Diskrétní matematika B – 6. týden
Základy teorie grup

Michal Bulant

Masarykova univerzita
Fakulta informatiky

jaro 2014

Obsah přednášky

Doporučené zdroje

- Jan Slovák, Martin Panák, Michal Bulant, *Matematika drsně a svižně*, MU Brno, 2013, 774 s. (též jako 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).
- Nathan Carter. *Visual Group Theory*, The Mathematical Association of America, 2009, 297 s. (Viz web).
- Ask a silly question ... , *Why do I need to learn this stuff?* (Abstruse Goose).

Chceme abstraktně pracovat s objekty a se situacemi, ve kterých je možné rovnice

$$a \cdot x = b$$

vždy jednoznačně řešit (tak jako u lineárních rovnic jsou objekty a a b dány, zatímco x hledáme).
Jde o tzv. **teorii grup**. Všimněme si, že zatím nic nevíme o povaze objektů, ani co znamená ta „tečka“ v rovnici.

Struktury s jednou operací

- **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**.

Poznámka k nejednoznačnosti terminologie (multiplikativní vs. aditivní)

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

Příklad

1. Přirozená čísla (s nulou) $\mathbb{N}_0 = \{0, 1, 2, \dots\}$, spolu s kteroukoliv z operací sčítání a násobení jsou asociativní a komutativní pologrupa s jednotkovým prvkem, neexistují v ní ale inverzní prvky.
2. Celá čísla $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ tvoří grupoid vůči kterékoliv z operací sčítání, odčítání, násobení. Jsou dokonce komutativní grupou vzhledem ke sčítání, jsou však jen komutativní pologrupou vůči násobení (neexistují inverze k prvkům $a \neq \pm 1$). Operace odčítání není ani asociativní (např. $(5-3)-2 = 0 \neq 5-(3-2) = 4$). Všimněte si také, že pro odečítání je nula pravý neutrální prvek, ne však levý. Dokonce v tomto případě levý neutrální prvek neexistuje.
3. Racionální čísla $\mathbb{Q}$ jsou komutativní grupou vzhledem ke sčítání (celá čísla spolu se sčítáním jsou jejich podgrupou) a nenulová racionální čísla jsou kom. grupou vůči násobení.

Příklad (pokračování)

1. Pro $k \in \mathbb{N}$, množina všech k-tých odmocnin z jedničky, tj. množina $\{z \in \mathbb{C};\ z^k = 1\}$ je konečná grupa vůči násobení komplexních čísel. Např. pro $k = 2$ dostaneme grupu $\{-1, 1\}$ se dvěma prvky, které jsou oba samy sobě inverzí, zatímco pro $k = 4$ dostáváme grupu $G = \{1, i, -1, -i\}$.
2. Množina Mat_n všech čtvercových matic je (nekomutativní) pologrupa vzhledem k násobení matic a komutativní grupa vzhledem ke sčítání matic.
3. Množina všech lineárních zobrazení $\mathrm{Hom}(V, V)$ na vektorovém prostoru je pologrupa vzhledem ke skládání zobrazení a komutativní grupa vzhledem ke sčítání zobrazení.
4. V obou předchozích příkladech, podmnožina invertibilních objektů uvažované (multiplikativní) pologrupy tvoří grupu. V případě matic jde o tzv. grupu invertibilních (tj. regulárních) matic, ve druhém o grupu lineárních transformací vektorového prostoru (tj. invertibilních lineárních zobrazení).

Příliš stručná exkurze do univerzální algebry

Bystří studenti algebry si brzy povšimnou, že se mnohé pojmy a důkazy opakují pro různé situace. Skutečně se ukazuje, že základní pojmy a tvrzení je možné zavést a dokázat obecně pomocí univerzální algebry (příp. ještě obecněji v tzv. teorii kategorií).
Pro informatiky, kteří mají za sebou funkcionální programování (příp. práci s objekty, metodami, šablonami apod.), by to možná mohl být přirozený postup, my však na to bohužel nemáme dostatek času.
Pro všechny *struktury* (pologrupy, grupy, okruhy, tělesa, vektorové prostory, svazy, moduly atd.) lze definovat několik základních pojmů analogickým způsobem:

- **pod**struktury
- **homomorfismy** mezi strukturami stejného typu
- **součiny** struktur téhož typu

Grupy permutací

Zpravidla grupy a pologrupy potkáváme jako množiny zobrazení na pevně dané množině M, které jsou uzavřeny vůči skládání zobrazení. Často si ale tuto skutečnost přímo neuvědomujeme. Na každé konečné množině M, s $m = |M| \in \mathbb{N}$ prvky máme k dispozici m^m možných definic zobrazení (každý z m prvků můžeme zobrazit na kterýkoliv v M) a všechna taková zobrazení umíme skládat.

Pokud chceme, aby existovala k zobrazení $\alpha : M \to M$ jeho inverze α^{-1}, musí být α bijekcí. Složením dvou bijekcí vznikne opět bijekce a proto podmnožina S_m všech bijekcí na množině M o m prvcích je grupa. Říkáme jí **grupa permutací** na m prvcích.

Název **grupa permutací** přitom uvádí jinou souvislost, kdy místo bijekcí na konečné množině vnímáme permutace jako přerovnání rozlišitelných prvků. Potkávali jsme se s ní např. při studiu determinantů.

V grupě permutací S_3 na číslech $\{1, 2, 3\}$ si třeba označíme jednotlivá pořadí

$$a = (1, 2, 3),\ b = (2, 3, 1),\ c = (3, 1, 2),$$
$$d = (1, 3, 2),\ e = (3, 2, 1),\ f = (2, 1, 3).$$

Skládání našich permutací je pak zadáno tabulkou

$\cdot$	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

Všimněme si podstatného rozdílu mezi permutacemi a, b a c a dalšími třemi. Ty první tři tvoří tzv. **cyklus** generovaný prvkem b nebo prvkem c:

$$b^2 = c,\ b^3 = a,\ c^2 = b,\ c^3 = a$$

a samy o sobě jsou tyto tři prvky komutativní podgrupou. V ní a je neutrální prvek a b s c jsou vzájemně inverzní. Je tedy tato podgrupa *stejná* jako je grupa $\mathbb{Z}_3$ zbytkových tříd celých čísel modulo 3, resp. jako grupa třetích odmocnin z jedničky z jednoho z předchozích příkladů.

Další tři prvky jsou samy sobě inverzí a každý z nich je tedy společně s neutrálním prvkem a podgrupou *stejnou* jako je $\mathbb{Z}_2$. Říkáme, že b a c jsou **prvky řádu** 3, zatímco prvky d, e a f jsou řádu 2.

Obdobně se chovají všechny grupy permutací S_m.
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 $\sigma^k(x)$, $k = 1, 2, \dots,$ 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 $(1, 2, \dots, |M_x|)$ 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**.

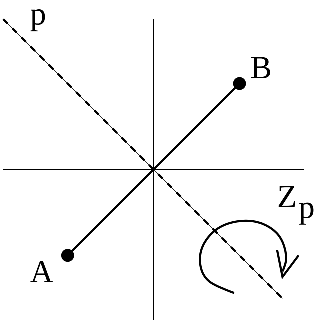
Každý cyklus zjevně můžeme poskládat z permutací sousedních prvků (necháme *probublat* první prvek nakonec) $\Rightarrow$ každou permutaci lze napsat jako složení transpozic.
To, jestli potřebujeme sudý nebo lichý počet permutací, je na našich volbách nezávislé.

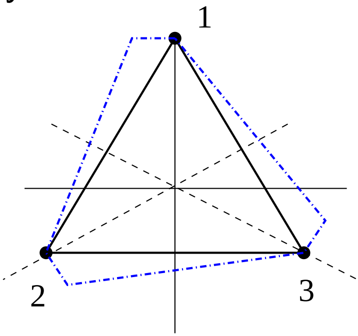
Máme proto dobře definováno zobrazení sgn : $S_m \to \mathbb{Z}_2 = \{\pm 1\}$, tzv. **paritu** permutace. Dokázali jsme si znovu tvrzení, která jsme již využívali při studiu determinantů:

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 z nich, tzn. že zobrazení* sgn *převádí složení permutací* $\sigma \circ \tau$ *na součin* $\operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau$ *v komutativní grupě* $\mathbb{Z}_2$*.*

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.

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, kterých 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 S_3 obdržíme právě stejný výsledek.

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. $D(k)$).

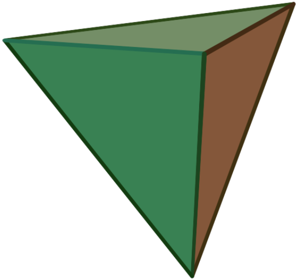
Tyto grupy jsou nekomutativní pro všechny $k \geq 3$.

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 S_4 (kam se zobrazují vrcholy?)
- grupa symetrií čtyřstěnu je celá S_4, pokud symetrie omezíme pouze na ty, které zachovávají orientaci, dostaneme podgrupu $A_4 \leq S_4$ 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 $(A, \cdot)$.

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

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

Příklad

(1) Pro každou grupu permutací $G = S_n$ jsme definovali zobrazení $\mathrm{sgn} : (S_n, \circ) \to (\mathbb{Z}_2, +)$ přiřazující permutaci její paritu (lichá=1, sudá=0). Jde o homomorfismus grup $(S_n, \circ)$ a $(\mathbb{Z}_2, +)$. Jádrem tohoto homomorfismu jsou permutace se sudou paritou.
(2) Grupa symetrií rovnostranného trojúhelníka D_6 je izomorfní s grupou permutací S_3. Stačí zvolit realizaci S_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.

(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 $(\mathbb{Z}_{p-1}, +)$ (plyne mj. z věty o existenci primitivního kořene).