathrm{Ker}(\varphi) = b + \mathrm{Ker}(\varphi)$.

Příklad – dosazovací homomorfismus

- Buď $R \leq S$ rozšíření okruhů a $a \in S$.
- Pak máme dosazovací homomorfismus $\varphi_a \colon R[x] \to S$, $\varphi_a(f) = f(a)$.
- Pak máme $\mathrm{Ker}(\varphi_a) = \{f \in R[x] \mid f(a) = 0\}$ a $R[x]/\mathrm{Ker}(\varphi_a) \cong R[a]$.

Příklad

Buď $a_1 = \sqrt[3]{2}$ a $a_2 = \sqrt[3]{2} \cdot e^{\frac{2\pi i}{3}} \in \mathbb{C}$ a uvažuje $\varphi_{a_i} \colon \mathbb{Q}[x] \to \mathbb{C}$. Pak

$$\mathrm{Ker}(\varphi_{a_1}) = (m_{a_1,\mathbb{Q}}) = (x^3 - 2) = (m_{a_1,\mathbb{Q}}) = \mathrm{Ker}(\varphi_{a_2}).$$

Speciálně $\mathbb{Q}[a_1] \cong \mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}[a_2]$!

Tohle je příklad obecného tvrzení – jednoznačnosti kořenového nadtělesa ireducibilního polynomu.