

7. WYKŁAD 7: GRUPY PERMUTACJI.

Twierdzenie 7.1 (Cayley'a). *Dowolna grupa G jest izomorficzna z pewną podgrupą grupy przekształceń $S(G)$.*

Dowód. Zdefiniujmy odwzorowanie $\Phi : G \rightarrow S(G)$ wzorem $\Phi(a) = \lambda_a$, gdzie $\lambda_a : G \rightarrow G$ jest przesunięciem lewostronnym. Wobec Twierdzenia 3.1 Φ jest dobrze określonym homomorfizmem.

Pokażemy, że Φ jest monomorfizmem. Ustalmy w tym celu $a \in \ker \Phi$. Wówczas:

$$\Phi(a) = id_G \Leftrightarrow \lambda_a = id_G \Leftrightarrow \forall b \in G (ab = b) \Leftrightarrow a = 1_G.$$

Ponadto, oczywiście, $\text{im} \Phi < S(G)$, a zatem $G \cong \text{im} \Phi < S(G)$. □

Uwaga 7.1. *Niech X i Y będą zbiorami równolicznymi. Wówczas $S(X) \cong S(Y)$.*

Dowód. Niech $f : X \rightarrow Y$ będzie bijekcją ustalającą równoliczność. Zdefiniujmy odwzorowanie $\Psi : S(X) \rightarrow S(Y)$ wzorem $\Psi(\sigma) = f \circ \sigma \circ f^{-1}$.

Pokażemy, że Ψ jest homomorfizmem. Ustalmy w tym celu $\sigma_1, \sigma_2 \in S(X)$. Wówczas

$$\begin{aligned} \psi(\sigma_1 \circ \sigma_2) &= f \circ \sigma_1 \circ \sigma_2 \circ f^{-1} = f \circ \sigma_1 \circ f^{-1} \circ f \circ \sigma_2 \circ f^{-1} \\ &= \psi(\sigma_1) \circ \psi(\sigma_2). \end{aligned}$$

Pokażemy, że ψ jest surjektywne. Ustalmy w tym celu $\tau \in S(Y)$. Wówczas

$$\tau = f \circ f^{-1} \circ \tau \circ f \circ f^{-1} = \psi(f^{-1} \circ \tau \circ f).$$

Pokażemy, że ψ jest różnowartościowe. Ustalmy w tym celu $\sigma \in \ker \psi$. Wówczas

$$\sigma \in \ker \psi \Leftrightarrow \psi(\sigma) = id_Y \Leftrightarrow f \circ \sigma \circ f^{-1} = id_Y \Leftrightarrow \sigma = id_X.$$

□

Wniosek 7.1. *Dowolna grupa n -elementowa G jest izomorficzna z pewną podgrupą grupy permutacji $S(n)$.*

Dowód. Ustalmy grupę G i niech $|G| = n$. Wówczas G jest równoliczna z $\{1, \dots, n\}$, zatem $S(G) \cong S(n)$. □

Wniosek 7.2. *Dla ustalonej liczby n istnieje skończona liczba grup parami nieizomorficznych rzędu n .*

Definicja 7.1. *Niech $\sigma \in S(n)$.*

(1) *Zbiór*

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

nazywamy **nośnikiem** *permutacji* σ .

(2) *Mówimy, że permutacje $\sigma_1, \sigma_2 \in S(n)$ są* **rozłączne** *(lub* **niezależne***), gdy*

$$\text{supp}(\sigma_1) \cap \text{supp}(\sigma_2) = \emptyset.$$

(3) *Permutację $\sigma \in S(n)$ nazywamy* **cyklem** *o długości* k *, gdy istnieje podzbiór* $A = \{a_1, \dots, a_k\} \subset \{1, \dots, n\}$ *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

$$\sigma(i) = i, \text{ dla } i \in \{1, \dots, n\} \setminus A.$$

Cykl taki zapisujemy jako

$$\sigma = (a_1, a_2, \dots, a_k).$$

Przyjmujemy ponadto, że $id_{\{1, \dots, n\}}$ jest cyklem o długości 1 i oznaczamy go jako (1).

(4) Cykl o długości 2 nazywamy **transpozycją**.

Przykłady:

(1) Rozważmy $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{pmatrix}$. Wówczas:

$$\text{supp}(\sigma) = \{1, 3, 4, 5, 6\}.$$

(2) Rozważmy $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$. Wówczas σ_1 i σ_2 są permutacjami rozłącznymi.

(3) Rozważmy $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$. Wówczas σ jest cyklem:

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

(4) Rozważmy $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$. Wówczas σ jest transpozycją:

$$\sigma = (1, 2).$$

Uwaga 7.2. Niech $S(n)$ będzie grupą permutacji.

- (1) Jeśli $\sigma \in S(n)$ i $a \in \text{supp}(\sigma)$, to $\sigma(a) \in \text{supp}(\sigma)$.
- (2) Jeśli $\sigma \in S(n)$ i $k \in \mathbb{N}$, to $\text{supp}(\sigma^k) \subset \text{supp}(\sigma)$.
- (3) Jeśli $\sigma \in S(n)$, to $\text{supp}(\sigma^{-1}) \subset \text{supp}(\sigma)$.
- (4) Jeśli $\sigma, \tau \in S(n)$ i $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$, to $\sigma \circ \tau = \tau \circ \sigma$.

Dowód. (1) Ustalmy $\sigma \in S(n)$ i $a \in \text{supp}(\sigma)$. Wówczas $\sigma(a) \neq a$ i ponieważ σ jest bijekcją, to $\sigma(\sigma(a)) \neq \sigma(a)$, czyli $\sigma(a) \in \text{supp}(\sigma)$.

(2) Ustalmy $\sigma \in S(n)$ i $k \in \mathbb{N}$. Ustalmy $a \in \text{supp}(\sigma^k)$. Wówczas $\sigma^k(a) \neq a$. Przypuśćmy nie wprost, że $\sigma(a) = a$. Wówczas:

$$\begin{aligned} \sigma(a) &= a \\ \sigma^2(a) &= \sigma(a) = a \\ \sigma^3(a) &= \sigma^2(a) = \sigma(a) = a \\ &\vdots \\ \sigma^k(a) &= \dots = a \end{aligned}$$

(3) Ustalmy $\sigma \in S(n)$ i $a \in \text{supp}(\sigma^{-1})$. Wówczas $\sigma^{-1}(a) \neq a$. Niech $\sigma^{-1}(a) = b$, $b \neq a$. Wówczas $a = \sigma(b)$ i ponieważ σ jest bijekcją, więc $\sigma(a) \neq \sigma(b)$, czyli $a \neq \sigma(a)$.

(4) Ustalmy $\sigma, \tau \in S(n)$ i niech $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$. Ustalmy $a \in \{1, \dots, n\}$ i rozważmy kilka przypadków.

(a) Niech $a \notin \text{supp}(\sigma) \cup \text{supp}(\tau)$. Wówczas $\sigma(a) = a$, $\tau(a) = a$, więc $\sigma \circ \tau(a) = \tau \circ \sigma(a)$.

(b) Niech $a \in \text{supp}(\sigma)$. Wówczas $\sigma(a) \in \text{supp}(\sigma)$. Dalej, $\sigma(a) \notin \text{supp}(\tau)$ oraz $a \notin \text{supp}(\tau)$. Zatem $\sigma \circ \tau(a) = \sigma(a) = \tau(\sigma(a)) = \tau \circ \sigma(a)$.

(c) Niech $a \in \text{supp}(\tau)$. Rozumowanie prowadzimy analogicznie.

□

Uwaga 7.3. Niech $S(n)$ będzie grupą permutacji.

- (1) Jeśli $\sigma \in S(n)$ oraz $\sigma = (a_1, \dots, a_k)$, to $\text{supp}(\sigma) = \{a_1, \dots, a_k\}$.

(2) Jeśli $\sigma \in S(n)$ oraz $\sigma = (a_1, \dots, a_k)$, to

$$\sigma = (a_2, \dots, a_1, a_1) = (a_3, \dots, a_1, a_2) = \dots = (a_k, \dots, a_{k-2}, a_{k-1}).$$

(3) Jeśli $\sigma \in S(n)$ oraz $\sigma = (a_1, \dots, a_k)$, to

$$\sigma^{-1} = (a_k, \dots, a_1).$$

Uwaga 7.4. Niech $S(n)$ będzie grupą permutacji.

(1) Dla $i, j \in \{1, \dots, n\}$ zachodzi $(i, j)^2 = (i, j) \circ (i, j) = (1)$.

(2) Dla $i, j \in \{1, \dots, n\}$ zachodzi $(i, j) = (j, i)$.

(3) Dla $i, j \in \{1, \dots, n\}$ zachodzi $(i, j) = (1, i) \circ (1, j) \circ (1, i)$.

Twierdzenie 7.2. Każda permutacja $\sigma \in S(n)$ da się przedstawić w postaci iloczynu cykli parami rozłącznych. Przedstawienie to jest jednoznaczne z dokładnością do kolejności cykli.

Dowód. Pokażemy istnienie stosownego rozkładu. Niech $m = |\text{supp}(\sigma)|$. Dowód poprowadzimy przez indukcję względem m . Jeżeli $m = 0$, to wówczas

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

a zatem $\sigma = (1)$.

Jeżeli $m \geq 2$, to założmy, że każda permutacja $\sigma \in S(n)$ taka, że

$$|\text{supp}(\sigma)| < m$$

daje się rozłożyć na iloczyn cykli parami rozłącznych. Ustalmy permutację $\sigma \in S(n)$ taką, że

$$|\text{supp}(\sigma)| = m.$$

Pokażemy, że σ daje się rozłożyć na iloczyn cykli parami rozłącznych. Ustalmy w tym celu $a_1 \in \text{supp}(\sigma)$ i rozważmy ciąg

$$b_1 = a_1, b_2 = \sigma(b_1), b_3 = \sigma(b_2), \dots$$

Oczywiście

$$\forall p \in \mathbb{N} (b_p \in \{1, \dots, n\}),$$

a zatem

$$\exists p_1, p_2 \in \mathbb{N} (b_{p_1} = b_{p_2}).$$

Wobec tego niech

$$k = \min\{p \in \mathbb{N} : b_{p+1} = b_s, \text{ dla pewnego } s \in \{1, \dots, p\}\}.$$

Pokażemy, że $s = 1$. Przypuśćmy bowiem, że $s > 1$. Wówczas w szczególności:

$$b_{k+1} = b_s \text{ dla pewnego } s \in \{2, \dots, k\}$$

i zgodnie z określeniem ciągu $(b_1, b_2, \dots)$:

$$\sigma(b_k) = b_{k+1} = b_s = \sigma(b_{s-1}),$$

ale ponieważ σ jest bijekcją, więc

$$b_k = b_{s-1}$$

czyli

$$b_{(k-1)+1} = b_{s-1} \text{ oraz } s-1 \in \{1, \dots, k-1\}.$$

Wszelako k było najmniejszą liczbą o powyższej własności, co daje sprzeczność.

Wobec tego liczby

$$b_1 = a_1, b_2 = \sigma(b_1), b_3 = \sigma(b_2), \dots, b_k = \sigma(b_{k-1})$$

są parami różne oraz

$$b_{k+1} = b_1.$$

Mamy więc

$$\sigma = \begin{pmatrix} b_1 & b_2 & \dots & b_k \\ b_2 & b_3 & \dots & b_1 \end{pmatrix} \circ \underbrace{\begin{pmatrix} c_1 & c_2 & \dots & c_{m-k} \\ \sigma(c_1) & \sigma(c_2) & \dots & \sigma(c_{m-k}) \end{pmatrix}}_{=\tau} = (b_1, \dots, b_k) \circ \tau.$$

Jeśli $m = k$, to $\sigma = (b_1, \dots, b_m)$ jest cyklem. Jeśli $m > k$, to $|\text{supp}(\tau)| = m - k < m$, więc na podstawie założenia indukcyjnego

$$\tau = \gamma_1 \circ \dots \circ \gamma_l,$$

gdzie $\gamma_i, i \in \{1, \dots, l\}$ są cyklami rozłącznymi. Wobec tego

$$\sigma = (b_1, \dots, b_k) \circ \gamma_1 \circ \dots \circ \gamma_l$$

oraz

$$\forall i \in \{1, \dots, l\} (\text{supp}(\gamma_i) \cap \text{supp}(b_1, \dots, b_k) = \emptyset).$$

Pokażemy jednoznaczność (z dokładnością do kolejności) stosownego rozkładu. Niech

$$\sigma = \gamma_1 \circ \dots \circ \gamma_{l_1} = \gamma'_1 \circ \dots \circ \gamma'_{l_2},$$

gdzie $\gamma_1, \dots, \gamma_{l_1}, \gamma'_1, \dots, \gamma'_{l_2}$ są cyklami oraz

$$\forall i, j \in \{1, \dots, l_1\} (\text{supp}(\gamma_i) \cap \text{supp}(\gamma_j) = \emptyset),$$

$$\forall i, j \in \{1, \dots, l_2\} (\text{supp}(\gamma'_i) \cap \text{supp}(\gamma'_j) = \emptyset).$$

Przypuśćmy, że

$$\forall i \in \{1, \dots, l_2\} (\gamma_1 \neq \gamma'_i).$$

Ustalmy $a_1 \in \text{supp}(\gamma_1) \subset \text{supp}(\sigma)$. Dla pewnego $i \in \{1, \dots, l_2\}$

$$a_1 \in \text{supp}(\gamma'_i)$$

i możemy – zmieniając ewentualnie numerację – założyć, że

$$a_1 \in \text{supp}(\gamma'_1).$$

Wobec tego:

$$\gamma_1 = (a_1, a_2, \dots, a_{k_1}),$$

$$\gamma'_1 = (a_1, a'_2, \dots, a'_{k_2}).$$

Ale ponieważ σ jest bijekcją, więc:

$$a'_2 = \sigma(a_1) = a_2,$$

$$a'_3 = \sigma(a_2) = a_3,$$

$$\vdots$$

zatem $\gamma_1 = \gamma'_1$, co jest sprzecznością. □

Przykłady:

(5) Rozważmy $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 2 & 5 & 4 & 5 & 8 & 7 \end{pmatrix} \in S(8)$. Wówczas:

$$\sigma = (1, 3, 2) \circ (4, 6, 5) \circ (7, 8).$$

(6) Rozważmy $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 5 & 1 & 6 & 7 & 8 & 4 \end{pmatrix} \in S(8)$. Wówczas:

$$\sigma = (1, 2, 3, 5, 6, 7, 8, 4).$$

Wniosek 7.3. Grupa $S(n)$ jest generowana przez zbiór wszystkich cykli.

Uwaga 7.5. Rząd cykli o długości k w grupie $S(n)$ jest równy k .

Dowód. Ustalmy $\gamma_1 = (a_1, a_2, \dots, a_k) \in S(n)$. Wówczas:

$$\gamma^k = \begin{pmatrix} a_1 & a_2 & \dots & a_k \\ a_1 & a_2 & \dots & a_k \end{pmatrix} = (1).$$

Ustalmy $i \in \{1, \dots, k-1\}$. Wówczas:

$$\gamma^i(a_1) = a_{i+1}$$

ale $i+1 \in \{2, \dots, k\}$, więc

$$\gamma^i(a_1) \neq a_1.$$

□

Twierdzenie 7.3 (Ruffiniego). Jeżeli $\sigma \in S(n)$ ma następujący rozkład na cykle rozłączne:

$$\sigma = \gamma_1 \circ \dots \circ \gamma_m$$

o długościach, odpowiednio, $k_1, \dots, k_m$, to wówczas

$$r(\sigma) = \text{NWW}(k_1, \dots, k_m).$$

Dowód. Ustalmy σ o rozkładzie jak w twierdzeniu. Niech $r(\sigma) = r$. Oznaczmy:

$$w = \text{NWW}(k_1, \dots, k_m)$$

oraz dobierzmy liczby naturalne $t_1, \dots, t_m$ tak, aby

$$\forall i \in \{1, \dots, m\} w = k_i t_i.$$

Wówczas

$$\begin{aligned} \sigma^w &= (\gamma_1 \circ \dots \circ \gamma_m)^w = \gamma_1^w \circ \dots \circ \gamma_m^w = \gamma_1^{k_1 t_1} \circ \dots \circ \gamma_m^{k_m t_m} \\ &= (\gamma_1^{k_1})^{t_1} \circ \dots \circ (\gamma_m^{k_m})^{t_m} = (1). \end{aligned}$$

Wobec tego $r|w$. Z drugiej strony:

$$(1) = \sigma^r = (\gamma_1 \circ \dots \circ \gamma_m)^r = \gamma_1^r \circ \dots \circ \gamma_m^r$$

oraz $\gamma_1^r, \dots, \gamma_m^r$ są cyklami parami rozłącznymi. Zatem:

$$\gamma_1^r = (1), \dots, \gamma_m^r = (1),$$

skąd $k_1|r, \dots, k_m|r$. Wobec tego $w|r$.

□

Przykład:

(7) Rozważmy $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 7 & 5 & 6 & 4 & 9 & 8 \end{pmatrix} \in S(9)$. Wówczas:

$$\sigma = (1, 2, 3) \circ (4, 7) \circ (8, 9),$$

a zatem $r(\sigma) = NWW(3, 2, 2) = 6$.

Uwaga 7.6. *Każdy cykl jest iloczynem transpozycji.*

Dowód. Wystarczy zauważyć, że

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

□

Wniosek 7.4. (1) *Każda permutacja $\sigma \in S(n)$ jest iloczynem transpozycji.*

(2) *Grupa $S(n)$ jest generowana przez zbiór wszystkich transpozycji.*

(3) *Grupa $S(n)$ jest generowana przez zbiór*

$$\{(1, 2), (1, 3), \dots, (1, n)\}.$$

Przykłady:

(8) Rozważmy $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 2 & 3 & 8 & 7 & 1 & 5 \end{pmatrix} \in S(8)$. Wówczas:

$$\begin{aligned} \sigma &= (1, 6, 7) \circ (2, 4, 3) \circ (5, 8) \\ &= (1, 7) \circ (1, 6) \circ (2, 3) \circ (2, 4) \circ (5, 8). \end{aligned}$$

(9) Rozważmy $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S(3)$. Wówczas:

$$\begin{aligned} \sigma &= (1, 2, 3) = (1, 3) \circ (1, 2) \\ &= (1, 3) \circ (1, 2) \circ (1, 2) \circ (1, 2). \end{aligned}$$

W szczególności rozkład permutacji na transpozycje nie jest jednoznaczny.

Lemat 7.1. *Niech $\sigma \in S(n)$ oraz $c_1, \dots, c_k \in \{1, \dots, n\}$. Niech*

$$\sigma = (1, c_1) \circ \dots \circ (1, c_k).$$

Jeśli $\sigma(s) = s$ dla pewnego $s \in \{1, \dots, n\}$, to element s występuje w ciągu $c_1, \dots, c_k$ parzystą liczbę razy.

Dowód. Jeśli $s \neq c_i$, dla $i \in \{1, \dots, k\}$, to s występuje w ciągu 0 razy. Załóżmy więc, że $s = c_i$, dla pewnego $i \in \{1, \dots, k\}$. Dowód prowadzimy metodą indukcji po k . Załóżmy, że dla wszelkich $p \in \{1, \dots, k-1\}$, jeżeli $c_1, \dots, c_p \in \{1, \dots, n\}$ oraz

$$\sigma = (1, c_1) \circ \dots \circ (1, c_p),$$

i jeśli $\sigma(s) = s$, dla pewnego $s \in \{1, \dots, n\}$, to element s występuje w ciągu $c_1, \dots, c_p$ parzystą liczbę razy. Niech

$$l = \max\{i \in \{1, \dots, k\} : s = c_i\}.$$

Ponadto oznaczmy

$$\tau_i = (1, c_i), \text{ dla } i \in \{1, \dots, k\}.$$

Wówczas

$$\begin{aligned} \tau_l \circ \tau_{l+1} \circ \dots \circ \tau_k(s) &= 1 \neq s, \\ \tau_1 \circ \dots \circ \tau_l \circ \tau_{l+1} \circ \dots \circ \tau_k(s) &= \sigma(s) = s. \end{aligned}$$

a zatem

$$\tau_1 \circ \tau_2 \circ \dots \circ \tau_{l-1}(s) \neq s.$$

Wobec tego

$$\exists i \in \{1, \dots, l-1\} (s = c_i).$$

Niech

$$m = \max\{i \in \{1, \dots, l-1\} : s = c_i\}.$$

Wówczas

$$\begin{aligned} \tau_m \circ \tau_{m+1} \circ \dots \circ \tau_l \circ \tau_{l+1} \circ \dots \circ \tau_k(s) &= s, \\ \tau_1 \circ \dots \circ \tau_m \circ \tau_{m+1} \circ \dots \circ \tau_l \circ \tau_{l+1} \circ \dots \circ \tau_k(s) &= \sigma(s) = s, \end{aligned}$$

a zatem

$$\tau_1 \circ \tau_2 \circ \dots \circ \tau_{m-1}(s) = s.$$

Tym samym w ciągu

$$c_m, \dots, c_l, \dots, c_k$$

s występuje dwa razy oraz

$$\tau_1 \circ \dots \circ \tau_{m-1} = (1, c_1) \circ \dots \circ (1, c_{m-1}),$$

przy czym $m-1 \in \{1, \dots, k-1\}$ i skoro $\tau_1 \circ \dots \circ \tau_{m-1}(s) = s$, to na podstawie założenia indukcyjnego w ciągu

$$c_1, \dots, c_{m-1}$$

s występuje parzystą liczbę razy. Tym samym w ciągu

$$c_1, \dots, c_k$$

s występuje parzystą liczbę razy. □

Lemat 7.2. Niech $\sigma \in S(n)$. Jeśli

$$\sigma = (a_1, b_1) \circ \dots \circ (a_k, b_k) = (1),$$

gdzie $a_i \neq b_i$, $i \in \{1, \dots, k\}$, to k jest liczbą parzystą.

Dowód. Ponieważ

$$\forall i \in \{1, \dots, k\} [(a_i, b_i) = (1, a_i) \circ (1, b_i) \circ (1, a_i)],$$

więc

$$\sigma = (1, a_1) \circ (1, b_1) \circ (1, a_1) \circ \dots \circ (1, a_k) \circ (1, b_k) \circ (1, a_k) = (1).$$

Stąd w szczególności

$$\forall i \in \{1, \dots, k\} [\sigma(b_i) = b_i.]$$

Wobec Lematu 7.1, element b_i , dla $i \in \{1, \dots, k\}$, pojawia się w ciągu

$$a_1, b_1, a_1, a_2, b_2, a_2, \dots, a_k, b_k, a_k$$

parzystą liczbę razy, a więc element b_i , dla $i \in \{1, \dots, k\}$, pojawia się w ciągu

$$b_1, b_2, \dots, b_k$$

parzystą liczbę razy. Zatem k jest liczbą parzystą. □

Twierdzenie 7.4. Niech $\sigma \in S(n)$ oraz

$$\sigma = \tau_1 \circ \dots \circ \tau_k = \tau'_1 \circ \dots \circ \tau'_l,$$

gdzie $\tau_1, \dots, \tau_k, \tau'_1, \dots, \tau'_l$ są transpozycjami. Wówczas

$$k \equiv l \pmod{2}.$$

Dowód. Wobec równości

$$\tau_1 \circ \dots \circ \tau_k = \tau'_1 \circ \dots \circ \tau'_l$$

mamy

$$\tau_1 \circ \dots \circ \tau_k \circ \tau_l'^{-1} \circ \dots \circ \tau_1'^{-1} = (1).$$

Wobec Lematu 7.2 liczba

$$k + l$$

jest parzysta, a zatem $k \equiv l \pmod{2}$. □

Definicja 7.2. Niech $\sigma \in S(n)$ oraz niech σ ma następujący rozkład na transpozycje:

$$\sigma = \tau_1 \circ \dots \circ \tau_m.$$

- (1) Liczbę $\text{sgn}(\sigma) = (-1)^m$ nazywamy **znakiem** permutacji σ .
- (2) Permutację σ nazywamy **parzystą**, jeśli $\text{sgn}(\sigma) = 1$, a więc gdy jest iloczynem parzystej liczby transpozycji i **nieparzystą** w przeciwnym wypadku.

Uwaga 7.7. (1) Cykl o długości k jest permutacją parzystą wtedy i tylko wtedy, gdy k jest liczbą nieparzystą.

- (2) Niech $\sigma \in S(n)$ i niech σ ma następujący rozkład na cykle rozłączne:

$$\sigma = \gamma_1 \circ \dots \circ \gamma_l,$$

przy czym niech k_i będzie długością cyklu γ_i , $i \in \{1, \dots, l\}$. Wówczas permutacja σ jest parzysta wtedy i tylko wtedy, gdy wśród liczb $k_1, \dots, k_l$ występuje parzysta liczba liczb parzystych.

Dowód. (1) Wynika wprost z tożsamości

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

- (2) Oczywiste wobec (1). □

Przykłady:

(10) Rozważmy $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 2 & 3 & 8 & 7 & 1 & 5 \end{pmatrix} \in S(8)$. Wówczas:

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

więc σ jest permutacją nieparzystą.

Twierdzenie 7.5. Niech $\sigma \in S(n)$. Rozważmy wielomiany:

$$\begin{aligned} f(x_1, \dots, x_n) &= \prod_{1 \leq i < j \leq n} (x_i - x_j), \\ f^\sigma(x_1, \dots, x_n) &= \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}). \end{aligned}$$

Wówczas σ jest parzysta wtedy i tylko wtedy, gdy $f = f^\sigma$ oraz σ jest nieparzysta wtedy i tylko wtedy, gdy $f = -f^\sigma$.

Dowód. Wielomiany f i f^σ różnią się co najwyżej znakiem, więc wystarczy pokazać, że σ jest parzysta wtedy i tylko wtedy, gdy $f = f^\sigma$. W tym celu zauważmy, że σ jest iloczynem stałej co do parzystości liczby transpozycji $\tau_1, \dots, \tau_k$ oraz że iloczyn dwóch permutacji jednakowej parzystości jest permutacją parzystą, zaś iloczyn dwóch permutacji różnych parzystości jest permutacją nieparzystą. Zarazem:

- jeśli $f = f^{\sigma_1}$ i $f = f^{\sigma_2}$, to $f = f^{\sigma_1 \circ \sigma_2}$,
- jeśli $f = -f^{\sigma_1}$ i $f = -f^{\sigma_2}$, to $f = f^{\sigma_1 \circ \sigma_2}$,
- jeśli $f = f^{\sigma_1}$ i $f = -f^{\sigma_2}$, to $f = -f^{\sigma_1 \circ \sigma_2}$.

Wobec tego wystarczy pokazać, że jeśli τ jest transpozycją, to $f = -f^\tau$.

Pokażemy najpierw, że jeśli $\tau = (k, k+1)$, gdzie $k \in \{1, \dots, n-1\}$, to $f = -f^\tau$. Istotnie:

$$f^\tau(x_1, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_{\tau(i)} - x_{\tau(j)}).$$

Tylko jeden czynnik $(x_{\tau(i)} - x_{\tau(j)})$ w iloczynie $\prod_{1 \leq i < j \leq n} (x_{\tau(i)} - x_{\tau(j)})$ spełnia $\tau(i) > \tau(j)$, a mianowicie

$$(x_{\tau(k)} - x_{\tau(k+1)}) = (x_{k+1} - x_k).$$

Zmieniając znak tego czynnika na przeciwny otrzymujemy f , a zatem $f = -f^\tau$.

Dalej, dla dowolnej transpozycji $\tau = (m, r)$, $1 \leq m < r \leq n$, zachodzi:

$$(m, r) = (m, m+1) \circ (m+1, m+2) \circ \dots \circ (r-2, r-1) \circ (r-1, r) \circ (r-2, r-1) \circ \dots \circ (m+1, m+2) \circ (m, m+1).$$

Zatem dowolna transpozycja jest iloczynem $2(r-m)-1$ transpozycji postaci $(k, k+1)$, przy czym liczba $2(r-m)-1$ jest nieparzysta, co kończy dowód. $\square$

Uwaga 7.8. Odwzorowanie $\text{sgn} : S(n) \rightarrow \{-1, 1\}$ jest homomorfizmem grup. Jego jądrem jest zbiór wszystkich permutacji parzystych.

Definicja 7.3. Podgrupę $A(n)$ grupy $S(n)$ złożoną ze wszystkich permutacji parzystych zwiemy **grupą alternującą** stopnia n .

Wniosek 7.5. Niech $n \geq 2$. Wówczas:

- (1) $A(n) \triangleleft S(n)$;
- (2) $S(n)/A(n) \cong \{-1, 1\} \cong \mathbb{Z}_2$;
- (3) $|A(n)| = \frac{n!}{2}$.

Twierdzenie 7.6. Niech $n \geq 2$. Wówczas:

- (1) grupa $A(n)$ jest generowana przez zbiór wszystkich permutacji będących iloczynem dwóch transpozycji;
- (2) grupa $A(n)$ jest generowana przez zbiór wszystkich cykli o długości 3;
- (3) grupa $A(n)$ jest generowana przez zbiór:

$$\{(1, 2, 3), (1, 2, 4), \dots, (1, 2, n)\};$$

- (4) grupa $A(n)$ jest generowana przez zbiór:

$$\{(1, i, j) : i, j \in \{2, \dots, n\}, i \neq j\}.$$

Dowód. (1) Oczywiste.

(2) Wystarczy zauważyć, że dla parami różnych $i, j, k, l \in \{1, \dots, n\}$:

$$(i, j) \circ (i, j) = (1),$$

$$(i, j) \circ (i, k) = (i, k, j),$$

$$(i, j) \circ (k, l) = (j, k, l) \circ (i, l, j).$$

(3) Oczywiste wobec (1) i (2).

(4) Oczywiste wobec (1) i (2).

□