Matematika IV – 2. přednáška
Základy teorie grup

Michal Bulant

Masarykova univerzita
Fakulta informatiky

2. 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*
- Jiří Rosický, *Algebra*, PřF MU, 2002.
- Peter J. Cameron. *Introduction to algebra*, Oxford University Press, 2001, 295 s. (Dostupné v knihovně PřF).

Plán přednášky

Opakování minulé přednášky

- **grupoid** $(G, \cdot)$ je množina G s binární operací $\cdot$

Opakování minulé přednášky

- **grupoid** $(G, \cdot)$ je množina G s binární operací $\cdot$
- **pologrupa** $(G, \cdot)$ je množina G s asociativní binární operací $\cdot$

Opakování minulé přednášky

- **grupoid** $(G, \cdot)$ je množina G s binární operací $\cdot$
- **pologrupa** $(G, \cdot)$ je množina G s asociativní binární operací $\cdot$
- **monoid** $(G, \cdot)$ je pologrupa $(G, \cdot)$ s jednotkovým (neutrálním) prvkem[1]

[1] Raději než jednotka používejme **jednotkový prvek** – důvod uvidíme později. Někdy se tomuto prvku rovněž říká jednička.

Opakování minulé přednášky

- **grupoid** $(G, \cdot)$ je množina G s binární operací $\cdot$
- **pologrupa** $(G, \cdot)$ je množina G s asociativní binární operací $\cdot$
- **monoid** $(G, \cdot)$ je pologrupa $(G, \cdot)$ s jednotkovým (neutrálním) prvkem[1]
- **grupa** $(G, \cdot)$ je monoid, ve kterém má každý prvek inverzi

[1] Raději než jednotka používejme **jednotkový prvek** – důvod uvidíme později. Někdy se tomuto prvku rovněž říká jednička.

Opakování minulé přednášky

- **grupoid** $(G, \cdot)$ je množina G s binární operací $\cdot$
- **pologrupa** $(G, \cdot)$ je množina G s asociativní binární operací $\cdot$
- **monoid** $(G, \cdot)$ je pologrupa $(G, \cdot)$ s jednotkovým (neutrálním) prvkem[1]
- **grupa** $(G, \cdot)$ je monoid, ve kterém má každý prvek inverzi
- **komutativní grupa** (grupoid, pologrupa, monoid apod.), je taková grupa (grupoid, ...), že operace $\cdot$ je komutativní. Často se v případě komutativních grup setkáte rovněž s pojmem **abelovská grupa**.

[1] Raději než jednotka používejme **jednotkový prvek** – důvod uvidíme později. Někdy se tomuto prvku rovněž říká jednička.

Permutace – opakování

- Množina bijekcí na množině M (konečné nebo nekonečné) tvoří spolu s operací skládání zobrazení grupu, tzv. **grupu permutací**.
- Je-li M konečná n prvková množina, pak tuto grupu značíme obvykle S_n nebo Σ_n, a platí $|\Sigma_n| = n!$.
- Každou permutaci lze zapsat jako součin nezávislých cyklů a jako součin (obecně nikoliv nezávislých) transpozic (cykly délky 2).
- Každá permutace má jednoznačně přiřazenou **sudou** nebo **lichou** paritu (podle počtu transpozic na něž se rozkládá nebo též podle počtu tzv. inverzí).

Rozklad na nezávislé cykly

Každá permutace σ rozkládá množinu M na disjunktní sjednocení maximálních invariantních podmnožin M_x, které dostaneme tak, že postupně vybíráme dosud nezpracované prvky $x \in M$ a do třídy rozkladu M_x přidáváme všechny akce iterací $\sigma^k(x)$, $k = 1, 2, \ldots,$ dokud není $\sigma^k(x) = x$.

Rozklad na nezávislé cykly

Každá permutace σ rozkládá množinu M na disjunktní sjednocení maximálních invariantních podmnožin M_x, které dostaneme tak, že postupně vybíráme dosud nezpracované prvky $x \in M$ a do třídy rozkladu M_x přidáváme všechny akce iterací $\sigma^k(x)$, $k = 1, 2, \ldots$, dokud není $\sigma^k(x) = x$.

Každou permutaci tak dostáváme jako složení jednodušších permutací, tzv. cyklů, které se chovají jako identická permutace vně M_x a tak jako σ na M_x.

Rozklad na nezávislé cykly

Každá permutace σ rozkládá množinu M na disjunktní sjednocení maximálních invariantních podmnožin M_x, které dostaneme tak, že postupně vybíráme dosud nezpracované prvky $x \in M$ a do třídy rozkladu M_x přidáváme všechny akce iterací $\sigma^k(x)$, $k = 1, 2, \ldots,$ dokud není $\sigma^k(x) = x$.

Každou permutaci tak dostáváme jako složení jednodušších permutací, tzv. cyklů, které se chovají jako identická permutace vně M_x a tak jako σ na M_x.

Pokud přitom očíslujeme prvky v M_x jako pořadí $(1, 2, \ldots, |M_x|)$ tak aby i odpovídalo $\sigma^i(x)$, pak je naše permutace prostým posunutím o jednu pozici v cyklu (tj. poslední prvek je zobrazen zpátky na první). Odtud název **cyklus**. Zjevně přitom tyto cykly komutují, takže je jedno, v jakém pořadí z nich permutaci σ složíme.

Nejjednodušší cykly jsou jednoprvkové pevné body permutace σ. Dvouprvkové $(x, \sigma(x))$, kde $\sigma(\sigma(x)) = x$ se nazývají **transpozice**.

Nejjednodušší cykly jsou jednoprvkové pevné body permutace σ. Dvouprvkové $(x, \sigma(x))$, kde $\sigma(\sigma(x)) = x$ se nazývají **transpozice**.

Každý cyklus zjevně můžeme poskládat z permutací sousedních prvků (necháme *probublat* první prvek nakonec) $\Rightarrow$ každou permutaci napsat jako složení transpozic sousedních prvků.
To, jestli potřebujeme sudý nebo lichý počet permutací, je na našich volbách nezávislé.

Nejjednodušší cykly jsou jednoprvkové pevné body permutace σ. Dvouprvkové $(x, \sigma(x))$, kde $\sigma(\sigma(x)) = x$ se nazývají **transpozice**.

Každý cyklus zjevně můžeme poskládat z permutací sousedních prvků (necháme *probublat* první prvek nakonec) $\Rightarrow$ každou permutaci napsat jako složení transpozic sousedních prvků.
To, jestli potřebujeme sudý nebo lichý počet permutací, je na našich volbách nezávislé.

Máme proto dobře definováno zobrazení $\mathrm{sgn} : \Sigma_m \to \mathbb{Z}_2 = \{\pm 1\}$, tzv. **paritu** permutace. Dokázali jsme si znovu tvrzení, která jsme již využívali při studiu determinantů:

Věta

Každá permutace konečné množiny je složením cyklů. Cyklus délky ℓ lze vyjádřit jako složení $\ell - 1$ transpozic. Parita cyklu délky ℓ je $(-1)^{\ell-1}$. Parita složení permutací je součinem parit jednotlivých permutací, tzn. že zobrazení sgn *převádí složení permutací $\sigma \circ \tau$ na součin* $\operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau$ *v komutativní grupě $\mathbb{Z}_2$ (nebo jinak vyjádřeno, v grupě $\{1, -1\}$ s obvyklým násobením.*

Příklad

Jsou dány permutace $f, g, h \in \Sigma_9$ předpisem

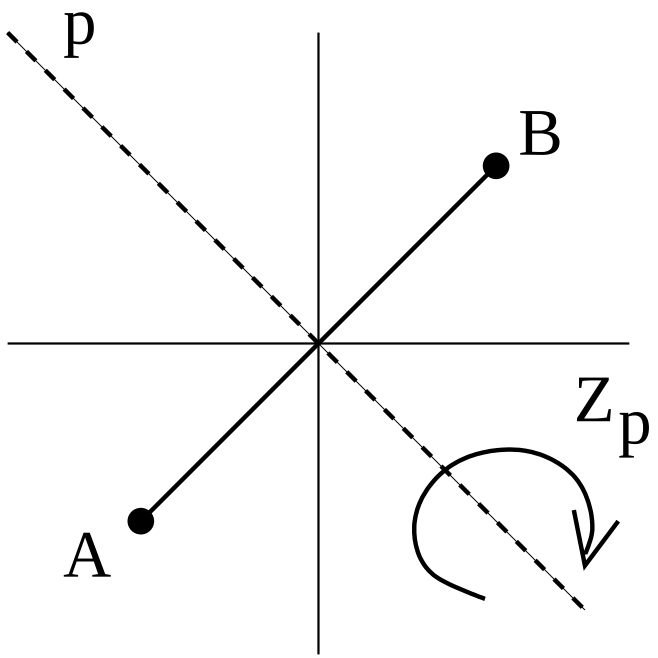
$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 5 & 2 & 3 & 7 & 1 & 9 & 8 \end{pmatrix},$$

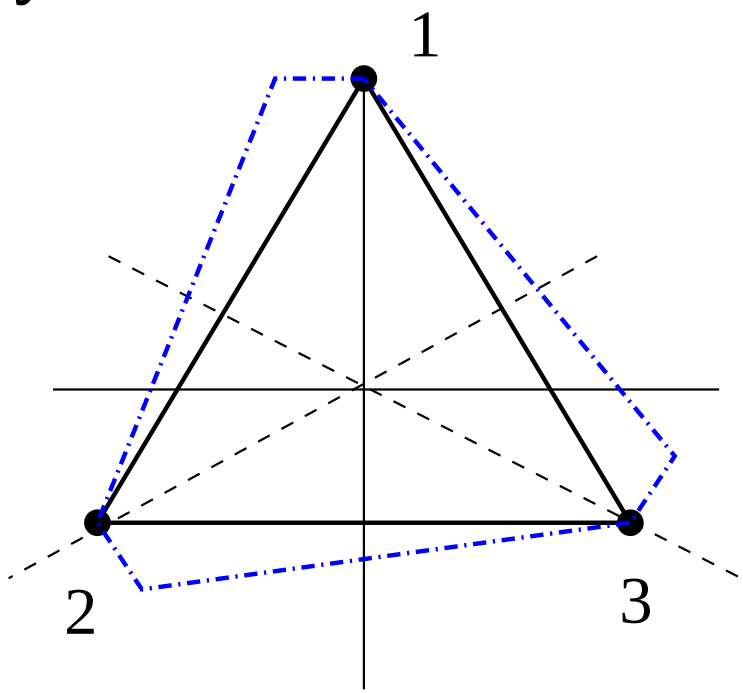
$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 6 & 5 & 1 & 9 & 7 & 8 & 3 & 4 \end{pmatrix}, \quad h = f \circ g.$$

1. Napište permutace f, g a h jako součin (tj. složení) navzájem nezávislých cyklů.
2. Určete paritu permutací f, g a h.
3. Spočtěte permutaci $f^{2011} \circ g^{2011}$ a napište ji jako součin navzájem nezávislých cyklů.
4. Určete počet inverzí permutace f.

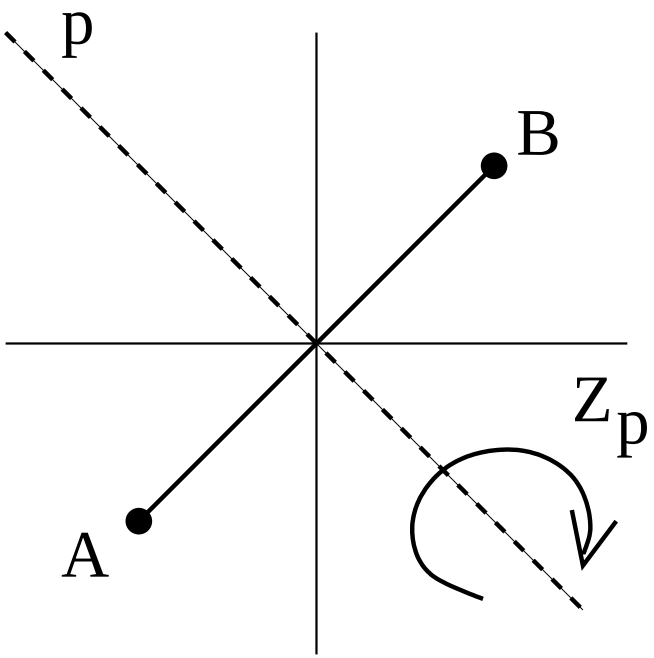
Plán přednášky

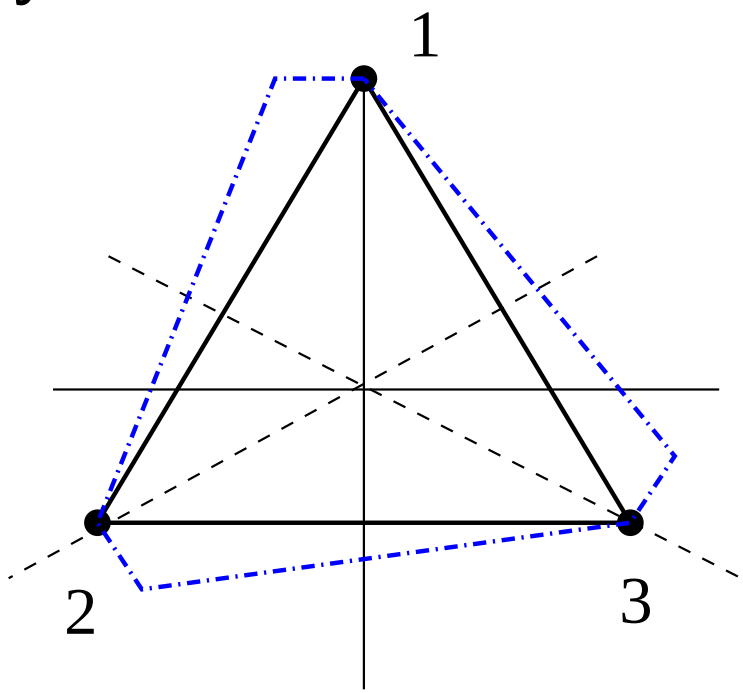
Uvažme ohraničený rovinný obrazec, např. rovnostranný trojúhelník. Ptáme se, **jak moc jsou symetrické?**





Uvažme ohraničený rovinný obrazec, např. rovnostranný trojúhelník. Ptáme se, **jak moc jsou symetrické?**





Tzn. vůči kterým trasformacím (zachovávajícím velikost) jsou invariantní? Všechny symetrie pevně zvoleného útvaru budou vždy tvořit grupu (většinou pouze s jediným prvkem, identickým zobrazením).

Symetrie rovnostranného trojúhelníku

Symetrií nacházíme několik: můžeme rotovat o $\pi/3$ nebo můžeme zrcadlit vůči osám stran.

Symetrie rovnostranného trojúhelníku

Symetrií nacházíme několik: můžeme rotovat o $\pi/3$ nebo můžeme zrcadlit vůči osám stran.

Abychom dostali celou grupu, musíme přidat všechna složení takovýchto transformací.
Víme z dřívějška, že složení dvou zrcadlení je vždy otočením. Složení takových zrcadlení v opačném pořadí dá otočení o stejný úhel, ale s opačnou orientací. V našem případě tedy zrcadlení kolem dvou různých os vygenerují postupnou opakovanou aplikací všechny symetrie, který bude dohromady šest.

Jestliže si umístíme trojúhelník v souřadnicích jako na obrázku, bude našich šest transformací zadáno maticemi

$$a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; b = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, \; c = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

$$d = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \; e = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, \; f = \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.$$

Sestavením tabulky pro násobení, tak jak jsme ji udělali pro grupu permutací Σ_3 obdržíme právě stejný výsledek.

$\cdot$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	a	f	d	e
c	c	a	b	e	f	d
d	d	e	f	a	b	c
e	e	f	d	c	a	b
f	f	d	e	b	c	a

Dihedrální grupy

Obdobně umíme nacházet grupy symetrií s k různými rotacemi a k zrcadleními. Stačí si k tomu vzít pravidelný k-úhelník. Takové grupy symetrií se často označují jako grupy D_{2k} a říká se jim **dihedrální grupy** řádu $2k$ (někdy též např $D(k)$).

Dihedrální grupy

Obdobně umíme nacházet grupy symetrií s k různými rotacemi a k zrcadleními. Stačí si k tomu vzít pravidelný k-úhelník. Takové grupy symetrií se často označují jako grupy D_{2k} a říká se jim **dihedrální grupy** řádu $2k$ (někdy též např $D(k)$).

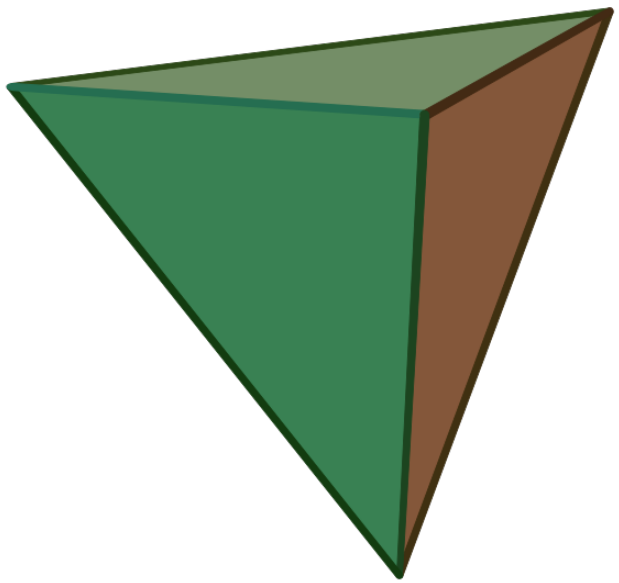
Tyto grupy jsou nekomutativní pro všechny $k \geq 3$.

Cyklické grupy

Stejně tak lze snadno najít obrazce, které mají pouze rotační symetrie a jde tedy o komutativní grupy, které se v chemii značí jako C_k. Říkáme jim **cyklické grupy** řádu k. K tomu postačí např. uvažovat pravidelný mnohoúhelník, u kterého nesymetricky ale pořád stejně pozměníme chování hran.

Příklad

- grupa symetrií čtverce D_8 má 8 prvků (4 osové symetrie, 3 netriviální rotace a identita) a lze ji chápat jako podgrupu Σ_4 (kam se zobrazují vrcholy?)
- grupa symetrií čtyřstěnu je celá Σ_4, pokud symetrie omezíme pouze na ty, které zachovávají orientaci, dostaneme podgrupu $A_4 \leq \Sigma_4$ sudých permutací.



Klasifikace symetrií

Věta

Nechť je M ohraničená množina v rovině $\mathbb{R}^2$. Pak grupa jejich symetrií je buď triviální nebo jedna z grup C_k, D_{2k}, s $k \geq 1$.

Podpologrupy a podgrupy

Definice

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 (resp. pologrupou) , nazýváme **podgrupa** (resp. podpologrupa) v $(A, \cdot)$.

Podpologrupy a podgrupy

Definice

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 (resp. pologrupou) , nazýváme **podgrupa** (resp. podpologrupa) v $(A, \cdot)$.

Věta

Nechť $(G, \circ)$ grupa. Pak $\emptyset \neq H \subseteq G$ je její podgrupa právě tehdy, když

1. $\forall a, b \in H : a \circ b \in H$;
2. $\forall a \in H : a^{-1} \in H$.

Podpologrupy a podgrupy

Definice

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 (resp. pologrupou) , nazýváme **podgrupa** (resp. podpologrupa) v $(A, \cdot)$.

Věta

Nechť $(G, \circ)$ grupa. Pak $\emptyset \neq H \subseteq G$ je její podgrupa právě tehdy, když

1. $\forall a, b \in H : a \circ b \in H$;
2. $\forall a \in H : a^{-1} \in H$.

Snadno se navíc vidí, že obě podmínky v předchozí větě lze shrnout do jediné: $\forall a, b \in H : a \circ b^{-1} \in H$.

Příklad

1. $\mathbb{Z}$ je podgrupa aditivních grup $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
2. Všechny podgrupy $(\mathbb{Z}, +)$ jsou vyčerpány množinami $m\mathbb{Z}$.
3. $(R^+, \cdot) \leq (R^*, \cdot)$.
4. Množina A_n všech sudých permutací na n-prvkové množině je podgrupou Σ_n.
5. $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$.

Podgrupa generovaná množinou

Jsou-li K, L podgrupy grupy G, je zřejmě i jejich průnik (nikoliv ovšem sjednocení!) podgrupou G. Totéž zřejmě dokonce platí i pro libovolný (třeba nekonečný) systém podmnožin.

Podgrupa generovaná množinou

Jsou-li K, L podgrupy grupy G, je zřejmě i jejich průnik (nikoliv ovšem sjednocení!) podgrupou G. Totéž zřejmě dokonce platí i pro libovolný (třeba nekonečný) systém podmnožin.
Odtud plyne následující definice:

Definice

Je-li M libovolná podmnožina grupy G, pak

$$\langle M \rangle = \bigcap_{M \subseteq H \leq G} H$$

je nejmenší (ve smyslu množinové inkluze) podgrupa G obsahující množinu M a nazývá se podgrupa generovaná množinou M.

Podgrupa generovaná množinou

Jsou-li K, L podgrupy grupy G, je zřejmě i jejich průnik (nikoliv ovšem sjednocení!) podgrupou G. Totéž zřejmě dokonce platí i pro libovolný (třeba nekonečný) systém podmnožin.
Odtud plyne následující definice:

Definice

Je-li M libovolná podmnožina grupy G, pak

$$\langle M \rangle = \bigcap_{M \subseteq H \leq G} H$$

je nejmenší (ve smyslu množinové inkluze) podgrupa G obsahující množinu M a nazývá se podgrupa generovaná množinou M.
Grupa G se nazývá **cyklická**, pokud ji lze vygenerovat některým jejím prvkem, tj. existuje $a \in G$ tak, že $G = \langle a \rangle = \langle \{a\} \rangle$.

Příklad

- $\mathbb{Z} = \langle 1 \rangle$.

Příklad

- $\mathbb{Z} = \langle 1 \rangle$.
- V $(\mathbb{Z}_m, +)$ je $\mathbb{Z}_m = \langle [1]_m \rangle$.

Příklad

- $\mathbb{Z} = \langle 1 \rangle$.
- V $(\mathbb{Z}_m, +)$ je $\mathbb{Z}_m = \langle [1]_m \rangle$.
- Podobně $(\mathbb{Z}_8, +) = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$.

Příklad

- $\mathbb{Z} = \langle 1 \rangle$.
- V $(\mathbb{Z}_m, +)$ je $\mathbb{Z}_m = \langle [1]_m \rangle$.
- Podobně $(\mathbb{Z}_8, +) = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$.
- $(\mathbb{Z}_7^\times, \cdot) = \langle 3 \rangle = \langle 5 \rangle$.

Příklad

- $\mathbb{Z} = \langle 1 \rangle$.
- V $(\mathbb{Z}_m, +)$ je $\mathbb{Z}_m = \langle [1]_m \rangle$.
- Podobně $(\mathbb{Z}_8, +) = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$.
- $(\mathbb{Z}_7^\times, \cdot) = \langle 3 \rangle = \langle 5 \rangle$.
- $(\mathbb{Z}_8^\times, \cdot)$ není cyklická.

Příklad

- $\mathbb{Z} = \langle 1 \rangle$.
- V $(\mathbb{Z}_m, +)$ je $\mathbb{Z}_m = \langle [1]_m \rangle$.
- Podobně $(\mathbb{Z}_8, +) = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$.
- $(\mathbb{Z}_7^\times, \cdot) = \langle 3 \rangle = \langle 5 \rangle$.
- $(\mathbb{Z}_8^\times, \cdot)$ není cyklická.
- $D_{2n} = \langle r, s \rangle$.

Homomorfismus

Definice

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

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

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:

Věta

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

1. *obraz neutrálního prvku $e_G \in G$ je neutrální prvek v H*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Věta

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

1. *obraz neutrálního prvku $e_G \in G$ je neutrální prvek v H*
2. *obraz inverze k prvku je inverzí obrazu, tj. $f(a^{-1}) = f(a)^{-1}$.*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Věta

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

1. *obraz neutrálního prvku $e_G \in G$ je neutrální prvek v H*
2. *obraz inverze k prvku je inverzí obrazu, tj. $f(a^{-1}) = f(a)^{-1}$.*
3. *obraz podgrupy $K \leq G$ je podgrupa $f(K) \leq H$.*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Věta

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

1. *obraz neutrálního prvku $e_G \in G$ je neutrální prvek v H*
2. *obraz inverze k prvku je inverzí obrazu, tj. $f(a^{-1}) = f(a)^{-1}$.*
3. *obraz podgrupy $K \leq G$ je podgrupa $f(K) \leq H$.*
4. *vzorem $f^{-1}(K) \leq G$ podgrupy $K \leq H$ je podgrupa.*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Věta

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

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

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Věta

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

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

Definice

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

Poznámka

Podobně jako v teorii grafů jsou i v algebře izomorfní objekty nerozlišitelné.

Definice

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

Poznámka

Podobně jako v teorii grafů jsou i v algebře izomorfní objekty nerozlišitelné.

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

Cyklické grupy ještě jednou

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 ještě jednou

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 ještě jednou

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 ještě jednou

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?

Příklad

(1) Pro každou grupu permutací $G = \Sigma_n$ jsme definovali zobrazení sgn : $(\Sigma_n, \circ) \to (\mathbb{Z}_2, +)$ přiřazující permutaci její paritu (lichá=1, sudá=0). Jde o homomorfismus grup $(\Sigma_n, \circ)$ a $(\mathbb{Z}_2, +)$. Jádrem tohoto homomorfismu jsou permutace se sudou paritou (tj. tzv. alterrnující grupa A_n).

Příklad

(1) Pro každou grupu permutací $G = \Sigma_n$ jsme definovali zobrazení $\text{sgn} : (\Sigma_n, \circ) \to (\mathbb{Z}_2, +)$ přiřazující permutaci její paritu (lichá=1, sudá=0). Jde o homomorfismus grup $(\Sigma_n, \circ)$ a $(\mathbb{Z}_2, +)$. Jádrem tohoto homomorfismu jsou permutace se sudou paritou (tj. tzv. alterrnující grupa A_n).
(2) Grupa symetrií rovnostranného trojúhelníka D_6 je izomorfní s grupou permutací Σ_3. Stačí zvolit realizaci Σ_3 tak, že za množinu tří prvků pro permutace vezmeme vrcholy trojúhelníka a jednotlivým symetriím přiřadíme permutace těchto vrcholů, které vyvolají.

Příklad

(1) Pro každou grupu permutací $G = \Sigma_n$ jsme definovali zobrazení $\text{sgn} : (\Sigma_n, \circ) \to (\mathbb{Z}_2, +)$ přiřazující permutaci její paritu (lichá=1, sudá=0). Jde o homomorfismus grup $(\Sigma_n, \circ)$ a $(\mathbb{Z}_2, +)$. Jádrem tohoto homomorfismu jsou permutace se sudou paritou (tj. tzv. alterrnující grupa A_n).
(2) Grupa symetrií rovnostranného trojúhelníka D_6 je izomorfní s grupou permutací Σ_3. Stačí zvolit 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 (co je jeho inverzí?). Pro komplexní čísla dostáváme netriviální jádro $\{2k\pi i;\ k \in \mathbb{Z}\}$.

Příklad

(4) Determinant matice je zobrazením, které každé matici skalárů z $\mathbb{K}$ přiřazuje nějaký skalár z $\mathbb{K}$ (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 $\det : G \to \mathbb{K} \setminus \{0\}$ multiplikativním homomorfismem grup.

Příklad

(4) Determinant matice je zobrazením, které každé matici skalárů z $\mathbb{K}$ přiřazuje nějaký skalár z $\mathbb{K}$ (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 $\det : G \to \mathbb{K} \setminus \{0\}$ multiplikativním homomorfismem grup.
(5) 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 $\frac{2\pi}{k}$.
(6) Multiplikativní grupa invertibilních zbytkových tříd $(\mathbb{Z}_p^\times, \cdot)$ je izomorfní aditivní grupě $(Z_{p-1}, +)$ (plyne z cykličnosti grupy – později snad dokážeme).

(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

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

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:

$$[0]_6 \mapsto ([0]_2, [0]_3),\ [1]_6 \mapsto ([1]_2, [2]_3)$$
$$[2]_6 \mapsto ([0]_2, [1]_3),\ [3]_6 \mapsto ([1]_2, [0]_3)$$
$$[4]_6 \mapsto ([0]_2, [2]_3),\ [5]_6 \mapsto ([1]_2, [1]_3)$$

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:

$$[0]_6 \mapsto ([0]_2, [0]_3),\ [1]_6 \mapsto ([1]_2, [2]_3)$$
$$[2]_6 \mapsto ([0]_2, [1]_3),\ [3]_6 \mapsto ([1]_2, [0]_3)$$
$$[4]_6 \mapsto ([0]_2, [2]_3),\ [5]_6 \mapsto ([1]_2, [1]_3)$$

(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 . 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?).

[3] 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:[3]

[3] 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:[3] 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. $v_i n_i \equiv 1 \pmod{m_i}$.

[3] 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:[3] 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 $a = \sum_i a_i v_i n_i$.

[3] 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.