Podstawy matematyki

Wykład 5 - Funkcje wielu zmiennych, wykresy, grupy, permutacje

Oskar Kędzierski

10 maja 2020

Funkcje wielu zmiennych

Definicja

Funkcją **wielu zmiennych** nazywamy dowolną funkcję

$$f\colon X_1 \times \ldots \times X_n \longrightarrow Y,$$

gdzie $X_1, \ldots, X_n, Y$ są zbiorami.

Uwaga

Dla $x_1 \in X_1, x_2 \in X_2, \ldots, x_n \in X_n$, na ogół, zamiast pisać $f((x_1, x_2, \ldots, x_n))$ piszemy $f(x_1, x_2, \ldots, x_n)$.

Przykład

Na przykład, funkcja $f\colon \mathbb{R}^3 \to \mathbb{R}$ zadaną wzorem $f(x_1, x_2, x_3) = x_1 - x_2 + x_3$ jest funkcją trzech zmiennych.

Funkcje wielu zmiennych cd.

Przykład

Macierze $M(m \times n; \mathbb{K})$ o m wierszach, n kolumnach i współczynnikach w ciele $\mathbb{K}$ można utożsamić z funkcjami

$$f\colon \{1, \ldots, m\} \times \{1, \ldots, n\} \to \mathbb{K}.$$

Utożsamienie jest zadane przez bijekcję, gdzie $A = [a_{ij}]$

$$M(m \times n; \mathbb{K}) \ni A \mapsto f_A \in \mathbb{K}^{\{1,\ldots,m\}\times\{1,\ldots,n\}} \text{ oraz } f_A(i,j) = a_{ij}.$$

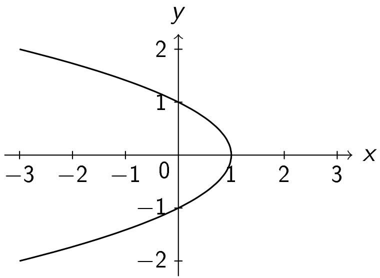
Wykres relacji

Definicja

Wykresem relacji $R \subset \mathbb{R}^m \times \mathbb{R}^n$ gdzie $n + m \leq 3$ nazywamy graficzne przedstawienie punktów $(x, y) \in \mathbb{R}^m \times \mathbb{R}^n$ takich, że xRy w **kartezjańskim układzie współrzędnych**.

Przykład

Wykres relacji $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x + y^2 = 1\}$



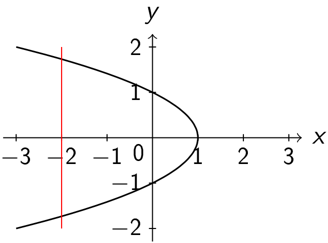
Wykres relacji – własności

Stwierdzenie

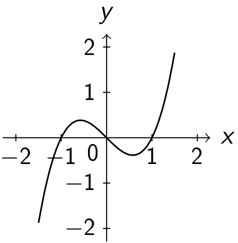
Relacja jest $R \subset \mathbb{R} \times \mathbb{R}$ jest funkcją wtedy i tylko wtedy, gdy każda prosta równoległa do osi $0y$ przecina wykres relacji w dokładnie jednym punkcie.

Przykład

$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x + y^2 = 1\}$



$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x^3 - x\}$



Funkcje rzeczywiste

Definicja

Dla dowolnego zbioru X funkcję

$$f : X \to \mathbb{R}$$

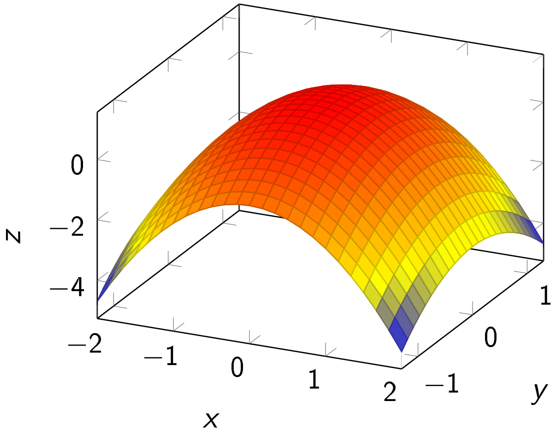
nazywamy **funkcją rzeczywistą.** Funkcję $f : \mathbb{R}^n \to \mathbb{R}$ nazywamy funkcją rzeczywistą n zmiennych rzeczywistych.

Przykład

Funkcja $f : \mathbb{R}^2 \to \mathbb{R}$ zadana wzorem $f(x, y) = 1 - x^2 - y^2$ jest funkcją rzeczywistą dwóch zmiennych rzeczywistych.

Funkcje rzeczywiste – przykład

wykres funkcji $f(x, y) = 1 - x^2 - y^2$



Zestawienie funkcji

Definicja

Dla dowolnych zbiorów $X, Y_1, \ldots, Y_n$ oraz funkcji $f_i \colon X \to Y_i$, gdzie $i = 1, \ldots, n$, funkcję

$$f \colon X \to Y_1 \times \cdots \times Y_n$$

zadaną wzorem $f(x) = (f_1(x), f_2(x), \ldots, f_n(x))$ dla $x \in X$ nazywamy **zestawieniem** funkcji $f_1, \ldots, f_n$. Piszemy $f = (f_1, \ldots, f_n)$.

Przykład

Funkcja $f \colon \mathbb{R}^2 \to \mathbb{R}^2$ zadana wzorem $f(x, y) = (x + y, x - y)$ jest zestawieniem funkcji $f_1, f_2 \colon \mathbb{R}^2 \to \mathbb{R}$ zadanych wzorami $f_1(x, y) = x + y$, $f_2(x, y) = x - y$.

Zestawienie funkcji cd.

Stwierdzenie

Jeśli co najmniej jedna funkcja f_i jest różnowartościowa, to funkcja $f = (f_1, \ldots, f_n)$ jest różnowartościowa. Jeśli funkcja $f = (f_1, \ldots, f_n)$ jest „na", to funkcje $f_1, \ldots, f_n$ sa funkcjami „na".

Uwaga

Funkcja $f \colon \mathbb{R}^2 \to \mathbb{R}^2$ zadana wzorem $f(x, y) = (x + y, x - y)$ jest różnowartościowa ale żadna z jej składowych nie jest różnowartościowa. Funkcja (id_X, id_X) nie jest „na" ale jej składowe są funkcjami „na". Zatem stwierdzenia odwrotne nie są prawdziwe.

Iloczyn kartezjański funkcji

Definicja

Dla dowolnych zbiorów $X_1, \dots, X_n$, $Y_1, \dots, Y_n$ oraz funkcji $f_i \colon X_i \to Y_i$, gdzie $i = 1, \dots, n$, funkcję

$$f \colon X_1 \times \cdots \times X_n \to Y_1 \times \cdots \times Y_n$$

zadaną wzorem $f(x_1, x_2, \dots, x_n) = (f_1(x_1), f_2(x_2), \dots, f_n(x_n))$ dla $x_i \in X_i$ nazywamy **iloczynem kartezjańskim** funkcji $f_1, \dots, f_n$. Piszemy $f = f_1 \times \ldots \times f_n$.

Przykład

Funkcja $f \colon \mathbb{R}^2 \to \mathbb{R}^2$ zadana wzorem $f(x, y) = (2x + 1, -y)$ jest iloczynem kartezjańskim funkcji $f_1, f_2 \colon \mathbb{R} \to \mathbb{R}$ zadanych wzorami $f_1(x) = 2x + 1,\ f_2(x) = -x$.

Iloczyn kartezjański funkcji cd.

Stwierdzenie

Funkcja $f = f_1 \times \ldots \times f_n$ jest różnowartościowa wtedy i tylko wtedy, gdy funkcje $f_1, \ldots, f_n$ są różnowartościowe. Funkcja $f = f_1 \times \ldots \times f_n$ jest funkcją „na” wtedy i tylko wtedy, gdy funkcje $f_1, \ldots, f_n$ są funkcjami „na”.

Przykład

Funkcja $f : \mathbb{R}^2 \to \mathbb{R}^2$ zadana wzorem $f(x, y) = (2x + 1, -y)$ jest wzajemnie jednoznaczna. Funkcja $f = f_1 \times f_2$ oraz funkcje $f_1(x) = 2x + 1,\ f_2(x) = -x$ są funkcjami wzajemnie jednoznacznymi.

Relacja odwrotna – przypomnienie

Definicja

Dla dowolnej relacji $R \subset X \times Y$ definiujemy relację odwrotną $R^{-1} \subset Y \times X$ warunkiem

$$yR^{-1}x \leftrightarrow xRy.$$

Stwierdzenie

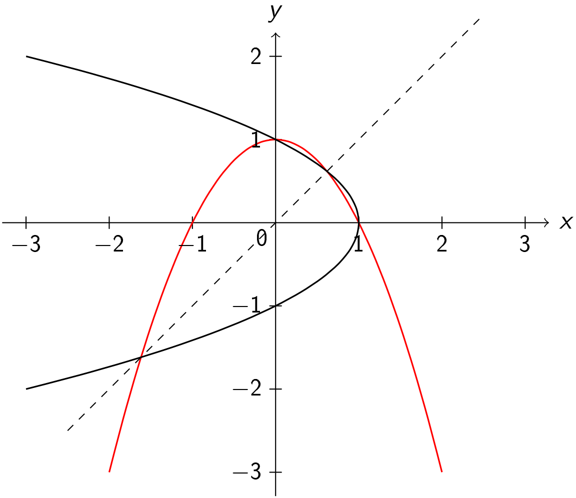
Dla dowolnej relacji $R \subset \mathbb{R} \times \mathbb{R}$ wykres relacji $R^{-1} \subset \mathbb{R} \times \mathbb{R}$ jest obrazem wykresu relacji R w symetrii prostopadłej względem prostej $U = \mathrm{lin}((1,1))$.

Dowód.

Odwzorowanie liniowe $\varphi \colon \mathbb{R} \times \mathbb{R} \ni (x,y) \mapsto (y,x) \in \mathbb{R} \times \mathbb{R}$ przeprowadza wykres relacji R na wykres relacji R^{-1}. Zauważmy, że $\varphi((1,1)) = 1 \cdot (1,1)$ oraz $\varphi((1,-1)) = (-1) \cdot (1,-1)$ zatem 1 oraz -1 są wartościami własnymi z prostopadłymi przestrzeniami własnymi $\mathbb{R}^2_{(1)} = \mathrm{lin}((1,1))$, $\mathbb{R}^2_{(-1)} = \mathrm{lin}((1,-1))$.

Wykres relacji odwrotnej – przykład

$$R \quad = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x + y^2 = 1\}$$
$$R^{-1} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y = 1\}$$



Funkcja odwrotna

Stwierdzenie

Funkcja $f\colon X \to Y$ jest funkcją wzajemnie jednoznaczną wtedy i tylko wtedy, gdy relacja odwrotna $f^{-1} \subset Y \times X$ jest funkcją.

Dowód.

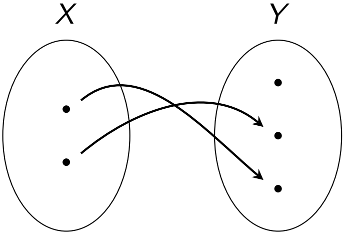
($\rightarrow$) funkcja wzajemnie jednoznaczna f posiada funkcję odwrotną $f^{-1}\colon Y \to X$, która jest zarazem relacją odwrotną,

($\leftarrow$) jeśli $f^{-1}\colon Y \to X$ jest funkcją, to $f^{-1} \circ f = \mathrm{id}_X$ oraz $f \circ f^{-1} = \mathrm{id}_Y$, zatem f jest funkcją wzajemnie jednoznaczną.

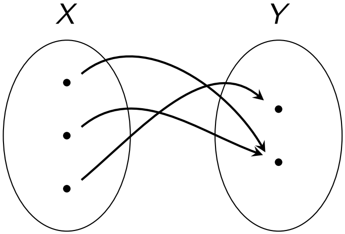
Przykład

Funkcją odwrotną do funkcji $f\colon \mathbb{R} \setminus \{1\} \to \mathbb{R} \setminus \{2\}$ zadaną wzorem $f(x) = \frac{2x+1}{x-1}$ jest funkcja $f^{-1}\colon \mathbb{R} \setminus \{2\} \to \mathbb{R} \setminus \{1\}$ zadana wzorem $f^{-1}(x) = \frac{x+1}{x-2}$.

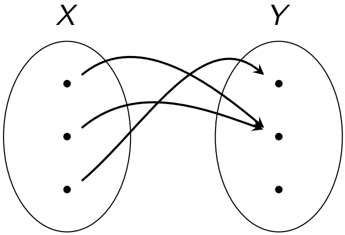
Funkcja odwrotna – przykład



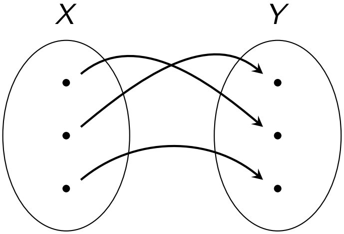
różnowartościowa ale nie „na’



„na” ale nie różnowartościowa

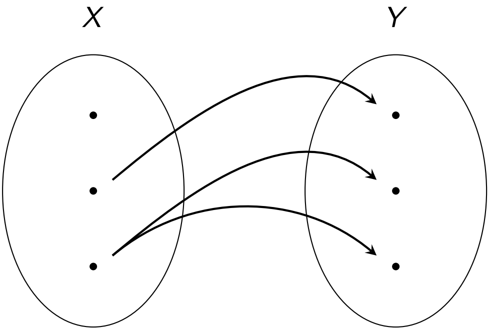


ani różnowartościowa ani „na”



wzajemnie jednoznaczna

Funkcja odwrotna – przykład cd.



to nie jest funkcja

Uwaga

Na poprzednim slajdzie, po odwróceniu kierunku strzałek, jedynie w przypadku funkcji wzajemnie jednoznacznej otrzymujemy funkcję.

Grupa

Definicja

Grupą nazywamy zbiór G wyposażony w funkcję $\cdot : G \times G \to G$, zwaną **działaniem** (lub **mnożeniem**), spełniającą warunki:

i) $\forall_{a,b,c \in G}\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (łączność działania),

ii) $\exists_{e \in G} \forall_{a \in G}\ a \cdot e = e \cdot a = a$ (istnienie elementu neutralnego względem działania),

iii) $\forall_{a \in G} \exists_{a^{-1} \in G}\ a \cdot a^{-1} = a^{-1} \cdot a = e$ (istnienie elementu odwrotnego względem działania).

Jeśli dodatkowo, zachodzi warunek $\forall_{a,b \in G}\ a \cdot b = b \cdot a$ grupę nazywamy **przemienną** (lub **abelową**). Grupę, która nie jest przemienna nazywamy grupą **nieprzemienną**. Liczbę elementów grupy G (gdy jest skończona) nazywamy **rzędem** grupy G.

Uwaga

Na ogół, zamiast $a \cdot b$ pisze się ab.

Własności

Stwierdzenie

Niech G będzie grupą. Wtedy

i) element neutralny $e \in G$ jest wyznaczony jednoznacznie,

ii) dla dowolnego $a \in G$ element odwrotny a^{-1} jest wyznaczony jednoznacznie,

iii) dla dowolnych $a, b \in G$ zachodzi $(ab)^{-1} = b^{-1}a^{-1}$.

Dowód.

i) przypuśćmy, że $e, e' \in G$ są elementami neutralnymi, wtedy $e = ee' = e'$,

ii) przypuśćmy, że dla pewnego $a \in G$ elementy $b, c \in G$ są elementami odwrotnymi do a, wtedy $b = be = b(ac) = (ba)c = ec = c$,

iii) $(ab)(b^{-1}a^{-1}) = aea^{-1} = aa^{-1} = e$, element odwrotny jest wyznaczony jednoznacznie.

Przykłady grup

i) $(\mathbb{Z}, +)$ z elementem neutralnym 0 jest grupą przemienną,

ii) dla dowolnego ciała $\mathbb{K}$, grupami przemiennymi są $(\mathbb{K}, +)$ z elementem neutralnym 0 (grupa addytywna ciała $\mathbb{K}$) oraz $(\mathbb{K} \setminus \{0\}, \cdot)$ z elementem neutralnym 1 (grupa multyplikatywna ciała $\mathbb{K}$),

iii) dla dowolnego ciała $\mathbb{K}$ grupą (przemienną dla $n = 1$ i nieprzemienną dla $n \geq 2$) jest zbiór macierzy odwracalnych $GL(n; \mathbb{K}) = \{A \in M(n \times n; \mathbb{K}) \mid \det A \neq 0\}$ o współczynnikach w ciele $\mathbb{K}$, z mnożeniem macierzy jako działaniem oraz macierzą identyczności I jako elementem neutralnym, odwrotnością macierzy A jest macierz odwrotna A^{-1},

iv) $(\mathbb{N}, +)$ z elementem neutralnym 0 **nie jest** grupą (nie istnieją elementy odwrotne),

v) $(\mathbb{R}_{>0}, \cdot)$ z elementem neutralnym 1 jest grupą przemienną,

Przykłady grup cd.

vi) pierwiastki $n-$tego stopnia z jedynki tj. $1, \varepsilon_n, \varepsilon_n^2, \ldots, \varepsilon_n^{n-1}$, gdzie $\varepsilon_n = e^{\frac{2\pi i}{n}}$, wraz z mnożeniem tworzą grupę przemienną rzędu n. Nazywamy ją **grupą cykliczną rzędu** n i oznaczamy C_n.

Rząd elementu grupy

Definicja

Rzędem elementu $a \in G$ nazywamy najmniejszą liczbę naturalną $n \geq 1$ taką, że $a^n = \overbrace{a \cdot a \cdot \ldots \cdot a}^{n \text{ razy}} = e$. Jeśli taka liczba nie istnieje, mówimy, że a ma **nieskończony rząd.** Rząd elementu a oznaczamy przez $rz(a)$.

Przykład

i) $rz(e) = 1$ oraz $rz(a) = rz(a^{-1})$ dla dowolnej grupy G, dowolnego elementu $a \in G$ oraz elementu neutralnego e,

ii) $rz\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right) = 2,\ rz\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right) = \infty$ w grupie $GL(2;\mathbb{R})$, bo $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^2 = I$ oraz $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \neq I$ dla $n \geq 1$,

iii) w grupie cyklicznej rzędu 6 mamy $rz(1) = 1, rz(\varepsilon_6^3) = 2, rz(\varepsilon_6^2) = rz(\varepsilon_6^4) = 3, rz(\varepsilon_6) = rz(\varepsilon_6^5) = 6.$

Permutacje

Definicja

Jeśli X jest zbiorem skończonym, to każdą funkcję wzajemnie jednoznaczną $f : X \to X$ nazywamy **permutacją** zbioru X.

Stwierdzenie

Permutacji zbioru n-elementowego X jest $n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$.

Dowód.

Konstruujemy funkcję wzajemnie jednoznaczną ze zbioru X na zbiór X. Pierwszy element zbioru X może przejść na n dowolnych elementów. Drugi element zbioru X może przejść na $n-1$ dowolnych elementów zbioru X (jeden został już wykorzystany), itd.

Permutacje cd.

Stwierdzenie

Jeśli $f, g\colon X \to X$ są permutacjami zbioru X, to permutacjami są też funkcje $g \circ f$ oraz f^{-1}.

Dowód.

Złożenie dwóch funkcji różnowartościowych (odp. funkcji „na") jest funkcją różnowartościową (odp. funkcją „na"). Funkcja odwrotna do funkcji wzajemnie jednoznacznej jest funkcją wzajemnie jednoznaczną.

Stwierdzenie

Niech X będzie zbiorem skończonym a $f\colon X \to X$ funkcją. Następujące warunki są równoważne:

i) f jest funkcją różnowartościową,

ii) f jest funkcją „na",

iii) f jest funkcją wzajemnie jednoznaczną.

Permutacje cd.

Dowód.

Z poprzedniego wykładu, jeśli złożenie $g \circ f$ jest funkcją różnowartościową (odp. funkcją „na”), to f (odp. g) jest funkcją różnowartościową (odp. funkcją „na”). Oraz, jeśli $g \circ f = g \circ f'$ (odp. $g \circ f = g' \circ f$) oraz g jest funkcją różnowartościową (odp. f funkcją „na”), to $f = f'$ (odp. $g = g'$).

Zauważmy, że gdy f jest funkcją różnowartościową lub funkcją „na”, w zbiorze $\{f^n \mid n \geq 1\}$ pewne złożenia muszą wystąpić co najmniej dwukrotnie (liczba funkcji $X \to X$ jest skończona), tzn. istnieją $m > m' \geq 1$ takie, że $f^m = f^{m'}$, co z powyższych własności daje, że $f^{m-m'} = \mathrm{id}_X$.

i) $\to$ ii) istnieje $n \geq 1$ takie, że $f^n = \mathrm{id}_X$. Gdy $n = 1$, to $f = \mathrm{id}_X$, gdy $n \geq 2$, to $f \circ f^{n-1} = \mathrm{id}_X$ zatem f jest funkcją „na”, bo id_X jest funkcją „na”

Permutacje cd.

Dowód.

ii) $\to$ iii) istnieje $n \geq 1$ takie, że $f^n = \mathrm{id}_X$. Gdy $n = 1$, to $f = \mathrm{id}_X$, gdy $n \geq 2$, to $f^{n-1} \circ f = \mathrm{id}_X$ zatem f jest funkcją różnowartościową (bo id_X jest funkcją różnowartościową), zatem f jest odwzorowaniem wzajmenie jednoznacznym,

iii) $\to$ i) oczywiste

Grupa permutacji

Wniosek

Wszystkie permutacje zbioru $n-$elementowego X tworzą grupę, oznaczaną $\mathrm{Sym}(X)$ (lub S_n dla $X = \{1, \ldots, n\}$).

Działaniem w tej grupie jest składanie funkcji, elementem neutralnym jest identyczność id_X a elementem odwrotnym do funkcji f jest funkcja odwrotna f^{-1}.

Dla dowolnych $f, g, h \in \mathrm{Sym}(X)$ zachodzą warunki

i) $(f \circ g) \circ h = f \circ (g \circ h)$,

ii) $f \circ \mathrm{id}_X = \mathrm{id}_X \circ f = f$,

iii) $f^{-1} \circ f = f^{-1} \circ f = \mathrm{id}_X$.

Jest to grupa rzędu $n!$, przemienna dla $n = 1, 2$, nieprzemienna dla $n \geq 3$.

Grupa permutacji cd.

Definicja

Grupę S_n wszystkich permutacji zbioru $\{1, \ldots, n\}$ nazywamy **grupą permutacji** (lub **grupą symetryczną**).

Zapis permutacji

Od tej pory przyjmujemy, że $X = \{1, 2, \dots, n-1, n\}$.
Permutacja $f \in S_n$ jest jednoznacznie wyznaczona przez obrazy kolejnych elementów $1, 2, \dots, n$.

Notacja

Permutację $f\colon \{1, \dots, n\} \to \{1, \dots, n\}$ zapisujemy przy pomocy tabelki
$$f = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ f(1) & f(2) & \dots & f(n-1) & f(n) \end{pmatrix}.$$

Zapis permutacji cd.

Przykład

Niech $n = 5$. Niech permutacja $f \in S_n$ będzie zadana warunkami

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

Wtedy

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

Przykład

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

Składanie permutacji

Permutacje składamy stosują najpierw tabelkę permutacji stojącej po prawej stronie złożenia, a potem tabelkę permutacji stojącej po lewej stronie złożenia.

Przykład

Niech

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

Wtedy

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

Widać, że $f \circ g \neq g \circ f$. Niech $\mathrm{id} = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{smallmatrix}\right)$. Wtedy

$$f \circ \mathrm{id} = \mathrm{id} \circ f = f, \quad g \circ \mathrm{id} = \mathrm{id} \circ g = g.$$

Składanie permutacji cd.

Przykład

Niech

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

Zauważmy, że

$$g^2 = g \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \mathrm{id}\,.$$

Zatem $rz(g) = 2$, to znaczy rząd elementu g to 2. Można sprawdzić, że $rz(f) = 6$.

Permutacja odwrotna

Permutację odwrotną liczymy zamieniając wiersze tabelki, a potem porządkując pierwszy wiersz.

Przykład

Niech

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

Wtedy

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

Można sprawdzić, że

$$f \circ f^{-1} = f^{-1} \circ f = g \circ g^{-1} = g^{-1} \circ g = \mathrm{id}\,.$$

Rząd potęgi elementu

Stwierdzenie

Niech $f \in S_N$ będzie permutacją rzędu n ($rz(f) = n$) zbioru $N-$elementowego, tj. $f^n = \text{id}$ oraz liczba $n \geq 1$ jest najmniejszą liczbą o tej własności. Wtedy, dla dowolnej liczby naturalnej $m \geq 1$ zachodzi

$$rz(f^m) = \frac{\text{NWW}(n, m)}{m}.$$

Dowód.

Niech $k \geq 1$ będzie taką liczbą naturalną, że $(f^m)^k = f^{mk} = \text{id}$. Podzielmy liczbę mk z resztą przez n. Istnieje zatem liczba naturalna l oraz liczba naturalna r spełniająca warunek $0 \leq r < n$ takie, że $mk = ln + r$. Ponieważ $f^{ln} = (f^n)^l = \text{id}^l = \text{id}$ mamy $(f^m)^k = f^{nl} f^r = f^r = \text{id}$. Z definicji liczby n wynika, że $r = 0$. Zatem $mk = ln$, czyli liczba mk jest wielokrotnością m i n. Najmniejsza taka liczba jest najmniejszą wielokrotnością m i n, zatem $mk = \text{NWW}(m, n)$.

Rząd potęgi elementu cd.

Przykład

Niech

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

gdzie $rz(f) = 6, rz(g) = 2$. Wtedy, na przykład

$$rz(f^3) = \frac{\mathrm{NWW}(3,6)}{3} = 2, \quad , rz(f^4) = \frac{\mathrm{NWW}(4,6)}{4} = 3,$$

oraz

$$rz(g^3) = \frac{\mathrm{NWW}(3,2)}{3} = 2, \quad , rz(g^4) = \frac{\mathrm{NWW}(4,2)}{4} = 1.$$

Rząd potęgi elementu cd.

Uwaga

Dla dowolnych liczb naturalnych $m, n \geq 1$ zachodzi wzór

$$\frac{\mathrm{NWW}(n,m)}{m} = \frac{n}{\mathrm{NWD}(n,m)},$$

zatem rząd potęgi elementu o rzędzie n jest nie większy od n.

Cykle

Niech $1 \leq k \leq n$ oraz niech $1 \leq i_1, i_2, \ldots, i_k \leq n$ będą parami różnymi liczbami naturalnymi.

Definicja

Cyklem nazywamy permutację $f \in S_n$ taką, że istnieją liczby $i_1, \ldots, i_k$ jak wyżej oraz

$$f(x) = \begin{cases} i_{j+1} & x = i_j,\ j = 1, \ldots, k-1 \\ i_1 & x = i_k \\ x & x \neq i_j \end{cases}$$

Piszemy wtedy $f = (i_1, i_2, \ldots, i_k)$. Liczbę k nazywamy długością cyklu.

Uwaga

Oczywiście $(i_1, i_2, \ldots, i_n) = (i_2, i_3, \ldots, i_n, i_1) = (i_3, i_4, \ldots, i_n, i_1, i_2) = \ldots = (i_n, i_1, i_2, \ldots, i_{n-2}, i_{n-1})$. Cykl długości 1 jest identycznością.

Cykle cd.

Przykład

Na przykład $f = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{smallmatrix}\right) = (1,3,5) = (3,5,1) = (5,1,3)$ oraz $f(1) = 3, f(3) = 5, f(5) = 1$ oraz $f(x) = x$ dla $x \neq 1,3,5$.

Przykład

Niech

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

Wtedy

$$f = (1,5,3)(2,4) \quad g = (1,2).$$

Cykle cd.

Definicja

Cykle $(i_1, i_2, \ldots, i_k)$ oraz $(j_1, j_2, \ldots, j_l)$ nazywamy **rozłącznymi** jeśli $i_s \neq j_t$ dla wszystkich $s = 1, \ldots, k, \; t = 1, \ldots, l$.

Definicja

Transpozycją nazywamy cykl długości 2, to jest postaci (i_1, i_2).

Przykład

Cykle $(1, 5, 3)$ oraz $(2, 4)$ są rozłączne. Cykle $(1, 2, 3)$ oraz $(1, 5)$ nie są rozłączne. Cykl $(2, 4)$ jest transpozycją, cykl $(1, 5, 3)$ nie jest transpozycją.

Własności cykli

Stwierdzenie

Rząd cyklu długości k jest równy k, tzn.

$$rz((i_1, \dots, i_k)) = k$$

.

Dowód.

Niech $f = (i_1, \dots, i_k)$. Wtedy dla $l \leq k$

$$f^l(x) = \begin{cases} i_{j+l} & x = i_j,\ j = 1, \dots, k-l \\ i_{j+l-k} & x = i_j,\ j = k-l+1, \dots, k \\ x & x \neq i_j \end{cases}$$

Pierwszym l, dla którego otrzymamy identyczność, to $l = k$.

Własności cykli cd.

Stwierdzenie

Niech cykle $f = (i_1, i_2, \ldots, i_k)$ oraz $g = (j_1, j_2, \ldots, j_l)$ będą rozłączne. Wtedy

$$f \circ g = g \circ f.$$

Mówimy, że cykle f, g są **przemienne**.

Dowód.

Permutowanie elementów dwóch rozłącznych zbiorów nie zależy od kolejności tych zbiorów.

Przykład

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

Własności cykli cd.

Uwaga

Cykle, które nie są rozłączne na ogół nie są przemienne

$$(1,2)(1,3) = (1,3,2), \qquad (1,3)(1,2) = (1,2,3).$$

Zatem

$$(1,2)(1,3) \neq (1,3)(1,2).$$

Własności cykli cd.

Stwierdzenie

Każdą permutację da sie przedstawić jako iloczyn parami rozłącznych cykli.

Przykład

Zamiast dowodu przedstawimy przykład. Niech $f \in S_9$ będzie równa

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 1 & 4 & 3 & 9 & 6 & 2 & 7 \end{pmatrix}.$$

Zaczynamy rozpisywać f jako iloczyn rozłącznych cykli startując od 1:

$$f = (1, \dots$$

Liczba 1 przechodzi na 5, zatem wypisujemy 5 jako kolejną liczbę w cyklu:

$$f = (1, 5 \dots$$

Własności cykli cd.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 1 & 4 & 3 & 9 & 6 & 2 & 7 \end{pmatrix}$$

Liczba 5 przechodzi na 3, zatem wypisujemy 3 jako kolejną liczbę w cyklu:

$$f = (1, 5, 3 \dots$$

Ponieważ liczba 3 przechodzi z powrotem na liczbę 1 kończymy cykl i zaczynamy następny startując od najmniejszej, niewykorzystanej do tej pory liczby. Jest to liczba 2.

$$f = (1, 5, 3)(2, \dots$$

Liczba 2 przechodzi na liczbę 8, a liczba 8 z powrotem na 2. Najmniejsza niewykorzystana liczba to 4, która przechodzi na siebie.

$$f = (1, 5, 3)(2, 8)(4)$$

Własności cykli cd.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 1 & 4 & 3 & 9 & 6 & 2 & 7 \end{pmatrix}$$

$$f = (1,5,3)(2,8)(4)$$

Najmniejsza niewykorzystana liczba, to liczba 6.

$$f = (1,5,3)(2,8)(4)(6,\ldots$$

Ostatecznie, kontynuując jak wyżej:

$$f = (1,5,3)(2,8)(4)(6,9,7).$$

Ogólny dowód wygląda analogicznie.

Kanoniczna/standardowa postać permutacji

i) rozkładamy permutację na cykle rozłączne,
ii) w każdym cyklu wybieramy element największy jako pierwszy,
iii) ustawiamy cykle porządkując je według pierwszego elementu, od najmniejszego do największego.

Uwaga: bierzemy pod uwagę cykle długości jeden.

Przykład

Postać standardowa permutacji
$f = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 1 & 4 & 3 & 9 & 6 & 2 & 7 \end{smallmatrix}\right) = (1,5,3)(2,8)(6,9,7)$, to

$$f = (4)(5,3,1)(8,2)(9,7,6).$$

Typ permutacji

Definicja

Mówimy, że permutacja $f \in S_n$ jest **typu** $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$ jeśli w rozkładzie na cykle rozłączne ma dokładnie λ_i cykli o długości i dla $i = 1, \dots, n$ (w zapisie pomijamy wyrazy z $\lambda_i = 0$).

Przykład

Permutacja $f = (1,5,3)(2,8)(6,9,7) \in S_9$ jest typu $1^1 2^1 3^2$.

Permutacja $f = (1,5,3)(2,8)(6,9,7) \in S_{10}$ jest typu $1^2 2^1 3^2$.

Transpozycja jest permutacją typu $1^{n-2} 2^1$.

Rząd permutacji

Stwierdzenie

Jeśli $f = h_1 \cdot \ldots \cdot h_k$ jest rozkładem permutacji f na parami rozłączne cykle to

$$rz(f) = \mathrm{NWW}(rz(h_1), \ldots, rz(h_k)).$$

Przykład

Niech $f = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 1 & 4 & 3 & 9 & 6 & 2 & 7 \end{smallmatrix}\right) = (1,5,3)(2,8)(6,9,7)$, wtedy

$$rz(f) = \mathrm{NWW}(3,2,3) = 6.$$

Rozkład na iloczyn transpozycji

Stwierdzenie

Niech $f = (i_1, i_2, \ldots, i_k)$ będzie cyklem. Wtedy

$$f = (i_k, i_{k-1})(i_k, i_{k-2}) \ldots (i_k, i_2)(i_k, i_1),$$

jest iloczynem $k-1$ transpozycji.

Przykład

$(1, 2, 9, 3, 5) = (5, 3)(5, 9)(5, 2)(5, 1)$

Wniosek

Każdą permutację można przedstawić jako iloczyn transpozycji.

Dowód.

W rozkładzie na iloczyn cykli rozkładamy każdy cykl na iloczyn transpozycji.

Rozkład na iloczyn transpozycji cd.

Uwaga

Rozkład na iloczyn transpozycji nie jest jednoznaczny. Na przykład, jeśli $f = (i_1, i_2, \ldots, i_k)$, to

$$f = (i_k, i_{k-1})(i_k, i_{k-2}) \ldots (i_k, i_2)(i_k, i_1)$$

oraz

$$f = (i_1, i_2)(i_2, i_3) \ldots (i_{k-2}, i_{k-1})(i_{k-1}, i_k).$$

Permutacje parzyste, znak permutacji

Definicja

Permutację, którą da się przedstawić jako iloczyn parzystej (odp. nieparzystej) liczby transpozycji nazywamy **parzystą** (odp. **nieparzystą**) i mówimy, że jej **znak** $\mathrm{sgn}(f)$ jest równy 1 (odpowiednio -1).

Przykład

Permutacje parzyste

$$\mathrm{sgn}(\mathrm{id}) = \mathrm{sgn}((1,2)(2,3)) = \mathrm{sgn}((1,2)(3,4)(5,6)(7,8)) = 1.$$

Permutacje nieparzyste

$$\mathrm{sgn}((1,2)) = \mathrm{sgn}((1,2)(1,3)(2,1)) = \mathrm{sgn}((1,2)(3,4)(5,6)) = -1.$$

Permutacje parzyste, znak permutacji cd.

Uwagi

i) przedstawienie jako iloczyn transpozycji nie jest jednoznaczne ale parzystość/nieparzystość jest zachowana, np. $(1,2,3) = (3,2)(3,1) = (2,1)(2,3) = (3,2)(1,3)(3,2)(2,3)$, zatem $\mathrm{sgn}((1,2,3)) = 1$.

ii) cykl o długości parzystej jest permutacją nieparzystą, a cykl o długości nieparzystej jest permutacją parzystą, tzn.

$$\mathrm{sgn}((i_1, \dots, i_k)) = (-1)^{k-1},$$

iii) iloczyn dwóch permutacji parzystych lub dwóch permutacji nieparzystych jest permutacją parzystą, iloczyn permutacji parzystej i nieparzystej jest permutacją nieparzystą, tzn.

$$\mathrm{sgn}(fg) = \mathrm{sgn}(f)\,\mathrm{sgn}(g).$$

Permutacje parzyste, znak permutacji cd.

Uwagi

iv) jeśli rząd permutacji jest liczbą nieparzystą to jest ona parzysta (w rozkładzie na cykle rozłączne każdy cykl jest długości nieparzystej),

v) twierdzenie odwrotne nie zachodzi, permutacja $(1,2)(3,4)$ jest parzysta a ma rząd równy 2,

vi) jeśli rząd permutacji jest liczbą parzystą to może ona być parzysta lub nieparzysta, na przykład permutacja $(1,2)$ ma rząd 2 a jest nieparzysta, permutacja $(1,2)(3,4)$ ma rząd 2 a jest parzysta.

Permutacje parzyste, znak permutacji cd.

Wniosek

Jeśli permutacja $f \in S_n$ jest typu $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$, to jest ona parzysta (odp. nieparzysta) wtedy i tylko wtedy, gdy liczba $\lambda_2 + \lambda_4 + \lambda_6 + \dots$ jest parzysta (odp. nieparzysta) oraz

$$\operatorname{sgn}(f) = (-1)^{\lambda_2 + \lambda_4 + \dots}.$$

Dowód.

$$\operatorname{sgn}(f) = \left[(-1)^{(1-1)}\right]^{\lambda_1} \left[(-1)^{(2-1)}\right]^{\lambda_2} \left[(-1)^{(3-1)}\right]^{\lambda_3} \cdot \ldots \cdot \left[(-1)^{(n-1)}\right]^{\lambda_n} =$$
$$= (-1)^{\lambda_2 + \lambda_4 + \dots},$$

to znaczy pomijamy cykle o długości nieparzystej, bo sa one permutacjami parzystymi, a mnożenie przez permutację parzystą nie zmienia parzystości.

Permutacje parzyste, znak permutacji cd.

Przykład

Permutacja $f = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 1 & 4 & 3 & 9 & 6 & 2 & 7 \end{smallmatrix}\right) = (1,5,3)(2,8)(6,9,7)$ jest nieparzysta jako iloczyn dwóch permutacji parzystych i jednej nieparzystej. Równoważnie, permutacja f jest typu $1^1 2^1 3^2$ zatem

$$\mathrm{sgn}(f) = (-1)^1 = -1,$$

zatem jest nieparzysta.

Macierz permutacji

Definicja

Dla dowolnej permutacji $f \in S_n$ definiujemy jej **macierz** $A_f = [a_{ij}] \in M(n \times n; \mathbb{Z})$ warunkiem

$$a_{ij} = \begin{cases} 0 & i \neq f(j) \\ 1 & i = f(j) \end{cases}$$

Stwierdzenie

Dla dowolnych permutacji $f, g \in S_n$ zachodzi

i) $A_{\mathrm{id}} = I$,

ii) $A_{fg} = A_f A_g$,

iii) $A_f^{-1} = A_{f^{-1}} = A_f^{\mathsf{T}}$,

iv) $\mathrm{sgn}(f) = \det A_f$.

Macierz permutacji cd.

Przykład

Niech $f = (1,4)(2,3) \in S_4$. Wtedy

$$A_f = A_f^\mathsf{T} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \quad A_f^2 = A_{f^2} = I.$$

Dodatkowo $\det A_f = 1$, zatem f jest parzysta.

Permutacje a wyznacznik

Uwaga

Można wykazać, że jeśli $A = [a_{ij}] \in M(n \times n; \mathbb{K})$, to

$$\det A = \sum_{f \in S_n} \operatorname{sgn}(f) a_{1f(1)} a_{2f(2)} \cdot \ldots \cdot a_{nf(n)} =$$

$$= \sum_{f \in S_n} \operatorname{sgn}(f) a_{f(1)1} a_{f(2)2} \cdot \ldots \cdot a_{f(n)n}.$$

Inwersje

Definicja

Dla ustalonej permutacji $f \in S_n$ **inwersją** nazywamy każdą parę liczb $1 \leq i < j \leq n$ taką, że $f(i) > f(j)$.

Uwaga

Liczba inwersji permutacji może się zmieniać od 0 (dla identyczności) do $\frac{n(n-1)}{2}$ (dla $f = \left(\begin{smallmatrix} 1 & 2 & \dots & n & n-1 \\ n & n-1 & \dots & 2 & 1 \end{smallmatrix}\right)$).

Stwierdzenie

Permutacje parzyste (odp. nieparzyste) posiadają parzystą (odp. nieparzystą) liczbę inwersji.

Dowód.

Niech

$$s(f) = \prod_{1 \leq i < j \leq n} \frac{x_{f(i)} - x_{f(j)}}{x_i - x_j}.$$

Inwersje cd.

Dowód.

Niech $k =$ liczba inwersji permutacji f, wtedy

$$s(f) = \begin{cases} -1 & 2 \nmid k, \\ 1 & 2 \mid k. \end{cases}$$

Dodatkowo

$$s(fg) = \prod_{1 \leq i < j \leq n} \frac{x_{fg(i)} - x_{fg(j)}}{x_i - x_j} =$$

$$= \prod_{1 \leq i < j \leq n} \frac{x_{f(i)} - x_{f(j)}}{x_i - x_j} \prod_{1 \leq i < j \leq n} \frac{x_{f(g(i))} - x_{f(g(j))}}{x_{f(i)} - x_{f(j)}}.$$

Niech $y_k = x_{f(k)}$, co jest równoważne $x_k = y_{f^{-1}(k)}$. Wtedy

$$\prod_{1 \leq i < j \leq n} \frac{x_{f(g(i))} - x_{f(g(j))}}{x_{f(i)} - x_{f(j)}} = \prod_{1 \leq i < j \leq n} \frac{y_{f^{-1}(f(g(i)))} - y_{f^{-1}(f(g(j)))}}{y_i - y_j} = s(g).$$

Inwersje cd.

Dowód.

Zachodzi zatem związek

$$s(fg) = s(f)s(g),$$

a ponieważ liczba inwersji transpozycji jest nieparzysta (ćwiczenie, użyj np. związku

$$(1,2) = (1,m)(2,n)(m,n)(2,n)(1,m),$$

dla $m, n \notin \{1,2\}$), to

$$\mathrm{sgn}(f) = s(f),$$

oraz liczba transpozycji w rozkładzie permutacji parzystej (odp. nieparzystej) na iloczyn transpozycji jest parzysta (odp. nieparzysta).

Inwersje cd.

Definicja

Dla ustalonej permutacji $f \in S_n$ **wektorem inwersji** nazywamy $n-$tkę liczb naturalnych $(a_1, \ldots, a_n) \in \mathbb{N}^n$, gdzie $a_j = |\{i \in \mathbb{N} \mid 1 \leq i < j \wedge f(i) > f(j)\}|$.

Uwaga

Pierwszy element wektora inwersji to 0. Suma liczb z wektora inwersji to liczba inwersji.

Niech $f = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{smallmatrix}\right)$. Wtedy wektor inwersji jest równy

$$(0, 1, 2, 2, 2),$$

a liczba inwersji permutacji f wynosi 7. Permutacja f jest nieparzysta.

Kod Lehmera

Definicja

Dla ustalonej permutacji $f \in S_n$ **kodem Lehmera** nazywamy $n-$tkę liczb naturalnych $(a_1, \ldots, a_n) \in \mathbb{N}^n$, gdzie $a_j = |\{i \in \mathbb{N} \mid 1 \leq j < i \wedge f(j) > f(i)\}|$.

Uwaga

Ostatni element kodu Lehmera to 0. Suma liczb z wektora inwersji to liczba inwersji.

Niech $f = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{smallmatrix}\right)$. Wtedy kod Lehmera permutacji f jest równy

$$(4, 3, 0, 0, 0),$$

a liczba inwersji permutacji f wynosi 7. Permutacja f jest nieparzysta.

Kod Lehmera cd.

Stwierdzenie

Funkcja

$$S_n \ni f \mapsto \{0,\ldots,n-1\} \times \{0,\ldots,n-2\} \times \ldots \times \{0,1\} \times \{0\},$$

jest bijekcją.

Dowód.

Funkcja jest dobrze określona, ponieważ od $f(i)$ większych może być co najwyżej $n-i$ liczb. Ponieważ dziedzina i przeciwdziedzina są równoliczne, wystarczy wykazać, że funkcja jest różnowartościowa (lub równoważnie, każdy kod jednoznacznie wyznacza permutację).

Kod Lehmera cd.

Dowód.

Dla ustalonego kodu $(a_1, \ldots, a_n)$ permutacja o zadanym kodzie dana jest przez

$$f(1) = a_1 + 1,$$

$$f(i) = (a_i + 1)\text{-ta liczb wśród}$$

$$\text{liczb } \{1, \ldots, n\} \setminus \{f(1), f(2), \ldots, f(i-1)\}.$$

Liczba $f(1)$ jest większa od a_1 liczb wśród $\{1, \ldots, n\}$. Po usunięciu $f(1)$, liczba $f(2)$ jest większa od $a_2 + 1$ pozostałych liczb, itd.

Kod Lehmera – Przykład

Znaleźć permutację $f \in S_6$ o kodzie $(4, 1, 2, 2, 0, 0)$.

$$\{1, 2, 3, 4, 5, 6\} \text{ skąd } f(1) = 5,$$

$$\{1, 2, 3, 4, 6\} \text{ skąd } f(2) = 2,$$

$$\{1, 3, 4, 6\} \text{ skąd } f(3) = 4,$$

$$\{1, 3, 6\} \text{ skąd } f(4) = 6,$$

$$\{1, 3\} \text{ skąd } f(5) = 1,$$

$$\{3\} \text{ skąd } f(6) = 3,$$

skąd

$$f = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 6 & 1 & 3 \end{smallmatrix}\right).$$

Średnia liczba inwersji

Stwierdzenie

Oczekiwana liczba inwersji w losowo wybranej permutacji zbioru $\{1, \ldots, n\}$ to $\frac{1}{2}\binom{n}{2}$.

Dowód.

Niech L_n oznacza sumę inwersji każdej permutacji w grupie S_n. Zatem poszukiwana liczba to $\frac{L_n}{n!}$. Ponieważ kody Lehmera to dokładnie elementy zbioru $\{0, \ldots, n-1\} \times \ldots \times \{0, \}$, to

$$
\begin{aligned}
L_n = (n-1)!(n-1) + L_{n-1} + \\
+ (n-1)!(n-2) + L_{n-1} + \\
\vdots \\
+ (n-1)!1 + L_{n-1} + \\
+ (n-1)!0 + L_{n-1} = \\
= (n-1)!\frac{n(n-1)}{2} + nLn - 1.
\end{aligned}
$$

Średnia liczba inwersji cd.

Stąd, po podzieleniu stronami przez $n!$

$$\frac{L_n}{n!} = \frac{n-1}{2} + \frac{L_{n-1}}{(n-1)!},$$

skąd

$$\frac{L_n}{n!} = \frac{n-1}{2} + \frac{n-2}{2} + \ldots + \frac{2}{2} + \frac{L_2}{2!} = \\ = \frac{1}{2}\binom{n}{2},$$

bo $L_2 = 1$.

Sprzężenie cyklu

Stwierdzenie

Jeśli $f \in S_n$ jest permutacją, to dla dowolnego cyklu $(i_1, i_2, \ldots, i_m) \in S_n$ zachodzi tożsamość

$$f \circ (i_1, i_2, \ldots, i_m) \circ f^{-1} = (f(i_1), f(i_2), \ldots, f(i_m)).$$

Dowód.

Ćwiczenie.

Permutacje ustalające jeden element

Stwierdzenie

Dla dowolnych $1 \leq j \leq n$, odwzorowanie pomiędzy zbiorami

$$A = \{f \in S_n \mid f(1) = j\},$$

$$B = \{g \in \{2, \ldots, n\} \to \{2, \ldots, n\} \mid g \text{ jest bijekcją}\},$$

dane wzorem

$$A \ni f \mapsto$$

$$\mapsto \left(\{2, \ldots, n\} \ni i \mapsto g(i) = \begin{cases} f(i) + 1 & \text{dla } f(i) < j \\ f(i) & \text{dla } f(i) > j \end{cases} \in \{2, \ldots, n\} \right) \in B.$$

jest bijekcją. Dodatkowo, dla dowolnego $f \in A$

$$\operatorname{sgn}(f) = (-1)^{j+1} \operatorname{sgn}(g).$$

Permutacje ustalające jeden element cd.

Dowód.

Ponieważ,

$$f|_{\{2,\dots,n\}}\colon \{2,\dots,n\} \to \{1,\dots,\check{j},\dots,n\},$$

jest także bijekcją, to

$$g\colon \{2,\dots,n\} \to \{2,\dots,n\},$$

jest także bijekcją. Dodatkowo, każda inwersja g jest inwersją dla f. Permutacja f posiada więcej inwersji, są to dokładnie inwersje w postaci $1 \leq k$ oraz $j = f(1) > f(k)$. Zachodzi to w dokładnie $j-1$ przypadkach, dla k takiego, że $f(k) = 1, 2, \dots, j-1$. Ponieważ

$$\operatorname{sgn}(f) = (-1)^{\text{liczba inwersji} f},$$

to

$$\operatorname{sgn}(f) = (-1)^{j-1}\operatorname{sgn}(g) = (-1)^{j+1}\operatorname{sgn}(g).$$

Równoważność definicji wyznacznika

Wniosek

Dla macierzy $A \in M(n \times n; \mathbb{K})$. Niech

$$\det A = \sum_{f \in S_n} \operatorname{sgn}(f) a_{1f(1)} a_{2f(2)} \cdot \ldots \cdot a_{nf(n)}.$$

Wtedy

$$\det A = \sum_{j=1}^{n} (-1)^{j+1} a_{1j} \det A_{1j},$$

gdzie $A_{1j} \in M((n-1) \times (n-1); \mathbb{K})$ jest macierzą powstałą z macierzy A przez wykreślenie pierwszego wiersza oraz j-tej kolumny z macierzy A, a funkcja det jest zdefiniowana jak wyżej.

Równoważność definicji wyznacznika cd.

Dowód.

$$\det A = \sum_{f \in S_n} \operatorname{sgn}(f) a_{1f(1)} a_{2f(2)} \cdot \ldots \cdot a_{nf(n)} =$$

$$= \sum_{j=1}^{n} \sum_{\substack{f \in S_n \\ f(1)=j}} \operatorname{sgn}(f) a_{1j} a_{2f(2)} \cdot \ldots \cdot a_{nf(n)} =$$

$$= \sum_{j=1}^{n} (-1)^{j+1} a_{1j} \sum_{\substack{f \in S_n \\ f(1)=j}} \operatorname{sgn}(g) a_{1j} a_{2f(2)} \cdot \ldots \cdot a_{nf(n)},$$

$$= \sum_{j=1}^{n} (-1)^{j+1} a_{1j} \det A_{1j}.$$