# Základní pojmy teorie grup

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

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)

$$e\cdot a = e\cdot a = a \quad \text{pro } \forall a \in G$$

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

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

Dk sporem: 1) nechť $e_1$ a $e_2$ jsou různé identity, pak

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

2) nechť $b_1$ a $b_2$ jsou inverzní k $a^{-1}$, pak

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

- zřejmě $(a^{-1})^{-1} = a$ a $(ab)^{-1} = b^{-1}a^{-1}$, neboť $(ab)(ab)^{-1} = abb^{-1}a^{-1} = e$
- pozn: v definici grupy lze zmírnit 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. krystalografické
  – 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 jejích realizacích, které jsou ale z matematického hlediska totéž (stejná struktura, říkáme, že jsou tyto realizace izomorfní)

**Def:** <u>Izomorfismus</u> dvou grup je vzájemně jednoznačné zobrazení $\varphi$ z $G_1$ na $G_2$, 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 multiplikativní tabulky

|   | e | a |
|---|---|---|
| e | ee | ea |
| a | ae | aa |

$\Rightarrow$

|   | e | a |
|---|---|---|
| a | $e = a^2$ | |

má mnoho realizací:

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

2) $(\{0,1\}, + \bmod 2) = Z_2$

3) bodové grupy

$C_s = \{E, \sigma\}$ (v pevných látkách značena m)

identita, zrcadlení

$C_i = \{E, i\}$ (též $\bar{1}$)

inverze

$C_2 = \{E, C_2\}$ (též 2)

rotace o 180°

(více o bodových grupách viz Cvičení: Bodové grupy)

4) grupa permutací 2-prvkové množiny

$S_2 = \left(\left\{\begin{pmatrix}1&2\\1&2\end{pmatrix}, \begin{pmatrix}1&2\\2&1\end{pmatrix}\right\}, \text{skládání permutací}\right)$

identická permutace, transpozice 1 a 2

5) maticové realizace, např.

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

zrcadlení roviny $(x,y)$ podél $x=y$

- ve skutečnosti mnoho dalších realizací, ale všechny izomorfní

$$G \sim Z_2 \sim C_s \sim C_i \sim C_2 \sim S_2 \sim M$$

---

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

**Př:** všechny tzv. <u>cyklické grupy</u> dané vztahem $a^n = e$ pro jisté $n$ jsou komutativní. V tomto případě $n = \#G$ a $G = \{\underbrace{e, a, a^2, \dots, a^{n-1}}_{n \text{ různých prvků}}\}$

- obvykle se vyskytují jako podgrupy větších grup neboť každý prvek konečné grupy $g \in G$ generuje cyklickou podgrupu (viz níže), neboť $g^n = e$ pro jisté $n$.

# Věta o přeuspořádání (rearrangement theorem)

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

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

všechny prvky grupy $G$ a každý právě jednou.

**Dk:** 1) Uvažujme lib. prvek $h' \in G$ a vynásobme ho $g^{-1}h' = h$,
(určitě $g^{-1} \in G$ a lze jím násobit)
pak ale $gh = g(g^{-1}h') = h' \in L_g(G)$
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
nechť $\exists\, h_1 \neq h_2 : gh_1 = gh_2$, ovšem aplikací $g^{-1}$ 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 multiplikativní 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 $\#G = 5$)

---

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

| e | a | b |
|---|---|---|
| a | b | e |
| b | e | a |

zde nemůže být e, ani a $\Rightarrow$ jediná možnost b

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

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

cyklická

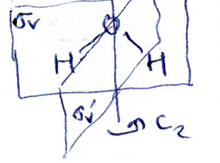
| e | a | b | c |
|---|---|---|---|
| a | b | c | e |
| b | c | e | a |
| c | e | a | b |

$\sim C_4 = \{E, C_4, C_2, C_4^3\}$, $C_2 = C_4^2$
otočení o $\frac{2\pi}{4} = 90°$

4-grupa (komutativní)

| e | a | b | c |
|---|---|---|---|
| a | e | c | b |
| b | c | e | a |
| c | b | a | e |

$\sim C_{2v} = \{E, C_2, \sigma_v, \sigma_v'\}$ roviny zrcadlení
(molekula vody má tuto symetrii)




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