

Definicja 1. Działaniem wewnętrznym (lub krótko - działaniem) w zbiorze G nazywamy funkcję

$$\circ : G \times G \rightarrow G.$$

Uwaga 1. Wartość funkcji $\circ : G \times G \rightarrow G$ na parze $(a, b) \in G \times G$ będziemy notować $a \circ b$ (zamiast $\circ(a, b)$) i nazywać wynikiem działania na elementach a i b .

Definicja 2. Działanie $\circ$ określone w zbiorze G nazywamy

1. przemennym, jeżeli dla dowolnych $a, b \in G$

$$a \circ b = b \circ a,$$

2. łącznym, jeżeli dla dowolnych $a, b, c \in G$

$$a \circ (b \circ c) = (a \circ b) \circ c.$$

Przykład 1.

1. $+, \cdot$ są działaniami łącznymi i przemennymi w $\mathbb{R}$;
2. działanie $\circ$ określone w zbiorze $\mathbb{R}$ w następujący sposób

$$a \circ b = 2ab - 4$$

jest przemienne, ale nie jest łączne;

3. działanie $*$ określone w zbiorze $\mathbb{Z}$ w następujący sposób

$$a * b = a + b + 6$$

jest przemienne i łączne;

Definicja 3. Element $e \in G$ nazywamy elementem neutralnym działania $\circ$ określonego w zbiorze G , jeżeli dla każdego $a \in G$

$$a \circ e = e \circ a = a.$$

Przykład 2.

1. 0 jest elementem neutralnym dodawania w $\mathbb{R}$;
2. 1 jest elementem neutralnym mnożenia w $\mathbb{R}$;
3. -6 jest elementem neutralnym działania $*$, określonego w zbiorze $\mathbb{Z}$ w następujący sposób $a * b = a + b + 6$.

Stwierdzenie 1. Działanie $\circ$ określone w zbiorze G posiada co najwyżej jeden element neutralny.

Dowód. Załóżmy, że $e_1, e_2 \in G$ są elementami neutralnymi działania $\circ$. Wtedy

$$e_2 = e_1 \circ e_2 = e_2 \circ e_1 = e_1.$$

Definicja 4. Niech $\circ$ będzie działaniem określonym w zbiorze G , zaś $e \in G$ jego elementem neutralnym. Element $a' \in G$ nazywamy elementem odwrotnym do elementu $a \in G$, jeżeli

$$a' \circ a = a \circ a' = e.$$

Przykład 3.

1. W zbiorze $\mathbb{R}$ ze zwykłym dodawaniem dla liczby $a \in \mathbb{R}$, $a' = -a$ (dla dodawania zwyczajowo mówi się o elemencie przeciwnym, zamiast o odwrotnym);
2. W zbiorze $\mathbb{R}$ ze zwykłym mnożeniem, $a' = \frac{1}{a}$ dla $a \neq 0$, 0 nie posiada natomiast elementu odwrotnego;

Stwierdzenie 2. Niech działanie wewnętrzne $\circ$ w zbiorze G będzie łączne i posiada element neutralny $e \in G$. Element $a \in G$ posiada co najwyżej jeden element odwrotny $a' \in G$.

Dowód. Załóżmy, że element $a \in G$ ma dwa elementy odwrotne $a', a'' \in G$. Wówczas

$$a' = a' \circ e = a' \circ (a \circ a'') = (a' \circ a) \circ a'' = e \circ a'' = a''.$$

Definicja 5. Grupą nazywamy parę $(G, \circ)$, gdzie G jest niepustym zbiorem, $\circ$ działaniem wewnętrznym w zbiorze G , które jest łączne, posiada element neutralny i względem którego każdy element zbioru G posiada element odwrotny. Grupę nazywamy przemienną (abelową), jeżeli działanie $\circ$ jest przemienne.

Wniosek 1.

1. W grupie istnieje dokładnie jeden element neutralny.
2. W grupie każdy element posiada dokładnie jeden element odwrotny.

Przykład 4.

1. Grupami są $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$.
2. Grupami nie są $(\mathbb{N}, +)$, $(\mathbb{R}, \cdot)$.

0.1 Grupy S_n

Niech $n \geq 2$, $n \in \mathbb{N}$. Symbolem S_n będziemy oznaczać od tej pory zbiór wszystkich bijekcji $\tau : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$. Bijekcję ze zbioru S_n nazywać będziemy **permutacją**. Permutację $\tau \in S_n$ notować będziemy w postaci dwuwierszowej

$$\tau = \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix}$$

lub krótko

$$\tau = (\tau(1) \dots \tau(n)).$$

Przykładowo przy $n = 4$ dla

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \in S_4,$$

widzimy, że $\tau(1) = 3, \tau(2) = 2, \tau(3) = 1, \tau(4) = 4$.

Stwierdzenie 3. Para $(S_n, \circ)$, gdzie $\circ$ oznacza składanie funkcji, jest grupą.

Stwierdzenie 4. Grupa S_n dla $n \geq 3$ nie jest przemienna.

Dowód. Niech

$$\tau = \begin{pmatrix} 1 & 2 & 3 & \dots \\ 2 & 1 & 3 & \dots \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 & 3 & \dots \\ 1 & 3 & 2 & \dots \end{pmatrix}.$$

Wtedy

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & \dots \\ 3 & 1 & 2 & \dots \end{pmatrix},$$

zaś

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & \dots \\ 2 & 3 & 1 & \dots \end{pmatrix}.$$

Stąd wnioskujemy, że $\sigma \circ \tau \neq \tau \circ \sigma$.

Uwaga 2. Od tej pory, dla uproszczenia zapisów, będziemy pomijać symbol $\circ$. Pojawi się zatem np. napis $\sigma\tau$ zamiast $\sigma \circ \tau$.

Definicja 6. Permutację $\tau \in S_n$ nazywamy cyklem długości k , $2 \leq k \leq n$ (albo cyklem k -wyrazowym), jeżeli istnieje k -elementowy podzbiór $A = \{a_1, \dots, a_k\}$ zbioru $\{1, \dots, n\}$ taki, że

$$1. \tau(a_1) = a_2, \tau(a_2) = a_3, \dots, \tau(a_{k-1}) = a_k, \tau(a_k) = a_1;$$

$$2. \tau(i) = i \text{ dla } i \notin A.$$

Cykl k -wyrazowy notować będziemy $(a_1, \dots, a_k)$, pomijając w zapisie liczby, które przechodzą na siebie i stosując przecinki. Przyjmujemy, że permutacja tożsamościowa jest cyklem długości 1.

Przykład 5.

1. Permutacja

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 5 & 2 & 6 \end{pmatrix} \in S_6,$$

jest cyklem długości 3; $\tau = (2, 4, 5)$.

2. Permutacja

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 5 & 2 & 6 \end{pmatrix} \in S_6,$$

nie jest cyklem;

Definicja 7. Cykl długości 2 nazywamy transpozycją.

Definicja 8. Cykle $\tau = (a_1, \dots, a_k), \sigma = (b_1, \dots, b_m) \in S_n$ nazywamy rozłącznymi, jeżeli zbiory $A = \{a_1, \dots, a_k\}, B = \{b_1, \dots, b_m\}$ są rozłączne.

Stwierdzenie 5. Jeżeli cykle $\tau, \sigma \in S_n$ są rozłączne, to $\tau\sigma = \sigma\tau$.

Twierdzenie 1. Dowolna permutacja ze zbioru S_n albo jest cyklem, albo daje się przedstawić jako iloczyn cykli rozłącznych. Dodatkowo, dwa przedstawienia danej permutacji w postaci iloczynu cykli rozłącznych różnią się tylko kolejnością czynników.

Nie podajemy tutaj dowodu powyższego twierdzenia. Pokażemy na przykładzie w jaki sposób rozłożyć daną permutację na iloczyn cykli rozłącznych. Niech

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 6 & 1 & 4 & 2 \end{pmatrix},$$
$$\tau = (1, 3, 5)(2, 7)(4, 6).$$

Stwierdzenie 6. Każdy cykl można przedstawić jako złożenie pewnej liczby transpozycji.

Dowód. Cykl długości 1, czyli permutację identycznościową można przedstawić w postaci

$$\tau = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} = (1, 2)(2, 1).$$

Niech $\tau = (a_1, \dots, a_k)$ będzie cyklem długości $k \geq 2$. Wtedy

$$(a_1, \dots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \dots (a_1, a_2).$$

Wniosek 2. Każdą permutację można przedstawić w postaci iloczynu pewnej ilości transpozycji.