G grup ciclic $\Rightarrow G \simeq (\mathbb{Z},+)$ sau $G \simeq (\mathbb{Z}_n,+)$ pentru un $n \in \mathbb{N}^*$

Subgrupurile și grupurile factor ale unui grup ciclic

Subgrupuri

- **Subgrupurile lui $\mathbb{Z}$:**

$n\mathbb{Z}$, cu $n \in \mathbb{N}$ ciclic $\langle n \rangle$

Pentru $n, m \in \mathbb{N}$ $\quad n\mathbb{Z} = m\mathbb{Z} \Leftrightarrow n = m$

Observație! $n\mathbb{Z} \subset m\mathbb{Z} \Leftrightarrow m \mid n$

- Fie $n \geq 2$. Subgrupurile lui $\mathbb{Z}_n$:

$\pi : \mathbb{Z} \to \mathbb{Z}_n$, $\pi(i) = \hat{i}$ morfism surjectiv de grupuri $\xRightarrow{\text{Exercițiu}}$

$\operatorname{Ker} \pi = n\mathbb{Z}$

$\Rightarrow (\exists)$ o corespondență bijectivă

$$\varphi : \{A \mid A \leq \mathbb{Z} \text{ cu } n\mathbb{Z} \subset A\} \to \{B \mid B \leq \mathbb{Z}_n\}$$

$$\varphi(A) \overset{\text{def.}}{=\!=} \pi(A)$$

$A \leq \mathbb{Z} \Rightarrow A = m\mathbb{Z}, m \in \mathbb{N}$

$n\mathbb{Z} \subset m\mathbb{Z} \Leftrightarrow m \mid n$

$$\varphi : \{m\mathbb{Z} \mid m \in \mathbb{N}, m \mid n\} \to \{B \mid B \leq \mathbb{Z}_n\}$$

$\varphi(m\mathbb{Z}) = \pi(m\mathbb{Z}) = \{ \underbrace{\widehat{mk}}_{} \mid k \in \mathbb{Z} \} = m\mathbb{Z}/_{n\mathbb{Z}}$ ciclic

$\widehat{mk} \to mk + n\mathbb{Z}$

$m\mathbb{Z} = \{ mk \mid k \in \mathbb{Z} \}$

Subgrupurile lui $\mathbb{Z}_n$ sunt $m\mathbb{Z}/_{n\mathbb{Z}}$, cu $m \in \mathbb{N}$, $m \mid n$.

Dacă $m, m' \mid n$ $\quad m\mathbb{Z}/_{n\mathbb{Z}} = m'\mathbb{Z}/_{n\mathbb{Z}} \Leftrightarrow$

$\Leftrightarrow m = m'$

$o(\hat{m}) = \frac{n}{m}$

$m\mathbb{Z}/_{n\mathbb{Z}} = \langle \hat{m} \rangle = \{ \hat{m}, \widehat{2m}, \dots, \underbrace{\frac{n}{m} \cdot m}_{\hat{0}} \}$

Consecință: orice subgrup al unui grup ciclic este ciclic.

$\frac{m\mathbb{Z}}{n\mathbb{Z}} \simeq \mathbb{Z}_{n/m}$

Grupuri factor

$\left. \begin{array}{l} G \text{ ciclic} \\ H \leq G \end{array} \right| \Rightarrow G/H \text{ ciclic}$

$G = \langle g \rangle \Rightarrow G/H = \langle \hat{g} \rangle$

$\quad\; \|$

$\{ g^i \mid i \in \mathbb{Z} \}$

- Pentru $\mathbb{Z}$:

Subgr. $n\mathbb{Z}$, $n \in \mathbb{N}$

$n = 0$ $\quad \mathbb{Z}/_{0\mathbb{Z}} = \mathbb{Z}/_{\{0\}} \simeq \mathbb{Z}$

$n=1$ $\qquad \mathbb{Z}/_{1\mathbb{Z}} = \mathbb{Z}/_{\mathbb{Z}} = \{0\}$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \simeq$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \mathbb{Z}_1$

$n \geq 2$ $\qquad \mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}_n$

$|G| = |H| \cdot [G:H]$
$\downarrow$
$|G/H|$

$|G/H| = \dfrac{|G|}{|H|}$

- $\mathbb{Z}_n$, $n \geq 2$

$\uparrow$

subgr. $m\mathbb{Z}/_{n\mathbb{Z}}$, cu $m \in \mathbb{N}$, $m|n$

$\dfrac{\mathbb{Z}_n}{m\mathbb{Z}/_{n\mathbb{Z}}}$ - ciclic
- are $\dfrac{n}{|m\mathbb{Z}/_{n\mathbb{Z}}|} = \dfrac{n}{n/m} = m$ elemente

$$\frac{\mathbb{Z}/n\mathbb{Z}}{m\mathbb{Z}/n\mathbb{Z}} \simeq \mathbb{Z}_m$$

Grupul simetric S_n

Fie $n \in \mathbb{N}$, $n \geq 2$.

Notăm $S_n = S(\{1, \dots, n\}) = \{\sigma \mid \sigma : \{1, \dots, n\} \to \{1, \dots, n\}\ \}$
funcție bijectivă
(permutare)

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$$

$|S_n| = n!$

Elementul neutru: e = funcția identică

Fixăm $\sigma \in S_n$

Pe $\{1, \dots, n\}$ definim relația $\sim$ prin

$$i \sim j \overset{def.}{\iff} (\exists)\ r \in \mathbb{Z} \text{ cu } \sigma^r(i) = j$$

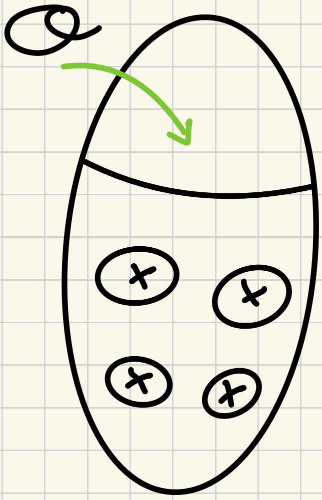
Atunci $\sim$ este relație de echivalență (**exercițiu**), iar clasele sale de echivalență s.n. **orbitele** lui σ.

O orbită s.n. **trivială** dacă are exact un element și **netrivială** altfel.

$\{i\}$ orbită trivială $\iff \sigma(i) = i$

Dacă există o singură orbită netrivială O ($m \geq 2$ elemente), σ s.n. **ciclu de lungime m.**

Observație! $(\forall)\ i \notin O \quad \sigma(i) = i$



Exemplu: Fie $m \geq 2$ și $i_1, \dots, i_m \in \{1, \dots, n\}$ distincte.

Considerăm $\sigma \in S_n$ definită prin

$$\sigma(i_1) = i_2,\ \sigma(i_2) = i_3, \dots, \sigma(i_{m-1}) = i_m,\ \sigma(i_m) = i_1$$

$\sigma(j)=j \quad (\forall)\ j \notin \{i_1,\dots,i_m\}$

Atunci σ este ciclu de lungime m, cu orbita netrivială $\{i_1, i_2, \dots, i_m\}$

σ se notează $(i_1\ i_2 \dots i_m)$

Propoziție: Fie $i \in \{1,\dots,n\}$. Atunci există un cel mai mic $m \in \mathbb{N}^*$ cu $\sigma^m(i)=i$ și orbita (clasa de echivalență) lui i este $\{i, \sigma(i), \dots, \sigma^{m-1}(i)\}$, care are m elemente.

Dem.:

S_n grup finit $\Rightarrow \sigma$ are ordin finit
$\Rightarrow \sigma^{o(\sigma)} = e \Rightarrow \sigma^{o(\sigma)}(i)=i$
$(o(\sigma)>0)$

Fie m cel mai mic (în $\mathbb{N}^*$) cu $\sigma^m(i)=i$
Arăt că $i, \sigma(i), \dots, \sigma^{m-1}(i)$ sunt oricare două distincte.

Dacă $0 \le p < q \le m-1$ cu $\sigma^p(i) = \sigma^q(i)$

$\xRightarrow{\sigma^{-p}} \sigma^{q-p}(i)=i$, $0 < q-p < m$ | Contradicție cu minimalitatea lui m

Arăt că clasa de echivalență a lui $i =$
$= \{ i, \sigma(i), \dots, \sigma^{m-1}(i) \}$
$\qquad \|$
$\{ \sigma^{x}(i) \mid x \in \mathbb{Z} \}$

Fie $x \in \mathbb{Z}$, împart la m

$$x = c \cdot m + R$$

$$\sigma^{x}(i) = \sigma^{R + c \cdot m}(i) = \sigma^{R}(\underbrace{(\sigma^{m})^{c}(i)}_{i})$$

$$= \sigma^{R}(i) \in \{ i, \dots, \sigma^{m-1}(i)$$

$$\sigma^{m}(i) = i$$

Corolar: Dacă σ este ciclu de lungime $m \geq 2$, atunci $\sigma = (i_1 \; i_2 \dots i_m)$ pentru niște $i_1, \dots, i_m$ distincte

Dem.:

Fie $i \in$ orbitei netriviale $\Rightarrow$ orbita lui $i =$
$= \{ i, \sigma(i), \dots, \sigma^{m'-1}(i) \}$

m' min. cu $\sigma^{m'}(i) = i$

$\Rightarrow m' = m$

$$\sigma = (i \;\; \sigma(i) \;\; \sigma^{2}(i) \dots \sigma^{m-1}(i))$$

Def.: Spunem că două cicluri σ_1, σ_2 (cu orbite netriviale O_1, O_2) sunt disjuncte dacă $O_1 \cap O_2 = \emptyset$.

Propoziție: Dacă σ_1, σ_2 sunt cicluri disjuncte $\Rightarrow \sigma_1\sigma_2 = \sigma_2\sigma_1$

Dem.:

Fie $\sigma_1 = (i_1 \ i_2 \dots i_m)$

$\sigma_2 = (j_1 \ j_2 \dots j_p)$,

unde $\{i_1, \dots, i_m\} \cap \{j_1, \dots, j_p\} = \emptyset$

$\sigma_1\sigma_2 = (i_1 \ i_2 \dots i_m)(j_1 \ j_2 \dots j_p)$,

$i \notin \{i_1, \dots, i_m\} \cup \{j_1, \dots, j_p\}$ $\quad i \longmapsto i$

$i \in \{i_1, \dots, i_m\}$ $\quad i \longmapsto \sigma_1(i)$

$i \in \{j_1, \dots, j_p\}$ $\quad i \longmapsto \sigma_2(i)$

$\sigma_2\sigma_1 = (j_1 \dots j_p)(i_1 \dots i_m)$

$i \longmapsto i$

$i \longmapsto \sigma_1(i)$

$i \longmapsto \sigma_2(i)$

Propoziție: Fie $m \in \mathbb{N}^*$ și $\sigma_1, \dots, \sigma_m$ cicluri disjuncte două câte două, cu orbite netriviale $O_1, \dots, O_m$.
Fie $\sigma = \sigma_1 \dots \sigma_m$. Atunci clasa de echivalență (orbita) relativ la σ a unui i este:

- $\{i\}$, dacă $i \notin O_1 \cup \ldots \cup O_m$
- O_k dacă $i \in O_k$

Așadar, σ are exact m orbite netriviale, și anume $O_1, \ldots, O_m$.

Dem.:

Dacă $j \notin O_k$, atunci $\sigma_k(j) = j$.

Dacă $i \notin O_1 \cup \ldots \cup O_k \Rightarrow \sigma_k(i) = i, (\forall) k$

$$\Rightarrow \sigma(i) = (\sigma_1 \ldots \sigma_m)(i) = i$$

$\Rightarrow$ orbita lui i este $\{i\}$

Dacă $i \in O_k$. Observăm că pentru $p \neq k$ $\sigma_p(j) = j, (\forall) j \in O_k$

$$\sigma^r(i) = (\sigma_1 \ldots \sigma_m)^r(i) = \sigma_k^r(i), (\forall) r \in \mathbb{Z}$$

orbita lui i:

$$\{\sigma^r(i) \mid r \in \mathbb{Z}\} = \{\sigma_k^r(i) \mid r \in \mathbb{Z}\} = O_k$$

Teoremă: Fie $n \in \mathbb{N}$, $n \geq 2$ și $\sigma \in S_n$. Atunci există $r \in \mathbb{N}$ și $\sigma_1, \ldots, \sigma_r$ cicluri oricare două disjuncte, astfel că $\sigma = \sigma_1 \ldots \sigma_r$.

Mai mult, o astfel de reprezentare este unică până la o permutare a factorilor, adică, dacă $\sigma = \tau_1, \ldots, \tau_s$ cu $\tau_1, \ldots, \tau_s$ cicluri oricare două disjuncte, atunci $r = s$ și

$\{\sigma_1, \dots, \sigma_r\} = \{\tau_1, \dots, \tau_r\}$.

Orice permutare se scrie unic (până la ord. factorilor) ca produs de cicluri disjuncte.

Dem.:

Convenție: $r=0$ $\quad \sigma_1 \dots \sigma_r \overset{conv.}{=} e$

Fie $\sigma \neq e$ și fie $O_1, \dots, O_r$ orbitele netriviale ale lui σ.

Pentru fiecare $1 \le k \le r$ fie

$\sigma_k \in S_n$

$\sigma_k(i) = \sigma(i)$, pentru $i \in O_k$

$\sigma_k(i) = i$, pentru $i \notin O_k$

$\Rightarrow \sigma_k$ este un ciclu cu orbita netrivială O_k

$\sigma_1, \dots, \sigma_r$ oricare două disjuncte

$O_k \cap O_p = \emptyset$

$k \neq p$

Avem $\sigma = \sigma_1 \dots \sigma_r$

Observăm că dacă $j \in O_k$ și $p \neq k$, atunci $\sigma_p(j) = j$

Dacă $i \notin O_1 \cup \dots \cup O_m \Rightarrow \sigma_k(i) = i$, $(\forall)\, k$

$\sigma(i) = i$

Clar $(\sigma_1 \dots \sigma_r)(i) = i = \sigma(i)$

Dacă $i \in O_k$:

$$(\sigma_1 \dots \sigma_r)(i) = \sigma_k(i) = \sigma(i)$$

Așadar, $\sigma = \sigma_1 \dots \sigma_r$

Presupunem că $\sigma = \tau_1 \dots \tau_s$ cu $\tau_1, \dots, \tau_s$ cicluri disjuncte cu orbite $O'_1, \dots, O'_s$.

Propoziția precedentă $\Rightarrow$ σ are s orbite netriviale și anume $O'_1, \dots, O'_s$

Dar orbitele netriviale ale lui σ sunt $O_1, \dots, O_r$

$\Rightarrow s = r$ și $(\exists)\ \pi \in S_r$ a.î. $O'_k = O_{\pi(k)}$, $(\forall)\ 1 \le k \le r$

Arătăm că $\tau_k = \sigma_{\pi(k)}$, $(\forall)\ 1 \le k \le r$

Dacă $i \notin O'_k = O_{\pi(k)}$, atunci $\tau_k(i) = i$

$\sigma_{\pi(k)}(i) = i$

Dacă $i \in O'_k = O_{\pi(k)}$

$$\sigma(i) = (\tau_1 \dots \tau_r)(i) = \tau_k(i)$$

$$\sigma(i) = (\sigma_1 \dots \sigma_r)(i) = \sigma_{\pi(k)}(i)$$

$\Rightarrow$

$\Rightarrow \tau_k = \sigma_{\pi(k)}$

exemplu:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 6 & 5 & 8 & 7 & 10 & 1 & 4 & 9 & 2 \end{pmatrix} \in S_{10}$$

$$\sigma = (1\ 3\ 5\ 7)(2\ 6\ 10)(4\ 8)$$

Def.: Un ciclu de lungime doi s.n. transpoziție.

exercițiu: $(i_1\ i_2 \dots i_m) = (i_1\ i_2)\cdot(i_2\ i_3)\cdot\ldots\cdot(i_{m-1}\ i_m)$

Consecință: Orice permutare este produs de transpoziții.