ALGEBRA R 12

PRZYKŁAD Niech X będzie dowolnym zbiorem. $S_X = \{ f \in Map(X,X) : f \text{ jest bijekcją} \}$ z działaniem składania jest grupę. Elementem neutralnym tej grupy jest odwzorowanie identycznościowe

Gdy $X = \{1,2,3,\dots,n\}$ grupę S_X oznaczamy S_n.

PRZYKŁAD Omówimy dokładnie grupę S_3. Ma ona $3! = 6$ elementów, które oznaczymy $S_3 = \{e, o_1, o_2, s_1, s_2, s_3\}$

e: $e(1)=1$ $e(2)=2$ $e(3)=3$

o_1: $o_1(1)=2$ $o_1(2)=3$ $o_1(3)=1$

o_2: $o_2(1)=3$ $o_2(2)=1$ $o_2(3)=2$ $\rightarrow \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

s_1: $s_1(1)=1$ $s_1(2)=3$ $s_1(3)=2$

s_2: $s_2(1)=3$ $s_2(2)=2$ $s_2(3)=1$

s_3: $s_3(1)=2$ $s_3(2)=1$ $s_3(3)=3$ $\rightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Składanie permutacji:

$$s_3 \circ o_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = s_1$$

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $\qquad$ $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$$o_2 \circ s_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = s_2$$

$s_3 \circ o_2 \neq o_2 \circ s_3$ grupa S_3 jest NIEPRZEMIENNA!

Zapiszemy tabelkę działania tej grupy. Przy okazji pojawi się kilka ważnych faktów dotyczących grup w ogólności. Umawiamy się że najpierw wykonujemy permutację z kolumny a potem z wiersza, tzn

s_3 ↓

$o_2 \longrightarrow o_2 \circ s_3$

Od razu możemy wypisać pierwszy wiersz i pierwszą kolumnę — mnożenie przez e, oraz to co już wyliczyliśmy: $s_3 \circ o_2$ i $o_2 \circ s_3$ (na niebiesko)

Łatwo także zauważyć, że permutacje „typu s", czyli zamieniające miejscami dwa i tylko dwa elementy złożone ze sobą dają e: $s_1 \circ s_1 = e$, $s_2 \circ s_2 = e$, $s_3 \circ s_3 = e$. Takie permutacje (zamieniające dwa elementy) nazywają się transpozycje. Dalej stwierdzamy, że o_1 i o_2 nie mają tej własności że podniesione do kwadratu dają e, ale za to $o_1 \circ o_2 = o_2 \circ o_1 = e$. Wpisujemy to wreszcie w tabelkę na zielono

	e	o_1	o_2	s_1	s_2	s_3
e	e	o_1	o_2	s_1	s_2	s_3
o_1	o_1	o_2	e	s_2	s_3	s_1
o_2	o_2	e	o_1	s_3	s_1	s_2
s_1	s_1	s_3	s_2	e	o_1	o_2
s_2	s_2	s_1	s_3	o_2	e	o_1
s_3	s_3	s_2	s_1	o_1	o_2	e

Obliczamy teraz $o_2 \circ o_2$ i $o_1 \circ o_1$

$$o_2 \circ o_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = o_1$$

$$o_1 \circ o_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = o_2$$

Wyniki wpisujemy do tabelki na różowo

Żeby oszczędzić sobie mudnego wyliczania kolejnych mnożeń udowodnimy ogólny fakt

STWIERDZENIE Niech G będzie grupą. Odwzorowanie mnożenie z lewej i mnożenie z prawej strony przez ustalony element grupy są bijekcjami

$$l_g : G \to G \quad l_g(h) = gh \qquad r_g : G \to G \quad r_g(h) = hg$$

DOWÓD Dowód przeprowadzimy dla l_g, dla r_g robi się podobnie. Pokażemy, że l_g jest injekcją i surjekcją:

Injekcja: niech h, h' będą takie, że $l_g(h) = l_g(h')$, tzn $gh = gh'$. Działamy $\bar{g}$ z lewej: $\bar{g}gh = \bar{g}gh' \Rightarrow h = h'$

Surjekcja: Weźmy dowolne $h \in G$ i znajdźmy k: $l_g(k) = h$, tzn $gk = h$. Znowu działamy $\bar{g}$ z lewej: $\bar{g}gk = \bar{g}h \Rightarrow k = \bar{g}h$ ■

WNIOSEK: W tabelce działania grupy każdy element występuje tylko raz. Posługując się tym faktem możemy wypełnić wiersz i kolumnę odpowiadającą o_2 (na czerwono). Wiemy też że w wierszu i kolumnie dla o_2 są miejsca jedynie na „esy", zatem w kolorze błękitnym wpisujemy co się da. Żeby wypełnić tabelkę do końca potrzebujemy jeszcze wyliczyć przynajmniej jedno złożenie transpozycji

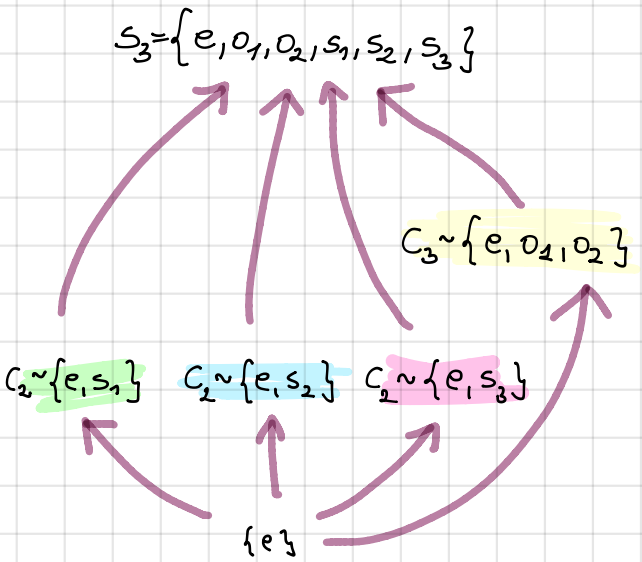
$$s_1 \circ s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = o_1$$

Resztę da się odgadnąć (na jasnozielono)

DEFINICJA: Podzbiór g zamknięty ze względu na mnożenie i branie odwrotności nazywamy podgrupę.

DEFINICJA Liczbę elementów grupy nazywamy rzędem grupy

Spójrzmy na tabelkę S_3 i poszukajmy podgrup



	e	o_1	o_2	s_1	s_2	s_3
e	e	o_1	o_2	s_1	s_2	s_3
o_1	o_1	o_2	e	s_2	s_3	s_1
o_2	o_2	e	o_1	s_3	s_1	s_2
s_1	s_1	s_3	s_2	e	o_1	o_2
s_2	s_2	s_1	s_3	o_2	e	o_1
s_3	s_3	s_2	s_1	o_1	o_2	e

Wewnętrzna struktura grupy S_3 opisana jest diagramem jak wyżej.
W S_3 są 4 podgrupy nie licząc trywialnej $\{e\}$.
Podgrupa rzędu 3, izomorficzna z $\mathbb{Z}_3$ (czyli C_3) oraz trzy podgrupy rzędu 2.

DEFINICJA **Rzędem** elementu g grupy G nazywamy najmniejszą liczbę naturalną n taką, że $g^n = e$. Jeśli dla żadnego n nie zachodzi $g^n = e$ mówimy, że rząd jest nieskończony.
Rząd elementu g oznaczamy $\text{ord}\, g$.
$\text{ord}\, s_i = 2$, $\text{ord}\, o_i = 3$ $\text{ord}\, e = 1$

Zmienimy teraz grupę (weźmy np S_5) i wprowadzimy kilka pojęć charakterystycznych dla grupy permutacji. Niech σ oznacza następującą permutację

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$$

Z pewnych powodów "pokolorujemy" elementy zbioru $\{1, 2, 3, 4, 5\}$ i powtórzymy σ kilka razy:

σ^2 (σ, σ):
1 2 3 4 5
2 4 5 1 3
4 1 3 2 5

σ:
1 2 5 4 3

σ:
2 4 3 1 5

σ:
4 1 5 2 3

$\sigma^5 = e$:
1 2 3 4 5
2 4 5 1 3

Okazuje się, że działając wielokrotnie tą samą permutacją pozostawiamy niezmienione pewne podzbiory zbioru $X = \{1,2,3,4,5\}$. Podzbiory te to $\{1,2,4\}$ i $\{3,5\}$.

Zbiory te nazywamy orbitami działania permutacji σ, albo w skrócie σ. Formalnie orbitę możemy zdefiniować następująco:

W zbiorze $X = \{1, 2, \ldots, n\}$ wprowadzamy relację związaną z ustalonym elementem σ: $i \sim j$ jeśli istnieje $r \in \mathbb{Z}$ takie, że $\sigma^r(i) = j$. Relacja ta jest relacją równoważności (łatwe sprawdzenie). Klasy równoważności tej relacji to orbity permutacji σ. Orbitę nazywamy trywialną jeśli ma tylko jeden element.

Zauważmy że permutacja działa na orbitach niejako oddzielnie. Zajmijmy się więc permutacjami mającymi tylko jedną nietrywialną orbitę. W naszej permutacji σ są dwie takie permutacje:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix} \qquad \sigma = \alpha \circ \beta = \beta \circ \alpha$$

DEFINICJA: Permutacja, która ma jedną nietrywialną orbitę nazywa się cyklem.

Powód tej nazwy stanie się jasny za chwilę. Istnieje wygodny sposób zapisywania cyklu: Wystartujmy od dowolnego i należącego do nietrywialnej orbity i stosujmy kolejno ϱ (które jest cyklem związanym z tą orbitą)

$$i \quad \varrho(i) \quad \varrho^2(i) \quad \varrho^3(i) \quad \varrho^4(i) \ldots$$

W powyższym ciągu prędzej czy później powtórzy się znowu i. Wtedy (a nawet krok wcześniej) pisanie można przerwać, gdyż powstały w ten sposób ciąg zawiera wszystkie elementy orbity a w kolejności elementów także informację o powtórzeniu cyklu na każdym elemencie orbity.

$$\alpha = (1\ 2\ 4) \qquad \beta = (3\ 5)$$

WŁASNOŚCI CYKLI:

(1) Rząd cyklu jest równy liczbie elementów nietrywialnej orbity.

(2) Cykle o rozłącznych orbitach są przemienne.

FAKT: Każda permutacja jest złożeniem pewnej liczby transpozycji. Rozkład ten NIE JEST jednoznaczny.

DOWÓD: Wiadomo, że każda permutacja jest złożeniem cykli. Wystarczy pokazać, że każdy cykl jest złożeniem transpozycji. Spójrzmy najpierw na przykład: Weźmy $\sigma \in S_5$, która jest jednym cyklem:

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

$$(1\ 3)(3\ 5)(5\ 4)(4\ 2)$$

1 2 3 4 5
1 4 3 2 5
1 5 3 2 4
1 3 5 2 4
3 1 5 2 4

Ogólnie każdy cykl $(i_1\ i_2 \ldots i_k)$ $i_j \in \{1, \ldots, n\}$ można rozłożyć na transpozycje w następujący sposób
$(i_1\ i_2\ i_3 \ldots i_{k-1}\ i_k) = (i_1\ i_2)(i_2\ i_3) \cdots (i_{k-1}\ i_k)$. Transpozycje te oczywiście nie są rozłączne. Rozkład nie jest jednoznaczny gdyż np. w dowolne miejsce można wstawić dwie transpozycje odwrotne, np: $(1\ 2)(2\ 1)$. ■

TWIERDZENIE: Dla każdej permutacji liczba transpozycji w rozkładzie tej permutacji na transpozycje ma ustaloną parzystość

DOWÓD: Obserwacja Złożenie permutacji z transpozycją zmienia liczbę orbit o 1. Najpierw przykład: $\rho \in S_8$

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 8 & 6 & 4 & 5 & 1 & 7 \end{pmatrix} = (1\ 3\ 8\ 7)(4\ 6\ 5)$$

$$\{1,2,3,4,5,6,7,8\} = \{1,3,7,8\} \cup \{4,5,6\} \cup \{2\}$$

trzy orbity

i) transpozycje "wewnątrz" cyklu:

$$\rho \circ (8\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 8 & 4 & 5 & 6 & 7 & 3 \\ 3 & 2 & 7 & 6 & 4 & 5 & 1 & 8 \end{pmatrix} = (1\ 3\ 7)(4\ 6\ 5)$$

$$\{1,2,3,4,5,6,7,8\} = \{1,3,7\} \cup \{4,5,6\} \cup \{8\} \cup \{2\}$$

cztery orbity

$$(8\ 3) \circ \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 8 & 6 & 4 & 5 & 1 & 7 \\ 8 & 2 & 3 & 6 & 4 & 5 & 1 & 7 \end{pmatrix} = (1\ 8\ 7)(4\ 6\ 5)$$

$$\{1,2,3,4,5,6,7,8\} = \{1,7,8\} \cup \{4,5,6\} \cup \{2\} \cup \{3\}$$

cztery orbity

ii) Transpozycje między cyklami

$$\rho \circ (8\ 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 8 & 7 & 6 \\ 3 & 2 & 8 & 6 & 4 & 7 & 1 & 5 \end{pmatrix} = (1\ 3\ 8\ 5\ 4\ 6\ 7)$$

$$\{1,3,4,5,6,7,8\} \cup \{2\}$$

dwie orbity!

$$(8\ 6) \circ \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 8 & 6 & 4 & 5 & 1 & 7 \\ 3 & 2 & 6 & 8 & 4 & 5 & 1 & 7 \end{pmatrix} = (1\ 3\ 6\ 5\ 4\ 8\ 7)$$

iii) Transpozycje z punktem stałym

$$(2\ 3) \circ \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 8 & 6 & 4 & 5 & 1 & 7 \\ 2 & 3 & 8 & 6 & 4 & 5 & 1 & 7 \end{pmatrix} = (1\ 2\ 3\ 8\ 7)(4\ 6\ 5)$$

$\{1,2,3,7,8\} \cup \{4,5,6\}$

dwie orbity!

Jeśli dodatkowa transpozycja jest wewnątrz nietrywialnej orbity orbita ta rozpada się na dwie, liczba orbit przyrasta o 1; jeśli dodatkowa transpozycja jest między nietrywialnymi orbitami, orbity te łączą się – liczba orbit maleje o 1; jeśli dodatkowa transpozycja ruszy punkt stały jest on dołączany do orbity – liczba orbit maleje o 1; ostatecznie transpozycja zamieniająca dwa punkty stałe dwie jednoelementowe orbity znikają i powstaje jedna dwuelementowa czyli liczba orbit maleje o 1.

Weźmy teraz dowolną permutację $\pi \in S_n$ i rozłóżmy ją na transpozycje na dwie sposoby:

$$\pi = \tau_1 \circ \tau_2 \circ \dots \circ \tau_k = \omega_1 \circ \omega_2 \circ \dots \circ \omega_l$$

Wiadomo, że k może być różne od l. Wiadomo także że $e \in S_n$ ma n orbit wobec tego

$$e = \overline{\pi} \circ \tau_k \circ \tau_{k-1} \circ \dots \circ \tau_1 = \overline{\pi} \circ \omega_l \circ \omega_{l-1} \circ \dots \circ \omega_1$$

$\overline{\pi}$: n orbit; τ_k: m orbit; τ_{k-1}: zmiana; τ_1: parzystości; $\overline{\pi}$: m orbit; ω_l: zmiana parzystości

$$(-1)^m = (-1)^m (-1)^k \qquad (-1)^n = (-1)^m \cdot (-1)^l$$

$$(-1)^k = (-1)^l$$

■

DEFINICJA: Liczbę $(-1)^{\text{liczba transpozycji w rozkładzie}}$ nazywamy znakiem permutacji i oznaczamy $\operatorname{sgn}(\sigma)$. Permutacje o dodatnim znaku nazywamy parzystymi, pozostałe niepazystymi.

WNIOSEK ①: Skoro cykl długości k to da się rozłożyć na $k-1$ transpozycji to znak cyklu długości k jest równy $(-1)^{k-1}$.

WNIOSEK ②: Niech $\pi = \rho_1 \rho_2 \dots \rho_l$ będzie rozkładem permutacji na cykle rozłączne długości, odpowiednio $k_1, k_2, \dots, k_l$, wtedy

$$\operatorname{sgn}(\pi) = (-1)^{k_1-1} (-1)^{k_2-1} \dots (-1)^{k_l-1}$$

WNIOSEK ③: Z samej definicji znaku permutacji zachodzi fakt

$$\forall_{\rho,\sigma} \quad \operatorname{sgn}(\rho \circ \sigma) = \operatorname{sgn}(\rho) \cdot \operatorname{sgn}(\sigma)$$

WNIOSEK ④: Jeśli przyjmiemy następującą realizację grupy $C_2 = \{1, -1\}$ z mnożeniem,

$\cdot$	1	-1
1	1	-1
-1	-1	1

to odwzorowanie $\operatorname{sgn}: S_n \longrightarrow C_2$ jest homomorfizmem grup, tzn zachowuje strukturę grupy.

Istnieje alternatywny sposób obliczania znaku permutacji. Omówimy go na przykładzie permutacji $\rho \in S_8$, której już używaliśmy.

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

DEFINICJA: Niech $X = \{1, 2, \dots, n\}$ i niech $\sigma \in S_n$. Inwersją w zbiorze X względem permutacji σ nazywamy parę (i, j) elementów X taką, że $i < j$ a $\sigma(i) > \sigma(j)$. Zbiór inwersji względem σ oznaczymy J_σ.

Wypiszmy inwersje w $\{1, \dots, 8\}$ względem ρ. Najpierw pary takie, że $i < j$, pod nimi stosowne pary wartości, dalej wybierzemy inwersje:

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

(1,2)	(1,3)	(1,4)	(1,5)	(1,6)	(1,7)	(1,8)
(3,2)	(3,8)	(3,6)	(3,4)	(3,5)	(3,1)	(3,7)
	(2,3)	(2,4)	(2,5)	(2,6)	(2,7)	(2,8)
	(2,8)	(2,6)	(2,4)	(2,5)	(2,1)	(2,7)
		(3,4)	(3,5)	(3,6)	(3,7)	(3,8)
		(8,6)	(8,4)	(8,5)	(8,1)	(8,7)
			(4,5)	(4,6)	(4,7)	(4,8)
			(6,4)	(6,5)	(6,1)	(6,7)
				(5,6)	(5,7)	(5,8)
				(4,5)	(4,1)	(4,7)
					(6,7)	(6,8)
					(5,1)	(5,7)
						(7,8)
						(1,7)

$$J_\rho = \{(1,2); (1,7); (2,7); (3,4); (3,5); (3,6); (3,7); (3,8); (4,7); (4,5); (4,6); (5,7); (6,7)\}$$

$$|J_\rho| = 13$$

$$\rho = (1\ 3\ 8\ 7)(4,6,5)$$

$$\operatorname{sgn}\rho = (-1)^3(-1)^2 = -1$$

FAKT Niech $\sigma \in S_n$ $\quad \operatorname{sgn}\sigma = (-1)^{|J_\sigma|}$

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

$$\rho \circ (3\,4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 4 & 3 & 5 & 6 & 7 & 8 \\ 3 & 2 & 6 & 8 & 4 & 5 & 1 & 7 \end{pmatrix} \begin{matrix} \leftarrow (3\,4) \\ \leftarrow \rho \end{matrix}$$

π

$$J_\pi = \{(1,2); (1,7); (2,7); (3,5); (3,6); (3,7); (4,5); (4,6); (4,7); (4,8); (5,7); (6,7)\} \qquad |J_\pi| = 12$$

$$J_\rho = \{(1,2); (1,7); (2,7); (3,4); (3,5); (3,6); (3,7); (3,8); (4,5); (4,6); (4,7); (5,7); (6,7)\}$$

τ jest złożeniem $(3\,4) \circ \rho$. Permutacja τ różni się od ρ zamianą miejscami $\rho(3)$ i $\rho(4)$. Para $(3,4)$ Była inwersją względem ρ, wobec tego nie jest inwersją względem τ. Ponadto pary mające 3 na początku wymieniają się z parami mającymi 4 na początku i odwrotnie. Ogólnie rzecz biorąc liczba inwersji spadła o 1.

Żeby więc „sprowadzić" permutację ρ do e (która ma zero inwersji) potrzebujemy $|J_\rho|$ transpozycji przestawiających kolejne elementy. Wobec tego mamy:

$$e = \rho \circ \tau_1 \circ \tau_2 \circ \dots \circ \tau_m \Rightarrow \rho = \tau_m \circ \tau_{m-1} \circ \dots \circ \tau_2 \circ \tau_1$$

τ_1, τ_2 — transpozycje postaci $(i, i+1)$; $m = |J_\rho|$; ρ da się przedstawić jako złożenie m transpozycji wobec tego $\operatorname{sgn}\rho = (-1)^m$

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

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

$$e = \rho \circ (1\,2)(4\,5)(6\,7)(3\,4)(5\,6)(4\,5)(6\,7)(3\,4)(5\,6)(2\,3)(6\,7)(1\,2)(7\,8)$$

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

13 transpozycji kolejnych wyrazów jak 13 inwersji w ρ.

Powyższe rozważanie dotyczące konkretnej permutacji nie stanowi oczywiście formalnego dowodu łatwo jednak nabyte doświadczenie „przetłumaczyć" na formalny dowód:

DOWÓD: Niech $\sigma \in S_m$ będzie dowolną, choć ustaloną permutacją. Niech J_σ oznacza zbiór inwersji tej permutacji. Zauważmy, że w zbiorze inwersji każdej permutacji różnej od e jest przynajmniej jedna inwersja postaci $(i, i+1)$. Gdyby tak nie było, to oznaczałoby że $\sigma(1) < \sigma(2) < \sigma(3) < \dots < \sigma(n)$ wobec tego $\sigma = e$. Złożenie $\sigma \circ (i\ i+1)$ ma o jedną inwersję mniej gdyż para $(i, i+1)$ nie jest już inwersją, ponadto inwersje postaci (i,k) zastępowane są przez $(i+1, k)$ a te postaci $(i+1, l)$ przez (i, l). Jedyną różnicę „na sztuki" tworzy inwersja $(i, i+1)$. W zbiorze inwersji permutacji $\sigma \circ (i\ i+1)$ też jest inwersja postaci $(j\ j+1)$ chyba, że $\sigma \circ (i\ i+1) = e$. Kontynuujemy składanie aż otrzymamy

$\sigma \circ \tau_1 \circ \tau_2 \circ \dots \circ \tau_k = e$. Nastąpi to dla $k = |J_\sigma|$, gdyż za każdym złożeniem liczba inwersji maleje o 1. Wobec tego $\sigma = \tau_k \circ \tau_{k-1} \circ \dots \circ \tau_1$ i $\operatorname{sgn}\sigma = (-1)^k$ ■

Wniosek: każdą permutację da się złożyć z permutacji kolejnych wyrazów. Można więc powiedzieć, że grupa permutacji jest generowana przez permutacje postaci $(i\ i+1)$.

W ten sposób zakończyliśmy badanie grupy permutacji. W dalszym ciągu wykładu do celów liniowych będziemy potrzebowali głównie pojęcia znaku permutacji. Na zakończenie omawiania elementów teorii grup zróbmy krótką wycieczkę w kierunku grup symetrii.