Przykłady

(1) $\underbrace{\{0,2,4,6\}}$ $\leq \mathbb{Z}_8$ (podgrupa) (L2 ZAD 3d))

to są wszystkie wielokrotności 2 w grupie $(\mathbb{Z}_8, +_8)$

$\mathbb{Z}_8$: skończona, więc jest skończenie wiele tych wielokrotności:

$2,\ 2+_8 2 = 4,\ 2+_8 2 +_8 2 = 6,\ 2+_8 2+_8 2+_8 2 = 0$

(2) $\underbrace{3\mathbb{Z}} := \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} = \{3k \mid k \in \mathbb{Z}\}$

wszystkie wielokrotności 3 w grupie $(\mathbb{Z}, +)$.

Też: $3\mathbb{Z} \underset{\text{podgrupa}}{<} (\mathbb{Z}, +)$

TW.

G: grupa, $g \in G$. Wtedy podzbiór $\{g^n \mid n \in \mathbb{Z}\} \subseteq G$ jest najmniejszą podgrupą G zawierającą element g.

Dowód Pokazujemy najpierw: $\{g^n \mid n \in \mathbb{Z}\} \leq G$

(i) $\forall m, n \in \mathbb{Z}$ $g^n g^m = g^{n+m}$ OK (zamkniętość na działanie)

(ii) $e = g^0 \in \{g^n \mid n \in \mathbb{Z}\}$ OK

(iii) $\forall m \in \mathbb{Z}$ $(g^m)^{-1} = g^{-m} \in \{g^n \mid n \in \mathbb{Z}\}$ OK

Pokazujemy „najmniejszość". Weźmy dowolną $H \leq G : g \in H$.

Mamy pokazać: $\{g^n \mid n \in \mathbb{Z}\} \overset{?}{\subseteq} H$. Dla $n > 0$ mamy:

$g^n = \underbrace{g \cdots g}_{n} \in H$, bo $g \in H \leq G$ | $e = g^0 \in H$. $g^{-n} = (g^{-1})^n \xRightarrow[H \leq G]{g^{-1} \in H} (g^{-1})^n \in H$ OK ∎

Def

Niech G będzie grupą i $g \in G$.

(1) $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$: podgrupa G

(2) Grupę G nazywamy cykliczną, gdy $\exists g \in G$ takie, że $G = \langle g \rangle$.

Przykłady

(1) $G = S_3$, $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Wtedy $\langle g \rangle = \{g^0, g^1, g^2\} = \{id, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\}$

(2) $G = \mathbb{Z}$, $g = 3$. Wtedy $\langle g \rangle = 3\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\}$

(3) $G = \mathbb{Z}_8$, $g = 2$. Wtedy $\langle 2 \rangle = \{0, 2, 4, 6\}$

(4) $G = \mathbb{Z}_n$, $g = 1$. Wtedy $\langle 1 \rangle = \{0, 1, \ldots, n-1\} = \mathbb{Z}_n$: cykliczna!

(5) $G = \mathbb{Z}$, $g = 1$. Wtedy $\langle 1 \rangle = \mathbb{Z}$: cykliczna!

TW.

Załóżmy, że G jest grupą cykliczną. Wtedy:

(1) Jeśli G jest skończona, to $\exists n > 0$ takie, że $G \cong \mathbb{Z}_n$.

(2) —— " —— nieskończona, to $G \cong \mathbb{Z}$.

W szczególności, każda grupa cykliczna jest przemienna.

Do dowodu potrzebujemy:

Lemat

Załóżmy, że G jest grupą, $g \in G$ i $G = \langle g \rangle$ (czyli G jest cykliczna).

Jeśli dla pewnego $k \in \mathbb{N}_{>0}$ mamy $g^k = e$, to $|G| \leq k$.

Dowód lematu

Wystarczy pokazać: $\langle g \rangle \overset{?}{\subseteq} \{g^0, g^1, \ldots, g^{k-1}\}$ (zał. $g^k = e$)

Weźmy dowolny $g^m \in \langle g \rangle$. Wtedy $m = lk + r$ dla pewnego $l \in \mathbb{Z}$ i $r = r_k(m) \in \{0, 1, \ldots, k-1\}$.

$g^m = g^{lk+r} = g^{lk} g^r = (g^k)^l g^r = e^l g^r = e g^r = g^r \in \{g^0, g^1, \ldots, g^{k-1}\}$ ∎

Dd TW ✓ pierwszy przypadek

(1) Załóżmy, że G jest cykliczna i $|G| = n \in \mathbb{N}_{>0}$.

Niech $g \in G$ takie, że $G = \langle g \rangle$. Definiujemy funkcję:

$f : \mathbb{Z}_n \to G$, $f(r) := g^r$.

CEL: f jest izomorfizmem 4 kroki

Krok 1 f jest „1-1"

Weźmy $i, j \in \mathbb{Z}_n : i < j$ i załóżmy nie wprost $f(i) = f(j)$.

Dojdziemy do sprzeczności. $g^i = f(i) = f(j) = g^j \ / \cdot g^{-i}$

$e = g^0 = g^i \cdot g^{-i} = g^j \cdot g^{-i} = g^{j-i}$

$0 \leq i < j < n \Rightarrow 0 < j - i < n$

$\xRightarrow[G = \langle g \rangle]{\text{Lemat}} |G| \leq j - i < n$ ↯ sprzeczn.

Ale $|G| = n$!

Krok 2 f jest „na"

Krok 1 $\Rightarrow$ f jest różnowartościową funkcją ze skończonego zbioru n-elementowego $(\mathbb{Z}_n)$ w zbiór n-elementowy (G).

Czyli f jest „na"!

Krok 3 $g^n = e$ ($f : \mathbb{Z}_n \to G$, $|G| = n$)

Krok 1 $\Rightarrow$ $0 \leq i < j < n \Rightarrow g^i \neq g^j$. Stąd

$\underbrace{\{g^0, g^1, \ldots, g^{n-1}\}}_{n \text{ elem.}} = G$ (bo $|G| = n$).

$g^n \in G \Longrightarrow \exists l \in \{0, 1, \ldots, n-1\}$ $g^n = g^l$. CEL: $l = 0$

Jeśli $l > 0$ to j.w. $g^{n-l} = e$, $0 < n - l < n \xRightarrow{\text{Lemat}} |G| \leq n - l < n$ ↯ !

Stąd $g^n = g^0 = e$ OK.

Krok 4 f jest homomorfizmem Weźmy $i, j \in \mathbb{Z}_n$

$f(i +_n j) = g^{i +_n j} = g^{i + j + ln} = g^{i+j}(g^n)^l \overset{\text{Krok 3}}{=} g^{i+j} e^l = g^i g^j = f(i) f(j)$ ok

(bo $i +_n j = r_n(i+j) = i + j + ln$ dla pewnego $l \in \mathbb{Z}$)

(2) Załóżmy, że $G = \langle g \rangle$ jest nieskończona. Definiujemy:

$f : \mathbb{Z} \to G$, $f(l) := g^l$.

$G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} \Longrightarrow f$ jest „na"

$\forall i, j \in \mathbb{Z}$ $f(i+j) = g^{i+j} = g^i g^j = f(i) f(j)$

Czyli f : homomorfizm.

Pozostaje: f jest „1-1"

Weźmy $i, j \in \mathbb{Z}$ $i < j$ załóżmy nie wprost $f(i) = f(j)$

$\Longrightarrow g^i = g^j \underset{\text{j.w.}}{\Longrightarrow} \underbrace{g^{j-i} = e \quad j - i > 0}$

$\Downarrow$

$|G| \leq j - i$

$\Downarrow$

G : skończona ↯ !

∎