__Przypomnienie__ $G, H$: grupy

$f: G \to H$ jest homomorfizmem, gdy $\forall x, y \in G \; f(xy) = f(x)f(y)$

__Nazewnictwo__

$f: G \to H$ homomorfizm. Wtedy:

- $f$ jest __monomorfizmem__, gdy $f$ jest „1-1"
- —"— __epimorfizmem__ ——"—— „na"
- —"— __endomorfizmem__, gdy $G = H$
- —"— __automorfizmem__, gdy $G = H$ i $f$: izomorfizm

(czyli „izomorfizm = monomorfizm + epimorfizm")

__Fakt__ (ZAD)

$G, H, N$: grupy, $\varphi: G \to H$, $\psi: H \to N$. Wtedy:

(i) $\varphi, \psi$: homomorfizmy $\Rightarrow$ $\psi \circ \varphi$: homomorfizm

(ii) $\varphi$: izomorfizm $\Rightarrow$ $\varphi^{-1}: H \to G$ izomorfizm.

(iii) $\underset{\substack{\uparrow \\ \text{izom jest } id_G}}{G \cong G}$, $G \cong H \overset{(ii)}{\Rightarrow} H \cong G$, $G \cong H$ i $H \cong N \overset{(i)}{\Rightarrow} G \cong N$

(tak jakby: „$\cong$ to relacja równoważności")

__Def.__

$\mathrm{Aut}(G) := \{\varphi \in \underbrace{S_G}_{\text{grupa bijekcji } G \to G} \mid \varphi: \text{automorfizm}\}$

__ZAD__

$\mathrm{Aut}(G) \underset{\substack{\uparrow \\ \text{podgrupa}}}{\leq} S_G$, czyli $\mathrm{Aut}(G)$ jest grupą $\begin{pmatrix}\text{samą} \\ \text{w sobie}\end{pmatrix}$.

__Przykłady__

(1) Zobaczymy na KONW że $\forall k \in \mathbb{Z}$ funkcja

$\varphi_k: \mathbb{Z} \to \mathbb{Z}$, $\varphi_k(x) = kx$

jest endomorfizmem $(\mathbb{Z}, +)$ i że wszystkie endomorfizmy $\mathbb{Z}$ są tej postaci. Łatwo zauważyć:

$\varphi_k$: automorfizm $\iff k \in \{-1, 1\}$

(czyli $\mathrm{Aut}(\mathbb{Z}) = \{\varphi_{-1}, \underbrace{\varphi_1}_{id}\}$.

| $(\mathrm{Aut}(\mathbb{Z}), \circ)$ | $\varphi_1$ | $\varphi_{-1}$ |
|---|---|---|
| $\varphi_1$ | $\varphi_1$ | $\varphi_{-1}$ |
| $\varphi_{-1}$ | $\varphi_{-1}$ | $\varphi_1$ |

„te same" tabelki

i $\mathrm{Aut}(\mathbb{Z}) \cong (\mathbb{Z}_2, +_2)$

$\varphi_1 \longmapsto 0$

$\varphi_{-1} \longmapsto 1$

(2) Zobaczymy na KONW że $\forall k \in \mathbb{Z}_n$ funkcja

$\varphi_k: \mathbb{Z}_n \to \mathbb{Z}_n$, $\varphi_k(x) = k \cdot_n x$

jest endomorfizmem $\mathbb{Z}_n$ i że wszystkie endomorfizmy są tej postaci. Wtedy mamy:

$\varphi_k \in \mathrm{Aut}(\mathbb{Z}_n) \iff k \in \mathbb{Z}_n^* \left(= \{m \in \mathbb{Z}_n \mid \mathrm{NWD}(n, m) = 1\}\right)$

Poza tym $\varphi_k \circ \varphi_l = \varphi_{k \cdot_n l}$. Stąd:

$\mathbb{Z}_n^* \ni k \longmapsto \varphi_k \in \mathrm{Aut}(\mathbb{Z}_n)$ jest izomorfizmem

i mamy $\mathrm{Aut}(\mathbb{Z}_n) \cong (\mathbb{Z}_n^*, \cdot_n)$. Np:

$\mathrm{Aut}(\mathbb{Z}_8) \cong \mathbb{Z}_8^*$ $\quad \mathbb{Z}_8^* = \{1, 3, 5, 7\}$

| $(\mathbb{Z}_8^*, \cdot_8)$ | 1 | 3 | 5 | 7 |
|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 |
| 3 | 3 | 1 | 7 | 5 |
| 5 | 5 | 7 | 1 | 3 |
| 7 | 7 | 5 | 3 | 1 |

$\Rightarrow \underset{\substack{\uparrow \\ \text{grupa Kleina}}}{K_4} \cong \mathbb{Z}_8^* \cong \mathrm{Aut}(\mathbb{Z}_8)$

__TW__

$f: G \to H$ homomorfizm. Wtedy mamy:

(i) $f(e_G) = e_H$ (ii) $\forall g \in G \; f(g^{-1}) = f(g)^{-1}$.

(iii) $\begin{pmatrix}\text{uogólnienie} \\ \underset{n=0}{(i)}, \underset{n=-1}{(ii)}\end{pmatrix}$ $\forall n \in \mathbb{Z} \; f(g^n) = f(g)^n$

(iv) $f$ „1-1" $\Rightarrow \forall g \in G \; \mathrm{ord}(g) = \mathrm{ord}(f(g))$

(v) $\forall g \in G \; \mathrm{ord}(g)$ skończony $\Rightarrow$ $\mathrm{ord}(f(g))$ skończony i $\mathrm{ord}(f(g)) \mid \mathrm{ord}(g)$

__Dowód__ Lista 3 ZAD 4K.

4K. Załóżmy, że $f: G \to H$ jest homomorfizmem grup, $g \in G$ i $n \in \mathbb{Z}$. Udowodnić, że:
(a) $f(g^n) = (f(g))^n$; (iii)
(b) jeśli $f$ jest różnowartościowy, to $\mathrm{ord}_G(g) = \mathrm{ord}_H(f(g))$; (iv)
(c) jeśli $\mathrm{ord}_G(g) = k$ jest skończony, to $g^n = e$ wtedy i tylko wtedy, gdy $k|n$.

(v) $g^k = e_G \Rightarrow f(g^k) = f(e_G) \overset{(i)}{=} e_H$

$f(g^k) \overset{(iii)}{=} f(g)^k = e_H \overset{\text{ZAD 4K (c)}}{\Longrightarrow} \mathrm{ord}(f(g)) \mid k = \mathrm{ord}(g)$ ∎

Pojęcie grupy wzięło z pojęcia __grupy przekształceń__ (u nas: __podgrupa $S_X$__ dla pewnego $X$).

Zobaczymy, że każdą grupę możemy rozumieć jako grupę przekształceń. Do tego służy:

__TW. Cayley'a__

Dla dowolnej grupy $G$ istnieje monomorfizm $\alpha: G \to S_G$ ($S_G$ to grupa bijekcji $G \to G$)

__Dowód__ (szkic)

Bierzemy $g \in G$ i mamy znaleźć $F_g: G \to G$.

Definiujemy $F_g$ jako $F_g(x) := g \underset{\substack{\uparrow \\ \text{działanie w } G}}{\cdot} x$ $(x \in G)$

Sprawdza się (pominiemy):

(i) $\forall g \; F_g$ jest bijekcją, czyli $F_g \in S_G$.

(ii) $\forall g, h \in G \; F_g \circ F_h = F_{gh}$ czyli funkcja

$\alpha: G \to S_G$ $\alpha(g) = F_g$ jest homomorfizmem.

(iii) $\alpha$ jest „1-1". ∎