Diskrétní matematika B – 8. týden
Teorie grup – dokončení a aplikace

Michal Bulant

Masarykova univerzita
Fakulta informatiky

jaro 2014

Obsah přednášky

1. Normální podgrupy a faktorgrupy
   - Hlavní věty o grupách
2. Akce grupy na množině

Doporučené zdroje

- Jan Slovák, Martin Panák, Michal Bulant, *Matematika drsně a svižně*, MU Brno, 2013, 774 s. (též jako e-text).
- *Předmětové záložky v IS MU*
- Jiří Rosický, *Algebra*, PřF MU, 2002.
- Peter J. Cameron. *Introduction to algebra*, Oxford University Press, 2001, 295 s. (Dostupné v knihovně PřF).
- Nathan Carter. *Visual Group Theory*, The Mathematical Association of America, 2009, 297 s. (Viz web).
- Groupprops, The Group Properties Wiki (beta) (Viz `http://groupprops.subwiki.org/wiki/Main_Page`).

Charakterizace konečných komutativních grup

Věta (Hlavní věta konečných komutativních grup)

Je-li G konečná komutativní grupa, pak platí:

$$G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k},$$

pro vhodná $n_1, \ldots, n_k \in \mathbb{N} \setminus \{1\}$ splňující $n_{i+1} \mid n_i$ pro $1 \leq i \leq k-1$. Tento rozklad je přitom jednoznačný.

Důsledek

- *Každé prvočíslo p, dělící řád grupy G, dělí n_1.*
- *Je-li n součinem různých prvočísel, pak jedinou komutativní grupou řádu n je (až na izomorfismus) cyklická grupa $\mathbb{Z}_n$.*

Příklad

Určete všechny komutativní grupy řádu 180.

Řešení

Protože $180 = 2^2 \cdot 3^2 \cdot 5$, dostáváme, že možné hodnoty n_1 jsou

$$n_1 = 2^2 \cdot 3^2 \cdot 5, \quad 2^2 \cdot 3 \cdot 5, \quad 2 \cdot 3^2 \cdot 5 \quad \text{nebo} \quad 2 \cdot 3 \cdot 5.$$

Pro $n_1 = 2 \cdot 3 \cdot 5$ dostáváme možné hodnoty $n_2 = 2, 3$ nebo 6. V prvních dvou případech dostáváme díky podmínce $n_3 \mid n_2$ spor. Jediná komutativní grupa řádu 6 je $\mathbb{Z}_6$, proto v tomto případě dostáváme grupu $Z_{30} \times \mathbb{Z}_6$. Ve zbylých (ještě jednodušších) případech dostáváme další komutativní grupy řádu 180: $\mathbb{Z}_{60} \times \mathbb{Z}_3, \mathbb{Z}_{90} \times \mathbb{Z}_2, \mathbb{Z}_{180}$.

Existence podgrup daného řádu

Připomeňme, že Lagrangeova věta říká, že řád podgrupy vždy dělí řád grupy. Přirozenou opačnou otázkou pak je, jak je to s existencí podgrup řádů dělících řád grupy. V případě cyklické grupy je situace jednoduchá – již z teorie čísel víme, že zde existují podgrupy všech řádů (je-li g generátor grupy řádu n, pak pro $d \mid n$ má prvek $g^{n/d}$ řád d, a proto rovněž generuje podgrupu tohoto řádu). Situace v případě necyklických, či dokonce nekomutativních, grup je podstatně složitější. U komutativních grup lze podgrupy „vyčíst“ z Hlavní věty, obecný případ alespoň částečně popisují následující věty.

Věta (Cauchy)

Je-li konečná grupa G řádu dělitelného prvočíslem p, pak obsahuje prvek řádu p.

Věta (Sylowova)

Konečná grupa G řádu $p^\alpha m$ (p je prvočíslo, $p \nmid m$) má vždy podgrupu řádu p^α. Pro počet n_p takových podgrup platí $n_p \equiv 1 \pmod p$ a $n_p \mid m$.

Důkaz Cauchyovy věty.

Důkaz není úplně triviální, naznačme jej alespoň v případě komutativní grupy G. Budeme postupovat úplnou matematickou indukcí. Je tedy $|G| > 1$. Pokud $|G| = p$, jsme hotovi. Buď nyní $|G| > p$ a $x \in G, x \neq e$ libovolný. Pokud p dělí řád r prvku x, tj. $r = p \cdot n$, pak p je řádem prvku x^n.

Nechť tedy $p \nmid r$ a označme $N = \langle x \rangle$. Zřejmě $N \lhd G$ a $|G/N| < |G|$. Protože $p \nmid |N|$, nutně $p \mid |G/N|$ a můžeme využít indukční předpoklad. V grupě G/N tedy existuje prvek yN řádu p (odkud $y \notin N, y^p \in N$), odkud dostáváme $\langle y^p \rangle \neq \langle y \rangle$, zejména je tedy řád y^p menší než řád y. Ze znalosti vztahu pro řád mocniny (viz teorie čísel) dostáváme, že řád y je násobkem p a jsme v situaci z předchozího odstavce. □

Jordan-Hölderova věta

Jak jsme viděli, v některých případech jsme schopni z informací o normální podgrupě $N \lhd G$ a o faktorgrupě G/N získat informaci o celé grupě G. Jednoduché grupy, které tento proces nepřipouštějí, jsou základními stavebními kameny grup (analogie prvočísel).

Definice

Posloupnost podgrup grupy G

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

se nazývá kompoziční řada (též J.-H. řada), pokud $N_i \lhd N_{i+1}$ a N_{i+1}/N_i je prostá.

Příklad

Pro D_8 máme např. kompoziční řady $\{e\} \lhd \langle s \rangle \lhd \langle s, r^2 \rangle \lhd D_8$ a $\{e\} \lhd \langle r^2 \rangle \lhd \langle r \rangle \lhd D_8$.

Věta (Jordan-Hölderova)

Konečná grupa má vždy kompoziční řadu, která je jednoznačně určená až na izomorfismus faktorů (tj. počet členů dvou takových řad je stejný a příslušné faktorgrupy jsou izomorfní.

Vztah normálních podgrup a homomorfismů

Všechna jádra homomorfismů jsou normální podgrupy. Naopak, jestliže je podgrupa $H \subset G$ 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, p je dobře definované, 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**.

Duální pojmy

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

Věty o izomorfismu

Věta (první, základní)

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

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

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 faktorgrupa 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 podgrupa 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 $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ 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 odvoďte 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.

Již jsme viděli, že často potkáváme grupy jako množiny transformací nějaké pevné množiny. Musí přitom být všechny invertibilní a zároveň musí být naše množina transformací uzavřená na skládání. Často ale také chceme pracovat s pevně zvolenou grupou, jejíž prvky reprezentujeme jako zobrazení na nějaké množině, přitom ale ne nutně jsou zobrazení příslušná různým prvkům grupy různá. Např. všechna otočení roviny kolem počátku o všechny možné úhly odpovídají grupě reálných čísel. Otočení o 2π je ale identické zobrazení.

Akce grupy

Definice

Levá akce grupy G na množině X je homomorfismus grupy G do podgrupy invertibilních prvků v pologrupě X^X všech zobrazení $X \to X$. Takový homomorfismus si také můžeme představit jako zobrazení $\varphi : G \times X \to X$, které splňuje

$$\varphi(a \cdot b, x) = \varphi(a, \varphi(b, x)),$$

odtud název „levá akce“. Často budeme k vyjádření akce prvku grupy na prvku X používat pouze zápis $a \cdot x$ (byť jde o jinou tečku než u násobení uvnitř grup). Definiční vlastnost pak vypadá takto:

$$(a \cdot b) \cdot x = a \cdot (b \cdot x).$$

Definice

Obraz prvku $x \in X$ v akci celé grupy G nazýváme **orbita** X_x prvku x, tj.

$$X_x = \{y = \varphi(a, x);\; a \in G\}.$$

Pro každý bod $x \in X$ definujeme **izotropní podgrupu** (též **stabilizátor**) $G_x \subseteq G$ akce φ:

$$G_x = \{a \in G;\; \varphi(a, x) = x\}.$$

Jestliže pro každé dva prvky x, $y \in X$ existuje $a \in G$ tak, že $\varphi(a, x) = y$, pak říkáme, že akce φ je **tranzitivní**.

Snadno se vidí, že u tranzitivních akcí je celý prostor jedinou orbitou a všechny izotropní podgrupy mají stejnou mohutnost. Typický příklad tranzitivní akce grupy G je přirozená akce na množině levých tříd G/H pro jakoukoliv podgrupu H. Definujeme ji vztahem

$$g \cdot (aH) = (ga)H.$$

Burnsideovo lemma

Věta

Pro každou akci konečné grupy G na konečné množině X platí:

1. *pro každý prvek $x \in X$ je*

$$|G| = |G_x| \cdot |X_x|,$$

2. *(Burnsideovo lemma) je-li N počet orbit akce G na X, pak*

$$|G| = \frac{1}{N} \sum_{g \in G} |X^g|,$$

kde $X^g = \{x \in X;\ g \cdot x = x\}$ označuje množinu pevných bodů akce prvku g.

Důkaz.

Důkaz – viz [MDS]. $\square$

Použití Burnsideova lemmatu

Příklad

Kolika způsoby můžeme vytvořit náhrdelník z 3 černých a 6 bílých korálků stejného tvaru? Kusy stejné barvy nerozlišujeme a za stejné náhrdelníky považujeme všechny, které lze na sebe převést symetrií v rovině.

Řešení

Pro řešení úlohy si náhrdelník představíme jako obarvení pevně označených vrcholů pravidelného devítiúhelníka. Za množinu X volíme všechna možná taková obarvení. Každé takové obarvení je jednoznačně určeno pozicí tří černých korálků. Velikost množiny X je tedy $\binom{9}{3} = 84$.
Víme, že grupou všech symetrií je grupa D_9 složená z 9 rotací (včetně identity) a stejného počtu reflexí. Stejné náhrdelníky jsou ty, které leží ve stejné orbitě akce grupy D_9 na množině všech konfigurací X. Zajímá nás tedy počet orbit N.

Řešení (dokončení)

Pro výpočet N stačí probrat prvky D_9 a všímat si velikostí X^g:
Identita je jediný prvek řádu 1, $|X^{\mathrm{id}}| = 84$. Příspěvek do sumy je 84.
Zrcadlení g jsou všechna řádu 2 a je jich 9. Přitom je zjevně $|X^g| = 4$, celkový příspěvek je proto $4 \cdot 9 = 36$.
Dvě rotace g o úhel $2\pi/3$ nebo $4\pi/3$ mají řád 3 a $|X^g| = 3$. Jejich příspěvek je tedy 6.
Konečně zbývajících rotací (řádu 9 v D_9) je 6 a nenechávají na místě žádný prvek, do celkové sumy tedy ničím nepřispívají.
Celkem dostáváme podle formule z Burnsidova lemmatu:

$$N = \frac{1}{|D_9|} \sum_{g \in D_9} |X^g| = \frac{126}{18} = 7.$$

Najděte si příslušných sedm různých náhrdelníků!

Příklad

Určete počet obarvení políček tabulky 3×3 třemi barvami, považujeme-li za stejná obarvení, která na sebe přejdou při nějaké symetrii tabulky (tedy rotací nebo zrcadlením).

Příklad

Určete počet obarvení stěn (resp. hran) krychle dvěma barvami, považujeme-li za stejná ta obarvení, která na sebe přejdou při nějakém otočení krychle.

Příklad

Kolik různých náramků lze sestavit právě z devíti bílých, šesti červených a tří černých korálků? (dva náramky považujeme za stejné, pokud se liší pouze nějakou rotací v prostoru).