Grupy.

Grupa to para $(G, \circ)$ takie, że

0. $\circ$ jest działanie na G
1. działanie $\circ$ jest łączne
2. istnieje element neutralny działania $\circ$ na G
3. $\forall x \in G \; \exists y \in G \quad x \circ y = e$ gdzie $e \in G$ element neutralny.

Przykłady: 1. $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, są grupami
2. $(\mathbb{N}, +)$ $(\mathbb{Q}, \cdot)$ NIE są grupami.

NOWY: Dla $n \in \mathbb{N}^+$ definiujemy grupę CYKLICZNĄ

$\mathbb{C}_n = (\{0, \dots, n-1\} \; +_n)$

$a +_n b = (a+b) \bmod n$ ← reszta z dzielenia przez n.

GRUPY $\mathrm{Sym}(X)$.

Def. Niech X, Y zbiory. Funkcję $f: X \to Y$ nazywamy bijekcją gdy:

1. f jest różnowartościowe tzn $(\forall x_1, x_2) \; f(x_1) = f(x_2) \to x_1 = x_2$
2. f jest "na" tzn $\forall y \in Y \; \exists x \in X \quad f(x) = y$

Przykład $f(x) = 2x+1 : \mathbb{R} \to \mathbb{R}$ jest bijekcją...

1. Jeśli $f(x_1) = f(x_2)$ tzn $2x_1 + 1 = 2x_2 + 1 \to x_1 = x_2$
2. Niech $y \in \mathbb{R}$ Wez $x = \frac{y-1}{2}$. Wtedy $f(x) = y$.

Przykład $f(x) = x^2 : \mathbb{R} \to \mathbb{R}$: NIE jest bijekcją:

1. nie jest różnowart: $f(1) = f(-1)$.
2. nie jest "na" $(\nexists x) f(x) = (-1)$.

Przykład: Funkcja $f: \{1,2,3,4\} \to \{1,2,3,4\}$

zadana: $\begin{array}{c|c|c|c} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{array}$.

Def. Niech X zbiór. Grupę symetrii zbioru X nazywamy:

$Sym(X) = (\{f: X \to X : f \text{ jest bijekcją}\}, \circ)$

$\circ$ składanie funkcji: $(f \circ g)(x) = f(g(x))$

Przykład. $X = \{1,2,3\}$.

Każdy element grupy $Sym(X)$ jest funkcją którą możemy zapisać tabelką np: $\begin{array}{c|c|c} 1 & 2 & 3 \\ 2 & 3 & 1 \end{array}$

$|Sym(X)| = 3! = 6$.

Działanie: Niech f zadane przez $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$,

g zadane przez $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ to

$f \circ g(1) = f(g(1)) = f(2) = 3$

$f \circ g(2) = f(g(2)) = f(1) = 2$

Zatem tabelka dla $f \circ g$: $\begin{array}{c|c|c} 1 & 2 & 3 \\ 3 & 2 & 1 \end{array}$

TW. Dla dowolnego zbioru X. $Sym(X)$ jest grupą.

$Sym(X) = (\{f: X \to X : \text{bijekcja}\}, \circ)$

0). Złożenie bijekcji jest bijekcją ćw.

1. Składanie funkcji jest łączne: $f, g, h \in Sym\, X$

$(\forall x \in X)$ $f \circ (g \circ h)(x) = f((g \circ h)(x)) = f(g(h(x)))$

$\underline{(f \circ g)} \circ \underline{h}\,(x) = (f \circ g)(h(x)) = f(g(h(x)))$ ||

Więc $f \circ (g \circ h) = (f \circ g) \circ h$

2. Element neutralny w $S_n(X)$:

$e = id : X \to X$ gdzie $\forall x \quad id(x) = x$

Spr: Niech $f \in S_n(X)$

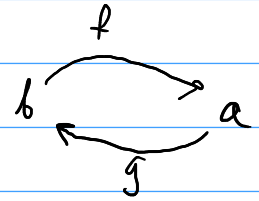
$\forall x \quad f \circ id(x) = f(id(x)) = f(x)$

$f \circ id = f$.

3. Element odwrotny do $f \in S_n(X)$.

to taka funkcja $g : X \to X$, że

$a \in X$: $g(a) = b$ gdy $f(b) = a$



(możliwe bo f jest bijekcją)

Ozn: Funkcja odwrotna do f oznaczamy f^{-1}. □

Grupy permutacji:

Dla $n \in \mathbb{N}^+$ definiujemy grupę permutacji S_n:

Def: $S_n = S_n(\{1,2,3,\dots,n\}) = (\{f : \{1,\dots n\} \to \{1,\dots n\} \text{ bijekcja}\}, \circ)$

Oznaczenia:

Elementy S_n są postaci: $\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 3 & 1 & n & \dots & 2 \end{pmatrix}$

dowolna permutacja elementów $1,2,3,\dots n$

- Element $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ rozumiemy jako funkcję $f : \{1,2,3\} \to \{1,2,3\}$ zadaną tabelką $\begin{array}{c|c} 1 & 2 \\ 2 & 3 \end{array} \quad \begin{array}{c|c} 2 & 3 \\ 3 & 1 \end{array} \quad \begin{array}{c|c} 3 & 1 \\ 1 & 2 \end{array}$

- Obliczenie w grupie S_n, $n = 3$.

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \overset{?}{=} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

II I

- $\left(\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\right)(1) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\left(\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}(1)\right) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}(2) = 3$

- Element neutralny w S_3 to $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$. Spr. ćw

- Element odwrotny do $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ to:

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\circ\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}^{-1}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$$

Potęgowanie w grupie.

Def. Niech $(G,\circ)$ grupa, $g\in G$, $k\in\mathbb{Z}$.

$$g^k=\begin{cases}\overbrace{g\circ g\circ\dots\circ g}^{k\times} & k=1,2,3,\dots\\ e & k=0\\ (g^{-1})^{(-k)} & k=-1,-2,\dots\end{cases}$$

$g^1=g$

g^{-1} – element przeciwny do g

Przykład.

W S_3: $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}^{-3}=\left(\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}^{-1}\right)^3=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}^3=$

$\left(\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\circ\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right)\circ\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\circ\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=e$

TW (Własności potęgowania).
Niech $(G,\circ)$ grupa. Wtedy: $\forall a,b\in G,\ k,l\in\mathbb{Z}$:

1. $a^k\circ a^l=a^{k+l}$
2. $(a^k)^l=a^{k\cdot l}$
3. Jeśli $(G,\circ)$ jest przemienne to $(a\circ b)^k=a^k\circ b^k$.

$a\cdot b=b\cdot a$

Dowód. 1. Gdy $k,l>0$ wtedy

$$a^k\circ a^l=\underbrace{(a\circ a\circ\dots\circ a}_{k\times}a)\circ\underbrace{(a\circ\dots\circ a)}_{l}\overset{\text{łączność}}{=}\underbrace{a\circ a\circ\dots\circ a}_{k+l}=a^{k+l}$$

Gdy $k>0$ $l<0$ $\quad k>-l$

$$a^k\circ a^l=\underbrace{(a\circ\dots a)}_{k}\circ\underbrace{(a^{-1})\circ\dots\circ(a^{-1})}_{-l}=\dots\underbrace{a\circ\dots\circ e}_{k-(-l)=k+l}=a^{k+l}$$

2. $(a \circ b)^k \overset{k>0}{=} (a \circ b) \circ (a \circ b) \circ \dots \circ (a \circ b) \overset{\text{łączność}}{=}$

$a \circ b \circ a \circ b \circ \dots \circ a \circ b \overset{\text{P}}{=}$

$\underbrace{(a \circ a \circ \dots \circ a)}_{k} \circ \underbrace{(b \circ b \circ \dots \circ b)}_{k} = a^k \circ b^k$ □

Rząd elementu.

Def Niech $(G, \circ)$ - grupa, $g \in G$.

Rzędem elementu g nazywamy liczbę naturalną lub symbol ∞

$$\operatorname{ord}(g) = \begin{cases} \min\{n \in \mathbb{N}^+ : g^n = e\} & \text{jeśli istnieje} \\ \infty & \text{w przeciwnym wypadku} \end{cases}$$

Przykład w grupie $(\mathbb{R} \setminus \{0\}, \cdot)$ tu $e = 1$

$\operatorname{ord}(7) = \infty$ bo $\forall n \in \mathbb{N}^+ \quad 7^n > 1$

$\operatorname{ord}(1) = 1$

$\operatorname{ord}(-1) = 2$.

F: W grupie skończonej każdy element ma rząd skończony.

D-d Niech $(G, \circ)$ skończona, $g \in G$.

Zauważmy: bo G - skończona.

Istnieje $k \neq l \in \mathbb{N}^+$ że $g^k = g^l \quad / \circ g^{-l}$

$g^k \circ g^{-l} = g^l \circ g^{-l}$

$g^{k-l} = g^{l-l} = g^0 = e$

$g^{k-l} = e$

$k - l > 0$

$\operatorname{ord}(g) < \infty$. □

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

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

2. Jeśli dodatkowo f jest bijekcją to f nazywamy izomorfizmem

Przykład: $f(x) = 2^x : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$
jest izomorfizmem.

bo: f jest bijekcją ....
f jest homomorfizmem bo:

$a, b \in \mathbb{R}$ $f(a+b) = 2^{a+b} = 2^a \cdot 2^b = f(a) \cdot f(b)$.