Matematika IV – 4. přednáška
Součiny a rozklady grup

Michal Bulant

Masarykova univerzita
Fakulta informatiky

16. 3. 2011

Obsah přednášky

Doporučené zdroje

- Martin Panák, Jan Slovák, **Drsná matematika**, *e*-text.
- *Předmětové záložky v IS MU*

Doporučené zdroje

- Martin Panák, Jan Slovák, **Drsná matematika**, *e*-text.
- *Předmětové záložky v IS MU*
- R. B. Ash, Abstract algebra, `http://www.math.uiuc.edu/~r-ash/Algebra.html`.
- Jiří Rosický, *Algebra*, PřF MU, 2002.
- Peter J. Cameron. *Introduction to algebra*, Oxford University Press, 2001, 295 s. (Dostupné v knihovně PřF).

Plán přednášky

(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!

(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

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

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

(7) 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.

Příklad

(7) 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:

$$
\begin{array}{ll}
[0]_6 \mapsto ([0]_2, [0]_3), & [1]_6 \mapsto ([1]_2, [2]_3) \\
[2]_6 \mapsto ([0]_2, [1]_3), & [3]_6 \mapsto ([1]_2, [0]_3) \\
[4]_6 \mapsto ([0]_2, [2]_3), & [5]_6 \mapsto ([1]_2, [1]_3)
\end{array}
$$

Příklad

(7) 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:

$$\begin{aligned} [0]_6 &\mapsto ([0]_2, [0]_3), & [1]_6 &\mapsto ([1]_2, [2]_3) \\ [2]_6 &\mapsto ([0]_2, [1]_3), & [3]_6 &\mapsto ([1]_2, [0]_3) \\ [4]_6 &\mapsto ([0]_2, [2]_3), & [5]_6 &\mapsto ([1]_2, [1]_3) \end{aligned}$$

(8) 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 nesoudělná, pak

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

Čínská zbytková věta (Chinese remainder theorem)

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

Věta

Jsou-li k, m 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

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

Tento izomorfismus se často s výhodou využívá k reprezentaci velkých čísel při distribuovaných výpočtech pracujících s dělitelností, kdy na každém počítači stačí pracovat s jedním (relativně malým) modulem.

Důkaz CRT:

Sestrojíme požadovaný izomorfismus f [1]. 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?).

[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 je automaticky bijekcí.

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]

[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 je automaticky bijekcí.

Důkaz CRT:

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

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

je obrazem nějakého $a \in \mathbb{Z}_m$. To je ale totéž jako najít $a \in \mathbb{Z}$ takové, že $a \equiv a_1 \pmod{m_1}, \dots, a \equiv a_k \pmod{m_k}$, 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. $v_i n_i \equiv 1 \pmod{m_i}$.

[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 je automaticky bijekcí.

Důkaz CRT:

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

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

je obrazem nějakého $a \in \mathbb{Z}_m$. To je ale totéž jako najít $a \in \mathbb{Z}$ takové, že $a \equiv a_1 \pmod{m_1}, \dots, a \equiv a_k \pmod{m_k}$, 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 je automaticky bijekcí.

Cyklické grupy

Pro libovolný prvek a v grupě G existuje minimální podgrupa $\{e = a^0, a = a^1, a^2, a^3, \dots\}$, která jej obsahuje[2].
Je zjevné, že je tato podgrupa komutativní, a pokud je celá grupa G konečná, nutně musí jednou nastat případ $a^k = e$.

[2] Co znamenají ty mocniny?

Cyklické grupy

Pro libovolný prvek a v grupě G existuje minimální podgrupa $\{e = a^0, a = a^1, a^2, a^3, \dots\}$, která jej obsahuje[2].
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.

[2] Co znamenají ty mocniny?

Cyklické grupy

Pro libovolný prvek a v grupě G existuje minimální podgrupa $\{e = a^0, a = a^1, a^2, a^3, \dots\}$, která jej obsahuje[2].
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* je základem mnoha kryptografických protokolů – ElGamal, Diffie-Hellman, DSA).

[2] Co znamenají ty mocniny?

Cyklické grupy

Pro libovolný prvek a v grupě G existuje minimální podgrupa $\{e = a^0, a = a^1, a^2, a^3, \dots\}$, která jej obsahuje[2].
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* je základem mnoha kryptografických protokolů – ElGamal, Diffie-Hellman, DSA). 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).

---

[2] Co znamenají ty mocniny?

Plán přednášky

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:

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:

- $a^{-1} \cdot a = e \in H$,

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 $a^{-1} \cdot b = (b^{-1} \cdot a)^{-1} = h^{-1} \in H$,

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.

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.

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.

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:

Věta

Pro třídy rozkladu grupy platí:

1. *Levé a pravé třídy rozkladu podle podgrupy $H \subset G$ splývají právě tehdy, když pro každé $a \in G$, $h \in H$ platí $a \cdot h \cdot a^{-1} \in H$.*

Věta

Pro třídy rozkladu grupy platí:

1. *Levé a pravé třídy rozkladu podle podgrupy* $H \subset G$ *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

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.*
$$|G| = |G/H| \cdot |H|$$

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.*

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.*

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 $a^n = e$.*

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 $\mathbb{Z}_p$.*

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

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

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

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

Plán přednášky

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

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).

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.

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) .

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.

[3] 255 stran "tvrdé" matematiky

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[3]).

[3] 255 stran "tvrdé" matematiky

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[3]).

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

[3] 255 stran "tvrdé" matematiky

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[3]).
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.

[3] 255 stran "tvrdé" matematiky

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**.

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

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

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 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).

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 $\mathrm{SL}_n(\mathbb{R})$.

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

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 $N_G(B) = G$).

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 (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.

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