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

- dvojice množina (neprázdná) & binární operace $(M, \circ)$ (konečná či nekonečná)

$M \neq \emptyset$

$M \circ M \to M$ ← musí být uzavřená vůči operaci ← binární operace na množině

grupoid → (asociativita, závorky) pologrupa → (neutr. prvek) monoid → (inverzní prvek) grupa → (komutativita) abelovská grupa

neutrální prvek → $a \circ e = e \circ a = a \quad \forall a \in M$

inverzní prvek → $a^{-1} \circ a = a \circ a^{-1} = e$ (musí existovat pro každé a)

→ každý prvek musí mít právě jeden inverzní

→ neutrální prvek je vždy jen jeden $e = \bar{e} \circ e = \bar{e}$

podgrupy: $H = (N, \circ)$ je grupa & $N \subset M$

$(\mathbb{Z}, \cdot)$ - musí uzavřená vůči operaci

$(\mathbb{Q}, \circ)$ $a \circ b = \frac{a+b}{2}$: grupoid

$(\mathbb{R}^+, \circ)$ $a \circ b = \frac{a \cdot b}{a+b}$: pologrupa

$(\mathbb{R}, \cdot)$: monoid

* Cayleyho tabulka

- triviální podgrupy: | grupa samotná
  obsahující pouze neutrální prvek
- existují v každé grupě s alespoň dvěma prvky
- vlastní

Řád grupy (podgrupy)

= počet prvků množiny M

- může být nekonečný

- řád podgrupy dělí řád grupy (u konečných) = Lagrangeova věta
  (neplatí to ale platí naopak) - tj. nemusí pro každý dělitel existovat podgrupa

→ grupa s prvočíselným řádem má pouze triviální podgrupy

- podgrupa generovaná množinou N → $\langle N \rangle$
  - nejmenší podgrupa obsahující N
- množina generátorů grupy G $\langle M \rangle = G$

- grupový obal → získám mocněním všech prvků $\langle N \rangle$
(tj. sjednocením všechny grupy $\langle N \rangle$)

(- podgrupa $\langle N \rangle$ = průnik všech podgrup obsahujících N)?

cyklické grupy - musí existovat prvek a ; $\langle a \rangle = G$
- generátor cyklické grupy

$\mathbb{Z}_n^+$ - generátorem jsou všechna $k \leq n$ nesoudělná s n
→ $\gcd(k,n) = 1$
⇒ (grupa $G = \langle k \rangle$ pokud $\gcd(k,n) = 1$)

$\mathbb{Z}_n^\times$ - tedy že najdu jeden generátor, ostatní najdu umocňováním generátoru na mocniny nesoudělné s řádem

Malá Fermatova Věta : $\boxed{a^{p-1} \equiv 1 \pmod p}$

V cyklické grupě je počet generátorů = $\varphi(m)$ (řád grupy)

$\#x \rightarrow \gcd(x,m) = 1 \quad \forall x < m$

- vždy platí : $a^n = e$ (v [redacted] grupě)
- podgrupa cyklické grupy je také cyklická

Multiplikativní grupy : $\mathbb{Z}_n^\times$ řád grupy = $\varphi(n) = m$
- pro prvočísla $\varphi(p) = p-1$

počet generátorů [redacted] grupy = $\varphi(m)$ (platí [redacted] pro všechny cyklické)
- první nějak najdu → další umocňováním na čísla nesoudělná s řádem m

cyklické jsou pouze pro $n = 2$, $n = 4$, $n = p^k$, $n = 2p^k$
p - liché prvočíslo

Aditivní grupy $\mathbb{Z}_n^+$ - řád grupy = n

$\varphi(n)$ = počet generátorů

- generátory jsou čísla nesoudělná s n
- všechny aditivní grupy $\mathbb{Z}_n^+$ jsou cyklické

Homomorfismus: dvě grupy G, H a zobrazení $\varphi: G \to H$

takové, že $g_1, g_2 \in G$, $h_1, h_2 \in H$: $\varphi(g_1) \overset{H}{\circ} \varphi(g_2) =$

$= \varphi(g_1 \overset{G}{\circ} g_2)$; $[\varphi(g_1) = h_1, \varphi(g_2) = h_2]$

- neutrální prvky se mapují na sebe
- struktura podgrupy musí zůstat stejná ~~(podgrupy)~~

Izomorfismus: homomorfismus, který je bijekí

- dvě nekonečné cyklické grupy jsou izomorfní
- izomorfismus zachovává cykličnost

- počet izomorfismů = počet generátorů

další: v každé grupě lze jednoznačně dělit !

pro libovolné $a, b \in G$ $\quad a \circ x = b \quad y \circ a = b$ má jediné řešení

- cyklické grupy mají všechny podgrupy také cyklické
- n-tá mocnina prvku a v grupě

$$a^n = \underbrace{a \circ a \circ \dots \circ a}_{n\text{-krát}}$$

$$a^0 = e$$

$$a^{-n} = \underbrace{a^{-1} \circ a^{-1} \circ a^{-1} \dots \circ a^{-1}}_{n\text{-krát}}$$

$\Rightarrow (\mathbb{Z}, +)$ je cyklická a všechny prvky lze vygenerovat $\langle -1 \rangle$ nebo $\langle 1 \rangle$