

MB104 Matematika IV - 3. demonstrované cvičení

Jan Herman

5. března 2008

Obsah

- 1 Krátké opakování
- 2 Homomorfismy
 - Rest z minula a další příklady
- 3 Rozklady podle podgrup
 - Příklady
 - Lagrangeova věta a její důsledky
- 4 Normální podgrupy
 - Definice normální podgrupy
 - Příklady
 - Normální podgrupy jako jádra homomorfismů
- 5 Faktorgrupy
 - Definice
 - Příklady

Co už byste měli umět

- **grupa** - asociativita, neutrální prvek, inverzní prvky
- **podgrupa** - podmnožina, která je sama grupou
- **homomorfismus**
 - zobrazení zachovávající operaci
 - $f : (G, \cdot) \rightarrow (H, \circ); f(a \cdot b) = f(a) \circ f(b)$
 - **jádro** - podgrupa, která se zobrazí na neutrální prvek
- **rozklad grupy podle podgrupy**
 - $G/H = \{aH \mid a \in G\}$
 - $aH = bH \Leftrightarrow a \in bH \Leftrightarrow b^{-1}a \in H$
- **normální podgrupa**
 - levý rozklad stejný jako pravý
 - možno faktorizovat
 - korespondence s jádry homomorfismů

Co už byste měli umět

- **grupa** - asociativita, neutrální prvek, inverzní prvky
- **podgrupa** - podmnožina, která je sama grupou
- **homomorfismus**
 - zobrazení zachovávající operaci
 - $f : (G, \cdot) \rightarrow (H, \circ); f(a \cdot b) = f(a) \circ f(b)$
 - **jádro** - podgrupa, která se zobrazí na neutrální prvek
- **rozklad grupy podle podgrupy**
 - $G/H = \{aH \mid a \in G\}$
 - $aH = bH \Leftrightarrow a \in bH \Leftrightarrow b^{-1}a \in H$
- **normální podgrupa**
 - levý rozklad stejný jako pravý
 - možno faktorizovat
 - korespondence s jádry homomorfismů

Co už byste měli umět

- **grupa** - asociativita, neutrální prvek, inverzní prvky
- **podgrupa** - podmnožina, která je sama grupou
- **homomorfismus**
 - zobrazení zachovávající operaci
 - $f : (G, \cdot) \rightarrow (H, \circ); f(a \cdot b) = f(a) \circ f(b)$
 - **jádro** - podgrupa, která se zobrazí na neutrální prvek
- **rozklad grupy podle podgrupy**
 - $G/H = \{aH \mid a \in G\}$
 - $aH = bH \Leftrightarrow a \in bH \Leftrightarrow b^{-1}a \in H$
- **normální podgrupa**
 - levý rozklad stejný jako pravý
 - možno faktorizovat
 - korespondence s jádry homomorfismů

Co už byste měli umět

- **grupa** - asociativita, neutrální prvek, inverzní prvky
- **podgrupa** - podmnožina, která je sama grupou
- **homomorfismus**
 - zobrazení zachovávající operaci
 - $f : (G, \cdot) \rightarrow (H, \circ); f(a \cdot b) = f(a) \circ f(b)$
 - **jádro** - podgrupa, která se zobrazí na neutrální prvek
- **rozklad grupy podle podgrupy**
 - $G/H = \{aH \mid a \in G\}$
 - $aH = bH \Leftrightarrow a \in bH \Leftrightarrow b^{-1}a \in H$
- **normální podgrupa**
 - levý rozklad stejný jako pravý
 - možno faktorizovat
 - korespondence s jádry homomorfismů

Co už byste měli umět

- **grupa** - asociativita, neutrální prvek, inverzní prvky
- **podgrupa** - podmnožina, která je sama grupou
- **homomorfismus**
 - zobrazení zachovávající operaci
 - $f : (G, \cdot) \rightarrow (H, \circ); f(a \cdot b) = f(a) \circ f(b)$
 - **jádro** - podgrupa, která se zobrazí na neutrální prvek
- **rozklad grupy podle podgrupy**
 - $G/H = \{aH \mid a \in G\}$
 - $aH = bH \Leftrightarrow a \in bH \Leftrightarrow b^{-1}a \in H$
- **normální podgrupa**
 - levý rozklad stejný jako pravý
 - možno faktorizovat
 - korespondence s jádry homomorfismů

Homomorfismy

Příklad 1

Najděte všechny homomorfismy z grupy (Σ_3, \circ) do grupy $(\mathbb{Z}_6, +)$ a pro každý určete jeho jádro.

Příklad 2

Najděte všechny homomorfismy z grupy $(\mathbb{Z}, +)$ do sebe sama (neboli všechny **automorfismy** $(\mathbb{Z}, +)$) a určete jejich jádra a obrazy.

Příklad 3

Najděte všechny homomorfismy z grupy $(\mathbb{Z}, +)$ do grupy $(\mathbb{Z}_{10}, +)$ a popište jejich jádra a obrazy.

Homomorfismy

Příklad 1

Najděte všechny homomorfismy z grupy (Σ_3, \circ) do grupy $(\mathbb{Z}_6, +)$ a pro každý určete jeho jádro.

Příklad 2

Najděte všechny homomorfismy z grupy $(\mathbb{Z}, +)$ do sebe sama (neboli všechny **automorfismy** $(\mathbb{Z}, +)$) a určete jejich jádra a obrazy.

Příklad 3

Najděte všechny homomorfismy z grupy $(\mathbb{Z}, +)$ do grupy $(\mathbb{Z}_{10}, +)$ a popište jejich jádra a obrazy.

Homomorfismy

Příklad 1

Najděte všechny homomorfismy z grupy (Σ_3, \circ) do grupy $(\mathbb{Z}_6, +)$ a pro každý určete jeho jádro.

Příklad 2

Najděte všechny homomorfismy z grupy $(\mathbb{Z}, +)$ do sebe sama (neboli všechny **automorfismy** $(\mathbb{Z}, +)$) a určete jejich jádra a obrazy.

Příklad 3

Najděte všechny homomorfismy z grupy $(\mathbb{Z}, +)$ do grupy $(\mathbb{Z}_{10}, +)$ a popište jejich jádra a obrazy.

Rozklady podle podgrup

Příklad 4

Popište levý rozklad grupy (Σ_3, \circ) podle její podgrupy $\langle(1, 2)\rangle$.

Příklad 5

Popište levý rozklad grupy $(\mathbb{C}, +)$ podle podgrupy $(\mathbb{R}, +)$.

Rozklady podle podgrup

Příklad 4

Popište levý rozklad grupy (Σ_3, \circ) podle její podgrupy $\langle(1, 2)\rangle$.

Příklad 5

Popište levý rozklad grupy $(\mathbb{C}, +)$ podle podgrupy $(\mathbb{R}, +)$.

Lagrangeova věta a její důsledky

Věta (Lagrange)

Nechť G je grupa a H její podgrupa. Potom

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

Důsledek

Nechť G je n -prvková konečná grupa, H její podgrupa.

- $|H|$ dělí n
- pro $a \in G$ platí $\text{ord}_G a | n$
- $\forall a \in G : a^n = 1_G$
- pro p prvočíslo, $p \nmid a \in \mathbb{Z}$ platí $a^{p-1} \equiv 1 \pmod{p}$
- pro $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$ platí $a^{\varphi(m)} \equiv 1 \pmod{m}$

Lagrangeova věta a její důsledky

Věta (Lagrange)

Nechť G je grupa a H její podgrupa. Potom

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

Důsledek

Nechť G je n -prvková konečná grupa, H její podgrupa.

- $|H|$ dělí n
- pro $a \in G$ platí $\text{ord}_G a | n$
- $\forall a \in G : a^n = 1_G$
- pro p prvočíslo, $p \nmid a \in \mathbb{Z}$ platí $a^{p-1} \equiv 1 \pmod{p}$
- pro $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$ platí $a^{\varphi(m)} \equiv 1 \pmod{m}$

Lagrangeova věta a její důsledky

Věta (Lagrange)

Nechť G je grupa a H její podgrupa. Potom

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

Důsledek

Nechť G je n -prvková konečná grupa, H její podgrupa.

- $|H|$ dělí n
- pro $a \in G$ platí $\text{ord}_G a | n$
- $\forall a \in G : a^n = 1_G$
- pro p prvočíslo, $p \nmid a \in \mathbb{Z}$ platí $a^{p-1} \equiv 1 \pmod{p}$
- pro $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$ platí $a^{\varphi(m)} \equiv 1 \pmod{m}$

Lagrangeova věta a její důsledky

Věta (Lagrange)

Nechť G je grupa a H její podgrupa. Potom

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

Důsledek

Nechť G je n -prvková konečná grupa, H její podgrupa.

- $|H|$ dělí n
- pro $a \in G$ platí $\text{ord}_G a | n$
- $\forall a \in G : a^n = 1_G$
- pro p prvočíslo, $p \nmid a \in \mathbb{Z}$ platí $a^{p-1} \equiv 1 \pmod{p}$
- pro $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$ platí $a^{\varphi(m)} \equiv 1 \pmod{m}$

Lagrangeova věta a její důsledky

Věta (Lagrange)

Nechť G je grupa a H její podgrupa. Potom

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

Důsledek

Nechť G je n -prvková konečná grupa, H její podgrupa.

- $|H|$ dělí n
- pro $a \in G$ platí $\text{ord}_G a | n$
- $\forall a \in G : a^n = 1_G$
- pro p prvočíslo, $p \nmid a \in \mathbb{Z}$ platí $a^{p-1} \equiv 1 \pmod{p}$
- pro $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$ platí $a^{\varphi(m)} \equiv 1 \pmod{m}$

Lagrangeova věta a její důsledky

Věta (Lagrange)

Nechť G je grupa a H její podgrupa. Potom

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

Důsledek

Nechť G je n -prvková konečná grupa, H její podgrupa.

- $|H|$ dělí n
- pro $a \in G$ platí $\text{ord}_G a | n$
- $\forall a \in G : a^n = 1_G$
- pro p prvočíslo, $p \nmid a \in \mathbb{Z}$ platí $a^{p-1} \equiv 1 \pmod{p}$
- pro $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$ platí $a^{\varphi(m)} \equiv 1 \pmod{m}$

Využití Lagrangeovy věty

Příklad 6

Kolik tříd obsahuje levý rozklad grupy (Σ_7, \circ) podle podgrupy $\langle (1, 2) \circ (3, 4, 5, 6, 7) \rangle$?

Příklad 7

Spočtěte $9^{2008} \equiv ? \pmod{17}$.

Využití Lagrangeovy věty

Příklad 6

Kolik tříd obsahuje levý rozklad grupy (Σ_7, \circ) podle podgrupy $\langle (1, 2) \circ (3, 4, 5, 6, 7) \rangle$?

Příklad 7

Spočtěte $9^{2008} \equiv ? \pmod{17}$.

Normální podgrupy

Definice

Podgrupu H grupy G nazýváme normální, platí-li

$$\forall a \in G : \forall h \in H : a \cdot h \cdot a^{-1} \in H.$$

Značíme $H \trianglelefteq G$.

Poznámka (Ekvivalentní definice normální podgrupy)

Podgrupu H grupy G nazýváme normální, splývá-li levý rozklad G podle H s pravým. Jinými slovy: $\forall a \in G : aH = Ha$.

Normální podgrupy

Definice

Podgrupu H grupy G nazýváme normální, platí-li

$$\forall a \in G : \forall h \in H : a \cdot h \cdot a^{-1} \in H.$$

Značíme $H \trianglelefteq G$.

Poznámka (Ekvivalentní definice normální podgrupy)

Podgrupu H grupy G nazýváme normální, splývá-li levý rozklad G podle H s pravým. Jinými slovy: $\forall a \in G : aH = Ha$.

Normální podgrupy

Příklad 8

Najděte všechny normální podgrupy grupy (Σ_3, \circ) .

Příklad 9

Dokažte, že pro všechna $n \in \mathbb{N}$ je A_n normální podgrupa (Σ_n, \circ) (A_n značí množinu (grupu) všech sudých permutací n -prvkové množiny).

Normální podgrupy

Příklad 8

Najděte všechny normální podgrupy grupy (Σ_3, \circ) .

Příklad 9

Dokažte, že pro všechna $n \in \mathbb{N}$ je A_n normální podgrupa (Σ_n, \circ) (A_n značí množinu (grupu) všech sudých permutací n -prvkové množiny).

Normální podgrupy

Příklad 10

Dokažte, že každá podgrupa komutativní grupy je normální.

Poznámka

Opačně to neplatí! Tedy komutativní podgrupa nekomutativní grupy může a nemusí být její normální podgrupou.

Normální podgrupy

Příklad 10

Dokažte, že každá podgrupa komutativní grupy je normální.

Poznámka

Opačně to neplatí! Tedy komutativní podgrupa nekomutativní grupy může a nemusí být její normální podgrupou.

Normální podgrupy jako jádra homomorfismů

Věta

Jádro homomorfismu $f : G \rightarrow H$ je normální podgrupou grupy G .

Poznámka

Uvidíme, že platí i opačná korespondence - každá normální podgrupa G je jádrem nějakého homomorfismu z G .

Příklad 11

Nechť $G = GL_n(\mathbb{R})$ a H je její podgrupa sestávající se z matic s determinantem rovným 1. Ukažte, že $H \trianglelefteq G$.

Normální podgrupy jako jádra homomorfismů

Věta

Jádro homomorfismu $f : G \rightarrow H$ je normální podgrupou grupy G .

Poznámka

Uvidíme, že platí i opačná korespondence - každá normální podgrupa G je jádrem nějakého homomorfismu z G .

Příklad 11

Nechť $G = GL_n(\mathbb{R})$ a H je její podgrupa sestávající se z matic s determinantem rovným 1. Ukažte, že $H \trianglelefteq G$.

Normální podgrupy jako jádra homomorfismů

Věta

Jádro homomorfismu $f : G \rightarrow H$ je normální podgrupou grupy G .

Poznámka

Uvidíme, že platí i opačná korespondence - každá normální podgrupa G je jádrem nějakého homomorfismu z G .

Příklad 11

Nechť $G = GL_n(\mathbb{R})$ a H je její podgrupa sestávající se z matic s determinantem rovným 1. Ukažte, že $H \trianglelefteq G$.

Faktorové grupy

Definice

Je-li H normální podgrupa (G, \cdot) , můžeme na množině (levých) rozkladových tříd G/H definovat operaci \cdot takto:

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

Pak je $(G/H, \cdot)$ grupa. Nazýváme ji **faktorovou grupou** (zkráceně **faktorgrupou**) grupy G podle normální podgrupy H .

Příklad 12

Popište faktorgrupu $(\mathbb{Z}, +)$ podle podgrupy $n\mathbb{Z}$, $n \in \mathbb{N}$.

Příklad 13

Popište faktorgrupu grupy $(\mathbb{Z}, +) \times (\mathbb{Z}, +)$ podle podgrupy $H = \{(m, n) : 6 \mid 2m - n\}$

Faktorové grupy

Definice

Je-li H normální podgrupa (G, \cdot) , můžeme na množině (levých) rozkladových tříd G/H definovat operaci \cdot takto:

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

Pak je $(G/H, \cdot)$ grupa. Nazýváme ji **faktorovou grupou** (zkráceně **faktorgrupou**) grupy G podle normální podgrupy H .

Příklad 12

Popište faktorgrupu $(\mathbb{Z}, +)$ podle podgrupy $n\mathbb{Z}$, $n \in \mathbb{N}$.

Příklad 13

Popište faktorgrupu grupy $(\mathbb{Z}, +) \times (\mathbb{Z}, +)$ podle podgrupy $H = \{(m, n) : 6 \mid 2m - n\}$

Faktorové grupy

Definice

Je-li H normální podgrupa (G, \cdot) , můžeme na množině (levých) rozkladových tříd G/H definovat operaci \cdot takto:

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

Pak je $(G/H, \cdot)$ grupa. Nazýváme ji **faktorovou grupou** (zkráceně **faktorgrupou**) grupy G podle normální podgrupy H .

Příklad 12

Popište faktorgrupu $(\mathbb{Z}, +)$ podle podgrupy $n\mathbb{Z}$, $n \in \mathbb{N}$.

Příklad 13

Popište faktorgrupu grupy $(\mathbb{Z}, +) \times (\mathbb{Z}, +)$ podle podgrupy $H = \{(m, n) : 6 \mid 2m - n\}$

Faktorové grupy

Příklad 14

Ukažte, že normální podgrupa H grupy G je jádrem nějakého homomorfismu z G .

Poznámka

Ukázali jsme tedy, že normální podgrupy jsou v oboustranné korespondenci s jádry homomorfismů.

Příklad 15

Dokažte, že $\mathbb{V}_4 = \{id, (1, 2) \circ (3, 4), (1, 3) \circ (2, 4), (1, 4) \circ (2, 3)\}$ je normální podgrupa grupy (\mathbb{A}_4, \circ) (grupy sudých permutací na množině $\{1, 2, 3, 4\}$). Určete, jaké známé grupě je izomorfní faktorgrupa $\mathbb{A}_4/\mathbb{V}_4$. Sestrojte endomorfismus f grupy \mathbb{A}_4 (tedy homomorfismus $f : \mathbb{A}_4 \rightarrow \mathbb{A}_4$), jehož jádrem je \mathbb{V}_4 .

Faktorové grupy

Příklad 14

Ukažte, že normální podgrupa H grupy G je jádrem nějakého homomorfismu z G .

Poznámka

Ukázali jsme tedy, že normální podgrupy jsou v oboustranné korespondenci s jádry homomorfismů.

Příklad 15

Dokažte, že $V_4 = \{id, (1, 2) \circ (3, 4), (1, 3) \circ (2, 4), (1, 4) \circ (2, 3)\}$ je normální podgrupa grupy (\mathbb{A}_4, \circ) (grupy sudých permutací na množině $\{1, 2, 3, 4\}$). Určete, jaké známé grupě je izomorfní faktorgrupa \mathbb{A}_4/V_4 . Sestrojte endomorfismus f grupy \mathbb{A}_4 (tedy homomorfismus $f : \mathbb{A}_4 \rightarrow \mathbb{A}_4$), jehož jádrem je V_4 .

Faktorové grupy

Příklad 14

Ukažte, že normální podgrupa H grupy G je jádrem nějakého homomorfismu z G .

Poznámka

Ukázali jsme tedy, že normální podgrupy jsou v oboustranné korespondenci s jádry homomorfismů.

Příklad 15

Dokažte, že $\mathbb{V}_4 = \{id, (1, 2) \circ (3, 4), (1, 3) \circ (2, 4), (1, 4) \circ (2, 3)\}$ je normální podgrupa grupy (\mathbb{A}_4, \circ) (grupy sudých permutací na množině $\{1, 2, 3, 4\}$). Určete, jaké známé grupě je izomorfní faktorgrupa $\mathbb{A}_4/\mathbb{V}_4$. Sestrojte endomorfismus f grupy \mathbb{A}_4 (tedy homomorfismus $f : \mathbb{A}_4 \rightarrow \mathbb{A}_4$), jehož jádrem je \mathbb{V}_4 .