Przykłady działań

Działania modulo n $(n \in \mathbb{N}_{\geq 2} = \{2, 3, 4, \dots\})$

Niech $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ oraz $r_n : \mathbb{Z} \to \mathbb{Z}_n$ będzie funkcją n-tej reszty tzn. $\forall x \in \mathbb{Z}\ \forall r \in \mathbb{Z}_n$:

$r_n(x) = r \iff r$ jest resztą z dzielenia x przez $n \iff$

$\iff n \mid x - r$ | np. $r_5(-7) = 3$

Definiujemy działania dodawania i mnożenia modulo n ($+_n$ i $\cdot_n$) na zbiorze $\mathbb{Z}_n$. Weźmy $x, y \in \mathbb{Z}_n$:

$$x +_n y := r_n(x+y), \quad x \cdot_n y := r_n(x \cdot y)$$

$+_n$: dodawanie modulo n; $\cdot_n$: mnożenie modulo n.

Np. $3 +_5 4 = r_5(3+4) = r_5(7) = 2$, $3 \cdot_5 4 = r_5(12) = 2$

Tabelka $+_2$: (na $\mathbb{Z}_2 = \{0, 1\}$)

$+_2$	0	1
0	0	1
1	1	0

← działanie $*$ z poprzedniego wykładu! (dane tabelką)

Udowodnimy teraz łączność $+_n$.

Weźmy $x, y, z \in \mathbb{Z}_n$. Pokażemy, że:

$$(x +_n y) +_n z \overset{?}{=} r_n(x+y+z) \overset{?}{=} x +_n (y +_n z).$$

$(x +_n y) +_n z \overset{(i)}{=} r_n((x +_n y) + z)$

Będziemy używali prostej obserwacji:

$$\boxed{\forall a, b \in \mathbb{Z} \quad r_n(a) = r_n(b) \iff n \mid a - b}$$

Z def. r_n ⇓

$$n \mid (x +_n y) - (x+y) = \underbrace{(x +_n y) + z}_{a} - \underbrace{(x+y+z)}_{b}$$

⇓ prosta obserwacja

$$r_n((x +_n y) + z) \overset{(ii)}{=} r_n(x+y+z) \overset{(i)}{\underset{(ii)}{\Longrightarrow}} (x +_n y) +_n z = r_n(x+y+z)$$

analogicznie

Oczywiście 0 jest elementem neutralnym $+_n$.

Ponadto, 0 — " — odwrotnym do samego siebie (jak każdy element neutralny).

$\forall x \in \mathbb{Z}_n$ jeśli $x \neq 0$, to $n - x \in \mathbb{Z}_n$ i wtedy:

$x +_n (n-x) = 0 = (n-x) +_n x$, czyli $n-x$ jest elementem odwrotnym do x. Czyli $(\mathbb{Z}_n, +_n)$ jest grupą.

$+_n$: przemienne $\Rightarrow$ $(\mathbb{Z}_n, +_n)$: grupa przemienna.

A co z $\cdot_n$? Podobnie jak dla $+_n$ pokazuje się:

$$a \cdot_n (b \cdot_n c) = r_n(abc) = (a \cdot_n b) \cdot_n c$$

czyli $\cdot_n$ jest łączne. Oczywiście $\cdot_n$ jest przemienne, 1: elem. neutralny $\cdot_n$. Ale 0 nie ma elem. odwrotnego względem $\cdot_n$. Stąd $(\mathbb{Z}_n, \cdot_n)$ NIE jest grupą.

Kolejne przykłady: skończone grupy symetrii

Niech $n \in \mathbb{N}_{>0}$. Definiujemy $S_n := S_{\{1, \dots, n\}}$: zbiór wszystkich bijekcji z $\{1, \dots, n\}$ w $\{1, \dots, n\}$.

Takie bijekcje nazywamy permutacjami zbioru $\{1, \dots, n\}$.

Wtedy $(S_n, \circ)$ jest grupą i wiemy, że $|S_n| = n!$.

$\circ$: składanie permutacji

Dla $\sigma \in S_n$ ozn.: $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$.

$S_1 = \{\underbrace{\begin{pmatrix} 1 \\ 1 \end{pmatrix}}_{id}\}$, $S_2 = \{\underbrace{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}}_{id}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\}$,

$S_3 = \{\underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}}_{id}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix}\}$

Tabelka S_2:

$\circ$	id	$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$
id	id	$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$	id

Grupy S_1 i S_2 są przemienne, ale S_3 nie:

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

$$\neq$$

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

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

↑ przykład pokazujący, że S_3 nie jest przemienna.

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

Czyli np. $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\Big(\underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}(1)}_{2}\Big) = 3$

Podobnie dla wszystkich $n \geq 3$: S_n nie jest przemienna.

Podsumujmy

- $\forall n \in \mathbb{N}_{>1}$ mamy $(\mathbb{Z}_n, +_n)$: grupa przemienna.
- $\forall n \in \mathbb{N}_{>2}$ — " — $(S_n, \circ)$: grupa nieprzemienna.