MI-SPOL-1

Teorie grup: Grupoidy, pologrupy, monoidy a grupy. Podgrupy, cyklické grupy a jejich generátory

M je neprázdná množina a ∘ binární operace nad ní.

- **Grupoid:** uspořádaná dvojice $(M, \circ)$, kde $\circ : M \times M \to M$
- **Pologrupa:** grupoid, kde ∘ je asociativní
- **Monoid:** pologrupa, kde ∃ neutrální prvek e t.ž. $\forall a \in M$ platí $a \circ e = e \circ a = a$
- **Grupa:** monoid, kde ∃ inverzní prvky: $\forall a \in M \exists a^{-1} \in M$ t.ž. $a \circ a^{-1} = a^{-1} \circ a = e$
- **Abelovská grupa:** grupa, kde ∘ je komutativní

Grupoid ⊃ pologrupa ⊃ monoid ⊃ grupa ⊃ abelovská grupa

V monoidu existuje **právě jeden neutrální prvek**

- sporem, pokud $\exists e' \neq e$, pak $e' = e \circ e' = e$, což je spor s tím, že $e \neq e'$

V grupě má každý prvek **právě jeden inverzní prvek**

- sporem: $a \in G, a^{-1} = b \in G$
  předpoklad, že $\exists c \neq b$ t.ž. $c = a^{-1}$
  potom: $c = c \circ e = c \circ (a \circ b) = (c \circ a) \circ b = e \circ b = b \Rightarrow$ spor

Konečná množina jde zapsat do **Cayleyho tabulky**

- na osách prvky množiny, v tabulce výsledky operace
- lze z ni vyčíst:
  - uzavřenost množiny (v tabulce se vyskytují pouze prvky množiny)
  - neutrální prvek (v jeho řádku a sloupci se opakuje první řádek a sloupec tabulky)
  - inverzní prvek -- nalezne se tak, že se v daném řádku najde neutrální prvek
  - komutativita operace (tabulka symetrická po hlavní diagonále)
- tvoří latinský čtverec (každý řádek a sloupec obsahuje všechny prvky množiny)

V každé grupě lze **jednoznačně dělit**

- $a \circ x = b$ a $y \circ a = b$ mají pro každé a, b jediné řešení
- každý prvek má jedinou inverzi a řešením rovnic je jsou prvky $a^{-1} \circ b$

Konečná grupa jde zapsat i do **Cayleyho orientovaného grafu**

- vrcholy jsou prvky M
- orientovaná hrana (a, b) patří do E právě když $b = a \circ c$ pro jisté c

Podgrupa: Buď $G = (M, \circ)$ grupa. Podgrupou G nazveme libovolnou dvojici $H = (N, \circ)$ takovou, že $N \subset M$ a $(N, \circ)$ je grupa.

V každé grupě existují aspoň 2 podgrupy (**triviální**):

- $(\{e\}, \circ)$
- $G = (M, \circ)$

Netriviální podgrupy jsou **vlastní**.

Pro každé $i \in I$ buď H_i podgrupa $G = (M, \circ)$. Potom platí, že $H' = \bigcap_{i \in I} H_i$ je také podgrupa G .

$G = (M, \circ)$ a $N \subset M$ neprázdná množina. Dvojice $H = (N, \circ)$ je podgrupa G právě když $\forall a, b \in N$ platí $a \circ b^{-1} \in N$

Řád grupy $G = (M, \circ)$ ($\#G$) je počet prvků množiny M. Pokud M nekončená, řád je též nekonečný.

Lagrangeova věta: Buď H podgrupa konečné grupy G. Potom řád H dělí řád G.

- důsledek: grupa s prvočíselným řádem má pouze triviální podgrupy

G grupa konečného řádu n, p prvočíslo dělící n. Pokud p^k dělí n, pak grupa G obsahuje podgrupu řádu p^k.

$G = (M, \circ)$ grupa a $N \subset M$ neprázdná množina. Množina $\langle N \rangle := \bigcap \{H : H$ je podgrupa G obsahující $N\}$ je podgrupou G obsahující množinu N.

- $\langle N \rangle$ je grupa podle věty o průniku grup
- každá z H obsahuje N, takže i jejich průnik obsahuje N

Podgrupa $\langle N \rangle$ grupy $G = (M, \circ)$, $N \subset M$ je **podgrupa generovaná množinou** N. N je **generující množina** grupy $\langle N \rangle$.

Pokud je $N = \{a\}$, pak a je **generátor** grupy $\langle a \rangle$

Pokud $G = (M, \circ) grupa$ a $N \subset M$, všechny prvky patřící do $\langle N \rangle$ lze získat pomocí grupového obalu $\langle N \rangle = \{a_1^{k_1} \circ a_2^{k_2} \circ ... \circ a_n^{k_n} : n \in \mathbb{N}, k_i \in \mathbb{Z}, a_i \in N\}$

- důsledek: $\langle a \rangle = \{a^k : k \in Z\}$ -- k je i záporné a $g^{-n} = (g^{-1})^n$

Grupa $\mathbb{Z}_n^+$ je rovna $\langle k \rangle, k \in \mathbb{Z}_n^+$ právě když k **a** n **jsou nesoudělná.**

Grupa $G = (M, \circ)$ je **cyklická**, pokud existuje $a \in M$ t.ž. $\langle a \rangle = G$. Prvek a je **generátor** G.

$\mathbb{Z}_n^+$ cyklické pro všechna n, jejich generátory jsou všechny kladná $k \leq n$ nesoudělná s n.

$(\mathbb{Z}, +)$ je cyklická -- generátory jsou 1 a -1 (**problematická státnicová otázka**)

- $\langle 1 \rangle = 1^k, k \in \mathbb{Z}$
  - kladné k generuje kladná čísla: $1^n = 1 + 1 + 1 + ...$ s n sčítanci
  - záporné k generuje záporná čísla: $1^{-n} = (1^{-1})^n = 1^{-1} + 1^{-1} + 1^{-1} + ... = (-1) + (-1) + (-1) + ...$ s n sčítanci
- $\langle -1 \rangle = -1^k, k \in \mathbb{Z}$
  - kladné k generuje záporná čísla: $-1^n = (-1) + (-1) + (-1) + ...$ s n sčítanci
  - záporné k generuje kladná čísla: $-1^{-n} = (-1^{-1})^n = (-1)^{-1} + (-1)^{-1} + (-1)^{-1} + ... = 1 + 1 + 1 + ...$ s n sčítanci

Řád prvku $g \in G$ **(**$ord(g)$**)** je nejmenší takové m kde platí $g^m = e$. Pokud neexistuje, řád g je nekonečno.

- $ord(g) = \#\langle g \rangle$

$\mathbb{Z}_n^\times$ je **cyklická právě když** n je $2, 4, p^k$ nebo $2p^k$, kde p je liché prvočíslo a k kladné přorozené číslo.

Pokud G cyklická řádu n a a je její generátor, pak a^k je také generátor právě když k a n jsou nesoudělná.

Počet generátorů v cyklcické grupě řádu n je $\varphi(n)$, kde φ je Eulerova funkce (počet přirozených čísel menších než n, která jsou s n nesoudělná)

- $\mathbb{Z}_p^\times$ je cyklická řádu $p-1$ a má $\varphi(p-1)$ generátorů
- pro φ není znám efektivní algoritmus

Libovolná **podgrupa cyklické grupy** je opět **cyklická**

V grupě řádu n platí pro všechny prvky a, že $a^n = e$

Malá Fermatova věta: Pro libovolné prvočíslo p a libovolné $1 \leq a < p$ platí $a^{p-1} \equiv 1 \pmod p$

Buďte $G = (M, \circ_G)$ a $H = (N, \circ_H)$ dva grupoidy. Zobrazení $h : M \to N$ je **homomorfismus** G **do** H, jestliže $\forall x, y \in M$ platí $h(x \circ_G y) = h(x) \circ_H h(y)$

Buď h izomorfismus $G = (M, \circ_G)$ do $H = (N, \circ_H)$. Potom $h(G) = (h(M), \circ_H)$ je grupa.

- důsledky:
  - neutrální prvek jedné grupy se zobrazí vždy na neutrální prvek druhé
  - inverze se zachovají: $h(x^{-1}) = h(x)^{-1}$

Dvě **nekonečné grupy jsou izomorfní**.
Pro každé $n \in \mathbb{N}$ jsou dvě **cyklické grupy řádu** n **izonorfní**.