Matematika IV – 4. přednáška
Rozklady grup, okruhy

Michal Bulant

Masarykova univerzita
Fakulta informatiky

13. 3. 2013

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

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 $H \triangleleft G$) . 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 $H \lhd G$) . 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.

[1]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[1]).

[1] 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[1]).
V nekomutativním případě je situace výrazně složitější – až v roce 1982 (samozřejmě s pomocí počítačů) se podařilo završit úsilí o úplnou klasifikaci jednoduchých grup.

[1] 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[1]).
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.

[1] 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 faktorgrupa 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 odvoďte 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

Plán přednášky

S grupami se potkáváme nejčastěji jako s množinami transformací. U skalárů i vektorů ale vystupovalo hned více obdobných struktur zároveň.

Jako standardní příklady mějme na mysli **skaláry** (tj. celá čísla $\mathbb{Z}$, racionální čísla $\mathbb{Q}$, reální či komplexní čísla $\mathbb{R}, \mathbb{C}$) a **množiny polynomů nad takovými skaláry** R. Klasickým příkladem konečného okruhu je pak $\mathbb{Z}_m$.

S grupami se potkáváme nejčastěji jako s množinami transformací. U skalárů i vektorů ale vystupovalo hned více obdobných struktur zároveň.
Jako standardní příklady mějme na mysli **skaláry** (tj. celá čísla $\mathbb{Z}$, racionální čísla $\mathbb{Q}$, reální či komplexní čísla $\mathbb{R}, \mathbb{C}$) a **množiny polynomů nad takovými skaláry** R. Klasickým příkladem konečného okruhu je pak $\mathbb{Z}_m$.

Definice

Komutativní grupa $(R, +)$ s neutrálním prvkem $0 \in R$, spolu s další operací $\cdot$ splňující

- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, pro všechny $a, b, c \in R$ *(asociativita)*;
- $a \cdot b = b \cdot a$, pro všechny $a, b \in R$ *(komutativita)*;
- existuje prvek 1 takový, že pro všechny $a \in R$ platí $1 \cdot a = a$ *(existence jedničky)*;
- $a \cdot (b + c) = a \cdot b + a \cdot c$, pro všechny $a, b, c \in R$ *(distributivita)*;

se nazývá **komutativní okruh**. Takový okruh zapisujeme $(R, +, \cdot)$.

Definice

Jestliže v komutativním okruhu R platí $c \cdot d = 0$ právě, když je alespoň jeden z prvků c a d nulový, pak okruh R nazýváme **oborem integrity**.

Příklad

- Okruhy $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot)$ jsou obory integrity.
- Okruh Gaussových celých čísel $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ je oborem integrity.
- Okruh $(\mathbb{Z}_4, +, \cdot)$ není obor integrity, narozdíl od $(\mathbb{Z}_5, +, \cdot)$.

Definice

Jestliže v komutativním okruhu R platí $c \cdot d = 0$ právě, když je alespoň jeden z prvků c a d nulový, pak okruh R nazýváme **oborem integrity**.

Příklad

- Okruhy $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot)$ jsou obory integrity.
- Okruh Gaussových celých čísel $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ je oborem integrity.
- Okruh $(\mathbb{Z}_4, +, \cdot)$ není obor integrity, narozdíl od $(\mathbb{Z}_5, +, \cdot)$.

Pokud neplatí vlastnost komutativity operace $\cdot$, hovoříme o nekomutativním okruhu (nebo pouze o okruhu). V dalším se ovšem omezíme pouze na okruhy komutativní.

Definice

Jestliže v komutativním okruhu R platí $c \cdot d = 0$ právě, když je alespoň jeden z prvků c a d nulový, pak okruh R nazýváme **oborem integrity**.

Příklad

- Okruhy $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot)$ jsou obory integrity.
- Okruh Gaussových celých čísel $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ je oborem integrity.
- Okruh $(\mathbb{Z}_4, +, \cdot)$ není obor integrity, narozdíl od $(\mathbb{Z}_5, +, \cdot)$.

Pokud neplatí vlastnost komutativity operace $\cdot$, hovoříme o nekomutativním okruhu (nebo pouze o okruhu). V dalším se ovšem omezíme pouze na okruhy komutativní.
Operaci $+$ budeme říkat **sčítání** a operaci $\cdot$ **násobení**. Navíc budeme vždy předpokládat existenci **jedničky** 1 pro operaci násobení, neutrálnímu prvku pro sčítání říkáme **nula**.

Základní vlastnosti operací v okruhu

V každém komutativním okruhu R s jedničkou platí následující vztahy (které nám jistě připadají samozřejmé u skalárů)

1. $0 \cdot c = c \cdot 0 = 0$ pro všechny $c \in R$,
2. $-c = (-1) \cdot c = c \cdot (-1)$ pro všechny $c \in R$,
3. $-(c \cdot d) = (-c) \cdot d = c \cdot (-d)$ pro všechny $c, d \in R$,
4. $a \cdot (b - c) = a \cdot b - a \cdot c$,

Dělitelnost v okruhu

Obecně říkáme, že $a \in R$ **dělí** $c \in R$, jestliže existuje b tak, že $a \cdot b = c$. Skutečnost že $c \in R$ je dělitelné $a \in R$ zapisujeme $a|c$.

Dělitelnost v okruhu

Obecně říkáme, že $a \in R$ **dělí** $c \in R$, jestliže existuje b tak, že $a \cdot b = c$. Skutečnost že $c \in R$ je dělitelné $a \in R$ zapisujeme $a|c$. Dodatečnou vlastností oboru integrity oproti obecnému okruhu je **neexistence netriviálních dělitelů nuly**. Okamžitě odtud také vyplývá jednoznačnost dělitelů:

Dělitelnost v okruhu

Obecně říkáme, že $a \in R$ **dělí** $c \in R$, jestliže existuje b tak, že $a \cdot b = c$. Skutečnost že $c \in R$ je dělitelné $a \in R$ zapisujeme $a|c$. Dodatečnou vlastností oboru integrity oproti obecnému okruhu je **neexistence netriviálních dělitelů nuly**. Okamžitě odtud také vyplývá jednoznačnost dělitelů:

Věta

Platí-li v oboru integrity $a = b \cdot c$ a $b \neq 0$, pak c je jednoznačně dáno volbou a, b.

Dělitelnost v okruhu

Obecně říkáme, že $a \in R$ **dělí** $c \in R$, jestliže existuje b tak, že $a \cdot b = c$. Skutečnost že $c \in R$ je dělitelné $a \in R$ zapisujeme $a|c$. Dodatečnou vlastností oboru integrity oproti obecnému okruhu je **neexistence netriviálních dělitelů nuly**. Okamžitě odtud také vyplývá jednoznačnost dělitelů:

Věta

Platí-li v oboru integrity $a = b \cdot c$ a $b \neq 0$, pak c je jednoznačně dáno volbou a, b.

Důkaz.

Pro $a = bc = bc'$ totiž platí $0 = b \cdot (c - c')$ a $b \neq 0$, proto $c = c'$. □

Dělitelé jedničky, tj. invertibilní prvky v R, se nazývají **jednotky**. Jednotky v komutativním okruhu vždy tvoří komutativní grupu. Netriviální (komutativní) okruh, ve kterém jsou všechny nenulové prvky invertibilní, se nazývá (komutativní) **těleso**.

Dělitelé jedničky, tj. invertibilní prvky v R, se nazývají **jednotky**.
Jednotky v komutativním okruhu vždy tvoří komutativní grupu.
Netriviální (komutativní) okruh, ve kterém jsou všechny nenulové prvky invertibilní, se nazývá (komutativní) **těleso**.
V české literatuře se někdy v případě komutativního tělesa můžete setkat s pojmenováním **pole** (z angl. *field*).

Typickým příkladem komutativních těles jsou číselné obory $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Dále pak všechny okruhy zbytkových tříd $\mathbb{Z}_p$ s prvočíselným p.

Typickým příkladem komutativních těles jsou číselné obory $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Dále pak všechny okruhy zbytkových tříd $\mathbb{Z}_p$ s prvočíselným p. Základním příkladem nekomutativního okruhu s jedničkou je množina $\mathrm{Mat}_k(R)$ všech čtvercových matic nad okruhem R s k řádky a sloupci. Jak jsme viděli dávno, není to ani obor integrity.

Typickým příkladem komutativních těles jsou číselné obory $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Dále pak všechny okruhy zbytkových tříd $\mathbb{Z}_p$ s prvočíselným p.
Základním příkladem nekomutativního okruhu s jedničkou je množina $\mathrm{Mat}_k(R)$ všech čtvercových matic nad okruhem R s k řádky a sloupci. Jak jsme viděli dávno, není to ani obor integrity.
Jako příklad nekomutativního okruhu, kde existují inverze k nenulovým prvkům (tzv. okruh s dělením) uveďme okruh kvaternionů

$$\mathbb{H} = \{a + b \cdot i + c \cdot j + d \cdot k;\ a, b, c, d \in \mathbb{R}\},$$

se sčítáním *po složkách* a násobením odvozeným ze základních relací

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

Obor integrity vs. těleso

Věta

Každý konečný obor integrity je těleso.

Důkaz.

Dokazuje se prostřednictvím homomorfismu $f : R \to R$, $f(x) = ax$ (je to injekce, proto surjekce, proto je R těleso (rozmyslete!). $\square$

Obor integrity vs. těleso

Věta

Každý konečný obor integrity je těleso.

Důkaz.

Dokazuje se prostřednictvím homomorfismu $f : R \to R$, $f(x) = ax$ (je to injekce, proto surjekce, proto je R těleso (rozmyslete!). $\square$

A co obráceně? Samozřejmě je každé těleso oborem integrity.

Obor integrity vs. těleso

Věta

Každý konečný obor integrity je těleso.

Důkaz.

Dokazuje se prostřednictvím homomorfismu $f : R \to R$, $f(x) = ax$ (je to injekce, proto surjekce, proto je R těleso (rozmyslete!). $\square$

A co obráceně? Samozřejmě je každé těleso oborem integrity.

Příklad

Zřejmě je např. $\mathbb{Z}$ obor integrity, který není těleso.

Polynomy

Polynomem rozumíme jakýkoliv konečný výraz, který lze poskládat ze známých konstantních prvků R a jedné neznámé proměnné pomocí operací sčítání a násobení:

Polynomy

Polynomem rozumíme jakýkoliv konečný výraz, který lze poskládat ze známých konstantních prvků R a jedné neznámé proměnné pomocí operací sčítání a násobení:

Definice

Nechť R je jakýkoliv (dále vždy) komutativní okruh skalárů. Polynomem nad R rozumíme konečný výraz

$$f(x) = \sum_{i=0}^{k} a_i x^i$$

kde $a_i \in R$, $i = 0, 1, \ldots, k$, jsou tzv. **koeficienty polynomu**. Je-li $a_k \neq 0$, říkáme, že $f(x)$ má **stupeň** k, píšeme $\mathrm{st}\, f = k$. Nulový polynom nemá stupeň, polynomy stupně nula jsou právě nenulové prvky v R, kterým říkáme konstantní polynomy.

Polynomy

Polynomem rozumíme jakýkoliv konečný výraz, který lze poskládat ze známých konstantních prvků R a jedné neznámé proměnné pomocí operací sčítání a násobení:

Definice

Nechť R je jakýkoliv (dále vždy) komutativní okruh skalárů. Polynomem nad R rozumíme konečný výraz

$$f(x) = \sum_{i=0}^{k} a_i x^i$$

kde $a_i \in R$, $i = 0, 1, \ldots, k$, jsou tzv. **koeficienty polynomu**. Je-li $a_k \neq 0$, říkáme, že $f(x)$ má **stupeň** k, píšeme $\operatorname{st} f = k$. Nulový polynom nemá stupeň, polynomy stupně nula jsou právě nenulové prvky v R, kterým říkáme konstantní polynomy.
Polynomy $f(x)$ a $g(x)$ jsou stejné, jestliže mají stejné koeficienty. Množinu všech polynomů nad okruhem R budeme značit $R[x]$.

Každý polynom zadává zobrazení $f : R \to R$, jehož hodnota vznikne dosazením hodnoty c za nezávislou proměnnou x, tj.

$$f(c) = a_0 + a_1 c + \cdots + a_k c^k.$$

Všimněme si, že konstantní polynomy odpovídají právě konstantním zobrazením.

Každý polynom zadává zobrazení $f : R \to R$, jehož hodnota vznikne dosazením hodnoty c za nezávislou proměnnou x, tj.

$$f(c) = a_0 + a_1 c + \cdots + a_k c^k.$$

Všimněme si, že konstantní polynomy odpovídají právě konstantním zobrazením.

Kořen polynomu $f(x)$ je takový prvek $c \in R$, pro který je $f(c) = 0 \in R$.

Každý polynom zadává zobrazení $f : R \to R$, jehož hodnota vznikne dosazením hodnoty c za nezávislou proměnnou x, tj.

$$f(c) = a_0 + a_1 c + \cdots + a_k c^k.$$

Všimněme si, že konstantní polynomy odpovídají právě konstantním zobrazením.

Kořen polynomu $f(x)$ je takový prvek $c \in R$, pro který je $f(c) = 0 \in R$.

Obecně se může stát, že různé polynomy definují stejná zobrazení. Např. polynom $x^2 + x \in \mathbb{Z}_2[x]$ zadává identicky nulové zobrazení. Obecněji, pro každý konečný okruh $R = \{a_0, a_1, \dots, a_k\}$ zadává polynom $f(x) = (x - a_0)(x - a_1)\dots(x - a_k)$ identicky nulové zobrazení. Zároveň ale platí tvrzení, které dokážeme zanedlouho:

Věta

Jestliže je R nekonečný okruh, pak dva polynomy $f(x)$ a $g(x)$ nad R jsou stejné právě tehdy, když jsou stejná příslušná zobrazení f a g.

Dva polynomy $f(x) = \sum_i a_i x^i$ a $g(x) = \sum_i b_i x^i$ umíme přirozeně také sčítat i násobit:

$$(f+g)(x) = (a_0+b_0) + (a_1+b_1)x + \cdots + (a_k+b_k)x^k$$
$$(f \cdot g)(x) = (a_0 b_0) + \cdots + (a_0 b_\ell + + \cdots + a_\ell b_0)x^\ell + \ldots$$

kde uvažujeme nulové koeficienty všude, kde v původním výrazu pro polynomy nenulové koeficienty nejsou a u sčítání nechť je k maximální ze stupňů f a g.

Tato definice vskutku odpovídá příslušným operacím sčítání a násobení hodnot zobrazení $f, g : R \to R$, díky vlastnostem *skalárů* v původním okruhu R.

Tato definice vskutku odpovídá příslušným operacím sčítání a násobení hodnot zobrazení $f, g : R \to R$, díky vlastnostem *skalárů* v původním okruhu R.

Přímo z definice vyplývá, že množina polynomů $R[x]$ nad komutativním okruhem s jedničkou je opět komutativním okruhem s jedničkou, přičemž jedničkou v $R[x]$ je opět jednička 1 v okruhu R vnímaná jako polynom stupně nula.

Lemma

Okruh polynomů nad oborem integrity je opět obor integrity.

Tato definice vskutku odpovídá příslušným operacím sčítání a násobení hodnot zobrazení $f, g : R \to R$, díky vlastnostem *skalárů* v původním okruhu R.

Přímo z definice vyplývá, že množina polynomů $R[x]$ nad komutativním okruhem s jedničkou je opět komutativním okruhem s jedničkou, přičemž jedničkou v $R[x]$ je opět jednička 1 v okruhu R vnímaná jako polynom stupně nula.

Lemma

Okruh polynomů nad oborem integrity je opět obor integrity.

Důkaz.

Máme ukázat, že v $R[x]$ mohou být netriviální dělitelé nuly pouze tehdy, jestliže jsou už v R. To je ale zřejmé z výrazu pro násobení polynomů. Jsou-li $f(x)$ a $g(x)$ polynomy stupně k a ℓ jako výše, pak koeficient u $x^{k+\ell}$ v součinu $f(x) \cdot g(x)$ je součin $a_k \cdot b_\ell$ a ten musí být nenulový, pokud nejsou dělitelé nuly v R. □

Formální mocninné řady

V Matematice III jsme pracovali s formálními mocninnými řadami a neformálně jsme prohlásili, že *s nimi můžeme provádět analogické operace jako s polynomy*. Nyní toto tvrzení můžeme zasadit do formálního algebraického kontextu:

Formální mocninné řady

V Matematice III jsme pracovali s formálními mocninnými řadami a neformálně jsme prohlásili, že *s nimi můžeme provádět analogické operace jako s polynomy*. Nyní toto tvrzení můžeme zasadit do formálního algebraického kontextu:

Definice

Nechť R je okruh skalárů. *Formální mocninou řadou* nad R rozumíme (obecně nekonečný) **formální** výraz $f(x) = \sum_{i=0}^{\infty} a_i x^i$, kde $a_i \in R$, $i = 0, 1, \ldots$, jsou tzv. **koeficienty řady**.

Formální mocninné řady

V Matematice III jsme pracovali s formálními mocninnými řadami a neformálně jsme prohlásili, že *s nimi můžeme provádět analogické operace jako s polynomy*. Nyní toto tvrzení můžeme zasadit do formálního algebraického kontextu:

Definice

Nechť R je okruh skalárů. *Formální mocninou řadou* nad R rozumíme (obecně nekonečný) **formální** výraz $f(x) = \sum_{i=0}^{\infty} a_i x^i$, kde $a_i \in R$, $i = 0, 1, \dots$, jsou tzv. **koeficienty řady**.

Snadno se ukáže, že s dříve definovanými operacemi sčítání a násobení tvoří formální mociné řady okruh, který značíme $R[[x]]$ (a jehož je $R[x]$ podokruhem).tvoří formální mociné řady okruh, který značíme $R[[x]]$ (a jehož je $R[x]$ podokruhem). Sami si zkuste rozmyslet, že invertibilními prvky tohoto okruhu jsou právě mocninné řady, které mají invertibilní absolutní člen.