Diskrétní matematika B – 7. týden
Teorie grup

Michal Bulant

Masarykova univerzita
Fakulta informatiky

jaro 2014

Obsah přednášky

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).

(Přímý) součin grup

Definice

Pro každé dvě grupy $(G, \cdot)$, $(H, \circ)$ definujeme **součin grup** $(G \times H, *)$ takto: Jako množina je $G \times H$ skutečně (kartézský) součin, na kterém definujeme grupové násobení po složkách, tj. $(a, x) * (b, y) = (a \cdot b, x \circ y)$.

Poznámka

Rozmyslete si, že jde o grupu a že součin komutativních grup je zase komutativní!

Zobrazení

$$p_G : G \times H \ni (a, x) \mapsto a \in G, \quad p_H : G \times H \ni (a, x) \mapsto x \in H$$

jsou surjektivní homomorfismy (tzv. **projekce**) s jádry

$$\ker p_G = \{(e_G, x);\ x \in H\} \qquad \ker p_H = \{(a, e_H); a \in G\}.$$

Příklad

(1) Grupa $\mathbb{Z}_6$ je izomorfní součinu $\mathbb{Z}_2 \times \mathbb{Z}_3$.
Toto lze nahlédnout buď geometrickou úvahou (prostřednictvím grup symetrií v rovině) nebo přímou konstrukcí izomorfismu.
V aditivní notaci vypadá izomorfismus takto:

$$[0]_6 \mapsto ([0]_2, [0]_3),\ [1]_6 \mapsto ([1]_2, [2]_3)$$
$$[2]_6 \mapsto ([0]_2, [1]_3),\ [3]_6 \mapsto ([1]_2, [0]_3)$$
$$[4]_6 \mapsto ([0]_2, [2]_3),\ [5]_6 \mapsto ([1]_2, [1]_3)$$

(2) Dihedrální grupa D_8 (tj. grupa symetrií čtverce, $\langle r, s | r^4 = 1, s^2 = 1, srs = r^{-1} \rangle$) **není** izomorfní součinu $\mathbb{Z}_2 \times \mathbb{Z}_4$, přestože mají stejný počet prvků (D_8 není komutativní).

Čínská zbytková věta (Chinese remainder theorem)

Předchozí příklad je speciálním případem tzv. *Čínské zbytkové věty*.

Věta

Jsou-li $k, m \in \mathbb{N}$ *nesoudělná, pak*

$$(\mathbb{Z}_{km}, +) \cong (\mathbb{Z}_k, +) \times (\mathbb{Z}_m, +).$$

a obecněji

Věta

Jsou-li $m_1, m_2, \cdots, m_k$ *po dvou nesoudělná, pak*

$$(\mathbb{Z}_{\prod m_i}, +) \cong (\mathbb{Z}_{m_1}, +) \times (\mathbb{Z}_{m_2}, +) \times \cdots \times (\mathbb{Z}_{m_k}, +).$$

Důkaz CRT:

Sestrojíme požadovaný izomorfismus f. Označme $m = \prod_i m_i$ a pro libovolné $[a]_m \in \mathbb{Z}_m$ položme $f([a]_m) = ([a]_{m_1}, \ldots, [a]_{m_k})$. Snadno se ověří, že jde o injektivní homomorfismus (co je jádrem?). Zbývá dokázat, že jde i o surjekci, tedy, že libovolný prvek

$$([a_1]_{m_1}, \ldots, [a_k]_{m_k}) \in (\mathbb{Z}_{m_1}, +) \times \cdots \times (\mathbb{Z}_{m_k}, +)$$

je obrazem nějakého $a \in \mathbb{Z}_m$. To je ale totéž jako najít $a \in \mathbb{Z}$ takové, že $a \equiv a_1 \pmod{m_1}, \ldots a \equiv a_k \pmod{m_k}$, což se udělá malým (ale šikovným) trikem:[1]
Pro libovolné $1 \leq i \leq k$ položme $n_i = m/m_i$ a protože $(m_i, n_i) = 1$ (zde jsme využili *nesoudělnost po dvou*), najdeme podle Bezoutovy věty u_i a v_i tak, že $u_i m_i + v_i n_i = 1$, tj. $v_i n_i \equiv 1 \pmod{m_i}$.
Hledané a pak najdeme jako

$$a = \sum_i a_i v_i n_i.$$

[1] A nešlo by to ještě šikovněji? Pokud nám stačí existence izomorfismu, tak stačí využít toho, že injektivní zobrazení mezi množinami o stejném počtu prvků

Cyklické grupy

Libovolný prvek a v grupě G je obsažen v minimální podgrupě $\{e = a^0, a = a^1, a^2, a^3, \dots\}$, která jej obsahuje.
Je zjevné, že je tato podgrupa komutativní, a pokud je celá grupa G konečná, nutně musí jednou nastat případ $a^k = e$.
Nejmenší k s touto vlastností nazýváme **řád prvku** a v G. Grupa G je **cyklická**, je-li celé G generované nějakým svým prvkem a výše uvedeným způsobem. Zjistit pro konkrétní cyklickou grupu generátor je obecně obtížný problém. I při znalosti generátoru $g \in G$ je ale obecně velkým problémem zjistit pro dané $a \in G$ číslo k, pro které $g^k = a$ (tzv. *problém diskrétního logaritmu*).
Z definice přímo vyplývá, že každá cyklická grupa je izomorfní buď grupě celých čísel $\mathbb{Z}$ (pokud je nekonečná) nebo některé grupě zbytkových tříd $(\mathbb{Z}_k, +)$ (když je konečná).

Rozklady podle podgrup

Uvažme grupu G a její podgrupu H. Na množině prvků grupy G definujeme relaci $a \sim_H b$ jestliže $b^{-1} \cdot a \in H$, tj. $a^{-1} \cdot b \in H$ (tyto dvě podmínky jsou zřejmě ekvivalentní, není to ale totéž jako podmínky $a \cdot b^{-1}$ nebo $b \cdot a^{-1}$).
Je to relace ekvivalence:

- $a^{-1} \cdot a = e \in H$,
- je-li $b^{-1} \cdot a = h \in H$, potom $a^{-1} \cdot b = (b^{-1} \cdot a)^{-1} = h^{-1} \in H$,
- je-li $c^{-1} \cdot b \in H$ a zároveň je $b^{-1} \cdot a \in H$, potom $c^{-1} \cdot a = c^{-1} \cdot b \cdot b^{-1} \cdot a \in H$.

Celá grupa G se tedy rozpadá na tzv. **levé třídy rozkladu** podle podgrupy H vzájemně ekvivalentních prvků.
Třídu příslušející prvku a značíme $a \cdot H$ (zřejmě $a \in a \cdot H$) a skutečně platí, že

$$a \cdot H = \{a \cdot h;\ h \in H\},$$

neboť prvek b je ve stejné třídě s a, právě když jde takovýmto způsobem vyjádřit.
Množinu všech levých tříd rozkladu podle podgrupy H označujeme G/H.
Obdobně definujeme pravé třídy rozkladu $H \cdot a$. Příslušná ekvivalence je: $a \sim b$, jestliže $a \cdot b^{-1} \in H$. Proto

$$H\backslash G = \{H \cdot a;\ a \in G\}.$$

Věta

Pro třídy rozkladu grupy platí:

1. *Levé a pravé třídy rozkladu podle podgrupy $H \leq G$ splývají právě tehdy, když pro každé $a \in G$, $h \in H$ platí $a \cdot h \cdot a^{-1} \in H$.*
2. *Všechny třídy (levé i pravé) mají shodnou mohutnost jako podgrupa H.*
3. *Zobrazení $a \cdot H \mapsto H \cdot a^{-1}$ zadává bijekci mezi levými a pravými třídami rozkladu G podle H.*

Poznámka

Rozmyslete si, proč je v posledním tvrzení a^{-1} a nikoliv a.

Důsledek

Nechť G je konečná grupa s n prvky (tj. G je řádu n), H její podgrupa. Potom

1. *Mohutnost $n = |G|$ je součinem mohutnosti H a mohutnosti G/H, tj.*
$$|G| = |G/H| \cdot |H|$$
2. *Přirozené číslo $|H|$ je dělitelem čísla n.*
3. *Je-li $a \in G$ prvek řádu k, pak k dělí n.*
4. *pro každé $a \in G$ je $a^n = e$.*
5. *je-li mohutnost grupy G prvočíslo p , pak je G izomorfní cyklické grupě $\mathbb{Z}_p$.*

Druhému tvrzení se říkává Lagrangeova věta, předposlednímu malá Fermatova věta (častěji ovšem ve speciálním případě grupy $(\mathbb{Z}_p^\times, \cdot)$).

Snadnými důsledky předchozího jsou následující věty:

Věta (Malá Fermatova)

Pro libovolné prvočíslo p a číslo $a \in \mathbb{Z}$ nedělitelné p platí

$$a^{p-1} \equiv 1 \pmod{p}.$$

Věta (Eulerova)

Pro libovolné $m \in \mathbb{N}$ a každé $a \in \mathbb{Z}$ splňující $(a, m) = 1$ platí

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Normální podgrupy

Podgrupy H, pro které platí, že $a \cdot h \cdot a^{-1} \in H$ pro všechna $a \in G$, $h \in H$, se nazývají **normální podgrupy** (značíme $H \lhd G$). Snadno se nahlédne platnost následujícího

Tvrzení

Podgrupa H je normální právě tehdy, když pro každé $a \in G$ platí $a \cdot H = H \cdot a$ (jinými slovy: levý rozklad G podle podgrupy H je shodný s pravým rozkladem).

Důsledek

- $1 \lhd G$, $G \lhd G$
- *V komutativní grupě je každá podgrupa normální.*
- *Je-li H podgrupa konečné grupy G, kde $|H| = |G|/2$, pak je H normální.*

Příklad

- Dihedrální grupa D_{2n} má vždy normální podgrupu izomorfní $\mathbb{Z}_n$. Levý (i pravý) rozklad podle této podgrupy je dvojprvková množina
$$\{\mathbb{Z}_n, s \cdot \mathbb{Z}_n\}.$$
- $\langle r^2 \rangle = \{id, r^2\}$ je normální podgrupa v D_8. Levý rozklad podle této podgrupy je čtyřprvková množina
$$\{\{id, r^2\}, \{r, r^3\}, \{s, sr^2\}, \{sr, sr^3\}\}.$$

Pro normální podgrupy je dobře definováno násobení na G/H vztahem

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

Skutečně, volbou jiných reprezentantů $a \cdot h$, $b \cdot h'$ dostaneme opět stejný výsledek

$$(a \cdot h \cdot b \cdot h') \cdot H = ((a \cdot b) \cdot (b^{-1} \cdot h \cdot b) \cdot h') \cdot H.$$

Věta

Je-li H normální podgrupou G, tvoří rozklad G/H s násobením definovaným prostřednictvím reprezentantů grupu. Je-li G komutativní, je i G/H komutativní.

Příklad

$$n\mathbb{Z} = \{na;\ a \in \mathbb{Z}\} \subset \mathbb{Z}$$

zadává pro libovolné $n \in \mathbb{N}$ podgrupu $\mathbb{Z}$ a její faktorgrupou (až na izomorfismus) je aditivní grupa zbytkových tříd $\mathbb{Z}_n$ (přitom pro $n = 1$ jde o triviální grupu).

Příklad

Nechť G je grupa řádu 14, která má normální podgrupu řádu 2. Dokažte, že G je komutativní.

Řešení

Označme danou normální podgrupu N. Pak G/N je grupa a její řád je $|G/N| = \frac{|G|}{|N|} = 7$. Podle Lagrangeovy věty je řád každého jejího prvku buď 1 nebo 7. To ovšem znamená, že řád aspoň jednoho prvku je 7, a tedy že G/N je cyklická. Nechť $N = \{e, n\}$, kde e je neutrální prvek G a generátor grupy G/N je $[a]$. Protože N je normální, je $ana^{-1} \in N$, ale protože $ana^{-1} = e \implies n = e$, musí být $ana^{-1} = n$, tedy $na = an$. Protože $[a]$ generuje G/N, je každý prvek G/N tvaru $[a]^k$, $k = 0, \ldots, 6$, tedy $[a^k]$. Každý prvek G je tak tvaru a^k, nebo $a^k n$, a protože prvky a a n spolu komutují, komutují spolu libovolné prvky G. [Později uvidíme, že nutně $G \cong \mathbb{Z}_{14}$.]

Jednoduché (prosté) grupy

Naproti tomu existují i grupy, které nemají žádné vlastní normální podgrupy, takové grupy se nazývají **jednoduché** (simple). Znalost těchto grup je velmi důležitá, protože z nich je v jistém smyslu *složena* každá konečná grupa.

Mezi konečnými komutativními grupami je situace skutečně jednoduchá – prostými jsou pouze grupy $\mathbb{Z}_p$ pro prvočíselné p (podobně i každá prostá grupa lichého řádu je nutně izomorfní $\mathbb{Z}_p$ – důkaz tohoto faktu je ale značně netriviální[2]).

V nekomutativním případě je situace výrazně složitější – až v roce 1982 (samozřejmě s pomocí počítačů) se podařilo završit úsilí o úplnou klasifikaci jednoduchých grup.

Například alternující grupa A_n (tj. podgrupa sudých permutací grupy Σ_n) je jednoduchá pro $n \geq 5$, z čehož (s pomocí tzv. Galoisovy teorie) plyne nemožnost existence obecných vzorců pro kořeny polynomů stupně 5 a vyššího.

[2] 255 stran "tvrdé" matematiky

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:
$\mathbb{Z}_{60} \times \mathbb{Z}_3, \mathbb{Z}_{90} \times \mathbb{Z}_2, \mathbb{Z}_{180}$.

Věta (Cauchy)

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

Důkaz.

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 $x \in G$ 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.