Homomorfizmy.

Def. Niech $(G, \circ)$, $(H, *)$ grupy.

1. funkcję $\varphi: G \to H$ nazywamy homomorfizmem, gdy
   $(\forall g_1, g_2 \in G)\ \varphi(g_1 \circ g_2) = \varphi(g_1) * \varphi(g_2)$

2. funkcję $\varphi: G \to H$ nazywamy izomorfizmem gdy φ jest homomorfizmem i bijekcją

- Grupy $(G, \circ)$, $(H, *)$ nazywamy izomorficznymi gdy istnieje $\varphi: G \to H$ izomorfizm.

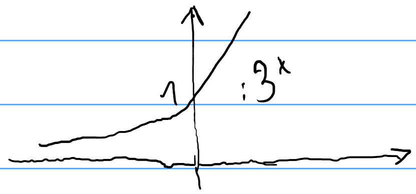
Przykład: Rozważmy grupy $\overset{G}{(\mathbb{R}, +)}$, $\overset{H}{((0, \infty), \cdot)}$

Funkcja $\varphi(x) = 3^x : \mathbb{R} \to (0, \infty)$ jest homomorfizmem
(a nawet izomorfizmem G i H.)

izomorfizm

hom: $\varphi(x+y) = 3^{x+y} = \underline{3^x} \cdot 3^y = \varphi(x) \cdot \varphi(y)$.

φ jest bijekcją:



- różnowart.
- jest na zbiór $(0, \infty)$.

Przykład 2. wtedy $n \in \mathbb{N}^+$
Rozważmy grupy $(\mathbb{Z}, +)$, $\mathbb{C}_n = (\{0, 1, \dots, n-1\}, +_n)$

funkcja $\varphi_n(x) = x \pmod n$ = reszta z dziel. x przez n
$\varphi_n(x): \mathbb{Z} \to \{0, \dots, n-1\}$
jest homomorfizmem grup $(\mathbb{Z}, +)$ i $\mathbb{C}_n$

Dowód: $(\forall x, y \in \mathbb{Z})\ \varphi_n(x+y) = (x+y) \pmod n =$

$(x \pmod n + y \pmod n) \pmod n = (\varphi_n(x) + \varphi_n(y)) \pmod n =$
$\varphi_n(x) +_n \varphi_n(y)$. $\square$

Fakt. Niech $(G, \circ)$, $(H, *)$ grupy $e_G \in G$, $e_H \in H$ elementy neutralne, $\varphi: G \to H$ homomorfizm. Wtedy

1. $\varphi(e_G) = e_H$
2. $(\forall g \in G)$ $\varphi(g^{-1}) = (\varphi(g))^{-1}$

D-d. 1. Niech $g \in G$, rozważmy

$$\varphi(g) * \varphi(e_G) \stackrel{h}{=} \varphi(g \circ e_G) = \varphi(g)$$

- Więc $\varphi(e_G)$ jest elementem neutralnym dla działania $*$ na zbiorze $\{\varphi(g) : g \in G\}$
- e_H jest także elementem neutralnym dla działania $*$ na $\{\varphi(g) : g \in G\}$

Element neutralny działania na zbiorze jest jedyny więc $e_H = \varphi(e_G)$ $\square$

2. Rozważmy: niech $g \in G$

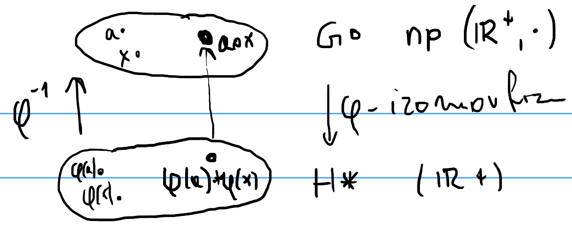
$$\varphi(g) * \varphi(g^{-1}) \stackrel{h}{=} \varphi(g \circ g^{-1}) = \varphi(e_G) \stackrel{(1)}{=} e_H$$

$$\varphi(g) * \varphi(g^{-1}) = e_H \quad \Big| \ (\varphi(g))^{-1} *$$

$$\cancel{(\varphi(g))^{-1} * \varphi(g)} * \varphi(g^{-1}) = (\varphi(g))^{-1} * e_H$$

$$\varphi(g^{-1}) = (\varphi(g))^{-1} \qquad \square$$

Koment: • to że grupy są izomorficzne rozumiemy że są niemal identyczne.



ILOCZYN KARTEZJAŃSKI GRUP

Def. Niech $(G,\circ)$, $(H,*)$ grupy. Na zbiorze
$G\times H = \{(g,h) : g\in G,\ h\in H\}$ definiujemy działanie $\otimes$

$$(g_1,h_1)\otimes(g_2,h_2) = (g_1\circ g_2,\ h_1 * h_2).$$

Fakt Niech $(G,\circ)$, $(H,*)$ jak wyżej:
$(G\times H,\otimes)$ jest grupą.

D-d ćw

Przykład: $(\mathbb{R}^+,\cdot)$, $(\mathbb{Z},+)$

Na zbiorze $\mathbb{R}^+\times\mathbb{Z}$ def działanie

- $(r,n)\otimes(s,m) = (r\cdot s,\ n+m)$
- Element neutralny to $e=(1,0)$.
- Element odwrotny do (r,n) to $(r^{-1},-n)$

Spr $(r,n)\otimes(r^{-1},-n) = (r\cdot r^{-1},\ n-n) = (1,0) = e$.

Przykład. $(\mathbb{R},+)\times(\mathbb{R},+)$

Na zbiorze $\mathbb{R}\times\mathbb{R}=\mathbb{R}^2$ def działanie

$$(a,b)\oplus(x,y) = (a+x,\ b+y).$$

- To jest dodawanie wektorów.

- Produkt wielu grup.

Dla grup $(H_1,\overset{1}{\circ})$, $(H_2,\overset{2}{\circ})$, $(H_3,\overset{3}{\circ})$ Wtedy

na zbiorze $H_1\times H_2\times H_3 = \{(h_1,h_2,h_3) : h_i\in H_i\}$

definiujemy $\circ$: $(h_1, h_2, h_3) \circ (g_1, g_2, g_3) = (h_1 \overset{1}{\circ} g_1, h_2 \overset{2}{\circ} g_2, h_3 \overset{3}{\circ} g_3)$

Wtedy $(H_1 \times H_2 \times H_3, \circ)$ jest grupą.

Uwaga. Niech $(G, \circ), (H, *)$ grupy, oraz $(G \times H, \otimes)$ produkt.

to funkcje $\cdot\ \varphi: G \times H \to G$, $\varphi(g, h) = g$ jest homomorfizmem.

$\cdot\ \psi: G \to G \times H$, $\psi(g) = (g, e)$ jest homomorfizmem.

bo: $\psi(g_1 \circ g_2) = (g_1 \circ g_2, e) = (g_1 \circ g_2, e * e) = (g_1, e) \otimes (g_2, e)$

$= \psi(g_1) \otimes \psi(g_2)$, więc ψ jest homomorfizmem.

φ jest homomorf $\leftarrow$ ćwiczenie.

Rząd elementu w produkcie grup.

Przykład: $\mathbb{C}_3 \times \mathbb{C}_5 = (\{0,1,2\} \times \{0,1,2,3,4\}, +)$

Ord$(1,1)$: szukamy n, że $\underbrace{(1,1) + (1,1) + \dots + (1,1)}_{n \times} = (0,0)$.

$n = 15$ bo $n | 3$ i $n | 5$

Ogólnie: G, H grupy.

ord(g,h) w $G \times H$:

ord(g,h) = NWW$\{$ Ord(g), Ord(h). $\}$

PODGRUPY:

Def Niech $(G,\circ)$ grupa $H \subseteq G$ ($H \neq \emptyset$, podzbiór). Wtedy H nazywamy podgrupą grupy G, gdy:

1. $(\forall h_1, h_2 \in H)\quad h_1 \circ h_2 \in H$
2. $(\forall h \in H)\quad h^{-1} \in H$

ozn $H \leq G$.

Przykład. $G = (\mathbb{Z}, +)$, $H = 2\mathbb{Z} = \{2 \cdot k : k \in \mathbb{Z}\}$

$2\mathbb{Z} \leq \mathbb{Z}$ jest podgrupą

Przykład. $G = S_3$ - grupa permutacji
$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \underset{\text{izo}}{\overset{!!!}{\cong}} \mathbb{C}_2$

Uwaga: Dla dowolnej grupy G, oraz $H \leq G$ $e \in H$
bo: $H \neq \emptyset$ to istnieje $h \in H$ więc (2) $h^{-1} \in H$
więc (1) $e = h \circ h^{-1} \in H$ □

Fakt Niech $(G,\circ)$ grupa $H \leq G$. Wtedy $(H,\circ)$ jest grupą.