

# Matematika IV – 3. přednáška

## Rozklady grup

Michal Bulant

Masarykova univerzita  
Fakulta informatiky

3. 3. 2008

# Obsah přednášky

1 Rozklady podle podgrup

2 Normální podgrupy

## 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*
- Jiří Rosický, *Algebra*, PŘF MU, 2002.
- Peter J. Cameron. *Introduction to algebra*, Oxford University Press, 2001, 295 s. (Dostupné v knihovně PŘF).

# Plán přednášky

1 Rozklady podle podgrup

2 Normální podgrupy

# 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.  $a^{-1} \cdot b \in H$ .

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.  $a^{-1} \cdot b \in H$ .

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.  $a^{-1} \cdot b \in H$ .

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.  $a^{-1} \cdot b \in H$ .

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.

Třidu 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 říká 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

1 Rozklady podle podgrup

2 Normální podgrupy

# 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  $H \triangleleft G$ ). 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  $H \triangleleft G$ ). 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  $H \triangleleft G$ ). 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

- $1 \triangleleft G$ ,  $G \triangleleft G$
- 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.*

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

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.



# 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<sup>1</sup>).

# 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<sup>1</sup>).

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

# 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<sup>1</sup>).

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  $\Sigma_n$ ) 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.

---

<sup>1</sup>255 stran “tvrdé” matematiky

# Vztah normální podgrup a homomorfismů

Všechna jádra homomorfismů jsou normální podgrupy. Naopak, jestliže je podgrupa  $H \subset G$  normální, pak zobrazení (projekce na faktorgrupu)

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

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.**

# Věty o izomorfismu

## Věta (první, základní)

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

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

*který je injektivní.*

*Zejména dostáváme  $G / \ker f \cong f(G)$ .*

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  $N_G(B) = G$ ).

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  $(A \cap B) \triangleleft A$  a platí*

$$AB/B \cong A/(A \cap B).$$

### Věta (třetí)

*Jsou-li  $A, B \triangleleft G$  normální podgrupy splňující  $A \leq B$ , pak  $B/A \triangleleft G/A$  a platí*

$$(G/A)/(B/A) \cong G/B.$$



### Věta (třetí)

*Jsou-li  $A, B \triangleleft G$  normální podgrupy splňující  $A \leq B$ , pak  $B/A \triangleleft G/A$  a platí*

$$(G/A)/(B/A) \cong G/B.$$

### Věta (čtvrtá, svazový izomorfismus)

*Nechť je  $N \triangleleft G$ . 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  $A, B \triangleleft G$  normální podgrupy splňující  $A \leq B$ , pak  $B/A \triangleleft G/A$  a platí*

$$(G/A)/(B/A) \cong G/B.$$

### Věta (čtvrtá, svazový izomorfismus)

*Nechť je  $N \triangleleft G$ . 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  $D_8 / \langle r^2 \rangle$ .

## Příklad

Zdánlivě paradoxní je příklad homomorfismu  $\mathbb{C}^* \rightarrow \mathbb{C}^*$  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

$$\tilde{f} : \mathbb{C}^* / \mathbb{Z}_k \rightarrow \mathbb{C}^* .$$

Tento příklad ukazuje, že u nekonečných grup nejsou počty s mohutnostmi tak přehledné jako u konečných grup