

Základní pojmy teorie grup

①

Def. Grupa je množina G s binární operací (násobení, sčítání apod.) pro kterou platí: 1) G je uzavřená vůči $\cdot$, tj. $a \cdot b \in G$ pro $a, b \in G$

2) asociativita: pro $\forall a, b, c \in G$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

3) existuje identita $e \in G$: (též jednotkový či neutrální prvek)
 $e \cdot a = e \cdot a = a$ pro $\forall a \in G$

4) inverzní prvek: pro $\forall a \in G$ $\exists a^{-1} \in G$: $a^{-1} \cdot a = a \cdot a^{-1} = e$

- grupovou (binární) operaci často nijak neznámíme, tj. píšeme ab
- identita e a inverzní prvek a^{-1} jsou jednoznačné

Dk sporem: 1) necht' e_1 a e_2 jsou různé identity, pak

$$e_1 e_2 = e_1 \text{ a zároveň } e_1 e_2 = e_2 \Rightarrow e_1 = e_2 \text{ spor}$$

2) necht' b_1 a b_2 jsou inverzní k a^{-1} , pak

$$b_1 a = e = b_2 a \mid \cdot a^{-1} \Rightarrow b_1 = b_2 \text{ spor}$$

- zřejmě $(a^{-1})^{-1} = a$ a $(ab)^{-1} = b^{-1} a^{-1}$, neboť $(ab)(ab)^{-1} = ab b^{-1} a^{-1} = e$

- pozn: v definici grupy lze zmínit axiomy např. jen na levé násobení, ale výše uvedené je standardní def.

• počet prvků grupy = řád grupy, značení $\#G$ nebo $|G|$

- konečný nebo nekonečný - diskrétní grupy, např.
krytografické
- spojité - především Lieovy (později)

též po částech spojité (též smíšené)

např. $O(3)$ má dvě oddělené části

vlastní ($\det=1$) a nevlastní ($\det=-1$) rotace

• mluvíme o abstraktní grupě (daná např. vztahy mezi prvky nebo multiplikativní tabulkou)

a jejich realizacích, které jsou ale z matematického

hlediska totéž (stejná struktura, říkáme, že

jsou tyto realizace izomorfní)

Def: Izomorfismus dvou grup je vzájemně jednoznačné zobrazení

$\varphi: G_1 \rightarrow G_2$, které zachovává grupovou operaci,

tj. pokud $\varphi: a_1 \mapsto a_2$
a $\varphi: b_1 \mapsto b_2$ pak $\varphi: a_1 b_1 \mapsto a_2 b_2$

neboli $\varphi(a_1 b_1) = \varphi(a_1) \varphi(b_1)$

- značíme $G_1 \sim G_2$ (G_1 je izomorfní s G_2)

Př: Nejjednodušší (kromě triviální jednoprvkové grupy $\{e\}$) konečnou grupou je dvouprvková grupa $\{e, a\}$, pro kterou platí $a^2 = e$, což můžeme zapsat pomocí multiplikační tabulky

$$\begin{array}{c|cc} & e & a \\ \hline e & ee & ea \\ a & ae & aa \end{array} \Rightarrow \begin{array}{c|c} e & a \\ \hline a & e=a^2 \end{array}$$

má mnoho realizací:

1) $(\{1, -1\}, \cdot) = G$ (násobení 1 a -1)

2) $(\{0, 1\}, + \text{ mod } 2) = \mathbb{Z}_2$

4) grupa permutací
2-prvkové množiny

$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$, $\begin{matrix} \text{slučování} \\ \text{permutací} \end{matrix}$
 $\begin{matrix} \nearrow \\ \text{identická} \\ \text{permutace} \end{matrix}$ $\begin{matrix} \uparrow \\ \text{transpozice 1 a 2} \end{matrix}$

3) bodové grupy
 $C_5 = \{E, \sigma\}$ (v pevných látkách značena m)

$\begin{matrix} \nearrow & \nwarrow \\ \text{identita} & \text{zrcadlení} \end{matrix}$
 $C_1 = \{E, i\}$ (též π)
 $\begin{matrix} \uparrow \\ \text{inverze} \end{matrix}$

$C_2 = \{E, C_2\}$ (též 2)
 $\begin{matrix} \nearrow \\ \text{rotace o } 180^\circ \end{matrix}$

5) maticové realizace, např.

$M = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$, $\begin{matrix} \text{násobení} \\ \text{matic} \end{matrix}$

$\nwarrow$
zrcadlení roviny (x, y) podél $x=y$

(více o bodových grupách viz Cvičení: Bodové grupy)

- ve skutečnosti mnoho dalších realizací, ale všechny izomorfní

$$G \sim \mathbb{Z}_2 \sim C_5 \sim C_1 \sim C_2 \sim S_2 \sim M$$

Def: Grupa G je komutativní (též abelovská), pokud pro $\forall a, b \in G: ab = ba$.

Př: všechny tzv. cyklické grupy dané vztahem $a^n = e$ pro jisté n jsou komutativní. V tomto případě $n = \#G$ a $G = \{e, a, a^2, \dots, a^{n-1}\}$
 $\begin{matrix} \text{n různých prvků} \end{matrix}$

- obvykle se vyskytují jako podgrupy větších grup

neboť každý prvek konečné grupy $a \in G$ generuje

cyklickou podgrupu (viz níže), neboť $a^n = e$ pro jisté n .

Věta o přeuspořádání (rearrangement theorem)

③

VoP: Pro libovolný fixní prvek $g \in G$ obsahují množiny

$$L_g(G) = \{gh \mid h \in G\} \quad \text{levé posunutí}$$

$$R_g(G) = \{hg \mid h \in G\} \quad \text{právé posunutí}$$

všechny prvky grupy G a každý právě jednou.

Dk: 1) Uvažujme lib. prvek $h' \in G$ a vynásobíme ho $\tilde{g}^{-1}h' = h$,
pak ale $gh = g(\tilde{g}^{-1}h') = h' \in L_g(G)$ (určitě $\tilde{g}^{-1} \in G$ ale ji násobit)

toto dle předpokladu
patří do $L_g(G)$

takže každý prvek z G patří do $L_g(G)$ a obdobně pro $R_g(G)$.

2) jednoznačnost dokážeme sporem

necht' $\exists h_1 \neq h_2 : gh_1 = gh_2$, ovšem aplikací $\tilde{g}^{-1}$ zleva

dostaneme $h_1 = h_2$, což je spor. c.b.d
(což bylo dokázáno)

- druhá část důkazu je důležitá v případě nekonečných grup

- z VoP plyne, že multiplikační tabulka konečné grupy

musí mít na každém řádku a v každém sloupci

všechny prvky grupy, jen zpermutované,

ovšem pozor! toto není dostatečná podmínka, aby

určitá tabulka definovala grupu

(viz protipříklad pro $\#G = 5$)

Pr: 3-prvková grupa je jen jedna - cyklická $a^3 = e$

$$\begin{array}{c|cc} e & a & b \\ a & b & e \\ b & e & a \end{array} \quad \text{zde nemůže být } e, \text{ ani } a \Rightarrow \text{jediná možnost } b$$

$$\sim C_3 = \{E, C_3, C_3^2\}, \text{ kde } C_3 \text{ je rotace o } \frac{2\pi}{3} = 120^\circ$$

4-prvkové grupy jsou dvě (přesvědčte se, že další není)

cyklická

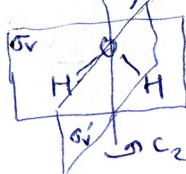
$$\begin{array}{c|cccc} e & a & b & c \\ a & b & c & e \\ b & c & e & a \\ c & e & a & b \end{array} \quad \sim C_4 = \{E, C_4, C_2, C_4^3\}$$

otočení
o $\frac{2\pi}{4} = 90^\circ$

4-grupa (komutativní) roviny zrcadlení

$$\sim C_{2v} = \{E, C_2, \sigma_v, \sigma_v'\}$$

(molekula vody
má tuto symetrii)



ale i $\sim D_2 \sim C_{2h}$
(později)

Př: 5-prvková pouze jedna (pro každé prvočíslo je pouze cyklická)

e	a	b	c	d
a	b	c	d	e
b	c	d	e	a
c	d	e	a	b
d	e	a	b	c

$$a^5 = e$$

ovšem např.

není grupou

neboť

$$(ab)d = cd = a$$

$$\text{ale } a(bd) = ac = d$$

a není tedy splněna asociativita

e	a	b	c	d
a	e	c	d	b
b	d	e	a	c
c	b	d	e	a
d	c	a	b	e

(4)

• Podgrupy

Def: Podgrupa H grupy G (značeno $H \leq G$) je podmnožina grupy G , která je sama o sobě grupou se stejnou binární operací.

Př: cyklická grupa C_4 má podgrupy $\{E\}$ a $\{E, C_2\}$ (a C_4)

4-grupa C_{2v} má podgrupy $\{E\}$, $\{E, C_2\}$, $\{E, \sigma_v\}$ a $\{E, \sigma_v'\}$ (a C_{2v})

ovšem např. $\{E, \sigma_v, \sigma_v'\}$ není podgrupou: $\sigma_v \sigma_v' = C_2$

Věta: Neprázdná podmnožina $H \subset G$ je podgrupou G , právě když $gh^{-1} \in H$ pro všechny $g, h \in H$.

Dk: $\Rightarrow$ zřejmé ($h^{-1} \in H \Rightarrow gh^{-1} \in H$)

$\Leftarrow$ ukážeme, že pak H splňuje axiomy grupy:

1) pokud $g \in H$, pak $gg^{-1} = e \in H$

2) položíme $g = e \in H$, pak $eh^{-1} \in H \Rightarrow h^{-1} \in H$ pro $h \in H$

3) víme, že $h^{-1} \in H \Rightarrow g(h^{-1})^{-1} = gh \in H$ pro $g, h \in H$ c.b.d.

Věta: Průnik dvou podgrup H_1 a H_2 grupy G je opět podgrupou G .

Dk: plyne z předchozí věty, neboť jsou-li H_1 a H_2 podgrupy,

pak $e \in H_1 \cap H_2$ (tj. jde o neprázdnou podmnožinu G)

a pokud $g, h \in H_1 \cap H_2$, pak určitě (jde o podgrupy) $gh^{-1} \in H_1 \cap H_2$ c.b.d.

Věta: Pro každý prvek konečné grupy G existuje přirozené n takové, že $g^n = e$. n se nazývá řád prvku.

Dk: V konečné grupě musí existovat $p > q$ takové, že $g^p = g^q$.

Položíme $p = q + n$, pak $g^{q+n} = g^q g^n = g^q \Rightarrow g^n = e$. c.b.d.

Generátory grupy a podgrupa (u Lieových grup budou generátory něco jiného, prvky Lieovy algebry)

- pokud je n řád prvku g , pak $\{e, g, \dots, g^{n-1}\}$ tvoří podgrupu G generovanou prvkem g , která je cyklická

- obecněji dostaneme podgrupu grupy G z více prvků $g_1, \dots, g_n \in G$ vezmeme-li všechny součiny těchto prvků a jejich inverzí (u konečných grup stačí součiny, neboť pokud $g_i^n = e$, pak $g_i^{-1} = g_i^{n-1}$, ovšem u nekonečných grup takto inverzní prvek obecně nedostaneme)

Věta: Pro libovolnou podmnožinu $X \subset G$ existuje nejmenší podgrupa G obsahující X . Její prvky tvoří všechny konečné součiny prvků z X a jejich inverzí.

Důk: Necht' $H_i \leq G$ jsou všechny podgrupy obsahující $X \subset H_i$ proti Pak $S = \bigcap H_i \leq G$ je (dle věty o průniku dvou podgrup) též podgrupou grupy G a zřejmě nejmenší takovou.

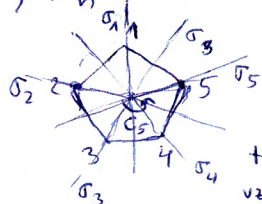
- značíme $S = \langle X \rangle$ = podgrupa generovaná množinou X
- pokud $\langle X \rangle = G$, říkáme, že X generuje grupu G
- nejmenší množinu prvků, které generují celou grupu, nazýváme generátory grupy, u reprezentací pak stačí najít repr. generátorů, zbytek

Př: např. maticovým násobením

1) $\langle \emptyset \rangle = \{e\}$ ← nejmenší podgrupa

2) $\langle g \rangle = \{e, g, \dots, g^{n-1}\}$ - cyklická podgrupa pro prvek řádu n

3) $D_n = \langle \{C_n, \sigma_1\} \rangle$ - grupa symetrií pravidelného n -úhelníku v rovině



- stačí dva prvky a vztahy

$$\left\{ \begin{array}{l} C_n^n = E \Rightarrow C_n^{-1} = C_n^{n-1} \\ \sigma_1^2 = E \Rightarrow \sigma_1^{-1} = \sigma_1 \\ \sigma_1 C_n \sigma_1 = C_n^{-1} \Rightarrow \sigma_1 C_n = C_n^{n-1} \sigma_1 \\ \Rightarrow \sigma_1 C_n^2 = C_n^{n-1} \sigma_1 C_n = C_n^{n-2} \sigma_1 \quad \text{atd.} \end{array} \right.$$

tyto vztahy určují celou grupu D_n

abstraktně lze grupu D_n zadat pomocí

$$\langle \{r, s\} \mid r^n = s^2 = e, srs = r^{-1} \rangle - \text{anglicky jde o "presentation" of the group } D_n$$

$$\text{atd. } (sr)^2 = e$$

• Levé a pravé rozkladové třídy (left / right cosets)

Def: Je-li $H \leq G$ (podgrupou G), pak množinu $gH = \{gh \mid h \in H\}$ nazveme levou (rozkladovou) třídou příslušnou k podgrupě H .
Podobně $Hg = \{hg \mid h \in H\}$ je prava (rozkladová) třída.

Věta: Dvě levé (nebo pravé) třídy g_1H a g_2H obsahují buď stejné prvky a nebo jsou disjunktní.

Dk: buď jsou disjunktní
anebo obsahují alespoň jeden společný prvek,
pak ale $g_1h_k = g_2h_e$ pro jisté h_k a $h_e \in H$ dle VoP
 $\Rightarrow g_2^{-1}g_1 = h_e h_k^{-1} \in H$ a tedy $g_2^{-1}g_1 H = H \Rightarrow g_1 H = g_2 H$ c.b.d.

- každý prvek $g \in G$ patří do jisté třídy, konkrétně $gH = Hg$.
- pokud $g' \in gH$, pak $g'H = gH$, neboť mají alespoň jeden společný prvek g' .
- pokud je H konečná podgrupa, pak $\#gH = \#H \Rightarrow$

Lagrangeova věta: Pokud G je konečná grupa řádu $\#G$

a H její podgrupa řádu $\#H$, pak $\#H$ dělí $\#G$

a $m = \frac{\#G}{\#H}$ se nazývá index podgrupy H v grupě G .

Dk: zřejmý z výše uvedeného.

- důsledek: řád prvku dělí $\#G$

$\Rightarrow$ všechny grupy, jejichž počet prvků je prvočíslo, jsou cyklické

Pr: C_{3v} - jediná 6-prvková grupa různá od cyklické C_6 levé třídy podgrupy C_3

podgrupa C_3

E	C_3	C_3^2	$\sigma_v, \sigma_v', \sigma_v''$
C_3	C_3^2	E	$\sigma_v', \sigma_v'', \sigma_v$
C_3^2	E	C_3	$\sigma_v'', \sigma_v, \sigma_v'$
σ_v	σ_v''	σ_v	E, C_3^2, C_3
σ_v'	σ_v	σ_v''	C_3, E, C_3^2
σ_v''	σ_v'	σ_v	C_3^2, C_3, E

podgrupy: $C_3 \sim \{E, C_3, C_3^2\} \Rightarrow \sigma_v C_3 = \{\sigma_v, \sigma_v'', \sigma_v'\}$
 $C_3 \sim \{E, \sigma_v\} \Rightarrow C_3 \{E, \sigma_v\} = \{C_3, \sigma_v'\}$
 $C_3^2 \{E, \sigma_v\} = \{C_3^2, \sigma_v''\}$

a pod pro podgrupy $\{E, \sigma_v'\}$ a $\{E, \sigma_v''\}$

$\Leftarrow$ atd.

$\sigma_v C_3 = \sigma_v''$
 $\sigma_v C_3^2 = \sigma_v'$