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

$a^5 = e$ $\sim C_5$

ovšem např.

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

není grupou neboť $(ab)d = cd = a$ ale $a(bd) = ac = d$ a není tedy splněna asociativita

---

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

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

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

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

3) víme, že $h^{-1} \in H \Rightarrow g(h^{-1})^{-1} = gh \in H$ pro $\forall g, h \in H$ 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 a $h \in H_1 \cap H_2$, 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 <u>řád prvku</u>.

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

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

- <u>Generátory grupy a podgrup</u> (u Lieových grup budou generátory něco jiného, prvky Lieovy algebry)

- pokud je n řád prvku g, pak $\{e, g, \dots, g^{n-1}\}$ tvoří <u>podgrupu</u> G <u>generovanou prvkem g</u>, 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)

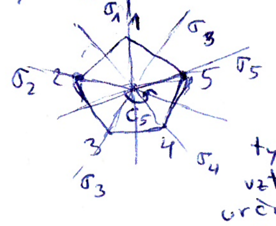
<u>Věta:</u> Pro libovolnou podmnožinu $X \subset G$ existuje nejmenší podgrupa G obsahující X. Její prvky tvoří všechny konečné součiny prvků z X a jejich inverzí.

<u>Dk:</u> Nechť $H_i \leq G$ jsou všechny podgrupy obsahující $X \subset H_i$ pro $\forall i$. Pak $S = \bigcap_i H_i \leq G$ 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, nazveme generátory grupy, v reprezentaci pak stačí najít repr. generátorů, zbytek např. maticovým násobením

<u>Př:</u>

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

$$C_n^n = E \Rightarrow C_n^{-1} = C_n^{n-1}$$
$$\sigma_1^2 = E \Rightarrow \sigma_1^{-1} = \sigma_1$$
$$\sigma_1 C_n \sigma_1 = C_n^{-1} \Rightarrow \sigma_1 C_n = C_n^{n-1} \sigma_1$$
$$\Rightarrow \sigma_1 C_n^2 = C_n^{n-1} \sigma_1 C_n = C_n^{n-2} \sigma_1 \quad \text{atd.}$$

tyto vztahy určují celou grupu D_n

abstraktně lze grupu D_n zadat pomocí

$\langle \{r, s\} \mid r^5 = s^2 = e,\ srs = r^{-1} \rangle$ - anglicky jde o „presentation" of the group D_n

$srs = r^{-1} \Leftrightarrow (sr)^2 = e$

- **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 pravá (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

a nebo obsahují alespoň jeden společný prvek,

pak ale $g_1 h_k = g_2 h_e$ pro jisté h_k a h_e z 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 a 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 $\#G$

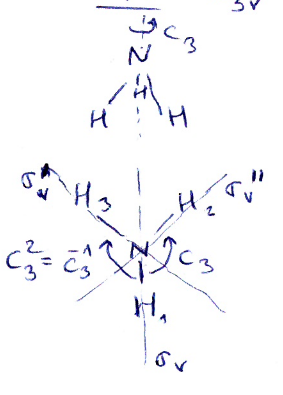
a $m = \dfrac{\#G}{\#H}$ se nazývá index podgrupy H v grupě G.

Dk: zřejmý z výše uvedeného.

- důsledek: řád prvku dělí $\#G$

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

Př: C_{3v} – jediná 6-prvková grupa různá od cyklické C_6 levé třídy



$\overbrace{E \quad C_3 \quad C_3^2}^{\text{podgrupa } C_3}$

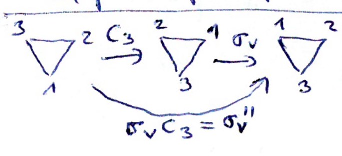
E	C_3	C_3^2	σ_v	σ_v'	σ_v''
C_3	C_3^2	E	σ_v'	σ_v''	σ_v
C_3^2	E	C_3	σ_v''	σ_v	σ_v'
σ_v	σ_v''	σ_v'	E	C_3^2	C_3
σ_v'	σ_v	σ_v''	C_3	E	C_3^2
σ_v''	σ_v'	σ_v	C_3^2	C_3	E

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

$C_s \sim \{E, \sigma_v\} \Rightarrow C_3\{E, \sigma_v\} = \{C_3, \sigma_v'\}$

$C_3^2\{E, \sigma_v\} = \{C_3^2, \sigma_v''\}$

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

$\Leftarrow$  atd.