Wykład 7
Grupy permutacji

1 Znak permutacji

Niech n będzie ustaloną liczbą naturalną i $X_n = \{1, 2, \ldots, n\}$. Każdą permutację $f \in S_n$ można zapisać w postaci dwuwierszowej tablicy

$$f = \begin{pmatrix} 1 & 2 & \ldots & i & \ldots & n \\ f(1) & f(2) & \ldots & f(i) & \ldots & f(n) \end{pmatrix}, \tag{1}$$

w której w pierwszym wierszu umieszczone są wszystkie elementy zbioru X_n (najczęściej w porządku rosnącym), zaś w drugim wierszu umieszczone są kolejne obrazy tych elementów przy odwzorowaniu f. Niech

$$X_f = \{x \in X_n \ : \ f(x) \neq x\}. \tag{2}$$

Wtedy dla $x \in X_f$ jest $x \neq f(x)$, skąd $f(x) \neq f(f(x))$, więc $f(x) \in X_f$. Stąd $f(X_f) \subseteq X_f$, a ponieważ f jest różnowartościowe i zbiór X_f jest skończony, więc $f(X_f) = X_f$. Z tego powodu w zapisie permutacji f pomijamy zazwyczaj *punkty stałe* f, tzn. takie i, że $f(i) = i$. Np. zamiast $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ można pisać $\begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}$. Przy tej notacji dla permutacji f mamy wzór:

$$f^{-1} = \begin{pmatrix} f(1) & f(2) & \ldots & f(n) \\ 1 & 2 & \ldots & n \end{pmatrix}. \tag{3}$$

Ponadto

$$e = \begin{pmatrix} 1 & 2 & \ldots & i & \ldots & n \\ 1 & 2 & \ldots & i & \ldots & n \end{pmatrix}. \tag{4}$$

Przykład 7.1. Notacja dwuwierszowa umożliwia szybkie składanie permutacji (przypominamy, że to składanie odbywa się od strony prawej do lewej!). Np. dla $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$ oraz $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$ mamy:

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 5 \\ 4 & 5 & 2 & 1 \end{pmatrix}$$

oraz $g^{-1} = \begin{pmatrix} 3 & 4 & 5 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$.

Definicja 7.2. *Inwersją permutacji* $f \in S_n$ nazywamy taki podzbiór dwuelementowy $\{i, j\}$ zbioru X_n, że $i < j$ oraz $f(i) > f(j)$. Zbiór wszystkich inwersji permutacji $f \in S_n$ oznaczamy przez I_f.

Przykład 7.3. $I_e = \emptyset$, więc $|I_e| = 0$, czyli **permutacja tożsamościowa nie posiada inwersji**. Dla permutacji f z Przykładu 7.1 mamy, $I_f = \{\{1,2\},\{3,5\},\{4,5\}\}$, czyli $|I_f| = 3$.

Przykład 7.4. Niech $i, j \in X_n$, $i < j$. Oznaczmy przez (i,j) permutację zbioru X_n, która zamienia miejscami elementy i, j oraz nie zmienia pozostałych elementów zbioru X_n (takie permutacje nazywamy *transpozycjami*). Zatem

$$(i,j) = \begin{pmatrix} 1 & 2 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & n \\ 1 & 2 & \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots & n \end{pmatrix}. \tag{5}$$

Stąd $I_{(i,j)} = \{\underbrace{\{i,i+1\},\{i,i+2\},\{i,i+3\},\dots,\{i,j-1\},\{i,j\}}_{j-i},$
$\underbrace{\{i+1,j\},\{i+2,j\},\{i+3,j\},\dots,\{j-1,j\}}_{(j-1)-i}\}.$
Zatem $|I_{(i,j)}| = (j-i)+(j-1)-i = 2(j-i)-1$. Uzyskaliśmy więc, że **każda transpozycja posiada nieparzystą liczbę wszystkich inwersji**.

Definicja 7.5. *Znakiem permutacji* $f \in S_n$ nazywamy liczbę $sgn(f)$ określoną wzorem:

$$sgn(f) = (-1)^{|I_f|}. \tag{6}$$

Powiemy, że permutacja $f \in S_n$ jest *parzysta*, jeśli $sgn(f) = 1$ oraz, że f jest *nieparzysta*, jeśli $sgn(f) = -1$. Zbiór wszystkich permutacji parzystych $f \in S_n$ będziemy oznaczali przez A_n.

Przykład 7.6. Na mocy Przykładu 7.4, **dowolna transpozycja jest permutacją nieparzystą**. Ponieważ $sgn(e) = (-1)^0 = 1$, więc permutacja tożsamościowa jest permutacją parzystą.

Twierdzenie 7.7. *Dla dowolnych permutacji* $f_1, f_2, \dots, f_k \in S_n$ *zachodzi wzór:*

$$sgn(f_1 \circ f_2 \circ \dots \circ f_k) = sgn(f_1) \cdot sgn(f_2) \cdot \dots \cdot sgn(f_k). \tag{7}$$

W szczególności $sgn(f^{-1}) = sgn(f)$ *dla dowolnego* $f \in S_n$.

Dowód. Niech $f, g \in S_n$. Oznaczmy przez P_n rodzinę wszystkich podzbiorów dwuelementowych zbioru X_n. Niech $h \in S_n$. Weźmy dowolne $A \in P_n$. Wtedy $A = \{i,j\}$ dla pewnych $i, j \in X_n$, $i \neq j$. Oznaczmy $sgn_h(A) = sgn\left(\frac{h(i)-h(j)}{i-j}\right)$. Określenie to jest poprawne, bo

$$\frac{h(j)-h(i)}{j-i} = \frac{-(h(i)-h(j))}{-(i-j)} = \frac{h(i)-h(j)}{i-j}.$$

Ponadto $A \in I_h \Leftrightarrow sgn_h(A) = -1$. Wynika stąd wzór:

$$sgn(h) = \prod_{A \in P_n} sgn_h(A). \tag{8}$$

Łatwo zauważyć, że dowolna permutacja $g \in S_n$ wyznacza bijekcję $G\colon P_n \to P_n$ przy pomocy wzoru $G(A) = \{g(i), g(j)\}$ dla $A = \{i, j\}$. Wynika stąd, że dla dowolnych $f, g \in S_n$ zachodzi wzór:

$$sgn(f) = \prod_{A \in P_n} sgn_f(G(A)). \tag{9}$$

Ponadto dla $A \in P_n$ mamy

$$sgn_f(G(A)) \cdot sgn_g(A) = sgn_{f \circ g}(A). \tag{10}$$

Rzeczywiście, $A = \{i, j\}$ dla pewnych $i, j \in X_n$, $i \neq j$ oraz

$$sgn_f(G(A)) = sgn_f(\{g(i), g(j)\}) = sgn\left(\frac{f(g(i)) - f(g(j))}{g(i) - g(j)}\right)$$

oraz

$$sgn_g(A) = sgn\left(\frac{g(i) - g(j)}{i - j}\right).$$

Ale $sgn(x) \cdot sgn(y) = sgn(x \cdot y)$ dla dowolnych liczb rzeczywistych x, y, więc

$$sgn_f(G(A)) \cdot sgn_g(A) = sgn\left(\frac{f(g(i)) - f(g(j))}{g(i) - g(j)} \cdot \frac{g(i) - g(j)}{i - j}\right) =$$

$$= sgn\left(\frac{(f \circ g)(i) - (f \circ g)(j)}{i - j}\right) = sgn_{f \circ g}(A).$$

Zatem na mocy (8), (9) i (10) mamy

$$sgn(f \circ g) = \prod_{A \in P_n} sgn_{f \circ g}(A) = \prod_{A \in P_n} [sgn_f(G(A)) \cdot sgn_g(A)] =$$

$$= \prod_{A \in P_n} sgn_f(G(A)) \cdot \prod_{A \in P_n} sgn_g(A) = \prod_{A \in P_n} sgn_f(A) \cdot \prod_{A \in P_n} sgn_g(A) =$$

$$= sgn(f) \cdot sgn(g).$$

W szczególności, $1 = sgn(e) = sgn(f \circ f^{-1}) = sgn(f) \cdot sgn(f^{-1})$, czyli $sgn(f^{-1}) = sgn(f)$.

Jeśli dla pewnego $k \geq 2$ i dla dowolnych $f_1, f_2, \ldots, f_k \in S_n$, $sgn(f_1 \circ f_2 \circ \ldots \circ f_k) = sgn(f_1) \cdot sgn(f_2) \cdot \ldots \cdot sgn(f_k)$ oraz $g_1, \ldots, g_k, g_{k+1} \in S_n$, to na mocy pierwszej części dowodu i tego, że $g_1 \circ \ldots \circ g_k \circ g_{k+1} = (g_1 \circ \ldots \circ g_k) \circ g_{k+1}$ otrzymamy, że $sgn(g_1 \circ \ldots \circ g_k \circ g_{k+1}) = sgn(g_1 \circ \ldots \circ g_k) \cdot sgn(g_{k+1}) = sgn(g_1) \cdot \ldots \cdot sgn(g_k) \cdot sgn(g_{k+1})$. Kończy to dowód naszego twierdzenia. □

Wniosek 7.8. *Dla $n \geqslant 2$ A_n jest podgrupą normalną indeksu 2 grupy S_n.*

Dowód. Ponieważ $sgn(e) = 1$, więc $e \in A_n$. Niech $f, g \in A_n$. Wtedy $sgn(f) = sgn(g) = 1$, skąd z Twierdzenia 7.7, $sgn(g^{-1}) = 1$ oraz $sgn(f \circ g^{-1}) = sgn(f) \cdot sgn(g^{-1}) =$

$1 \cdot 1 = 1$, czyli $f \circ g^{-1} \in A_n$. Zatem A_n jest podgrupą grupy S_n. Dalej, $n \geqslant 2$, więc $(1,2) \in S_n$ oraz z Przykładu 7.4, $sgn((1,2)) = -1$, więc $(1,2) \notin A_n$. Weźmy dowolne $g \in S_n$. Jeśli $g \notin A_n$, to $sgn(g) = -1$, skąd na mocy Twierdzenia 7.7 $sgn((1,2) \circ g) = (-1) \cdot (-1) = 1$, czyli $f = (1,2) \circ g \in A_n$. Ale $(1,2) \circ (1,2) = e$, więc $g = (1,2) \circ f \in (1,2)A_n$. Oznacza to, że $S_n = A_n \cup (1,2)A_n$, więc ostatecznie $(S_n : A_n) = 2$. Zatem ze Stwierdzenia 4.14, $A_n \lhd S_n$. $\square$

2 Permutacje rozłączne

Stwierdzenie 7.9. *Dla dowolnych permutacji $f, g \in S_n$ równoważne są warunki:*
(i) $X_f \cap X_g = \emptyset$,
(ii) dla każdego $x \in \{1, 2, \ldots, n\}$: $f(x) = x$ lub $g(x) = x$.

Dowód. $(i) \Rightarrow (ii)$. Załóżmy, że istnieje $x \in \{1, 2, \ldots, n\}$ taki, że $f(x) \neq x$ i $g(x) \neq x$. Wtedy $x \in X_f$ i $x \in X_g$, więc $x \in X_f \cap X_g$, co przeczy temu, że $X_f \cap X_g = \emptyset$. Wobec tego dla każdego $x \in \{1, 2, \ldots, n\}$: $f(x) = x$ lub $g(x) = x$.

$(ii) \Rightarrow (i)$. Załóżmy, że $X_f \cap X_g \neq \emptyset$. Zatem istnieje $x \in \{1, 2, \ldots, n\}$ takie, że $x \in X_f$ i $x \in X_g$, czyli $f(x) \neq x$ i $g(x) \neq x$. Zatem mamy sprzeczność. $\square$

Definicja 7.10. Permutacje $f, g \in S_n$ nazywamy *rozłącznymi*, jeżeli $X_f \cap X_g = \emptyset$.

Stwierdzenie 7.11. *Niech $f, f_1, \ldots, f_k \in S_n$ będą takie, że permutacje f i f_j są rozłączne dla każdego $j = 1, \ldots, k$. Wówczas permutacje f i $f_1 \circ f_2 \circ \ldots \circ f_k$ też są rozłączne.*

Dowód. Zastosujemy indukcję względem k. Dla $k = 1$ teza jest oczywista. Niech $k \in \mathbb{N}$, $k > 1$, będzie takie, że teza zachodzi dla liczby $k - 1$. Załóżmy, że permutacje f i f_j są rozłączne dla każdego $j = 1, \ldots, k$. Wtedy z założenia indukcyjnego permutacje f i $g = f_1 \circ \ldots \circ f_{k-1}$ są rozłączne. Weźmy dowolne $x \in \{1, 2, \ldots, n\}$ takie, że $f(x) \neq x$. Wówczas ze Stwierdzenia 7.9, $g(x) = x$ oraz $f_k(x) = x$. Ale $f_1 \circ \ldots \circ f_k = g \circ f_k$, więc $(f_1 \circ \ldots \circ f_k)(x) = g(f_k(x)) = g(x) = x$. Zatem permutacje f i $f_1 \circ \ldots \circ f_k$ są rozłączne. $\square$

Stwierdzenie 7.12. *Jeżeli permutacje $f, g \in S_n$ są rozłączne, to dla dowolnych liczb naturalnych k, l permutacje f^k i g^l też są rozłączne.*

Dowód. Na mocy Stwierdzenia 7.11 permutacje f i g^l są rozłączne. Wobec tego znowu na mocy Stwierdzenia 7.11 permutacje g^l i f^k są rozłączne. $\square$

Stwierdzenie 7.13. *Jeżeli permutacje $f, g \in S_n$ są rozłączne, to*
(i) $f \circ g = g \circ f$,
(ii) jeżeli $f \circ g = e$, to $f = g = e$,
(iii) $o(f \circ g) = [o(f), o(g)]$.

Dowód. (i) Dla $x \in X_n \setminus (X_f \cup X_g)$ jest $f(x) = g(x) = x$, więc $(f \circ g)(x) = f(g(x)) = f(x) = x = g(x) = g(f(x)) = (g \circ f)(x)$. Ponadto dla $x \in X_f$ jest $f(x) \in X_f$, więc $f(x) \notin X_g$ oraz $g(f(x)) = f(x)$ i $f(g(x)) = f(x)$, bo $g(x) = x$, gdyż $x \notin X_g$. Zatem dla $x \in X_f$ mamy, że $(f \circ g)(x) = (g \circ f)(x)$. Podobnie pokazujemy, że $(f \circ g)(x) = (g \circ f)(x)$ dla $x \in X_g$. Stąd ostatecznie $f \circ g = g \circ f$.

(ii) Załóżmy, że $g \neq e$. Wtedy istnieje $x \in X_n$ takie, że $g(x) \neq x$, skąd $x \in X_g$, więc $g(x) \in X_g$, czyli $g(x) \notin X_f$ i $f(g(x)) = g(x)$. Ale $x = e(x) = (f \circ g)(x) = f(g(x)) = g(x)$ i mamy sprzeczność. Stąd $g = e$ i w konsekwencji $f = e$.

(iii) Oznaczmy $k = o(f)$, $l = o(g)$, $m = [k, l]$, $s = o(f \circ g)$. Wtedy $e = (f \circ g)^s = f^s \circ g^s$ na mocy (i), więc z (ii) i ze Stwierdzenia 7.12, $f^s = e$ i $g^s = e$. Zatem $k \mid s$ i $l \mid s$, skąd $m \mid s$. Ale na mocy (i) $(f \circ g)^m = f^m \circ g^m = e \circ e = e$, bo $k \mid m$ i $l \mid m$, więc $s \mid m$. Zatem $m \mid s$ i $s \mid m$, skąd $s = m$. □

Stwierdzenie 7.14. *Jeśli permutacje $f_1, f_2, \ldots, f_k \in S_n$ $(k \geq 2)$ są parami rozłączne (tzn. dla dowolnych różnych liczb $i, j \in \{1, 2, \ldots, n\}$ permutacje f_i i f_j są rozłączne), to zachodzi wzór*:

$$o(f_1 \circ f_2 \circ \ldots \circ f_k) = [o(f_1), o(f_2), \ldots, o(f_k)].$$

Dowód. Zastosujemy indukcję względem naturalnego $k \geq 2$. Dla $k = 2$ teza wynika ze Stwierdzenia 7.13. Niech teraz $k > 2$ będzie taką liczbą naturalną, że teza zachodzi do liczby $k - 1$. Niech permutacje $f_1, f_2, \ldots, f_k \in S_n$ będą parami rozłączne. Wtedy z założenia indukcyjnego dla permutacji $g = f_2 \circ \ldots \circ f_k$ mamy, że $o(g) = [o(f_2), \ldots, o(f_k)]$. Dalej, ze Stwierdzenia 7.11 permutacje f_1 i g są rozłączne oraz $f_1 \circ f_2 \circ \ldots \circ f_k = f_1 \circ g$, więc ze Stwierdzenia 7.13, $o(f_1 \circ f_2 \circ \ldots \circ f_k) = [o(f_1), o(g)]$. Zatem $o(f_1 \circ f_2 \circ \ldots \circ f_k) = [o(f_1), [o(f_2), \ldots, o(f_k)]]$. Ale z elementarnej teorii liczb wiemy, że dla dowolnych liczb naturalnych $a_1, a_2, \ldots, a_k$ $(k > 2)$ zachodzi wzór: $[a_1, [a_2, \ldots, a_k]] = [a_1, a_2, \ldots, a_k]$, więc $o(f_1 \circ f_2 \circ \ldots \circ f_k) = [o(f_1), o(f_2), \ldots, o(f_k)]$. □

3 Rozkład permutacji na cykle

Niech A będzie niepustym zbiorem oraz niech $b_0, b_1, \ldots, b_{r-1}$ $(r \geqslant 2)$ będą różnymi elementami zbioru A. Wówczas permutację postaci

$$\begin{pmatrix} b_0 & b_1 & \ldots & b_{r-2} & b_{r-1} \\ b_1 & b_2 & \ldots & b_{r-1} & b_0 \end{pmatrix} \tag{11}$$

nazywamy *cyklem*, a liczbę r — jego długością. Cykl (11) zapisujemy prościej jako $(b_0, b_1, \ldots, b_{r-1})$. Zatem transpozycje są to dokładnie cykle długości 2. Z określenia cyklu mamy od razu wzór:

$$(b_0, b_1, \ldots, b_{r-1})(b_i) = b_{i \oplus_r 1} \tag{12}$$

dla każdego $i = 0, 1, \ldots, r-1$.

Ze wzoru (12) natomiast przez prostą indukcję uzyskujemy, że

$$(b_0, b_1, \ldots, b_{r-1})^k(b_i) = b_{i \oplus_r k} \tag{13}$$

dla $k, i = 0, 1, \ldots, r-1$.

Ze wzoru (13) mamy w szczególności, że $(b_0, b_1, \ldots, b_{r-1})^k(b_0) = b_k \neq b_0$ dla naturalnych $k < r$, więc $(b_0, b_1, \ldots, b_{r-1})^k \neq e$ dla naturalnych $k < r$. Ponadto ze wzoru (13) wynika, że $(b_0, b_1, \ldots, b_{r-1})^r = e$. W ten sposób udowodniliśmy następujące

Stwierdzenie 7.15. *Rząd dowolnego cyklu długości r jest równy r.* □

Teraz udowodnimy, że każdy cykl długości r jest złożeniem $r-1$ transpozycji.

Stwierdzenie 7.16. *Dla dowolnych różnych elementów $a_1, a_2, \ldots, a_r \in A$ $(r \geq 2)$ zachodzi wzór:*

$$(a_1, a_2, \ldots, a_r) = (a_1, a_r) \circ (a_1, a_{r-1}) \circ \ldots \circ (a_1, a_2). \tag{14}$$

Dowód. Indukcja wzgldem $r \geqslant 2$. Dla $r = 2$ teza jest oczywista. Jeżeli zaś teza zachodzi dla pewnego naturalnego $r \geq 2$ i $a_1, a_2, \ldots, a_r, a_{r+1}$ są różnymi elementami zbioru A, to z założenia indukcyjnego

$$(a_1, a_3, \ldots, a_r, a_{r+1}) = (a_1, a_{r+1}) \circ (a_1, a_r) \circ \ldots \circ (a_1, a_3),$$

więc

$$(a_1, a_{r+1}) \circ (a_1, a_r) \circ \ldots \circ (a_1, a_3) \circ (a_1, a_2) = (a_1, a_3, \ldots, a_r, a_{r+1}) \circ (a_1, a_2) =$$
$$= \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_r & a_{r+1} \\ a_2 & a_3 & a_4 & \ldots & a_{r+1} & a_1 \end{pmatrix} = (a_1, a_2, \ldots, a_r, a_{r+1}). \ \square$$

Wniosek 7.17. *Cykl jest permutacją parzystą wtedy i tylko wtedy, gdy jego długość jest liczbą nieparzystą.*

Dowód. Niech $f = (a_1, a_2, \ldots, a_r)$ będzie cyklem długości r. Wtedy ze Stwierdzenia 7.16 mamy, że f jest złożeniem $r-1$ transpozycji. Zatem z Twierdzenia 7.7 i z Przykładu 7.6 mamy, że $sgn(f) = (-1)^{r-1}$, skąd mamy tezę. □

Stwierdzenie 7.18. *Dla dowolnych różnych elementów $a_0, a_1, \ldots, a_{r-1}$ zbioru A i dla dowolnej permutacji $f \in S(A)$ zachodzi wzór:*

$$f \circ (a_0, a_1, \ldots, a_{r-1}) \circ f^{-1} = (f(a_0), f(a_1), \ldots, f(a_{r-1})). \tag{15}$$

Dowód. Oznaczmy $L = f \circ (a_0, a_1, \ldots, a_{r-1}) \circ f^{-1}$ i $P = (f(a_0), f(a_1), \ldots, f(a_{r-1}))$. Należy wykazać, że $L = P$. Ponieważ $f \in S(A)$, więc wystarczy udowodnić, że $L(f(a)) = P(f(a))$ dla każdego $a \in A$. Jeśli $a \in A \setminus \{a_0, a_1, \ldots, a_{r-1}\}$, to $L((f(a)) = [f \circ (a_0, a_1, \ldots, a_{r-1})](a) = f(a)$ oraz $f(a) \notin \{f(a_0), f(a_1), \ldots, f(a_{r-1})\}$, więc $P(f(a)) = f(a)$.

Ponadto dla $i = 0, 1, \ldots, r-1$ mamy $L(f(a_i)) = [f \circ (a_0, a_1, \ldots, a_{r-1})](a_i) = f(a_{i\oplus_r 1})$ oraz $P(f(a_i)) = f(a_{i\oplus_r 1})$. □

Twierdzenie 7.19. *Każda permutacja $\neq e$ zbioru skończonego A jest złożeniem parami rozłącznych cykli. Przedstawienie permutacji w postaci złożenia parami rozłącznych cykli jest jednoznaczne z dokładnością do kolejności czynników.*

Dowód. Zastosujemy indukcję ze względu na liczbę n elementów zbioru A. Dla $n = 1$ i $n = 2$ teza jest oczywista. Załóżmy, że teza zachodzi dla permutacji zbiorów o liczbie elementów mniejszej niż n. Niech $f \neq e$ będzie permutacją zbioru n-elementowego A. Istnieje wtedy $a \in A$ takie, że $f(a) \neq a$. Rozpatrzmy ciąg $a_1 = a$, $a_2 = f(a_1)$, $a_3 = f(a_2), \ldots$ Ponieważ zbiór A jest skończony, więc wyrazy tego ciągu nie mogą być wszystkie różne. Niech a_{k+1} będzie najwcześniejszym jego wyrazem równym jednemu z wyrazów poprzednich, tzn. niech $a_{k+1} = a_s$ dla pewnego $s < k+1$. Jeżeli $s > 1$, to $f(a_k) = a_{k+1} = a_s = f(a_{s-1})$, skąd $a_k = a_{s-1}$, co przeczy minimalności $k+1$. Zatem $s = 1$ i wobec tego elementy $a_1, a_2 = f(a_1), \ldots, a_k = f(a_{k-1})$ są różne oraz $f(a_k) = a_{k+1} = a_1$. W zapisie permutacji f przestawmy kolumny tak, aby w pierwszym wierszu na początku występowały elementy $a_1, a_2, \ldots, a_k$. Wtedy

$$f = \begin{pmatrix} a_1 & a_2 & \ldots & a_{k-1} & a_k & a'_1 & \ldots & a'_{n-k} \\ a_2 & a_3 & \ldots & a_k & a_1 & f(a'_1) & \ldots & f(a'_{n-k}) \end{pmatrix} =$$
$$= (a_1, a_2, \ldots, a_k) \circ \begin{pmatrix} a'_1 & \ldots & a'_{n-k} \\ f(a'_1) & \ldots & f(a'_{n-k}) \end{pmatrix}.$$

Zatem f jest złożeniem cyklu $(a_1, \ldots, a_k)$ oraz permutacji $g = \begin{pmatrix} a'_1 & \ldots & a'_{n-k} \\ f(a'_1) & \ldots & f(a'_{n-k}) \end{pmatrix}$ zbioru $A' = \{a'_1, \ldots, a'_{n-k}\}$. Na mocy założenia indukcyjnego $g = e$ lub g jest złożeniem skończonej liczby cykli rozłącznych, z których każdy jest rozłączny z cyklem $(a_1, \ldots, a_k)$, skąd f jest iloczynem parami rozłącznych cykli.

Dla dowodu drugiej części twierdzenia przypuśćmy, że permutacja $f \neq e$ ma dwa istotnie różne przedstawienia w postaci złożenia (iloczynu) cykli rozłącznych:

$$f = (a_1, \ldots, a_k) \circ \ldots = (b_1, b_2, \ldots, b_s) \circ \ldots$$

Niech np. cykl $(b_1, b_2, \ldots, b_s)$ będzie różny od każdego z cykli występujących w pierwszym przedstawieniu permutacji f. Ponieważ $b_1 \in A$, więc element b_1 należy do pewnego cyklu występującego w pierwszym przedstawieniu permutacji f. Ale składanie cykli rozłącznych jest przemienne, więc można zakładać, że $b_1 = a_i$ dla pewnego $i = 1, 2, \ldots, k$. Ponadto

$$(a_1, \ldots, a_i, a_{i+1}, \ldots, a_k) = (a_i, a_{i+1}, \ldots, a_k, a_1, \ldots, a_{i-1}),$$

więc można zakładać, że $b_1 = a_1$. Wtedy $b_2 = f(b_1) = f(a_1) = a_2$, $b_3 = f(b_2) = f(a_2) = a_3$, itd. Wynika stąd, że $s = k$ oraz $(b_1, b_2, \ldots, b_s) = (a_1, a_2, \ldots, a_k)$. Uzyskana sprzeczność kończy dowód naszego twierdzenia. □

Z Twierdzenia 7.7, ze Stwierdzenia 7.14 oraz z dowodu Wniosku 7.17 wynika od razu nastpujące

Twierdzenie 7.20. *Jeżeli permutacja f jest złożeniem s cykli parami rozłącznych o długościach $r_1, r_2, \ldots, r_s$, to*
(i) $o(f) = [r_1, r_2, \ldots, r_s]$;
(ii) $sgn(f) = (-1)^{r_1+r_2+\ldots+r_s-s}$. □

Z Twierdzenia 7.19, ze Stwierdzenia 7.16 oraz z tego, że $e = (1,2) \circ (1,2)$ wynika od razu następujące

Twierdzenie 7.21. *Każda permutacja $f \in S_n$ dla $n \geqslant 2$ jest złożeniem skończonej liczby transpozycji.* □

Z Twierdzenia 7.7 i z Przykładu 7.6 mamy też następujące

Twierdzenie 7.22. *Permutacja $f \in S_n$ dla $n \geqslant 2$ jest permutacją parzystą wtedy i tylko wtedy, gdy f jest złożeniem parzystej liczby transpozycji.* □

Stwierdzenie 7.23. *Jeżeli x, y, z, t są różnymi elementami zbioru A, to w grupie permutacji $S(A)$ zachodzi wzór:*

$$[(x,y,z),(x,y,t)] = (x,y) \circ (z,t). \tag{16}$$

Dowód. Mamy

$$\begin{gathered}[(x,y,z),(x,y,t)] = (x,y,z)^{-1} \circ (x,y,t)^{-1} \circ (x,y,z) \circ (x,y,t) = \\ = (x,z,y) \circ (t,y,x) \circ (x,y,z) \circ (x,y,t) = \\ = \begin{pmatrix} x & y & z & t \\ y & x & t & z \end{pmatrix} = (x,y) \circ (z,t). \square\end{gathered}$$

Przykład 7.24. Niech w grupie S_4:

$$V = \{e, (1,2) \circ (3,4), (1,3) \circ (2,4), (1,4) \circ (2,3)\}. \tag{17}$$

Oznaczmy: $a = (1,2) \circ (3,4)$, $b = (1,3) \circ (2,4)$, $c = (1,4) \circ (2,3)$. Wtedy $a^2 = b^2 = c^2 = e$. Ponadto $a \circ b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (1,4) \circ (2,3) = c$, $b \circ a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = c$,

więc V jest podgrupą rzędu 4 grupy S_4 (izomorficzną z grupą czwórkową Kleina). Dla $f \in S_4$ na mocy Stwierdzenia 7.18 mamy, że $f \circ a \circ f^{-1} = f \circ (1,2) \circ (3,4) \circ f^{-1} = = [f \circ (1,2) \circ f^{-1}] \circ [f \circ (3,4) \circ f^{-1}] = (f(1), f(2)) \circ (f(3), f(4)) \in V$ i podobnie $f \circ b \circ f^{-1}, f \circ c \circ f^{-1} \in V$. Stąd $V \lhd S_4$. Ale $V \subseteq A_4$, więc $V \lhd A_4$. Dalej, $|A_4| = \frac{4!}{2} = 12$ i $|A_4/V| = \frac{|A_4|}{|V|} = \frac{12}{4} = 3$, więc grupa A_4/V jest abelowa, skąd z Twierdzenia 5.5, $A_4' \subseteq V$. Ponadto $e = [e, e]$, więc ze Stwierdzenia 7.23 każdy element grupy V jest komutatorem dwóch cykli długości 3, które na mocy Wniosku 7.17 są permutacjami parzystymi, więc $V \subseteq A_4'$ i ostatecznie $V = A_4'$. Z Przykładu 5.6 mamy zatem stąd, że w grupie A_4 nie istnieje podgrupa rzędu 6, chociaż 6 dzieli rząd grupy A_4. □

Twierdzenie 7.25. *Jeżeli A jest zbiorem o co najmniej trzech elementach, to $Z(S(A)) = \{e\}$.*

Dowód. Załóżmy, że tak nie jest. Wtedy istnieje zbiór A o co najmniej trzech elementach i istnieje $f \in Z(S(A))$ takie, że $f \neq e$. Zatem istnieje $a \in A$ takie, że $f(a) \neq a$. Oznaczmy $b = f(a)$. Wtedy a i b są różnymi elementami zbioru A i zbiór A posiada co najmniej trzy elementy, więc istnieje $c \in A \setminus \{a, b\}$. Dalej, $f \in Z(S(A))$, więc na mocy Stwierdzenia 7.18 $(b, f(c)) = f \circ (a, c) \circ f^{-1} = (a, c)$, skąd $\{b, f(c)\} = \{a, c\}$. Ale $c \neq b$, więc $c = f(c)$ oraz $a \neq b$, więc $a = f(c)$, czyli $a = c$ i mamy sprzeczność. Oznacza to, że $Z(S(A)) = \{e\}$. □

Twierdzenie 7.26. *Niech $m, \alpha_1, \alpha_2, \ldots, \alpha_s \in \mathbb{N}$ i niech $p_1, p_2, \ldots, p_s$ będą różnymi liczbami pierwszymi. Wówczas równoważne są warunki:*

(i) w grupie S_m istnieje element rzędu $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$;

(ii) $p_1^{\alpha_1} + p_2^{\alpha_2} + \ldots + p_s^{\alpha_s} \leq m$.

Dowód. $(i) \Rightarrow (ii)$. Niech $f \in S_m$ będzie elementem rzędu $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$. Ponieważ $p_1, \ldots, p_s \geq 2$ oraz $\alpha_1, \ldots, \alpha_s \in \mathbb{N}$, więc $n > 1$, skąd $f \neq e$. Zatem f jest iloczynem parami rozłącznych cykli o długościach $k_1, k_2, \ldots, k_r$, gdzie $k_1 + k_2 + \ldots + k_r \leq m$ oraz $[k_1, k_2, \ldots, k_r] = n$. Bez zmniejszania ogólności rozważań możemy zakładać, że istnieje liczba naturalna $l \leq r$ oraz istnieją liczby naturalne $t_1 < t_2 < \ldots < t_l = s$ takie, że $p_1^{\alpha_1} \cdot \ldots \cdot p_{t_1}^{\alpha_{t_1}} | k_1, p_{t_1+1}^{\alpha_{t_1+1}} \cdot \ldots \cdot p_{t_2}^{\alpha_{t_2}} | k_2, \ldots, p_{t_{l-1}+1}^{\alpha_{t_{l-1}+1}} \cdot \ldots \cdot p_s^{\alpha_s} | k_l$. Stąd wobec $l \leq r$ i $k_1 + k_2 + \ldots + k_r \leq m$ otrzymujemy, że

$$p_1^{\alpha_1} \cdot \ldots \cdot p_{t_1}^{\alpha_{t_1}} + p_{t_1+1}^{\alpha_{t_1+1}} \cdot \ldots \cdot p_{t_2}^{\alpha_{t_2}} + \ldots + p_{t_{l-1}+1}^{\alpha_{t_{l-1}+1}} \cdot \ldots \cdot p_s^{\alpha_s} \leq m. \tag{18}$$

Nasza implikacja będzie więc udowodniona, jeśli pokażemy, że $x_1 \cdot \ldots \cdot x_k \geq x_1 + \ldots + x_k$ dla dowolnych liczb naturalnych $x_1, \ldots, x_k \geq 2$. Dla $k = 1$ ta nierówność jest oczywista, a dla $k = 2$ wynika ona z tożsamości $x_1 \cdot x_2 - (x_1 + x_2) = (x_1 - 1) \cdot (x_2 - 1) - 1$. Przy założeniu, że ta nierówność zachodzi dla pewnej liczby naturalnej k weźmy dowolne liczby naturalne $x_1, \ldots, x_k, x_{k+1} \geq 2$. Wtedy z kroku dla $k = 2$ oraz z założenia indukcyjnego mamy, że $(x_1 \cdot \ldots \cdot x_k) \cdot x_{k+1} \geq x_1 \cdot x_2 \cdot \ldots \cdot x_k + x_{k+1} \geq x_1 + x_2 + \ldots + x_k + x_{k+1}$. Wobec tego na mocy zasady indukcji mamy udowodnioną naszą nierówność dla dowolnego $k \in \mathbb{N}$.

$(ii) \Rightarrow (i)$. Z założenia wynika, że cykle $\sigma_1 = (1, 2, \ldots, p_1^{\alpha_1}), \sigma_2 = (p_1^{\alpha_1}+1, \ldots, p_2^{\alpha_2}), \ldots,$ $\sigma_s = (p_{s-1}^{\alpha_{s-1}} + 1, \ldots, p_s^{\alpha_s})$, są parami rozłączne, należą do S_m i ich długościami są odpowiednio $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_s^{\alpha_s}$. Zatem rząd permutacji f będącej złożeniem tych cykli jest równy $[p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_s^{\alpha_s}] = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$. $\square$

Twierdzenie 7.27. *Niech $f, \sigma \in S_m$, gdzie $\sigma = (a_0, a_1, \ldots, a_{k-1})$. Wówczas $f \circ \sigma =$ $= \sigma \circ f$ wtedy i tylko wtedy, gdy istnieje $i \in \mathbb{Z}_k$ takie, że $f(a_j) = a_{j \oplus_k i}$ dla każdego $j = 0, 1, \ldots, k-1$. W szczególności w grupie S_m istnieje dokładnie $k \cdot (m-k)!$ permutacji przemiennych z cyklem długości k.*

Dowód. Weźmy dowolne $f \in S_m$. Wtedy $f \circ \sigma = \sigma \circ f \Leftrightarrow f \circ \sigma \circ f^{-1} = \sigma$. Ale ze Stwierdzenia 7.18 mamy $f \circ \sigma \circ f^{-1} = (f(a_0), f(a_1), \ldots, f(a_{k-1}))$, więc

$$f \circ \sigma = \sigma \circ f \Leftrightarrow (a_0, a_1, \ldots, a_{k-1}) = (f(a_0), f(a_1), \ldots, f(a_{k-1})). \tag{19}$$

Jeśli f spełnia (19), to $\{a_0, a_1, \ldots, a_{k-1}\} = \{f(a_0), f(a_1), \ldots, f(a_{k-1})\}$, skąd

$$f(x) \in \{a_0, a_1, \ldots, a_{k-1}\} \text{ dla każdego } x \in \{a_0, a_1, \ldots, a_{k-1}\} \tag{20}$$

oraz

$$f(x) \in \{1, 2, \ldots, m\} \setminus \{a_0, a_1, \ldots, a_{k-1}\} \text{ dla każdego } x \in \{1, 2, \ldots, m\} \setminus \{a_0, a_1, \ldots, a_{k-1}\}. \tag{21}$$

Wobec tego dla $A = \{a_0, a_1, \ldots, a_{k-1}\}$ mamy, że $f|A$ jest permutacją zbioru A i $f|(\{1, 2, \ldots, n\} \setminus A)$ jest permutacją zbioru $\{1, 2, \ldots, n\} \setminus A$. Ponadto istnieje $i \in \mathbb{Z}_k$ takie, że $f(a_0) = a_i$, co wobec wzoru (19) daje, że $f(a_1) = \sigma(a_i) = a_{i \oplus_k 1}$. Jeśli dla pewnego $j \in \mathbb{Z}_k$, $j < k-1$ jest $f(a_j) = a_{i \oplus_k j}$, to $f(a_{j+1}) = \sigma(a_{i \oplus_k j}) = a_{i \oplus_k \oplus_k 1} = a_{i \oplus_k (j+1)}$. Wobec tego przez indukcję mamy stąd, że $f(a_j) = a_{j \oplus_k i}$ dla każdego $j = 0, 1, \ldots, k-1$. Na odwrót, jeśli dla pewnego $i \in \mathbb{Z}_k$ jest $f(a_j) = a_{j \oplus_k i}$ dla każdego $j = 0, 1, \ldots, k-1$, to $(f(a_0), f(a_1), \ldots, f(a_{k-1})) = (a_i, a_{i \oplus_k 1}, \ldots, a_{i \oplus_k (k-1)}) = (a_0, a_1, \ldots, a_{k-1})$. Wobec tego na mocy (20) i (21) istnieje dokładnie $k \cdot (m-k)!$ permutacji przemiennych z cyklem σ. $\square$

Zagadka 1. Wyznacz wszystkie permutacje $f \in S_5$ przemienne z cyklem $\sigma = (5, 4, 3)$.

Zagadka 2. Wyznacz wszystkie permutacje $f \in S_8$ przemienne z permutacją $g = (1, 3) \circ (5, 4, 8)$.

Zagadka 3. Dla jakich $m \in \mathbb{N}$ w grupie S_m istnieje element rzędu 2160?

Zagadka 4. W grupie S_8 wyznacz permutację π taką, że $(1, 8, 4, 3) \circ (2, 5, 3) \circ (3, 1, 4) \circ (1, 5) \circ \pi \circ (1, 8, 4, 3) \circ (2, 5, 3)^{-1} = (1, 2, 3, 4, 5) \circ (2, 3, 4, 5, 6)^{-1}$. Wypisz wszystkie inwersje permutacji π, oblicz jej znak i jej rząd w grupie S_8.

Zagadka 5. Udowodnij, że każda permutacja nieparzysta $f \in S_m$ ma rząd parzysty.

Zagadka 6. Dla jakich liczb naturalnych n w grupie S_{12} istnieje element rzędu n?

Zagadka 7. W grupie S_{11} znajdź dwie permutacje nieparzyste f i g rzędu 30, które mają różne liczby punktów stałych.