

Podstawowe pojęcia i grupy permutacji

Antoni Kościelski

1 Podstawowe pojęcia

1.1 Algebry i działania

Najkrócej mówiąc, algebra to zbiór z działaniami w tym zbiorze.

Każde działanie ma określoną liczbę argumentów. Dla liczby naturalnej n przyjmujemy, że n -argumentowe działanie w zbiorze A to funkcja przekształcająca A^n w A .

0-argumentowe działanie w zbiorze A to funkcja nie wymagająca podawania argumentów. Takie działanie w zbiorze A utożsamiamy z elementem A będącym przyjmowaną przez to działanie wartością. Zamiast o działaniach 0-argumentowych częściej mówi się o stałych lub wyróżnionych elementach.

Przykładem algebry jest zbiór liczb rzeczywistych z dodawaniem, mnożeniem, zerem, jedynką i ewentualnie liczbą π , jeżeli jest nam do czegoś potrzebna. Inny przykład to zbiór $\mathcal{P}(A)$ wszystkich podzbiorów A z przekrojem (iloczynem zbiorów), różnicą symetryczną i zbiorem pustym.

Bardziej formalnie algebrę definiujemy jako układ (n -ka, n -krotka) postaci

$$\mathcal{A} = \langle A, f_1, f_2, \dots, c_1, c_2, \dots \rangle.$$

Wtedy zbiór A nazywamy nośnikiem lub uniwersum algebry $\mathcal{A}$, symbole $f_1, f_2, \dots$ oznaczają działania w zbiorze A (mające dodatnią liczbę argumentów), a symbole $c_1, c_2, \dots$ – stałe, czyli wyróżnione elementy zbioru A . Działania i stałe można wymieniać w dowolnej kolejności.

Najczęściej będziemy utożsamiać zbiór A z algebrą $\mathcal{A}$. W takim przypadku trzeba będzie domyślać się, z jakie są działania w algebrze A . Na przykład, będziemy mówić o algebrze liczb rzeczywistych rozumiejąc przez to algebrę złożoną ze zbioru liczb rzeczywistych i zwykłych działań: dodawania, mnożenia, operacji zmiany znaku, oraz z dwóch stałych: 0 i 1.

Działania, które wyżej zostały zdefiniowane nazywamy wewnętrznymi. Będziemy rozważać także działania zewnętrzne. Działaniem zewnętrznym w zbiorze A będziemy nazywać funkcję przekształcającą $X \times A$ w A , gdzie X jest pewnym, ustalonym zbiorem.

Przykładem działania zewnętrznego może być podnoszenie do całkowitej potęgi w zbiorze liczb wymiernych (jest to działanie przekształcające zbiór $Z \times Q$ w Q) oraz mnożenie wektora przez skalar przekształcające zbiór $\mathcal{R} \times \mathcal{R}^2$ w zbiór $\mathcal{R}^2$ wektorów o dwóch współrzędnych.

1.2 Rodzaje działań

Działania wyjątkowo będą miały więcej niż dwa argumenty. Działania dwuargumentowe często będą łączne. Działanie $\cdot$ w zbiorze A jest łączne, jeżeli równość

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

zachodzi dla wszystkich $x, y, z \in A$. Dla działań łącznych wyrażenia postaci $x_1 \cdot x_2 \cdot \dots \cdot x_n$ przyjmują tę samą wartość bez względu na rozstawienie nawiasów i dlatego zwykle są zapisywane jak wyżej, bez podawania nawiasów.

Działanie $\cdot$ w zbiorze A jest przemienne, jeżeli dla wszystkich $x, y \in A$ zachodzi równość

$$x \cdot y = y \cdot x.$$

Większość działań w matematyce szkolnej jest przemienne. Teraz będziemy często stykać się także z działaniami nieprzemiennymi.

Przykładem działania nieprzemienne jest składanie funkcji. Przypuśćmy, że mamy zbiór A i a, b, c – trzy różne elementy zbioru A . Weźmy funkcje $f : A \rightarrow A$ i $g : A \rightarrow A$ takie, że $f(a) = b$ i $f(b) = a$ oraz $g(a) = b$ i $g(b) = c$. Dla takich funkcji zachodzą równości

$$f(g(a)) = a \text{ oraz } g(f(a)) = c,$$

a więc złożenia $f \circ g$ i $g \circ f$ są różne.

Jeżeli mamy dwa dwuargumentowe działania $+$ i $\cdot$, oba w zbiorze A , to o działaniu $\cdot$ mówimy, że jest rozdzielne względem działania $+$, jeżeli dla wszystkich $x, y, z \in A$ zachodzą równości

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z) \text{ oraz } (y + z) \cdot x = (y \cdot x) + (z \cdot x).$$

1.3 Elementy neutralne i odwrotne

Przypuśćmy, że mamy algebrę A z działaniem $\cdot$. Element $e \in A$ nazywamy lewostronnym elementem neutralnym, jeżeli dla wszystkich $x \in A$ zachodzą równości

$$e \cdot x = x.$$

Element $e \in A$ nazywamy prawostronnym elementem neutralnym, jeżeli dla wszystkich $x \in A$ zachodzą równości

$$x \cdot e = x.$$

Element $e \in A$ będący jednocześnie lewo- i prawostronnym elementem neutralnym (a więc spełniający wszystkie wyżej wskazane równości) nazywamy elementem neutralnym.

Na oznaczenie działań najczęściej używamy dwóch symboli: $\cdot$ oraz $+$. Dla algebr z jednym działaniem mamy więc do wyboru dwa symbole oznaczające działanie. Zależnie od wyboru symbolu mówimy o tzw. zapisie multiplikatywnym lub addytywnym. Jeżeli stosujemy zapis multiplikatywny, to element neutralny nazywamy jednością lub jedyneką i oznaczamy symbolem 1. W przypadku zapisu addytywnego element neutralny nazywamy zerem i oznaczamy symbolem 0. Oczywiście, liczby naturalne 1 i 0 są odpowiednio elementami neutralnymi dla mnożenia i dodawania w algebrze liczb rzeczywistych.

Dla przykładu weźmy algebrę wszystkich funkcji A^A przekształcających A w A ze złożeniem. Działanie w tej algebrze (złożenie) jest łączne, funkcja identycznościowa jest elementem neutralnym.

Algebrą jest też zbiór $\{f \in N^N : 0 \notin f(N)\}$ wszystkich funkcji przekształcających N w N , które nie przyjmują wartości 0, ze złożeniem. W tej algebrze nie ma elementu neutralnego. Gdyby e było elementem neutralnym i $e(0) = a \neq 0$, to z jednej strony $(f \circ e)(0) = f(e(0)) = f(a)$, z drugiej strony $f \circ e = f$ i stąd $(f \circ e)(0) = f(0)$. Oczywiście, te równości nie mogą zachodzić dla dowolnych funkcji f z naszej algebry. Można sprawdzić, że każda funkcja e' taka, że $e'(n) = n$ dla $n \neq 0$ jest lewostronnym elementem neutralnym w rozważanej algebrze.

Lemat 1.1 *Jeżeli w algebrze jest lewostronny element neutralny e_L i jest prawostronny element neutralny e_R , to $e_L = e_R$. Wtedy każdy lewostronny i prawostronny element neutralny jest elementem neutralnym. W dowolnej algebrze istnieje najwyżej jeden element neutralny.*

Dowód. Oczywiście, zachodzą następujące równości:

$$e_R = e_L \cdot e_R = e_L. \quad \square$$

Dalej zakładamy, że w algebrze A mamy element neutralny e oraz $x \in A$. Element $y \in A$ nazywamy lewostronnym elementem odwrotnym do x , jeżeli

$$y \cdot x = e.$$

Element $y \in A$ nazywamy prawostronnym elementem odwrotnym do x , jeżeli

$$x \cdot y = e.$$

Element $y \in A$ nazywamy elementem odwrotnym do x , jeżeli jest jednocześnie elementem lewo- i prawostronnie odwrotnym do x .

Jeżeli stosujemy zapis addytywny, to elementy odwrotne nazywamy przeciwnymi.

Lemat 1.2 *Załóżmy, że rozważamy algebrę z łącznym działaniem i elementem neutralnym e . Niech x będzie ustalonym elementem tej algebry. Jeżeli w tej algebrze dla elementu x jest lewostronny element odwrotny y_L i jest prawostronny element odwrotny y_R , to $y_L = y_R$. Wtedy każdy lewostronny i każdy prawostronny element odwrotny do x jest elementem odwrotnym x . W takiej algebrze dla dowolnego x istnieje najwyżej jeden element odwrotny.*

Dowód. Zauważmy, że

$$y_L = y_L e = y_L (x y_R) = (y_L x) y_R = e y_R = y_R. \quad \square$$

2 Definicja i podstawowe własności grup

2.1 Definicje

Grupa to algebra z łącznym działaniem (mnożeniem) z elementem neutralnym i odwracaniem. Ma więc trzy działania oznaczane najczęściej $\cdot$, 1 i $^{-1}$. W grupie działania te spełniają równości

$$(x \cdot y) \cdot z = x \cdot (y \cdot z),$$

$$x \cdot 1 = x = 1 \cdot x,$$

$$x \cdot x^{-1} = x^{-1} \cdot x = 1.$$

dla wszystkich x, y, z należących do nośnika grupy.

Grupa może też zostać zdefiniowana jako algebra G z łącznym mnożeniem takim, że

$$\exists e \in G \forall x \in G ((a \cdot e = e \cdot x = x) \wedge (\exists y \in G (x \cdot y = y \cdot x = e))).$$

Obie definicje grupy są w zasadzie równoważne. Jeżeli algebra G jest grupą w sensie drugiej definicji, to można ją jednoznacznie rozszerzyć o element neutralny i operację odwracania.

Grupami są liczby całkowite z dodawaniem oraz liczby wymierne bez zera z mnożeniem. Grupą jest także zbiór podzbiorów $\mathcal{P}(X)$ zbioru X z różnicą symetryczną. Ważnym przykładem grupy jest zbiór $S_X = \{f \in X^X : f \text{ jest bijekcją}\}$ bijekcji przekształcających X na X ze złożeniem. Takie bijekcje nazywamy też permutacjami zbioru X , a S_X – grupą permutacji. Przyjmujemy też oznaczenie $S_n = S_{\{1, \dots, n\}}$.

Permutacje należące do S_n możemy definiować podając tabelkę funkcji. Zwykle tabelka ma postać

$$\begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}.$$

Taka tabelka oznacza funkcję $f : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ zdefiniowaną wzorami $f(i) = a_i$ dla wszystkich $i = 1, \dots, n$.

Grupy możemy też definiować podając tabelki mnożenia takie, jak np.

$\cdot$	a	b
a	a	b
b	b	a

oraz

$\cdot$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Podane tabelki definiują działania grupowe, ale przekonanie się o tym może sprawić trochę kłopotów.

2.2 Potęgowanie

W grupach możemy zdefiniować potęgowanie przyjmując, że dla dowolnej liczby naturalnej zachodzą równości

$$g^0 = 1, \quad g^{n+1} = g^n \cdot g \quad \text{oraz} \quad g^{-n} = (g^{-1})^n.$$

Jeżeli stosujemy zapis addytywny, to podane równości przyjmą postać

$$0 \cdot g = 0, \quad (n+1) \cdot g = n \cdot g + g \quad \text{oraz} \quad (-n) \cdot g = n \cdot (-g).$$

Potęgowanie w grupie ma następujące własności słuszne dla wszystkich liczb całkowitych n i m oraz dowolnych elementów grupy g i h :

1. $1^{-1} = 1$
2. $(g^{-1})^{-1} = g$
3. $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$
4. $(g^n)^m = g^{nm}$
5. $g^n \cdot g^m = g^{n+m}$

Znany ze szkoły wzór $(g \cdot h)^n = g^n \cdot h^n$ jest na ogół fałszywy. W szczególności, nie można w tym wzorze podstawić $n = -1$. Jest natomiast prawdziwy podany wyżej wzór na odwrotność iloczynu.

2.3 Rząd grupy i rząd elementu grupy

Jeżeli grupa jest skończona i ma n elementów, to mówimy o niej, że jest rzędu n . O grupach nieskończonych mówimy też, że mają rząd nieskończony. Oczywiście, rzędem grupy S_n jest $n!$.

Dla niektórych elementów g grupy G istnieje dodatnia liczba naturalna n taka, że $g^n = 1$. Wtedy najmniejszą liczbę spośród liczb n o podanych własnościach nazywamy rzędem elementu g . O pozostałych elementach mówimy, że nie mają określonego rzędu. W grupach skończonych każdy element ma określony rząd.

2.4 Prawo skracania

Lemat 2.1 (lewostronne prawo skracania) *Jeżeli w grupie zachodzi równość $g \cdot h_1 = g \cdot h_2$, to $h_1 = h_2$.*

Dowód. Aby dowieść lemat wystarczy podaną równość pomnożyć przez z lewej strony przez element odwrotny do g i skorzystać z prawa łączności. $\square$

W dowolnej grupie jest prawdziwe także prawostronne prawo skracania.

Prawa skracania zachodzą także w algebrach, które nie są grupami. Na przykład, dodatnie liczby naturalne z mnożeniem tworzą półgrupę z jednością, która nie jest grupą, ale zachodzą w niej oba prawa skracania.

Zdefiniujmy funkcje $f_g : G \rightarrow G$ takie, że

$$f_g(h) = g \cdot h.$$

Prawo skracania implikuje, że są to funkcje różnowartościowe. Są to także funkcje typu „na”. Nietrudno zauważyć, że funkcja f_g przyjmuje wartość h dla argumentu $x = g^{-1} \cdot h$. Tak więc funkcje f_g są permutacjami zbioru G , czyli $f_g \in S_G$.

2.5 Homomorfizmy grup

Zdefiniujemy jeszcze funkcję

$$\varphi : G \rightarrow G^G \text{ taką, że } \varphi(g) = f_g.$$

Funkcja ta ma dwie własności: spełnia równość

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \circ \varphi(g_2), \quad (1)$$

oraz jest różnowartościowa, a więc spełnia warunek jeżeli $g_1 \neq g_2$, to $\varphi(g_1) \neq \varphi(g_2)$.

Funkcję φ przekształcającą grupę G w inną algebrę (w tym przypadku G^G lub S_G ze złożeniem $\circ$) mającą własność (1) nazywamy homomorfizmem grupy G . Jeżeli dodatkowo jest ona różnowartościowa, to nazywamy ją monomorfizmem, a jeżeli jest bijekcją, to – izomorfizmem. Homomorfizm typu „na” nazywamy epimorfizmem.

Lemat 2.2 *Niech $\varphi(G)$ oznacza zbiór wartości przyjmowanych przez funkcję φ na zbiorze G . Jeżeli G jest grupą i φ jest homomorfizmem grupy G , to*

1. $\varphi(G)$ z działaniem $\circ$ jest algebrą,
2. $\varphi(1)$ jest elementem neutralnym w algebrze $\varphi(G)$ z działaniem $\circ$,
3. elementem odwrotnym do $\varphi(g)$ jest $\varphi(g^{-1})$,

4. $\varphi(G)$ z działaniem $\circ$ jest grupą (nawet, gdy $\circ$ jest jakimkolwiek działaniem binarnym). $\square$

Algebrę $\varphi(G)$ z działaniem $\circ$ nazywamy obrazem homomorficznym G (wyznaczonym przez homomorfizm φ).

Wniosek 2.3 *Obraz homomorficzny grupy jest grupą. Homomorfizm grupy przekształca element neutralny na element neutralny, a element odwrotny – na odwrotny.*

2.6 Badanie tabelek

Przypuśćmy, że mamy tabelkę

$\cdot$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

pewnego dwurgumentowego działania $\cdot$. Analizując ją łatwo sprawdzić, czy dla działania $\cdot$ istnieje element neutralny, czy są elementy odwrotne, czy działanie jest przemienne. Dość trudno sprawdzić, czy to działanie jest łączne.

Zauważmy, że jeżeli mamy tabelkę działania $\cdot$, to znamy funkcje f_g i φ zdefiniowane w rozdziałach 2.4 i 2.5. Wiemy z tych rozdziałów, że jeżeli tabelka przedstawia działanie grupowe, to φ jest izomorfizmem. Stąd wynika, że w poszczególnych wierszach tabelki znajdują się przepermutowane elementy grupy, a także każde dwa wiersze (z wyjątkiem wiersza z nagłówka) są różne. Analogiczne warunki spełniają kolumny tabelki.

Dla algebr skończonych prawdziwe jest także twierdzenie odwrotne.

Twierdzenie 2.4 *Jeżeli G jest skończoną algebrą z działaniem $\cdot$ i φ jest monomorfizmem, to G jest grupą.* $\square$

Twierdzenie to pozwala opracować algorytm sprawdzający łączność działania, mniej żmudny od naturalnego.

2.7 Podgrupy

Przypuśćmy, że G jest grupą z mnożeniem $\cdot$, elementem neutralnym 1 i odwracaniem $^{-1}$, a H jest podzbiorem G . Zbiór H może być zamknięty ze względu na działania w grupie G . Dokładniej, może spełniać następujące warunki:

1. $1 \in H$,
2. jeżeli $g, h \in H$, to także $g \cdot h \in H$
3. oraz jeżeli $g \in H$, to także $g^{-1} \in H$.

Jeżeli te warunki są spełnione, to H z działaniami z grupy G (a właściwie z ich obcięciami) jest pewną algebrą. Tę algebrę nazywamy podgrupą grupy G .

Nietrudno zauważyć, że zdefiniowany wyżej obraz homomorficzny $\varphi(G)$ jest podgrupą grupy S_G . Podgrupy mają następujące, oczywiste własności:

Lemat 2.5 *Podgrupa jest grupą.* $\square$

Lemat 2.6 *Dowolny przekrój podgrup grupy G jest podgrupą grupy G .* $\square$

Z przeprowadzonych już rozumowań wynika

Twierdzenie 2.7 (tw. Cayley) *Każda grupa G jest izomorficzna z podgrupą grupy S_G .* $\square$

Prawdziwe są też lematy:

Lemat 2.8 *Jeżeli zbiory X i Y są równoliczne, to grupy permutacji S_X i S_Y są izomorficzne.* $\square$

oraz

Lemat 2.9 *Jeżeli algebry A i B oraz algebry B i C są izomorficzne, to algebry A i C też są izomorficzne.* $\square$

Z twierdzenia Cayley i podanych lematów wynika

Wniosek 2.10 *Każda grupa rzędu n jest izomorficzna z podgrupą grupy S_n .* $\square$

Wniosek 2.11 *Dla każdej liczby naturalnej n istnieje (z dokładnością do izomorfizmu) skończenie wiele grup n elementowych. Jest więc przeliczalnie wiele grup skończonych.* $\square$

2.8 Generatory i generowanie

Przypuśćmy, że mamy grupę G z działaniem $\cdot$, podgrupę H grupy G i podzbiór X zbioru H . Następujące stwierdzenia są równoważne

1. H jest przekrojem rodziny podgrup grupy G złożonej z podgrup zawierających X ,
2. H jest najmniejszą podgrupą G zawierającą X ,

Jeżeli stwierdzenia te są prawdziwe, to H określamy jako podgrupę grupy G generowaną przez X , a X nazywamy zbiorem generatorów podgrupy H .

Zbiór X generuje grupę G (albo: grupa G jest generowana przez X), jeżeli G jest najmniejszą podgrupą G generowaną przez X . Nietrudno zauważyć, że X generuje G wtedy i tylko wtedy G jest jedyną podgrupą grupy G zawierającą X .

Czasem będziemy też mówić, że elementy $g_1, g_2, \dots, g_n$ generują grupę G . Zwrot ten i podobne oznaczają, że zbiór $\{g_1, g_2, \dots, g_n\}$ generuje grupę G .

3 Grupy permutacji

3.1 Rozkład na cykle

Niech $f : A \rightarrow A$ będzie bijekcją, a X – podzbiorem A , dowolnym i niepustym, takim, że

$$f(x) = y \Rightarrow (x \in X \iff y \in X). \quad (2)$$

Zauważmy, że wtedy

1. $f : X \rightarrow X$ (dokładniej: obcięcie f do zbioru X , a nie samo f),
2. f jest permutacją zbioru X ,
3. $f : A \setminus X \rightarrow A \setminus X$ oraz jest permutacją zbioru $A \setminus X$.

Mając zbiór X o własności (2) możemy zdefiniować dwie funkcje f_0 i f_1 takie, że

$$f_0(x) = \begin{cases} f(x) & \text{jeżeli } x \in X, \\ x & \text{jeżeli } x \notin X, \end{cases} \quad \text{oraz} \quad f_1(x) = \begin{cases} f(x) & \text{jeżeli } x \notin X, \\ x & \text{jeżeli } x \in X. \end{cases}$$

Lemat 3.1 Dla dowolnej permutacji f zbioru A zdefiniowane wyżej funkcje f_0 i f_1 są permutacjami zbioru A oraz spełniają równości $f = f_0 f_1 = f_1 f_0$. $\square$

Przedstawione fakty pozwalają rozłożyć dowolną permutację na iloczyn tzw. permutacji cyklicznych, choć w przypadku zbiorów nieskończonych pojawiają się kłopoty formalne. Najpierw nauczymy znajdować zbiory X o własności (2).

Takim jest dla dowolnego $x \in A$ zbiór

$$X = \{f^n(x) : n \in \mathbb{Z}\}. \quad (3)$$

Co więcej, tak definiujemy minimalne zbiory o własności (2), które nie dają się rozłożyć na mniejsze zbiory o tej własności. Te zbiory mogą być skończone, w tym jednoelementowe, lub nieskończone.

Lemat 3.2 Zbiór X zdefiniowany wzorem (3) jest nieskończony wtedy i tylko wtedy, gdy funkcja przyporządkowująca liczbie całkowitej n wartość $f^n(x)$ jest różnowartościowa. $\square$

Permutacje f_0 dla zbiorów X zdefiniowanych wzorem (3) nazywamy cyklicznymi.

Permutacje cykliczne dla nieskończonych X możemy definiować wskazując ciąg elementów zbioru A indeksowany liczbami całkowitymi, np. przedstawiamy je jako

$$(\dots, a_{-2}, a_{-1}, a_0, a_1, a_2, \dots).$$

Zapis $(\dots, a_{-2}, a_{-1}, a_0, a_1, a_2, \dots)$ oznacza funkcję $g : A \rightarrow A$ taką, że

$$g(a_i) = a_{i+1} \quad \text{dla } i \in \mathbb{Z} \quad \text{oraz} \quad g(x) = x \quad \text{dla } x \in A \setminus \{a_k : k \in \mathbb{Z}\}.$$

W szczególności, dla nieskończonego zbioru X definiowanego wzorem (3) funkcję f_0 można zdefiniować jako

$$(\dots, f^{-2}(x), f^{-1}(x), x, f(x), f^2(x), \dots).$$

Przykładem permutacji cyklicznej zbioru nieskończonego może być funkcja $g : \mathbb{R} \rightarrow \mathbb{R}$ taka, że

$$g(x) = \begin{cases} x+1 & \text{jeżeli } x \text{ jest liczbą całkowitą,} \\ x & \text{w przeciwnym razie.} \end{cases}$$

Permutację g możemy zapisać jako $(\dots, -2, -1, 0, 1, 2, \dots)$.

Jeżeli zbiór X definiowany wzorem (3) jest skończony, to jest on równy

$$X = \{x, f(x), f^2(x), \dots, f^{k-1}(x)\}$$

dla pewnej dodatniej liczby naturalnej k . Wtedy dla pewnych liczb $n \in \mathbb{Z}$ i $k \in \mathbb{N}$ zachodzi równość $f^n(x) = f^{n+k}(x)$. Zachodzi także równość $f^k(x) = x$. Stąd łatwo wywnioskować równość $f^n(x) = f^r(x)$, gdzie r jest resztą z dzielenia n przez k .

Dla opisanego funkcji f_0 w takiej sytuacji stosujemy zapis $(a_1, a_2, \dots, a_k)$. Oznacza on funkcję g definiowaną wzorami

$$g(a_i) = a_{i+1} \quad \text{dla } i < k, \quad g(a_k) = a_1 \quad \text{oraz} \quad g(x) = x \quad \text{dla } x \in A \setminus \{a_1, \dots, a_k\}.$$

Samą funkcję f_0 możemy określić jako $(x, f(x), f^2(x), \dots, f^{k-1}(x))$.

Analizując permutacje zbiorów skończonych wystarczy rozważać tylko permutacje cykliczne postaci $(a_1, a_2, \dots, a_k)$.

Dowolną permutację możemy przedstawić w postaci złożenia permutacji cyklicznych stosując następującą procedurę.

1. Sprawdzamy, czy istnieje $x \in A$ taki, że $f(x) \neq x$. Jeżeli nie istnieje, to permutacja f jest funkcją identycznościową (jest więc złożeniem zera permutacji cyklicznych).
2. Jeżeli mamy $x \in A$ taki, że $f(x) \neq x$, to znajdujemy zbiór $X = \{f^n(x) : n \in \mathbb{Z}\}$. Jeżeli A jest skończony, to możemy to zrobić obliczając kolejne wartości $x, f(x), f^2(x), \dots$ tak długo, aż obliczymy $f^k(x)$, które okaże się równe x .
3. Przedstawiamy f w postaci $f_0 f_1$. Permutacja f_0 jest cykliczna.
4. Następnie, rekurencyjnie znajdujemy rozkład permutacji f_1 .

Permutacje $\sigma, \tau \in S_X$ są rozłączne, jeżeli nie istnieje taki element $x \in X$, że $\sigma(x) \neq x$ i jednocześnie $\tau(x) \neq x$. Nietrudno zauważyć, że jeżeli σ i τ są permutacjami rozłącznymi, to $\sigma \circ \tau = \tau \circ \sigma$.

Twierdzenie 3.3 *Każdą permutację zbioru skończonego można przedstawić w postaci złożenia rozłącznych permutacji cyklicznych.* $\square$

Wniosek 3.4 *Jeżeli A jest zbiorem skończonym, to zbiór permutacji cyklicznych generuje grupę wszystkich permutacji zbioru A .* $\square$

Twierdzenie 3.5 *Przedstawienie permutacji w postaci iloczynu (złożenia) rozłącznych permutacji cyklicznych jest jednoznaczne z dokładnością do kolejności, w jakiej poszczególne czynniki zostały wymienione.* $\square$

Permutacje cykliczne postaci (a_1, a_2) nazywamy transpozycjami. W grupach S_n transpozycje postaci $(i, i+1)$ nazywamy transpozycjami elementów sąsiednich.

Twierdzenie 3.6 *Zbiór transpozycji generuje grupę wszystkich permutacji zbioru skończonego.* $\square$

Powyższe twierdzenie może być wnioskiem z następującego.

Twierdzenie 3.7 *Zbiór transpozycji elementów sąsiednich generuje grupę permutacji S_n .*

Dowód. Każdą permutację należącą do S_n można przedstawić w postaci iloczynu transpozycji elementów sąsiednich. Przedstawienie to można znaleźć śledząc działanie algorytmu sortowania bąbelkowego. Weryfikację szczegółów pozostawiam jako ćwiczenie. $\square$

3.2 Permutacje parzyste i nieparzyste

Permutację zbioru skończonego nazywamy parzystą wtedy i tylko wtedy, gdy jest złożeniem parzystej liczby transpozycji. Permutację zbioru skończonego nazywamy nieparzystą wtedy i tylko wtedy, gdy jest złożeniem nieparzystej liczby transpozycji.

Zauważmy, że permutacja nie jest parzysta, jeżeli żadne jej przedstawienie w postaci iloczynu transpozycji nie zawiera parzystej liczby czynników. Interesuje nas, czy istnieją permutacje, które są jednocześnie parzyste i nieparzyste, albo, czy istnieje permutacja, która nie jest parzysta.

3.3 Znak permutacji

Przyjmijmy, że $\sigma \in S_n$ oraz

$$\operatorname{sgn}(\sigma) = \prod_{i < j} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Liczbę $\operatorname{sgn}(\sigma)$ nazywamy znakiem permutacji σ .

Lemat 3.8 *Funkcja sgn ma następujące własności:*

1. $\operatorname{sgn}(\sigma) \in \{-1, 1\}$ dla dowolnej permutacji σ ,
2. sgn jest homomorfizmem przekształcającym grupę S_n w zbiór liczb wymiernych (lub całkowitych) z mnożeniem, w szczególności dla dowolnych permutacji $\sigma, \tau \in S_n$ zachodzi równość $\operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau)$,
3. $\operatorname{sgn}((a, b)) = -1$.

Dowód. Zauważmy, że jeżeli $\sigma \in S_n$, to

$$\{\{i, j\} : 1 \leq i, j \leq n \wedge i \neq j\} = \{\{\sigma(i), \sigma(j)\} : 1 \leq i, j \leq n \wedge i \neq j\}.$$

Oznaczmy te zbiory przez X i weźmy funkcję f , która parze $\{i, j\}$ liczb przyporządkowuje wartość $f(\{i, j\}) = |i - j|$. Nietrudno sprawdzić, że jest to poprawnie zdefiniowana funkcja i

$$|\operatorname{sgn}(\sigma)| = \frac{\prod_{i < j} |\sigma(j) - \sigma(i)|}{\prod_{i < j} |j - i|}.$$

Z tego wzoru wynika, że $|\operatorname{sgn}(\sigma)| = 1$, gdyż jest to iloraz dwóch iloczynów wartości funkcji f dla argumentów przebiegających ten sam zbiór X . W ten sposób dowiedliśmy część pierwszą lematu.

Aby dowieść część drugą, wystarczy w podobny sposób dowieść, że

$$\prod_{i < j} \frac{\sigma(j) - \sigma(i)}{j - i} = \prod_{i < j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)}$$

dla dowolnych permutacji σ i τ . Dalsze rachunki są oczywiste.

$$\begin{aligned} \operatorname{sgn}(\sigma \circ \tau) &= \prod_{i < j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} = \prod_{i < j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \prod_{i < j} \frac{\tau(j) - \tau(i)}{j - i} = \\ &= \prod_{i < j} \frac{\sigma(j) - \sigma(i)}{j - i} \prod_{i < j} \frac{\tau(j) - \tau(i)}{j - i} = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau). \end{aligned}$$

Część trzecią tezy lematu pozostawiam jako ćwiczenie. $\square$

Wniosek 3.9 *Następujące warunki są równoważne:*

1. σ jest permutacją parzystą,
2. $\operatorname{sgn}(\sigma) = 1$
3. w każdym przedstawieniu σ w postaci iloczynu transpozycji mamy parzystą liczbę czynników. $\square$

Obliczanie znaku permutacji jest bardzo proste. Wymaga np. ustalenia liczby tzw. inwersji. Inwersją permutacji

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

nazywamy parę pozycji w dolnej linijce tabelki σ , w której znajdujące się liczby są podane w innej kolejności, niż w górnej linijce. Na przykład, inwersję tworzą pozycje druga i czwarta. znajdujące się na tych pozycjach liczby 7 i 6 są podane w innej kolejności niż w górnej linijce tabelki. Jeżeli permutacja ma n inwersji, to jej znak jest równy $(-1)^n$. Wynika to z definicji znaku permutacji i przedstawionej analizy wzoru z definicji. Są też inne metody. Na przykład, znak permutacji można ustalić łatwo znajdując przedstawienie permutacji w postaci iloczynu permutacji cyklicznych.