

TEMAT: *Działania i wybrane struktury algebraiczne*

1.1 Notacja

Przyjmujemy następującą notację.

$\mathbb{N} = \{1, 2, 3, \dots\}$	zbiór liczb naturalnych
$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$	
$\mathbb{Z}$	zbiór liczb całkowitych
$\mathbb{Q}$	zbiór liczb wymiernych
$\mathbb{R}$	zbiór liczb rzeczywistych

Oznaczenia kwantyfikatorów

$\forall$	kwantyfikator ogólny (duży)	<i>dla każdego</i>
$\exists$	kwantyfikator szczegółowy (mały)	<i>istnieje</i>
$\exists!$		<i>istnieje dokładnie jeden</i>

Symbol sumy i iloczynu

Niech $n \in \mathbb{N}$ oraz niech $a_1, a_2, \dots, a_m, a_{m+1}, \dots, a_n$ to dowolny ciąg liczb.

Sumę $a_1 + a_2 + \dots + a_n$ oznaczamy symbolem $\sum_{i=1}^n a_i$. Symbol i to wskaźnik sumowania lub indeks sumowania, m to dolna granica sumowania, zaś n to górna granica sumowania.

Zauważmy że dla dowolnego $m \in \mathbb{N}$, $m < n$ oraz $c \in \mathbb{R}$ zachodzą równości
 $a_1 + a_2 + \dots + a_n = (a_1 + a_2 + \dots + a_m) + (a_{m+1} + a_{m+2} + \dots + a_n)$ oraz
 $c(a_1 + a_2 + \dots + a_n) = ca_1 + ca_2 + \dots + ca_n$, czyli

$$\sum_{i=1}^n a_i = \sum_{i=1}^m a_i + \sum_{i=m+1}^n a_i, \quad c \sum_{i=1}^n a_i = \sum_{i=1}^n ca_i.$$

Przykład 1.1.1. $\sum_{i=1}^6 i = 1 + 2 + 3 + 4 + 5 + 6 = 21$

$$\sum_{i=5}^9 \frac{i}{i+2} = \frac{5}{7} + \frac{6}{8} + \frac{7}{9} + \frac{8}{10} + \frac{9}{11}$$

$$\sum_{i=0}^n \left(\frac{1}{2}\right)^i = 1 + \frac{1}{2} + \frac{1}{4} + \dots + \left(\frac{1}{2}\right)^n = \frac{1 - \left(\frac{1}{2}\right)^{n+1}}{1 - \frac{1}{2}}$$

Iloczyn $a_1 \cdot a_2 \cdot \dots \cdot a_{n-1} \cdot a_n$ oznaczamy symbolem $\prod_{i=1}^n a_i$. Symbol i to wskaźnik iloczynu, m to dolny wskaźnik iloczynu, zaś n to górny wskaźnik iloczynu.

Przykład 1.1.2. $\prod_{i=0}^6 (9-i) = 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3$

$$\prod_{i=1}^n i = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (-1) \cdot n = n!$$

$$\underbrace{x \cdot x \cdot \dots \cdot x}_{n \text{ razy}} = \prod_{i=1}^n x$$

Definicja 1.1.3. Iloczynem kartezjańskim zbiorów A i B nazywamy zbiór

$$A \times B := \{(a, b) : a \in A \wedge b \in B\}.$$

Analogicznie definiujemy

$$A_1 \times A_2 \times \dots \times A_n := \{(a_1, a_2, \dots, a_n) : a_1 \in A_1 \wedge a_2 \in A_2 \wedge \dots \wedge a_n \in A_n\}.$$

Oznaczamy $A^2 = A \times A$ oraz $A^n = \underbrace{A \times A \times \dots \times A}_{n\text{-razy}}$.

Przykład 1.1.4. Wyznacz $A \times B$, $B \times A$, B^2 .

i) $A = \{3, 4, 5\}$, $B = \{5, 7\}$

$$A \times B = \{(3, 5), (3, 7), (4, 5), (4, 7), (5, 5), (5, 7)\}$$

$$B \times A = \{(5, 3), (5, 4), (5, 5), (7, 3), (7, 4), (7, 5)\}$$

$$B^2 = \{(5, 5), (5, 7), (7, 5), (7, 7)\}$$

$$A \times B \neq B \times A$$

ii) przedziały $A = (0, 1) \subset \mathbb{R}$, $B = (1, 2) \subset \mathbb{R}$

$$A \times B = \{(x, y) : 0 < x < 1 \wedge 1 < y < 2\}$$

$$B \times A = \{(x, y) : 1 < x < 2 \wedge 0 < y < 1\}$$

iii) $A = B = \mathbb{R}$

$$A \times B = B \times A = A^2 = B^2$$

Oznaczamy $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) : x, y \in \mathbb{R}\}$ - płaszczyzna rzeczywista

1.2 Działania wewnętrzne i ich własności

Niech A będzie zbiorem niepustym.

Definicja 1.2.1. Dowolną funkcję $h : A \times A \rightarrow A$ nazywamy działaniem wewnętrznym w zbiorze A . Wartość funkcji $h(a, b) \in A$ nazywamy wynikiem działania dla pary argumentów $a, b \in A$.

Przykład 1.2.2. i) Dodawanie jest działaniem wewnętrznym w $\mathbb{N}$.

ii) Odejmowanie nie jest działaniem wewnętrznym w $\mathbb{N}$.

iii) Dodawanie nie jest działaniem wewnętrznym w $\mathbb{R} \setminus \mathbb{Q}$.

Własności działań wewnętrznych

Definicja 1.2.3. Niech $*$: $A \times A \rightarrow A$ będzie działaniem wewnętrznym.

- i) Działanie $*$ nazywamy *przemienne*, jeśli $\forall a, b \in A \quad a * b = b * a$.
- ii) Działanie $*$ nazywamy *łącznym*, jeśli $\forall a, b, c \in A \quad (a * b) * c = a * (b * c)$.
- iii) Element $e \in A$ nazywamy *elementem neutralnym* działania $*$, jeśli

$$\exists e \in A \quad \forall a \in A \quad a * e = e * a = a.$$

$$\begin{cases} a * e = a \\ e * a = a \end{cases}$$

$$\begin{aligned} &(\mathbb{R}, +) \\ &1 + (2 + 3) \\ &= (1 + 2) + 3 \\ &= 1 + 2 + 3 \end{aligned}$$

Przykład 1.2.4. i) Dodawanie jest działaniem wewnętrznym łącznym i przemienne w $\mathbb{R}$. 0 jest elementem neutralnym.

$$\forall x \in \mathbb{R} \quad x + 0 = 0 + x = x$$

- ii) Mnożenie jest działaniem wewnętrznym łącznym i przemienne w $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. 1 jest elementem neutralnym.

$$x \cdot 1 = 1 \cdot x = x$$

Twierdzenie 1.2.5. Jeżeli element neutralny istnieje to jest jedyny.

Dowód. Przypuśćmy, że istnieją $e_1, e_2 \in A$ będące elementami neutralnymi w A . Wówczas $e_2 = e_1 * e_2 = e_1$. $\square$

Przykład 1.2.6. Niech X to dowolny zbiór.

- i) Zbiór pusty $\emptyset$ jest elementem neutralnym w $(P(X), \cup)$.

- ii) Zbiór X jest elementem neutralnym w $(P(X), \cap)$.

$\mathcal{P}(X)$ - zbiór potęgowy zbioru X
tj. rodzina wszystkich podzbiorów zbioru X

$$\forall A \in \mathcal{P}(X) \quad A \cap X = A = X \cap A$$

Definicja 1.2.7. Niech $*$: $A \times A \rightarrow A$ będzie działaniem wewnętrznym, posiadającym element neutralny $e \in A$. Dla dowolnego $a \in A$ każdy element $a' \in A$ taki, że $a * a' = a' * a = e$, nazywamy *elementem symetrycznym* do a względem działania $*$.

$$\forall a \in A \quad \exists a' \in A \quad a * a' = a' * a = e$$

Przykład 1.2.8. i) W $(\mathbb{R}, +)$ elementem symetrycznym do 5 jest -5 (tzw. element przeciwny).

$$5 + (-5) = (-5) + 5 = 0$$

- ii) W $(\mathbb{R}^*, \cdot)$ elementem symetrycznym do 5 jest $\frac{1}{5}$ (tzw. element odwrotny).

$$5 \cdot \frac{1}{5} = \frac{1}{5} \cdot 5 = 1$$

- iii) W $(\mathbb{R}, \circ)$, gdzie $x \circ y = x + y + 1$, elementem neutralnym jest -1 , zaś elementem symetrycznym do x jest $-2 - x$.

$$e = -1 \in \mathbb{R}$$

$$x \circ x' = e \Leftrightarrow x + x' + 1 = -1$$

$$x' = -2 - x$$

$$x \circ (-1) = x + (-1) + 1 = x$$

$$(-1) \circ x = -1 + x + 1 = x$$

Twierdzenie 1.2.9. Jeżeli działanie wewnętrzne jest łączne oraz posiada element neutralny, to każdy element posiada co najwyżej jeden element symetryczny.

Dowód. Rozważmy zbiór A z działaniem łącznym $\circ$. Niech e będzie elementem neutralnym działania $\circ$. Niech a', a'' to dwa elementy symetryczne do $a \in A$. Wówczas

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

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

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

$$a' = a''$$

$\square$

1.3 Podstawowe struktury algebraiczne

1.3.1 Pojęcie grupy

Struktura algebraiczna - zbiór wraz z działaniami wewnętrznymi w tymże zbiorze

Niech G będzie zbiorem niepustym, zaś $*$: $G \times G \rightarrow G$ działaniem wewnętrznym w G .

Definicja 1.3.1. i) Parę $(G, *)$ nazywamy *półgrupą*, jeżeli działanie jest łączne.

ii) Parę $(G, *)$ nazywamy *monoidem*, jeżeli działanie jest łączne i posiada element neutralny.

iii) Parę $(G, *)$ nazywamy *grupą*, jeżeli działanie jest łączne, posiada element neutralny oraz każdy element G posiada element symetryczny względem $*$ w G .

Jeśli dodatkowo działanie $*$ jest przemienne, to mówimy o *półgrupie przemiennej*, *monoidzie przemiennym*, *grupie przemiennej (abelowej)*.

Przykład 1.3.2. Oznaczmy $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. Czy podane struktury to półgrupy/grupy (przemienne)?

	$(\mathbb{N}, +)$	$(\mathbb{Z}, \cdot)$	$(\mathbb{Q}, +)$	$(\mathbb{Q}, \cdot)$	$(\mathbb{R}^*, +)$	$(\mathbb{R}^*, \cdot)$
wewnętrzność	✓	✓	✓	✓	nie $-1 + 1 = 0$ $0 \notin \mathbb{R}^*$	✓
łączność	✓	✓	✓	✓		✓
przemienność	✓	✓	✓	✓		✓
el. neutralny	brak $0 \notin \mathbb{N}$	✓ $1 \in \mathbb{Z}$	✓ $0 \in \mathbb{Q}$	✓ $1 \in \mathbb{Q}$		✓ $1 \in \mathbb{R}^*$
el. symetryczny		brak $2 \cdot b = 1$ $b = \frac{1}{2} \notin \mathbb{Z}$	✓ $a + a' = 0$ $a' = -a \in \mathbb{Q}$	brak $a \cdot a' = 1$ $a' = \frac{1}{a}$ nie dla $a = 0$		✓ $a \cdot a' = 1$ $a' = \frac{1}{a}$ $\forall a \in \mathbb{R}^*$
	półgrupa przemienna bez el. neutr.	monoid przemienny	grupa abelowa	monoid przemienny		grupa abelowa

Przykład 1.3.3. $(\mathbb{Z}, +)$ jest grupą przemienną. Rozwiązując w $\mathbb{Z}$ równanie $x + 5 = 8$, korzystamy z własności działania w grupie.

$$\begin{array}{ll}
 x + 5 = 8 & \\
 (x + 5) - 5 = 8 - 5 & \text{istnieje element przeciwny do 5, należący do } \mathbb{Z} \\
 x + (5 - 5) = 3 & \text{dodawanie jest łączne w } \mathbb{Z} \\
 x + 0 = 3 & \text{istnieje element neutralny} \\
 x = 3 &
 \end{array}$$

Przykład 1.3.4. Niech $X = \{1, 2, 4, \dots, 2^n, \dots\}$, $n \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$, zaś działanie $\circ$ to mnożenie liczb. Czy $(X, \circ)$ jest półgrupą/grupą (abelową)?

Jeśli $a, b, c \in X$, to istnieją $k, m, n \in \mathbb{N}_0$ takie, że $a = 2^n, b = 2^m, c = 2^k$.

wewnętrzne $a \circ b = 2^n \cdot 2^m = 2^{n+m} \in A$

przemienne $a \circ b = 2^n \cdot 2^m = 2^{n+m} = 2^{m+n} = 2^m \cdot 2^n = b \circ a$

łączne $(a \circ b) \circ c = 2^{n+m} \cdot 2^k = 2^{n+m+k} = 2^n \cdot 2^{m+k} = a \circ (b \circ c)$

el. neutralny $e = 2^s, s \in \mathbb{N}_0 \quad a \circ e = a \Leftrightarrow 2^{n+s} = 2^n \Rightarrow s = 0, e = 1 \in X$

brak el. odwrotnego $a \circ b = 1 \Leftrightarrow 2^{n+m} = 2^0 \Leftrightarrow m = \boxed{-n} \Rightarrow m = -n \notin \mathbb{N}_0$

$$2^0 = 1 = e$$

Wniosek: monoid przemienny (tj. półgrupa przemienna z jedyneką)

1.3.2 Grupa permutacji

W trakcie wykładu poznamy wiele przykładów grup, w tym grupy macierzy takie jak ogólna grupa liniowa, grupa ortogonalna i grupa unitarna. Zajmiemy się teraz grupami permutacji zbiorów skończonych.¹

Definicja 1.3.5. Niech X będzie zbiorem niepustym. Wzajemnie jednoznaczne (tj. bijektywne) odwzorowanie $\sigma : X \rightarrow X$ nazywamy *permutacją* zbioru X .

Zbiór wszystkich permutacji zbioru X będziemy oznaczać symbolem $S(X)$.

Twierdzenie 1.3.6. Niech X będzie zbiorem niepustym. Zbiór $S(X)$ wraz z działaniem składania odwzorowań ma strukturę grupy.

Dowód. Złożenie bijekcji jest bijekcją, zatem działanie jest wewnętrzne w zbiorze $S(X)$. Składanie odwzorowań jest działaniem łącznym. Elementem neutralnym jest funkcja identycznościowa id_X , która jest bijekcją. Funkcja odwrotna do danej bijekcji również jest bijekcją. $\square$

Grupę $(S(X), \circ)$ nazywamy *grupą permutacji* zbioru X lub *grupą symetryczną* zbioru X .

¹O innym ciekawym przykładzie grupy można przeczytać w dodatku na końcu wykładu.

Zajmiemy się teraz grupami permutacji zbiorów skończonych.

Niech X będzie zbiorem n -elementowym, gdzie $n \in \mathbb{N}$. Natura elementów nie będzie miała dla nas znaczenia. Bez straty dla ogólności rozumowań możemy przyjąć, że $X = \{1, 2, \dots, n\}$.

Grupę permutacji zbioru n -elementowego będziemy oznaczać symbolem S_n .

Liczba wszystkich permutacji zbioru n -elementowego (to jest moc zbioru S_n) jest równa $n!$.

Jeśli $\sigma, \tau \in S_n$, to zamiast $\sigma \circ \tau$ będziemy pisać krótko $\sigma\tau$.

Podobnie zamiast $\sigma \circ \sigma$ będziemy pisać σ^2 .

Często też zamiast o złożeniu permutacji mówi się o *iloczynie* permutacji.

Permutację $\sigma : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$, $j \mapsto \sigma(j)$ zapisujemy w postaci dwuwierszowej, podając wszystkie wartości przekształcenia.²

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

W szczególności $\text{id} : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$, $\text{id}(j) = j$ zapisujemy w postaci

$$\text{id} = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

Przykład 1.3.7. Permutacje $\tau, \sigma \in S_8$ dane są za pomocą przyporządkowań

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 8 & 4 & 7 & 1 & 6 & 2 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 3 & 7 & 8 & 1 & 5 & 2 \end{pmatrix}.$$

Podamy postać permutacji σ^{-1} , $\sigma\tau$ oraz $\tau\sigma$.

Wyznaczamy σ^{-1} . Z definicji $\sigma^{-1}(j) = k \Leftrightarrow \sigma(k) = j$.

$$\begin{array}{cccccccc} \sigma & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 4 & 6 & 3 & 7 & 8 & 1 & 5 & 2 \end{array} \quad \begin{array}{cccccccc} \sigma^{-1} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 6 & 8 & 3 & 1 & 7 & 2 & 4 & 5 \end{array}$$

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 8 & 3 & 1 & 7 & 2 & 4 & 5 \end{pmatrix}$$

Wyznaczamy $\tau\sigma(j) = \tau(\sigma(j))$, dla $j = 1, 2, \dots, n$.

$$\begin{array}{cccccccc} \sigma & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 4 & 6 & 3 & 7 & 8 & 1 & 5 & 2 \\ \tau & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 4 & 1 & 8 & 6 & 2 & 3 & 7 & 5 \end{array}$$

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 8 & 4 & 7 & 1 & 6 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 3 & 7 & 8 & 1 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 8 & 6 & 2 & 3 & 7 & 5 \end{pmatrix}$$

²Ciąg $\sigma(1), \sigma(2), \dots, \sigma(n)$, to liczby $1, 2, \dots, n$ ustawione w innym porządku.

W podobny sposób wyznaczamy $\sigma\tau(j) = \sigma(\tau(j))$, dla $j = 1, 2, \dots, n$.

$$\begin{array}{cccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \tau & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 3 & 5 & 8 & 4 & 7 & 1 & 6 & 2 \\ \sigma & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 3 & 8 & 2 & 7 & 5 & 4 & 1 & 6 \end{array} \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 2 & 7 & 5 & 4 & 1 & 6 \end{pmatrix}$$

Zauważmy, że $\tau\sigma \neq \sigma\tau$.³

Twierdzenie 1.3.8. i) Grupy S_1 oraz S_2 są grupami przemienne.

ii) Dla $n \geq 3$ grupy S_n są nieprzemienne.

Dowód. i) Jest oczywiste, że grupa jednoelementowa $S_1 = \left\{ \sigma = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$ jest przemienna. Dla $n = 2$ mamy

$$S_2 = \left\{ \sigma = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}.$$

Możemy sprawdzić, że $\sigma^2 = \tau^2 = \sigma$ oraz $\sigma\tau = \tau\sigma = \tau$. $\square$

Definicja 1.3.9. Permutację $\sigma \in S_n$ nazywamy *permutacją cykliczną rzędu k* lub *cyklem k -wyrazowym* lub *cyklem długości k* , jeśli istnieje w zbiorze $\{1, 2, \dots, n\}$ podzbiór k -elementowy $\{a_1, a_2, \dots, a_k\}$ taki, że

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

oraz

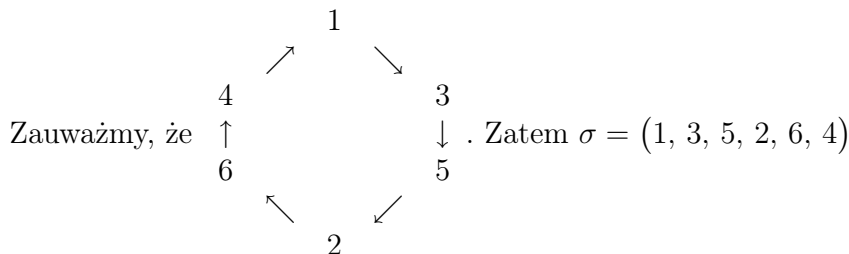
$$\forall j \in \{1, 2, \dots, n\} \setminus \{a_1, a_2, \dots, a_k\} \quad \sigma(j) = j.$$

Cykl k -wyrazowy oznaczamy symbolem $(a_1, a_2, \dots, a_k)$, pomijając w zapisie wyrazy, które przechodzą same na siebie.

Zgodnie z przyjętą definicją

$$(a_1, a_2, \dots, a_k) = (a_2, a_3, \dots, a_k, a_1) = (a_3, a_4, \dots, a_k, a_1, a_2) \quad \text{itd.}$$

Przykład 1.3.10. i) Rozważmy permutację $\sigma \in S_6$ postaci $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 1 & 2 & 4 \end{pmatrix}$.

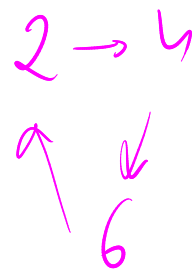


³Składanie odwzorowań nie jest działaniem przemennym,

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 5 & 2 \end{pmatrix} \quad \sigma = (2, 4, 6) \quad \sigma \in S_7$$

ii) Rozważmy permutację $\sigma \in S_7$ postaci $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 3 & 6 & 5 & 2 & 7 \end{pmatrix}$.

Permutacja ta jest cyklem 3-wyrazowym i możemy zapisać $\sigma = (2, 4, 6)$.



Zauważmy, że pisząc $\sigma = (2, 4, 6)$, musimy podać do jakiego zbioru S_n należy σ .

Dla przykładu, jeśli $\sigma \in S_6$, to $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 5 & 2 \end{pmatrix}$.

Jeśli zaś $\sigma \in S_7$, to $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 3 & 6 & 5 & 2 & 7 \end{pmatrix}$.

Definicja 1.3.11. Niech $k, l \in \mathbb{N}$. Dwa cykle $(a_1, a_2, \dots, a_k)$, $(b_1, b_2, \dots, b_l)$ nazywamy *rozłącznymi*, jeśli zbiory $\{a_1, a_2, \dots, a_k\}$, $\{b_1, b_2, \dots, b_l\}$ są rozłączne, to jest

$$\{a_1, a_2, \dots, a_k\} \cap \{b_1, b_2, \dots, b_l\} = \emptyset.$$

Twierdzenie 1.3.12. i) Składanie cykli rozłącznych jest przemienne.

ii) Jeśli $\sigma = (a_1, a_2, \dots, a_k)$ jest cyklem długości k to wówczas

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

$$\underbrace{\sigma \circ \dots \circ \sigma}_k = \sigma^k = \text{id} \quad \text{oraz} \quad \sigma^r \neq \text{id} \quad \text{dla} \quad 1 < r < k.$$

$$\text{id} = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

Ponadto dla dowolnego $m \in \mathbb{Z}$

$$\sigma^m = \sigma^{m \bmod k}.$$

iii) Każda permutacja jest cyklem lub może być przedstawiona jako złożenie (iloczyn) rozłącznych cykli. Przedstawienie to jest jednoznaczne z dokładnością do porządku czynników.

Przykład 1.3.13. Niech $\sigma = (1, 2, 3, 4, 5, 6) \in S_6$. Obliczmy kolejne potęgi tego cyklu.

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} = (1, 3, 5)(2, 4, 6)$$

$$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix} = (1, 4)(2, 5)(3, 6)$$

$$\sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix} = (1, 5, 3)(2, 6, 4)$$

$$\sigma^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} = (1, 6, 5, 4, 3, 2)$$

$$\sigma^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \text{id}$$



Zauważmy, że złożenie cykli nie musi być cyklem. ⁴

⁴Można uzasadnić, że jeśli σ jest cyklem długości k , to wówczas σ^l będzie cyklem długości k wtedy i tylko wtedy, gdy k i l są względnie pierwsze.

Uwaga 1.3.14. Niech $\sigma \in S_n$. Zbiór ⁵

$$\text{supp}(\sigma) = \{a \in \{1, 2, \dots, n\} : \sigma(a) \neq a\}$$

nazywamy *nośnikiem* permutacji. Mówimy, że permutacje $\sigma, \tau \in S_n$ są *rozłączne* lub *niezależne*, gdy ⁶

$$\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset.$$

Można uzasadnić, że składanie permutacji rozłącznych jest przemienne, czyli jeśli $\sigma, \tau \in S_n$ są rozłączne, to wówczas $\sigma\tau = \tau\sigma$.

Cykle rozłączne są permutacjami rozłącznymi. Można stąd wywnioskować, że jeśli $\sigma = \sigma_1\sigma_2 \dots \sigma_r$ jest rozkładem permutacji σ na parami rozłączne cykle, to wówczas dla dowolnej liczby naturalnej n zachodzi

$$\sigma^n = \sigma_1^n \sigma_2^n \dots \sigma_r^n.$$

Przykład 1.3.15. Rozważmy permutację $\sigma \in S_{10}$ postaci $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 2 & 4 & 3 & 5 & 9 & 8 & 10 & 1 & 7 \end{pmatrix}$.
Dokonamy jej rozkładu na cykle.

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 2 & 4 & 3 & 5 & 9 & 8 & 10 & 1 & 7 \end{pmatrix} = \underline{(1, 6, 9)} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 2 & 4 & 3 & 5 & 6 & 8 & 10 & 9 & 7 \end{pmatrix} = \\ &= (1, 6, 9)(3, 4) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 2 & 3 & 4 & 5 & 6 & 8 & 10 & 9 & 7 \end{pmatrix} = \\ &= (1, 6, 9)(3, 4)(7, 8, 10) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix} = (1, 6, 9)(3, 4)(7, 8, 10) \end{aligned}$$

Możemy wykorzystać otrzymany rozkład na parami rozłączne cykle, aby wyznaczyć σ^{15} oraz

σ^{-15} .
Mnożenie cykli rozłącznych jest przemienne, zatem

$$\sigma^{15} = (1, 6, 9)^{15} (3, 4)^{15} (7, 8, 10)^{15} = (3, 4)^{15} = (3, 4),$$

bowiem $(1, 6, 9)^3 = \text{id}$, $(3, 4)^2 = \text{id}$, $(7, 8, 10)^3 = \text{id}$.

Zatem

$$\sigma^{-15} = (3, 4)^{-1} = (4, 3).$$

Definicja 1.3.16. i) Cykl dwuwyrzowy nazywamy *transpozycją*.

ii) Transpozycję postaci $(k, k+1)$ nazywamy *transpozycją liczb sąsiednich*.

⁵angielskie *support* - nośnik

⁶Dwie permutacje σ, τ nazywamy rozłącznymi, jeśli zbiór elementów przesuniętych przez σ jest rozłączny od zbioru elementów przesuniętych przez τ .

Twierdzenie 1.3.17. i) Każdą permutację $\sigma \in S_n$, dla $n > 1$ można przedstawić jako złożenie pewnej liczby transpozycji.

ii) Każda transpozycja jest złożeniem nieparzystej liczby transpozycji liczb sąsiednich.

Dowód. i) Każda permutacja rozkłada się na iloczyn rozłącznych cykli. Każdy cykl $(a_1, a_2, \dots, a_k)$ rozkłada się na iloczyn transpozycji w sposób następujący ⁷

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

nie-
nowy qnr

ii) Niech $i < j$. Dla transpozycji (i, j) otrzymujemy następujący rozkład

$$(i, j) = (i, i+1)(i+1, i+2) \dots (j-2, j-1)(j-1, j)(j-2, j-1) \dots (i+1, i+2)(i, i+1).$$

W rozkładzie tym występuje $2(j-1) - 1$ czynników. $\square$

STOP

Uwaga 1.3.18. Rozkład permutacji na iloczyn transpozycji nie jest jednoznaczny.

Przykład 1.3.19. Rozważmy permutację $\sigma \in S_5$ postaci $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$.

Dokonamy rozkładu σ na iloczyn transpozycji. Otrzymujemy

$$\sigma = (1, 2, 3, 4, 5) = (1, 5)(1, 4)(1, 3)(1, 2)$$

Dla dowolnych $j, k \in \{1, 2, 3, 4, 5\}$ mamy $\boxed{(j, k)(j, k) = \text{id,}}$ stąd

$$\sigma = (1, 2, 3, 4, 5) = (1, 5)(2, 3)(2, 3)(1, 4)(1, 3)(1, 2) = (1, 5)(1, 4)(1, 3)(3, 5)(2, 4)(2, 4)(3, 5)(1, 2).$$

Definicja 1.3.20. i) Niech $\sigma \in S_n$. Mówimy, że liczby $j, k \in \{1, 2, \dots, n\}$ tworzą *inwersję* ⁸ w permutacji σ , jeśli $j < k$ oraz $\sigma(j) > \sigma(k)$.

ii) Permutację σ nazywamy *parzystą*, jeśli $\sigma \in S_1$ lub przy $n > 1$ liczba inwersji w permutacji σ jest parzysta.

iii) Permutację σ nazywamy *nieparzystą*, jeśli liczba inwersji w permutacji σ jest nieparzysta.

iv) Liczbę $(-1)^l$, gdzie l to liczba inwersji permutacji σ , nazywamy *znakiem permutacji* i oznaczamy symbolem $\text{sgn}(\sigma)$.

Liczba inwersji dla permutacji identycznościowej to 0.

Zatem $\boxed{\text{sgn}(\sigma) \in \{-1, 1\}}$. Permutacja σ jest parzysta wtedy i tylko wtedy gdy $\text{sgn}(\sigma) = 1$.

Podobnie, permutacja σ jest nieparzysta wtedy i tylko wtedy gdy $\text{sgn}(\sigma) = -1$.

⁷Wzór ten można uzasadnić indukcyjnie.

⁸Niektórzy autorzy używają określenia *nieporządek*.