Drsná matematika IV – 2. přednáška
Elementární teorie grup

Jan Slovák

Masarykova univerzita
Fakulta informatiky

27. 2. 2012

Obsah přednášky

Plán přednášky

Kde je dobré číst?

- vlastní poznámky, texty současného přednášejícího, GOOGLE, atd.

Kde je dobré číst?

- vlastní poznámky, texty současného přednášejícího, GOOGLE, atd.
- Riley, K.F., Hobson, M.P., Bence, S.J. Mathematical Methods for Physics and Engineering, second edition, Cambridge University Press, Cambridge 2004, ISBN 0 521 89067 5, xxiii + 1232 pp.
- bude doplněno . . . ...

Plán přednášky

připomenutí:

- **pologrupa** $(G, \cdot)$ je množina G s binární operací $\cdot$
- **grupa** $(G, \cdot)$ je pologrupa s jednotkou, ve které má každý prvek inverzi
- **komutativní grupa**, resp. **komutativní pologrupa**, je taková, kde je operace $\cdot$ komutativní.
- Je-li $(A, \cdot)$ grupa (případně pologrupa), pak její podmnožinu $B \subset A$, která je uzavřená vůči zúžení operace $\cdot$ a zároveň je spolu s touto operací grupou, nazýváme **podgrupa** v $(A, \cdot)$.

Definition

Zobrazení $f : G \to H$ mezi dvěmi grupami G a H se nazývá **homomorfismus grup**, jestliže respektuje násobení, tj. pro všechny prvky $a, b \in G$ platí

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

Povšimněme si, že násobení vlevo je uvnitř grupy G předtím, než zobrazujeme, zatímco vpravo jde o násobení v H poté, co zobrazujeme.

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Theorem

Pro každý homomorfismus $f : G \to H$ grup platí

1. *obraz jednotky $e \in G$ je jednotka v H*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Theorem

Pro každý homomorfismus $f : G \to H$ grup platí

1. *obraz jednotky $e \in G$ je jednotka v H*
2. *obraz podgrupy $K \subset G$ je podgrupa $f(K) \subset H$.*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Theorem

Pro každý homomorfismus $f : G \to H$ *grup platí*

1. *obraz jednotky* $e \in G$ *je jednotka v* H
2. *obraz podgrupy* $K \subset G$ *je podgrupa* $f(K) \subset H$.
3. *vzorem* $f^{-1}(K) \subset G$ *podgrupy* $K \subset H$ *je podgrupa.*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Theorem

Pro každý homomorfismus $f : G \to H$ grup platí

1. *obraz jednotky $e \in G$ je jednotka v H*
2. *obraz podgrupy $K \subset G$ je podgrupa $f(K) \subset H$.*
3. *vzorem $f^{-1}(K) \subset G$ podgrupy $K \subset H$ je podgrupa.*
4. *obraz inverze k prvku je inverzí obrazu. tj. $f(a^{-1}) = f(a)^{-1}$.*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Theorem

Pro každý homomorfismus $f : G \to H$ grup platí

1. *obraz jednotky $e \in G$ je jednotka v H*
2. *obraz podgrupy $K \subset G$ je podgrupa $f(K) \subset H$.*
3. *vzorem $f^{-1}(K) \subset G$ podgrupy $K \subset H$ je podgrupa.*
4. *obraz inverze k prvku je inverzí obrazu. tj. $f(a^{-1}) = f(a)^{-1}$.*
5. *je-li f zároveň bijekcí, pak i inverzní zobrazení f^{-1} je homomorfismus.*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Theorem

Pro každý homomorfismus $f : G \to H$ grup platí

1. *obraz jednotky $e \in G$ je jednotka v H*
2. *obraz podgrupy $K \subset G$ je podgrupa $f(K) \subset H$.*
3. *vzorem $f^{-1}(K) \subset G$ podgrupy $K \subset H$ je podgrupa.*
4. *obraz inverze k prvku je inverzí obrazu. tj. $f(a^{-1}) = f(a)^{-1}$.*
5. *je-li f zároveň bijekcí, pak i inverzní zobrazení f^{-1} je homomorfismus.*
6. *f je injektivní zobrazení právě, když $f^{-1}(e) = \{e\}$.*

Definition

Podgrupa $f^{-1}(e)$ jednotkového prvku $e \in H$ se nazývá **jádro** homomorfismu f a značíme ji $\ker f$. Bijektivní homomorfismus grup nazýváme **izomorfismus**.

Definition

Podgrupa $f^{-1}(e)$ jednotkového prvku $e \in H$ se nazývá **jádro** homomorfismu f a značíme ji $\ker f$. Bijektivní homomorfismus grup nazýváme **izomorfismus**.

Z předchozích tvrzení okamžitě vyplývá, že homomorfismus $f : G \to H$ s triviálním jádrem je izomorfismem na obraz $f(G)$.

Example

(1) Pro každou grupu permutací $G = \Sigma_n$ jsme definovali zobrazení $\mathrm{sgn} : \Sigma_n \to \mathbb{Z}_2$ přiřazující permutaci její paritu. Jde o homomorfismus grup. Jádrem tohoto homomorfismu jsou permutace se sudou paritou.

Example

(1) Pro každou grupu permutací $G = \Sigma_n$ jsme definovali zobrazení $\mathrm{sgn} : \Sigma_n \to \mathbb{Z}_2$ přiřazující permutaci její paritu. Jde o homomorfismus grup. Jádrem tohoto homomorfismu jsou permutace se sudou paritou.
(2) Grupa symetrií rovnostranného trojúhelníka je izomorfní s grupou permutací Σ_3. Zvolíme-li realizaci Σ_3 tak, že za množinu tří prvků pro permutace vezmeme vrcholy trojúhelníka a jednotlivým symetriím přiřadíme permutace těchto vrcholů, které vyvolají.

Example

(1) Pro každou grupu permutací $G = \Sigma_n$ jsme definovali zobrazení $\mathrm{sgn} : \Sigma_n \to \mathbb{Z}_2$ přiřazující permutaci její paritu. Jde o homomorfismus grup. Jádrem tohoto homomorfismu jsou permutace se sudou paritou.
(2) Grupa symetrií rovnostranného trojúhelníka je izomorfní s grupou permutací Σ_3. Zvolíme-li realizaci Σ_3 tak, že za množinu tří prvků pro permutace vezmeme vrcholy trojúhelníka a jednotlivým symetriím přiřadíme permutace těchto vrcholů, které vyvolají.
(3) Zobrazení $\exp : \mathbb{R} \to \mathbb{R}_+$ (nebo $\mathbb{C} \to \mathbb{C} \setminus 0$), je homomorfismus aditivní grupy reálných nebo komplexních čísel na multiplikativní grupu kladných reálných čísel, resp. na multiplikativní grupu všech nenulových komplexních čísel. V případě reálných čísel jde o izomorfismus. Pro komplexní čísla dostáváme netriviální jádro $2k\pi i$, $k \in \mathbb{Z}$.

Example

(4) Determinant matice je zobrazením, které každé matici skalárů z $\mathbb{K}$ přiřazuje nějaký skalár v $\mathbb{K}$ (pracovali jsme s $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$). Cauchyova věta o determinantu součinu čtvercových matic $\det(A \cdot B) = (\det A) \cdot (\det B)$ je tvrzením, že pro grupu $G = GL(n, \mathbb{K})$ invertibilních matic je $\det : G \to \mathbb{K} \setminus 0$ homomorfismem grup.

Example

(4) Determinant matice je zobrazením, které každé matici skalárů z $\mathbb{K}$ přiřazuje nějaký skalár v $\mathbb{K}$ (pracovali jsme s $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$).
Cauchyova věta o determinantu součinu čtvercových matic $\det(A \cdot B) = (\det A) \cdot (\det B)$ je tvrzením, že pro grupu $G = GL(n, \mathbb{K})$ invertibilních matic je $\det : G \to \mathbb{K} \setminus 0$ homomorfismem grup.
(5) Pro každé dvě grupy G, H definujeme **součin grup** $G \times H$ takto: Jako množina je $G \times H$ skutečně součin a násobení definujeme po složkách. tj. $(a, x) \cdot (b, y) = (a \cdot b, x \cdot y)$. Zobrazení

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

jsou surjektivní homomorfismy s jádry

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

Example

(6) Grupy zbytkových tříd $\mathbb{Z}_k$ jsou izomorfní grupám komplexních k–tých odmocnin z jedničky, což jsou zároveň izomorfní obrazy konečných grup otočení v rovině o celé násobky úhlu $\frac{2\pi}{k}$.

Example

(6) Grupy zbytkových tříd $\mathbb{Z}_k$ jsou izomorfní grupám komplexních k–tých odmocnin z jedničky, což jsou zároveň izomorfní obrazy konečných grup otočení v rovině o celé násobky úhlu $\frac{2\pi}{k}$.
(7) Grupa $\mathbb{Z}_6$ je izomorfní součinu $\mathbb{Z}_2 \times \mathbb{Z}_3$. Skutečně, $\mathbb{Z}_6 \subset \mathbb{C}^*$ je tvořeno body na jednotkové kružnici v komplexní rovině ve vrcholech pravidleného šestiúhelníku, $\mathbb{Z}_2$ pak odpovídá ± 1, $\mathbb{Z}_3$ pravidelnému trojúhelníku s jedním vrcholem v jedničce. Jestliže budeme ztotožňovat příslušné body s otočeními v rovině, které jedničku převede právě do nich, pak skládání dvou takových otočení bude vždy komutativní a kombinacemi jednoho otočení ze $\mathbb{Z}_2$ a jednoho ze $\mathbb{Z}_3$ dostaneme právě všechna otočení ze $\mathbb{Z}_6$.

Example

(6) Grupy zbytkových tříd $\mathbb{Z}_k$ jsou izomorfní grupám komplexních k–tých odmocnin z jedničky, což jsou zároveň izomorfní obrazy konečných grup otočení v rovině o celé násobky úhlu $\frac{2\pi}{k}$.
(7) Grupa $\mathbb{Z}_6$ je izomorfní součinu $\mathbb{Z}_2 \times \mathbb{Z}_3$. Skutečně, $\mathbb{Z}_6 \subset \mathbb{C}^*$ je tvořeno body na jednotkové kružnici v komplexní rovině ve vrcholech pravidleného šestiúhelníku, $\mathbb{Z}_2$ pak odpovídá ± 1, $\mathbb{Z}_3$ pravidelnému trojúhelníku s jedním vrcholem v jedničce. Jestliže budeme ztotožňovat příslušné body s otočeními v rovině, které jedničku převede právě do nich, pak skládání dvou takových otočení bude vždy komutativní a kombinacemi jednoho otočení ze $\mathbb{Z}_2$ a jednoho ze $\mathbb{Z}_3$ dostaneme právě všechna otočení ze $\mathbb{Z}_6$.
V aditivní notaci vypadá izomorfismus takto:

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

Libovolný prvek a v grupě G je obsažen v minimální podgrupě $\{a, a^2, a^3, \dots\}$, která jej obsahuje.
Je zjevné, že je tato podgrupa komutativní, a pokud je celá grupa G konečná, nutně musí jednou nastat případ $a^k = e$.

Libovolný prvek a v grupě G je obsažen v minimální podgrupě $\{a, a^2, a^3, \dots\}$, 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 grupa** je-li celé G generované nějakým svým prvkem a výše uvedeným způsobem.

Libovolný prvek a v grupě G je obsažen v minimální podgrupě $\{a, a^2, a^3, \dots\}$, 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 grupa** je-li celé G generované nějakým svým prvkem a výše uvedeným způsobem.
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).

Plán přednášky

Uvažme grupu G a její podgrupu H. Na množině prvků grupy G definujeme relaci $a \sim_H b$ jestliže $b^{-1} \cdot a \in H$.
Je to relace ekvivalence:

Uvažme grupu G a její podgrupu H. Na množině prvků grupy G definujeme relaci $a \sim_H b$ jestliže $b^{-1} \cdot a \in H$.
Je to relace ekvivalence:

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

Uvažme grupu G a její podgrupu H. Na množině prvků grupy G definujeme relaci $a \sim_H b$ jestliže $b^{-1} \cdot a \in H$.
Je to relace ekvivalence:

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

Uvažme grupu G a její podgrupu H. Na množině prvků grupy G definujeme relaci $a \sim_H b$ jestliže $b^{-1} \cdot a \in H$.
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 $a \cdot H$ 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 $a \cdot H$ 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 $a \cdot H$ 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

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

Theorem

Pro třídy rozkladu grupy platí:

Theorem

Pro třídy rozkladu grupy platí:

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

Theorem

Pro třídy rozkladu grupy platí:

1. *Levé a pravé třídy rozkladu podle podgrupy $H \subset G$ splývají právě, 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 s podgrupou H.*

Corollary

Nechť G je konečná grupa s n prvky, H její podgrupa. Potom

Corollary

Nechť G je konečná grupa s n prvky, H její podgrupa. Potom

1. *Mohutnost $n = |G|$ je součinem mohutnosti H a mohutnosti G/H, tj.*

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

Corollary

Nechť G je konečná grupa s n prvky, 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.*

Corollary

Nechť G je konečná grupa s n prvky, 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.*

Corollary

Nechť G je konečná grupa s n prvky, 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 $a^n = e$.*

Corollary

Nechť G je konečná grupa s n prvky, 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, pak je G izomorfní cyklické grupě $\mathbb{Z}_n$.*

Corollary

Nechť G je konečná grupa s n prvky, 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, pak je G izomorfní cyklické grupě $\mathbb{Z}_n$.*

Druhému tvrzení se říkává Lagrangeova věta, předposlednímu malá Fermatova věta.

Plán přednášky

Podgrupy H, pro které platí, že $a \cdot h \cdot a^{-1} \in H$ pro všechny $a \in G$, $h \in H$, se nazývají **normální podgrupy**.

Podgrupy H, pro které platí, že $a \cdot h \cdot a^{-1} \in H$ pro všechny $a \in G$, $h \in H$, se nazývají **normální podgrupy**.
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

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

Podgrupy H, pro které platí, že $a \cdot h \cdot a^{-1} \in H$ pro všechny $a \in G$, $h \in H$, se nazývají **normální podgrupy**.
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

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

Násobení na G/H má všechny vlastnosti grupy.

V komutativních grupách jsou všechny podgrupy normální. Podmnožina

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

zadává v celých číslech podgrupu a její faktorgrupou je právě (aditivní) grupa zbytkových tříd $\mathbb{Z}_n$.

V komutativních grupách jsou všechny podgrupy normální.
Podmnožina

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

zadává v celých číslech podgrupu a její faktorgrupou je právě (aditivní) grupa zbytkových tříd $\mathbb{Z}_n$.
Všechna jádra homomorfismů jsou normální podgrupy. Naopak, jestliže je podgrupa $H \subset G$ normální, pak zobrazení

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

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 a je zjevně na. Je tedy vidět, že normální podgrupy jsou právě všechna jádra homomorfismů.

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.

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.
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 $\mathbb{Z}_k$. Předchozí úvaha 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 přehledný jako u konečných grup