Def

G: grupa, $g \in G$. Definiujemy rząd g, ozn. $\operatorname{ord}(g)$, jako najmniejsze $n>0$ takie, że $g^n = e$. Jeśli takie $n>0$ nie istnieje, to definiujemy $\operatorname{ord}_G(g) = \infty$.

Często piszemy „$\operatorname{ord}(g)$" zamiast „$\operatorname{ord}_G(g)$".

Przykłady

(1) $2 \in \mathbb{Z}_8$, $\operatorname{ord}_{\mathbb{Z}_8}(2) = 4$, bo $\underbrace{2+_8 2}_{2 \text{ razy}} \neq 0$, $\underbrace{2+_8 2+_8 2}_{3 \text{ razy}} \neq 0$, $\underbrace{2+_8 2+_8 2+_8 2}_{4 \text{ razy}} = 0$

Uwaga (częsty błąd!)

$\underbrace{2+_8 2+_8 \ldots +_8 2}_{8 \text{ razy}} = 0$, ale $\operatorname{ord}_{\mathbb{Z}_8}(2) \neq 8$, bo 8 nie jest najmniejszą $n>0$, taką że $\underbrace{2+_8 \ldots +_8 2}_{n \text{ razy}} = 0$.

(2) $\operatorname{ord}_{S_2}\left(\begin{pmatrix}1&2\\2&1\end{pmatrix}\right) = 2$

(3) $\operatorname{ord}_{S_3}\left(\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right) = 3$

(4) $\operatorname{ord}_{\mathbb{Z}}(1) = \infty$

(5) $\operatorname{ord}_{\mathbb{Z}_n}(1) = n$

(6) G: grupa, $g \in G \Rightarrow \operatorname{ord}_G(g) = 1 \iff g = e$

Uwaga (KONW.)

Jeśli $f: G \to H$ homom. grup, $g \in G$, $n \in \mathbb{Z}$, to:

(i) $f(g^n) = f(g)^n$ (ii) f jest „1-1", to $\operatorname{ord}_G(g) = \operatorname{ord}_H(f(g))$

(iii) $k = \operatorname{ord}_G(g)$ skończony $\Rightarrow$ $(g^n = e \iff k \mid n)$.

TW.

G: grupa, $g \in G \Rightarrow \operatorname{ord}(g) = |\langle g \rangle|$

(rząd elementu g to moc najmniejszej podgrupy zawierającej g)

Dowód

1° $\operatorname{ord}(g) = n$ skończony

$g^n = e \overset{\text{Lemat}}{\Longrightarrow} |\langle g \rangle| \leq n$

$d \mid a$ $m = |\langle g \rangle| \leq n$.

TW. $\Rightarrow \langle g \rangle \cong \mathbb{Z}_m$

Krok 3 (popr. TW.) $\Rightarrow$ $g^m = e$, $m \leq n$, n: minimalne $\Rightarrow m = n$

czyli $|\langle g \rangle| = \operatorname{ord}(g)$, $m = n$

2° $\operatorname{ord}(g) = \infty$ Rozumując j.w. $\forall m \ \langle g \rangle \not\cong \mathbb{Z}_m$.

TW $\Rightarrow \langle g \rangle \cong \mathbb{Z} \Rightarrow |\langle g \rangle| = \infty = \operatorname{ord}(g)$. ∎

Wniosek

W szczególności: G skończona $\Rightarrow \forall g \in G \ \operatorname{ord}(g) < \infty$

Później zobaczymy, że $\operatorname{ord}(g) \mid |G|$.

Uwaga/Def

Ostatnie TW: $\operatorname{rząd}(g) = \operatorname{moc}\langle g \rangle$. Stąd często na moc grupy $(|G|)$ mówimy $\operatorname{rząd}(G)$.

Def G: grupa, $A \subseteq G$

$\langle A \rangle$ oznacza najmniejszą podgrupę G zawierającą A.

Jeśli $\langle A \rangle = G$, to mówimy, że G jest generowana przez A (lub A jest zbiorem generatorów G). Zamiast $\langle \{g_1, \ldots, g_n\} \rangle$ piszemy $\langle g_1, \ldots, g_n \rangle$.

TW. (bez dowodu)

A, G j.w. i $g \in G$. Wtedy $g \in \langle A \rangle$ wtedy i tylko wtedy, gdy $\exists a_1, \ldots, a_n \in A \ \exists k_1, \ldots, k_n \in \mathbb{Z}$ $g = a_1^{k_1} \cdot \ldots \cdot a_n^{k_n}$.

Przykłady

(1) $D_3 = \langle O_{\frac{2\pi}{3}}, S \rangle$ (dowolne sym. osiowe)

$O_{\frac{4\pi}{3}} = O_{\frac{2\pi}{3}} \circ O_{\frac{2\pi}{3}}$

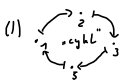
$O_{\frac{2\pi}{3}} \circ S$ ← pozostałe 2

(2) Podobnie: $D_n = \langle O_{\frac{2\pi}{n}}, S \rangle$ / $O_{\frac{4\pi}{n}} \circ S$ ← symetrie osiowe

GRUPY PERMUTACJI

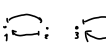
Chcemy opisać każdą permutację za pomocą pewnych permutacji prostych

Przykłady $\sigma \in S_6$ $\sigma = \begin{pmatrix}1&2&3&4&5&6\\2&3&5&4&1&1\end{pmatrix}$

(1) 

„nieistotna"

Powiemy, że „σ jest cyklem"

(2) $\tau \in S_4$ $\tau = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$   „τ nie jest cyklem"

Def

Niech $\sigma \in S_n$. Wtedy nośnik σ (ozn. X_σ) to:

$X_\sigma := \{ i \in \{1, 2, \ldots, n\} \mid \sigma(i) \neq i \}$.

Powyżej: (1) $X_\sigma = \{1, 2, 3, 5\}$

(2) $X_\tau = \{1, 2, 3, 4\}$

Def

(1) Niech $\sigma \in S_n$. Mówimy, że σ jest cyklem długości k, gdy $|X_\sigma| = k$ oraz możemy zapisać $X_\sigma = \{i_1, i_2, \ldots, i_k\}$ tak, że: $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \ldots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$.

Taki cykl zapisujemy $(i_1, i_2, \ldots, i_k)$.

(2) Cykl długości 2 nazywamy transpozycją.

Uwaga

Zapis z (1) nie jest jednoznaczny, np $(1,2) = (2,1)$.

Przykład

$S_2 = \{id, (1,2)\}$, $S_3 = \{id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$

Czyli S_2 i S_3 składają się z samych cykli!

Ale $\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} \in S_4$ już nie jest cyklem.

$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} = \underbrace{(1,2) \circ (3,4)}_{\text{iloczyn „rozłącznych" cykli}}$

Def

Niech $\sigma, \tau \in S_n$. Powiemy, że σ i τ są rozłączne, gdy $X_\sigma \cap X_\tau = \emptyset$, czyli gdy ich nośniki są rozłączne.

Przykład

Permutacje $(1,2)$ i $(3,4)$ są rozłączne.

TW. (dowód pomijamy)

Jeśli σ i τ to rozłączne permutacje z S_n, to $\sigma \circ \tau = \tau \circ \sigma$.

Rozłączne permutacje są ze sobą przemienne.