Permutacje

DEFINICJA 1 Niech X – dowolny niepusty zbiór. Każdą bijekcję $\sigma\colon X \to X$ nazywamy *permutacją* zbioru X. Zbiór wszystkich permutacji zbioru X oznaczamy symbolem S_X. W przypadku, gdy $X = [n] := \{1, 2, \ldots, n\}$ piszemy S_n zamiast $S_{[n]}$.

Dalej zakładamy, że zbiór X jest skończony.

Zadanie 1. Wykazać, że jeśli X jest zbiorem skończonym oraz $\sigma : X \to X$, to następujące stwierdzenia są równoważne:

- $\sigma \in S_X$;
- σ jest suriekcją;
- σ jest iniekcją.

Sposoby zapisywania permutacji

Tabelka: $\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$; np. $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ oznacza taką permutację σ zbioru [3], że $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 2$.

Wiersz: W przypadku permutacji zbioru $[n]$ górny wiersz tabelki możemy opuścić i napisać $\sigma(1)\sigma(2)\ldots\sigma(n)$. Permutacja z przykładu może więc zostać zapisana tak $\sigma : 312$.

Diagramy: (patrz: rysunek 1)

LEMAT 1 *Złożenie permutacji jest permutacją.*

Ponieważ składanie funkcji jest łączne, więc łączne jest składanie permutacji.

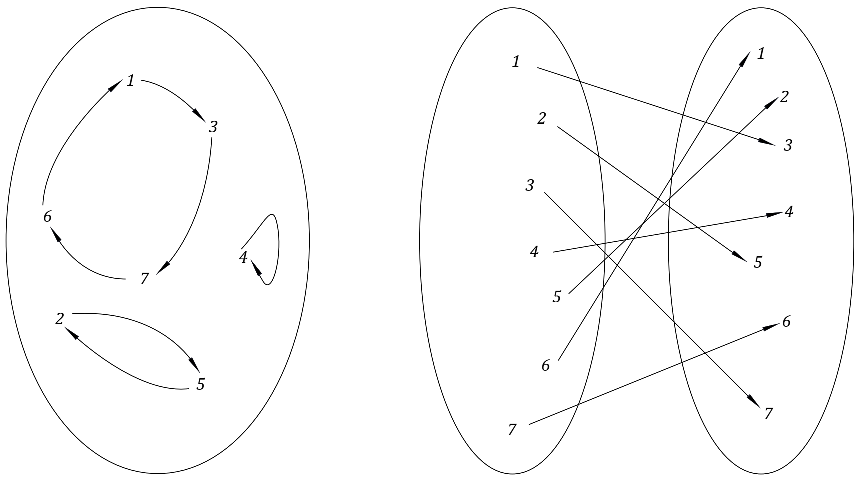
DEFINICJA 2 Permutację zbioru X, która przekształca każdy element $x \in X$ na siebie nazywamy *identycznością* i oznaczamy ε_X lub krótko ε.

Zauważmy, że ε jest elementem neutralnym składania permutacji, tzn.

$$\bigwedge_{\sigma \in S_X} \varepsilon\sigma = \sigma\varepsilon = \sigma.$$

LEMAT 2

$$\bigwedge_{\sigma \in S_X} \bigvee_{\tau \in S_X} \sigma\tau = \tau\sigma = \varepsilon$$



Rysunek 1: Oba diagramy przedstawiają permutację 3574216.

Lemat głosi, że każda permutacja ma odwrotną. Odwrotną do permutacji σ oznaczamy σ^{-1}. Np. jeśli $\sigma = 13524$, to $\sigma^{-1} = 14253$.

Definicja 3 Niepusty zbiór G z działaniem $\cdot$ nazywamy *grupą*, jeśli działanie to jest łączne, ma element neutralny i każdy element $g \in G$ ma element odwrotny. Jeśli działanie jest przemienne, to o G mówimy, że jest *grupą przemienną* bądź *abelową*.

Działanie w grupie nazywamy *składaniem* bądź *mnożeniem*. Jego symbol najczęściej opuszczamy. W przypadku, gdy grupa G jest przemienna, działanie jest często oznaczane znakiem $+$ i nazywane *dodawaniem*. Wtedy zamiast o elemencie odwrotnym, mówimy o elemencie przeciwnym. Element przeciwny do $g \in G$ oznaczamy $-g$.

Definicja 4 Niech G i H będa grupami. Odwzorowanie $\varphi\colon G \to H$ nazywamy *homomorfizmem (grup)* jeśli

$$\bigwedge_{u,v \in G} \varphi(uv) = \varphi(u)\varphi(v).$$

Jeśli nadto φ jest bijekcją, to nazywamy je *izomorfizmem* grup.

W świetle zebranych faktów, permutacje zbioru X tworza grupę. Teraz podamy inny przydatny

Przykład 1 Niech 2^Y – rodzina wszystkich podzbiorów skończonego zbioru Y. Niech działaniem w 2^Y będzie różnica symetryczna:

$$A \triangle B = (A \cup B) \setminus (A \cap B)$$

Można sprawdzić, że działanie to jest łączne, zbiór pusty $\emptyset$ jest jego elementem neutralnym, zaś elementem przeciwnym do dowolnego elementu jest on sam. Stąd 2^Y z działaniem $\triangle$ jest grupą. Jest to oczywiście grupa przemienna. Określmy, teraz funkcję *znaku.* Niech $|C|$ oznacza liczność zbioru $C \in 2^Y$. Wielkość

$$\operatorname{sgn}(C) = (-1)^{|C|}.$$

nazywamy znakiem zbioru C. Jest on równy 1, gdy C jest zbiorem o parzystej liczbie elementów, a -1, gdy liczność C jest nieparzysta. Nietrudno sprawdzić, że dla każdej pary A, $B \in 2^Y$ zachodzi wzór

$$\operatorname{sgn}(A \triangle B) = \operatorname{sgn}(A) \operatorname{sgn}(B). \tag{1}$$

(Funkcja znaku jest więc homomorfizmem grupy 2^Y w grupę $\{-1, 1\}$ ze zwykłym mnożeniem jako działaniem.)

Dla zbioru skończonego X i liczby całkowitej nieujemnej k, przez $\binom{X}{k}$ oznaczamy rodzinę wszystkich k-elementowych podzbiorów zbioru X. Na marginesie, zachodzi

Stwierdzenie 3 *Niech $\sigma \in S_X$. Odwzorowanie $\binom{X}{k} \ni A \mapsto \sigma[A]$ jest permutacją zbioru $\binom{X}{k}$.*

Dowód. (ćwiczenie)

Definicja 5 Niech na skończonym i niepustym zbiorze X będzie określona jakakolwiek relacja S o własności: $(x, y) \in S \Leftrightarrow (y, x) \notin S$. Relację taką nazwiemy *relacją strzałki* albo *orientacją* na X. Dla każdej permutacji $\sigma \in S_X$ określmy podzbiór $\bar{\sigma} \subset \binom{X}{2}$ wzorem

$$\{x, y\} \in \bar{\sigma} \Longleftrightarrow ((x, y) \in S \Leftrightarrow (\sigma(x), \sigma(y)) \notin S).$$

Znak permutacji σ określamy wzorem

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\bar{\sigma}) = (-1)^{|\bar{\sigma}|}.$$

Definicja 6 Permutację $\sigma \in S_X$ nazywamy *cyklem* długości $k \geqslant 1$, jeśli istnieje ciąg $x_1, x_2, \ldots, x_k$ różnych elementów zbioru X o tej własności, że $\sigma(x_1) = x_2, \ldots, \sigma(x_{k-1} = x_k$, $\sigma(x_k) = x_1$ i ponadto jeśli dla każdego $x \in X$

nie będącego elementem ciągu $\sigma(x) = x$. Permutacja σ bywa zapisywana tak

$$\sigma = (x_1 x_2 \dots x_k).$$

Niekiedy, by uniknąć dwuznaczności, między wyrazami wstawia się przecinki. Cykle długości dwa nazywamy *przestawieniami* albo *transpozycjami*

Przykład 2 Niech $\sigma = \begin{pmatrix} \# & \& & * & @ & \heartsuit & \spadesuit & \diamondsuit \\ \heartsuit & @ & \# & * & \diamondsuit & \spadesuit & \& \end{pmatrix}$. Permutacja σ jest cyklem. Mianowicie, $\sigma = (\#\heartsuit\diamondsuit\&@*)$. Zauważmy, że

$$\sigma = (\heartsuit\diamondsuit\&@*\#) = (\diamondsuit\&@*\#\heartsuit) = \dots,$$

to znaczy, tak zwana cykliczna zamiana wyrazów w cyklu nie zmienia permutacji. Jeśli chcemy, by wszystkie elementy zbioru X były reprezentowane w zapisie permutacji, to σ możemy przedstawić tak

$$\sigma = (\#\heartsuit\diamondsuit\&@*)(\spadesuit) = (\spadesuit)(\#\heartsuit\diamondsuit\&@*).$$

Niech teraz $\tau = \begin{pmatrix} \# & \& & \spadesuit & @ & \heartsuit & * & \diamondsuit \\ \spadesuit & \heartsuit & \# & * & \diamondsuit & \& & @ \end{pmatrix}$. Permutacja τ cyklem nie jest. Można ją jednak zapisać jako złożenie dwu cykli rozłącznych, to znaczy takich, że nie mają one wspólnych elementów:

$$\tau = (\spadesuit\#)(\&\heartsuit\diamondsuit@*).$$

Zadajmy teraz na $X = \{\#, \&, \spadesuit, @, \heartsuit, *, \diamondsuit\}$ orientację S w taki sposób, że $(x, y) \in S$ wtedy i tylko wtedy, gdy x poprzedza y w opisie zbioru X; np. $(\#, @) \in S$, ale $(*, \&) \notin S$. Zauważmy, że

$$\bar{\tau} = \{\{\#, \spadesuit\}, \{\#, *\}, \{\&, \spadesuit\}, \{\&, *\}, \{\&, \diamondsuit\}, \{@, *\}, \{@, \diamondsuit\}, \{\heartsuit, *\}, \{\heartsuit, \diamondsuit\}\}$$

Zbiór ten ma nieparzystą liczbę elementów, więc w zgodzie z definicją $\mathrm{sgn}(\tau) = -1$. Oblicz samodzielnie $\mathrm{sgn}(\sigma)$.

Zauważmy, że w przypadku identyczności $\bar{\varepsilon} = \emptyset$. W takim razie $\mathrm{sgn}(\varepsilon) = 1$.

Zadanie 2. Niech S będzie dowolną orientacją na X zaś $\sigma \in S_X$ niech będzie przestawieniem. Wykazać, że

$$\mathrm{sgn}(\sigma) = -1.$$

(Wskazówka: Jeśli $\sigma = (xy)$ i $z \in X \setminus \{x, y\}$, to albo oba zbiory $\{z, x\}, \{z, y\}$ należą do $\bar{\sigma}$ albo żaden.)

Lemat 4 *Dla każdej pary permutacji $\sigma, \tau \in S_X$,*

$$\overline{\tau\sigma} = \bar{\sigma} \triangle \sigma^{-1}(\bar{\tau}),$$

gdzie $\sigma^{-1}(\bar{\tau}) = \{\{\sigma^{-1}(u), \sigma^{-1}(v)\} \colon \{v, u\} \in \bar{\tau}\}$.

Dowód. Nietrudno zauważyć, że $\{u, v\} \in \overline{\tau\sigma}$ wtedy i tylko wtedy, gdy albo $\{u, v\} \in \bar{\sigma}$ i $\{\sigma(u), \sigma(v)\} \notin \bar{\tau}$, albo $\{u, v\} \notin \bar{\sigma}$ i $\{\sigma(u), \sigma(v)\} \in \bar{\tau}$. Innymi słowy, $\{u, v\} \in \overline{\tau\sigma}$ wtedy i tylko wtedy, gdy $\{u, v\}$ leży w jednym z dwu zbiorów $\bar{\sigma}$ albo $\sigma^{-1}(\bar{\tau})$. Ostatnia część równoważności oznacza, że $\{u, v\}$ leży w $\bar{\sigma} \triangle \sigma^{-1}(\bar{\tau})$. □

Twierdzenie 5 *Niech X będzie niepustym zbiorem skończonym oraz niech τ i σ będą elementami S_X. Wówczas*

$$\operatorname{sgn}(\tau\sigma) = \operatorname{sgn}(\tau) \operatorname{sgn}(\sigma).$$

Dowód. Zauważmy najpierw, że zbiory $\sigma^{-1}(\bar{\tau})$ oraz $\bar{\tau}$ mają tyle samo elementów. W takim razie $\operatorname{sgn}(\bar{\tau}) = \operatorname{sgn}(\sigma^{-1}(\bar{\tau}))$. Zgodnie z definicją znaku permutacji, wzorem (1) oraz poprzedzajacym lematem mamy

$$\operatorname{sgn}(\tau\sigma) = \operatorname{sgn}(\overline{\tau\sigma}) = \operatorname{sgn}(\bar{\sigma} \triangle \sigma^{-1}(\bar{\tau})) = \operatorname{sgn}(\bar{\sigma}) \operatorname{sgn}(\bar{\tau}) = \operatorname{sgn}(\tau) \operatorname{sgn}(\sigma).$$

□

Definicja 7 *Nośnikiem* permutacji $\sigma \in S_X$ nazywamy zbiór

$$\operatorname{supp}(\sigma) = \{x \in X \colon \sigma(x) \neq x\}.$$

Zauważmy, że jeśli σ jest cyklem długości $k > 1$, to znaczy, $\sigma = (x_1 x_2 \dots x_k)$, to jego nośnikiem jest $\{x_1, x_2, \dots, x_k\}$.

Lemat 6 *Jeśli permutacje σ, τ mają rozłączne nośniki, to są przemienne.*

Dowód. Niech $x \in \operatorname{supp}(\sigma)$. Wtedy także $\sigma(x) \in \operatorname{supp}(\sigma)$. Wobec tego elementy te nie należą $\operatorname{supp}(\tau)$ i mamy

$$\tau(\sigma(x)) = \sigma(x) = \sigma(\tau(x)).$$

Ta sama równość musi zachodzić także w przypadku, gdy $x \in \operatorname{supp}(\tau)$. Jeśli zaś x nie leży w żadnym z nośników, to

$$\tau(\sigma(x)) = x = \sigma(\tau(x)).$$

W rezultacie permutacje $\tau\sigma$ i $\sigma\tau$ przyjmują te same wartości, więc są równe. □

Twierdzenie 7 *Każda permutacja $\sigma \in S_X$ daje się przedstawić jako złożenie skończonej liczby cykli rozłącznych (inaczej, cykli o rozłącznych nośnikach).*

Dowód. Wybierzmy dowolny element $x \in X$. Przyjmijmy $x_1 = x$. Wtedy albo $\sigma(x_1) = x_1$, albo istnieje $k > 1$, że można utworzyć ciąg $x_1 = x, x_2 = \sigma(x_1), \ldots, x_k = \sigma(x_{k-1})$, złożony z różnych elementów, że $\sigma(x_k) = x_1$. Niech w pierwszym przypadku $\sigma_1 = (x_1)$, zaś w drugim $\sigma_1 = (x_1 \ldots x_k)$. Niech $C_1 = \{x_1, \ldots, x_k\}$ i $X_1 = X \setminus C_1$. Wybierzmy nowy $x \in X_1$ i określmy w taki sam sposób cykl σ_2 oraz zbiory C_2 i X_2. I tak dalej. Ponieważ X jest skończony, więc po skończonej liczbie kroków, powiedzmy m otrzymamy $X_m = \emptyset$. Wtedy, jak nietrudno zauważyć, będziemy mieli:

$$\sigma = \sigma_m \cdots \sigma_2 \sigma_1.$$

Wszystkie cykle są oczywiście rozłączne. □

Uwaga 1 W świetle lematu 6, w przedstawieniu permutacji w postaci złożenia rozłącznych cykli można cykle te napisać w dowolnej kolejności. Można wykazać, że przedstawienie permutacji w postaci cykli rozłącznych jest jedyne właśnie z dokładnością do kolejności cykli. Trzeba się jeszcze umówić, czy wypisuje się wszystkie cykle długości 1, czy też wszystkie się opuszcza. Stwierdzenie to nie jest dziwne jeśli spojrzeć na nie z perspektywy diagramów (rysunek 2).

Niech $\sigma = (x_1 x_2 \ldots x_k)$ – cykl długości $k > 1$. Cykl taki możemy przedstawić w postaci iloczynu transpozycji:

$$\sigma = (x_k x_1)(x_1 \ldots x_{k-1}) = \ldots = (x_k x_1)(x_{k-1} x_1) \cdots (x_2 x_1). \tag{2}$$

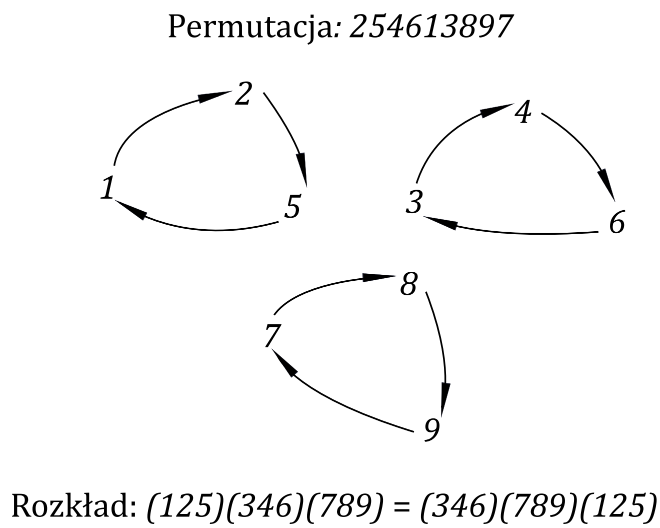
Na podstawie twierdzenia 5 i zadania 2 otrzymamy

$$\operatorname{sgn}(\sigma) = (-1)^{k-1}.$$

Stąd otrzymamy dwa interesujące wnioski.

Wniosek 8 *Jeśli permutacja σ jest złożeniem cykli $\sigma_1, \sigma_2, \ldots, \sigma_m$ o długościach $k_1, k_2, \ldots, k_m$, to*

$$\operatorname{sgn}(\sigma) = (-1)^{k_1 + k_2 + \cdots + k_m - m}.$$



Rysunek 2: Diagram permutacji i jej rozkład na cykle rozłączne.

Zauważmy, że skoro każdy cykl można przedstawić jako złożenie transpozycji oraz każda permutacja jest złożeniem pewnych cykli (nawet rozłącznych !), to każda permutacja daje się przedstawić, zresztą na wiele sposobów, jako złożenie transpozycji. Jeśli więc w poprzedzającym wniosku $\sigma_1, \ldots, \sigma_m$ to transpozycje, to otrzymamy

$$\mathrm{sgn}(\sigma) = (-1)^m.$$

Mamy więc

WNIOSEK 9 *Parzystość liczby transpozycji w przedstawieniu danej permutacji w postaci iloczynu transpozycji zależy jedynie od tej permutacji, a nie od konkretnego przedstawienia.*

UWAGA 2 Przy okazji, okazało się, że znak permutacji nie zależy także od wyboru konkretnej orientacji na X. Jest taki sam dla każdej orientacji!

DEFINICJA 8 Zbiór $A_n = \{\sigma \in S_n \colon \mathrm{sgn}(\sigma) = 1\}$ jest grupą ze składaniem permutacji. Nazywamy ją *podgrupą alternującą* grupy S_n.

Zauważmy, że permutacje należące do A_n można scharakteryzować jako te, które przedstawiają się w postaci iloczynu parzystej liczby transpozycji.