Matematika IV – 4. přednáška
Rozklady grup (faktorgrupy), okruhy a tělesa

Michal Bulant

Masarykova univerzita
Fakulta informatiky

10. 3. 2008

Obsah přednášky

Doporučené zdroje

- Martin Panák, Jan Slovák, **Drsná matematika**, *e*-text.
- R. B. Ash, Abstract algebra, `http://www.math.uiuc.edu/~r-ash/Algebra.html`.
- Jiří Rosický, *Algebra*, PřF MU, 2002.
- dále *Předmětové záložky v IS MU*

Duální pojmy

- Homomorfismus $f \Rightarrow$ normální podgrupa $\ker f$
- Normální podgrupa $H \Rightarrow$ homomorfismus $G \to G/H$

Všechna jádra homomorfismů jsou normální podgrupy. Naopak, jestliže je podgrupa $H \leq G$ normální, pak zobrazení (projekce na faktorgrupu)

$$p : G \to G/H, \quad a \mapsto a \cdot H$$

je surjektivní homomorfismus grup s jádrem H. Skutečně, přímo z definice násobení na G/H je vidět, že to musí být homomorfismus, který je zjevně na. Je tedy vidět, že **normální podgrupy jsou právě všechna jádra homomorfismů**.

Věty o izomorfismu

Věta (první, základní)

Pro libovolný homomorfismus grup $f : G \to K$ *je dobře definován také homomorfismus*

$$\tilde{f} : G/\ker f \to K,\ \tilde{f}(a \cdot H) = f(a),$$

který je injektivní.
Zejména dostáváme $G/\ker f \cong f(G)$.

Předchozí věta je nejčastěji používanou větou z vět o izomorfismech. Používá se zejména pro určení struktury faktorgrupy (resp. často spíše pro potvrzení, tj. důkaz, intuitivně zřejmé struktury).

Příklad

Čemu je izomorfní faktrogrupa regulárních matic řádu n nad $\mathbb{R}$ podle podgrupy matic determinantu 1 (tj., čemu se rovná $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R})$)?

Řešení

Postupujme nejprve intuitivně (především je třeba si uvědomit, že zmíněná faktorgrupa je normální!): dělíme regulární matice řádu n matice do tříd podle toho, jaký dávají (nenulový) determinant. Zdá se tedy, že zmíněnou faktorgrupou by mohla být grupa nenulových reálných čísel $\mathbb{R}^\times$ s operací násobení (díky Cauchyově větě o determinantu součinu matic).
To, že je to skutečně ono, dokážeme pomocí konstrukce surjektivního homomorfismu z $(\mathrm{GL}_n(\mathbb{R}), \circ)$ do $(\mathbb{R}^\times, \cdot)$, jehož jádrem bude právě $\mathrm{SL}_n(\mathbb{R})$.
Nyní už by mělo být vidět, že přirozenou volbou pro takový homomorfismus je $A \mapsto \det(A)$.

Příklad

Nechť $(G, \circ)$ je grupa nekonstantních lineárních zobrazení reálných čísel s operací skládání zobrazení, tj.

$$G = \{f : \mathbb{R} \to \mathbb{R} | f(x) = ax + b, a \in \mathbb{R}^\times, b \in \mathbb{R}\}.$$

Určete, která z podgrup

$$T = \{f : \mathbb{R} \to \mathbb{R} | f(x) = ax, a \in \mathbb{R}^\times\}$$
$$S = \{f : \mathbb{R} \to \mathbb{R} | f(x) = x + b, b \in \mathbb{R}\}$$

je normální a v případě normality určete strukturu příslušné faktorgrupy.

Řešení

Normální je S, hledaný homomorfismus na faktorgrupu $(\mathbb{R}^\times, \cdot)$ pak $f \mapsto a$ (pro $f(x) = ax + b$).

Další věty o izomorfismu

Součinem podgrup $A, B \leq G$ rozumíme podgrupu $AB = \{ab | a \in A, b \in B\}$. Normalizátorem podgrupy B v G rozumíme množinu $N_G(B) = \{g \in G;\ gB = Bg\}$ (tj. množinu těch prvků G, pro něž splývají příslušné levé a pravé třídy rozkladu; B je tedy normální podgrupou G, právě když $N_G(B) = G$).

Věta (druhá, diamantová)

Nechť $A, B \leq G$ jsou podgrupy splňující $A \leq N_G(B)$. Pak $(A \cap B) \lhd A$ a platí

$$AB/B \cong A/(A \cap B).$$

Věta (třetí)

Jsou-li $A, B \lhd G$ normální podgrupy splňující $A \leq B$, pak $B/A \lhd G/A$ a platí

$$(G/A)/(B/A) \cong G/B.$$

Věta (čtvrtá, svazový izomorfismus)

Nechť je $N \lhd G$. Pak existuje bijekce mezi množinou podgrup A obsahujících N a množinou podgrup A/N faktorgrupy G/N. Navíc normálním podgrupám odpovídají normální podgrupy.

Příklad

Určete svaz podgrup D_8 grupy symetrií čtverce a odvodte z něj svaz podgrup $D_8/ < r^2 >$.

Příklad

Zdánlivě paradoxní je příklad homomorfismu $\mathbb{C}^* \to \mathbb{C}^*$ definovaný na nenulových komplexních číslech vztahem $z \mapsto z^k$ s přirozeným k. Zjevně jde o surjektivní homomorfismus a jeho jádro je množina k-tých odmocnin z jedničky, tj. cyklická podgrupa $\mathbb{Z}_k$. První věta o izomorfismu tedy dává pro všechna přirozená k izomorfismus

$$\tilde{f} : \mathbb{C}^*/\mathbb{Z}_k \to \mathbb{C}^*.$$

Tento příklad ukazuje, že u nekonečných grup nejsou počty s mohutnostmi tak přehledné jako u konečných grup

S grupami se potkáváme nejčastěji jako s množinami transformací. U skalárů i vektorů ale vystupovalo hned více obdobných struktur zároveň.

Jako standardní příklady mějme na mysli **skaláry** (tj. celá čísla $\mathbb{Z}$, racionální čísla $\mathbb{Q}$, komplexní čísla $\mathbb{C}$) a **množiny polynomů nad takovými skaláry** R.

Definice

Komutativní grupa $(R, +)$ s neutrálním prvkem $0 \in R$, spolu s další operací $\cdot$ splňující

- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, pro všechny $a, b, c \in R$ *(asociativita)*;
- $a \cdot b = b \cdot a$, pro všechny $a, b \in R$ *(komutativita)*;
- existuje prvek 1 takový, že pro všechny $a \in R$ platí $1 \cdot a = a$ *(existence jedničky)*;
- $a \cdot (b + c) = a \cdot b + a \cdot c$, pro všechny $a, b, c \in R$ *(distributivita)*;

se nazývá **komutativní okruh**. Takový okruh zapisujeme $(R, +, \cdot)$.

Definice

Jestliže v okruhu R platí $c \cdot d = 0$ právě, když je alespoň jeden z prvků c a d nulový, pak okruh R nazýváme **oborem integrity**.

Příklad

- Okruhy $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot)$ jsou obory integrity.
- Okruh Gaussových celých čísel $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ je oborem integrity.
- Okruh $(\mathbb{Z}_4, +, \cdot)$ není obor integrity, narozdíl od $(\mathbb{Z}_5, +, \cdot)$.

Pokud neplatí vlastnost komutativity operace $\cdot$, hovoříme o nekomutativním okruhu. V dalším se ovšem omezíme pouze na okruhy komutativní.
Operaci $+$ budeme říkat **sčítání** a operaci $\cdot$ **násobení**. Navíc budeme vždy předpokládat existenci **jedničky** 1 pro operaci násobení, neutrálnímu prvku pro sčítání říkáme **nula**.

Základní vlastnosti operací v okruhu

V každém komutativním okruhu R s jedničkou platí následující vztahy (které nám jistě připadají samozřejmé u skalárů)

1. $0 \cdot c = c \cdot 0 = 0$ pro všechny $c \in R$,
2. $-c = (-1) \cdot c = c \cdot (-1)$ pro všechny $c \in R$,
3. $-(c \cdot d) = (-c) \cdot d = c \cdot (-d)$ pro všechny $c, d \in R$,
4. $a \cdot (b - c) = a \cdot b - a \cdot c$,

Dělitelnost v okruhu

Obecně říkáme, že $a \in R$ **dělí** $c \in R$, jestliže existuje b tak, že $a \cdot b = c$. Skutečnost že $c \in R$ je dělitelné $a \in R$ zapisujeme $a|c$. Dodatečnou vlastností oboru integrity oproti obecnému okruhu je **neexistence netriviálních dělitelů nuly**. Okamžitě odtud také vyplývá jednoznačnost dělitelů:

Věta

Platí-li v oboru integrity $a = b \cdot c$ a $b \neq 0$, pak c je jednoznačně dáno volbou a, b.

Důkaz.

Pro $a = bc = bc'$ totiž platí $0 = b \cdot (c - c')$ a $b \neq 0$, proto $c = c'$. □

Dělitelé jedničky, tj. invertibilní prvky v R, se nazývají **jednotky**.
Jednotky v komutativním okruhu vždy tvoří komutativní grupu.
Netriviální (komutativní) okruh, ve kterém jsou všechny nenulové prvky invertibilní, se nazývá (komutativní) **těleso**.
V české literatuře se někdy v případě komutativního tělesa můžete setkat s pojmenováním **pole** (z angl. *field*).

Typickým příkladem komutativních těles jsou číselné obory $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Dále pak všechny okruhy zbytkových tříd $\mathbb{Z}_p$ s prvočíselným p. Základním příkladem nekomutativního okruhu s jedničkou je množina $\mathrm{Mat}_k(R)$ všech čtvercových matic nad okruhem R s k řádky a sloupci. Jak jsme viděli dávno, není to ani obor integrity. Jako příklad nekomutativního tělesa uveďme těleso kvaternionů

$$\mathbb{H} = \{a + b \cdot i + c \cdot j + d \cdot k;\ a, b, c, d \in \mathbb{R}\},$$

se sčítáním *po složkách* a násobením odvozeným ze základních relací

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

Obor integrity vs. těleso

Věta

Každý konečný obor integrity je těleso.

Důkaz.

Dokazuje se prostřednictvím homomorfismus $f : R \to R$, $f(x) = ax$ (je to injekce, proto surjekce, proto je R těleso (rozmyslete!). □

A co obráceně? Samozřejmě je každé těleso oborem integrity.

Příklad

Zřejmě je např. $\mathbb{Z}$ obor integrity, který není těleso.

Polynomy

Polynomem rozumíme jakýkoliv konečný výraz, který lze poskládat ze známých konstantních prvků R a jedné neznámé proměnné pomocí operací sčítání a násobení:

Definice

Nechť R je jakýkoliv (dále vždy) komutativní okruh skalárů.
Polynomem nad R rozumíme konečný výraz

$$f(x) = \sum_{i=0}^{k} a_i x^i$$

kde $a_i \in R$, $i = 0, 1, \ldots, k$, jsou tzv. **koeficienty polynomu**. Je-li $a_k \neq 0$, říkáme, že $f(x)$ má **stupeň** k, píšeme $\operatorname{st} f = k$. Nulový polynom nemá stupeň, polynomy stupně nula jsou právě nenulové prvky v R, kterým říkáme konstantní polynomy.
Polynomy $f(x)$ a $g(x)$ jsou stejné, jestliže mají stejné koeficienty.
Množinu všech polynomů nad okruhem R budeme značit $R[x]$.

Každý polynom zadává zobrazení $f : R \to R$, jehož hodnota vznikne dosazením hodnoty c za nezávislou proměnnou x, tj.

$$f(c) = a_0 + a_1 c + \cdots + a_k c^k.$$

Všimněme si, že konstantní polynomy odpovídají právě konstantním zobrazením.

Kořen polynomu $f(x)$ je takový prvek $c \in R$, pro který je $f(c) = 0 \in R$.

Obecně se může stát, že různé polynomy definují stejná zobrazení. Např. polynom $x^2 + x \in \mathbb{Z}_2[x]$ zadává identicky nulové zobrazení. Obecněji, pro každý konečný okruh $R = \{a_0, a_1, \ldots, a_k\}$ zadává polynom $f(x) = (x - a_0)(x - a_1)\ldots(x - a_k)$ identicky nulové zobrazení. Zároveň ale platí tvrzení, které dokážeme zanedlouho:

Věta

Jestliže je R nekonečný okruh, pak dva polynomy $f(x)$ a $g(x)$ nad R jsou stejné právě tehdy, když jsou stejná příslušná zobrazení f a g.

Dva polynomy $f(x) = \sum_i a_i x^i$ a $g(x) = \sum_i b_i x^i$ umíme přirozeně také sčítat i násobit:

$$(f + g)(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_k + b_k)x^k$$
$$(f \cdot g)(x) = (a_0 b_0) + \cdots + (a_0 b_\ell + + \cdots + a_\ell b_0)x^\ell + \ldots$$

kde uvažujeme nulové koeficienty všude, kde v původním výrazu pro polynomy nenulové koeficienty nejsou a u sčítání nechť je k maximální ze stupňů f a g.

Tato definice vskutku odpovídá příslušným operacím sčítání a násobení hodnot zobrazení $f, g : R \to R$, díky vlastnostem *skalárů* v původním okruhu R.
Přímo z definice vyplývá, že množina polynomů $R[x]$ nad komutativním okruhem s jedničkou je opět komutativním okruhem s jedničkou, přičemž jedničkou v $R[x]$ je opět jednička 1 v okruhu R vnímaná jako polynom stupně nula.

Lemma

Okruh polynomů nad oborem integrity je opět obor integrity.

Důkaz.

Máme ukázat, že v $R[x]$ mohou být netriviální dělitelé nuly pouze, jetliže jsou už v R. To je ale zřejmé z výrazu pro násobení polynomů. Jsou-li $f(x)$ a $g(x)$ polynomy stupně k a ℓ jako výše, pak koeficient u $x^{k+\ell}$ v součinu $f(x) \cdot g(x)$ je součin $a_k \cdot b_\ell$ a ten musí být nenulový, pokud nejsou dělitelé nuly v R. □

Formální mocninné řady

V Matematice III jsme pracovali s formálními mocninnými řadami a neformálně jsme prohlásili, že *s nimi můžeme provádět analogické operace jako s polynomy*. Nyní toto tvrzení můžeme zasadit do formálního algebraického kontextu:

Definice

Nechť R je okruh skalárů. *Formální mocninou řadou* nad R rozumíme (obecně nekonečný) **formální** výraz $f(x) = \sum_{i=0}^{\infty} a_i x^i$, kde $a_i \in R$, $i = 0, 1, \ldots$, jsou tzv. **koeficienty řady**.

Snadno se ukáže, že s dříve definovanými operacemi sčítání a násobení tvoří formální mocniné řady okruh, který značíme $R[[x]]$ (a jehož je $R[x]$ podokruhem). Sami si zkuste rozmyslet, které prvky tohoto okruhu jsou invertibilní.