Geometryczna Teoria Grup
- skrypt do warsztatów w ramach WWW11

Niniejszy skrypt omawia najważniejsze pojęcia, których będziemy używać na warsztatach.

1 Grupy

Oznaczmy przez $\mathbb{E}_2$ zbiór izometrii[1] płaszczyzny $\mathbb{R}^2$. Najprostszą jest identyczność $\mathrm{id}(x) = x$. Jeśli $f, g \in \mathbb{E}_2$ izometriami, to są nimi również odwrotność[2] f^{-1} oraz złożenie[3] $f \circ g$. Operacja $\circ$ jest łączna, tj. $f \circ (g \circ h) = (f \circ g) \circ h$, a poza tym dla każdego $f \in \mathbb{E}_2$ zachodzi $f \circ \mathrm{id} = \mathrm{id} \circ f = f$, tzn. id jest elementem neutralnym dla $\circ$. Te własności oznaczają, że $(\mathbb{E}_2, \circ)$ jest przykładem grupy[4].

Definicja 1 (grupy)**.** Parę $(G, \circ)$, w której G jest zbiorem, zaś $\circ : G \times G \to G$ działaniem dwuargumentowym[5] nazwiemy *grupą*, jeśli spełnione są następujące warunki.

1. Dla każdych $a, b, c \in G$ zachodzi $a \circ (b \circ c) = (a \circ b) \circ c$ - działanie jest *łączne* i nie musimy zastanawiać się nad kolejnością działań w dowolnym iloczynie postaci $a_1 \circ a_2 \circ \ldots \circ a_k$.

2. Istnieje $e \in G$ takie, że dla każdego $a \in G$ zachodzi $a \circ e = e \circ a = a$ - działanie ma *element neutralny* e. Wówczas jest on wyznaczony jednoznacznie i z oznaczenia e na element neutralny będziemy jeszcze korzystać.

3. Dla każdego $a \in G$ istnieje $a^{-1} \in G$ takie, że $a \circ a^{-1} = a^{-1} \circ a = e$ - każdy element a ma *element odwrotny* a^{-1}. Tutaj również okazuje się, że może być tylko jedno takie a^{-1} i będziemy używać tego oznaczenia na element odwrotny dla a.

Jeśli w dodatku dla każdy $a, b \in G$ spełniony jest warunek $a \circ b = b \circ a$, to grupę $(G, \circ)$ nazywamy *przemienną*. Często zamiast $a \circ b$ piszemy po prostu ab.

Zamiast $(G, \circ)$ będziemy zwykle pisać G, jeśli wiadomo, o jakie działanie $\circ$ chodzi.
Przykłady:

- Zamiast izometrii $\mathbb{R}^2$ możemy rozważać izometrie $\mathbb{R}^n$ dla dowolnego $n \geqslant 1$ i podobnie jak poprzednio otrzymać grupę $(\mathbb{E}_n, \circ)$, składającą się z izometrii $\mathbb{R}^n$.

- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ są grupami przemiennymi, w których elementem neutralnym jest 0, zaś elementem odwrotnym względem a jest liczba przeciwna, czyli $-a$. W przypadku mnożenia uwzględnić należy fakt, że 0 nie daje się odwrócić[6]: $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ są grupami

[1] czyli wszystkich przekształceń $\phi : \mathbb{R}^2 \to \mathbb{R}^2$, które zachowują odległości między punktami. Tutaj każde z nich to przesunięcie o wektor, obrót względem punktu lub symetria względem prostej złożona z przesunięciem.
[2] którą można scharakteryzować przez $f^{-1} \circ f = f \circ f^{-1} = \mathrm{id}$
[3] $(f \circ g)(x) = f(g(x))$ dla $x \in \mathbb{R}^2$
[4] Widać przy okazji, że nie zakładamy przemienności działania.
[5] tzn. dla każdych $a, b \in G$ dany jest wyznaczony jednoznacznie element $a \circ b \in G$
[6] a liczby całkowite przy odwracaniu mogą nie dawać liczb całkowitych

przemiennymi, w których elementem neutralnym jest 1, zaś odwrotność liczby a to a^{-1}, rozumiane w sensie szkolnym.

- Dla $n \geqslant 1$ oznaczmy przez S_n zbiór wszystkich bijekcji $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$. Wówczas $(S_n, \circ)$ z $\circ$ będącym składaniem funkcji jest grupą.
- Dla $n \geqslant 3$ rozważmy n-kąt foremny na płaszczyźnie. Zbiór izometrii własnych tego wielokąta oznaczamy przez D_{2n} - są to izometrie płaszczyzny, które przekształcają wielokąt na niego samego. Zatem $D_{2n} \subset \mathbb{E}_2$, przy czym jest to zbiór zamknięty na składanie $\circ$ oraz branie odwrotności. $(D_{2n}, \circ)$ jest grupą, a w takiej sytuacji mówimy, że to podgrupa $(\mathbb{E}_2, \circ)$.
- Niech G będzie grafem ze zbiorem wierzchołków V oraz zbiorem krawędzi (zorientowanych, pojedynczych) $E \subset V \times V$. Automorfizmem grafu G nazywamy dowolną bijekcję $f : V \to V$, która dla każdych $a, b \in V$ spełnia warunek $(a, b) \in E \iff (f(a), f(b)) \in E$. Zbiór automorfizmów oznaczmy $\mathrm{Aut}(G)$. Jest to grupa z działaniem składania automorfizmów.
- Dla $n \geqslant 1$ mamy grupę $(\mathbb{Z}_n, +_n)$ reszt modulo n, z dodawaniem modulo n. Możemy określić ją, przyjmując $\mathbb{Z}_n = \{0, 1 \ldots, n-1\}$, $a +_n b = (a + b) \bmod n$ dla $a, b \in \mathbb{Z}_n$. (Zapis $x \bmod n$ oznacza resztę z dzielenia liczby x przez n.)

Definicja 2 (podgrupy)**.** Niech $(G, \circ)$ będzie grupą z elementem neutralnym e. Zbiór $H \subset G$ nazwiemy *podgrupą* G wtedy i tylko wtedy, gdy zawiera e i jest zamnkięty na działanie $\circ$ i branie odwrotności, tzn. spełnione są następujące warunki.

- Dla każdych $a, b \in H$ zachodzi $a \circ b \in H$.
- Dla każdego $a \in H$ jest prawdą, że $a^{-1} \in H$.

Ten fakt będziemy zapisywać symbolicznie jako $H < G$. W takiej sytuacji $(H, \circ)$ jest również grupą (z tym samym działaniem, co G).

Przykłady:

- Widzieliśmy, że D_{2n} jest podgrupą $\mathbb{E}_2$.
- Dla ustalonego $k \in \mathbb{Z}$ możemy rozważyć zbiór liczb podzielnych przez k, tzn. $k\mathbb{Z} = \{ka \mid a \in \mathbb{Z}\}$. Zbiór $k\mathbb{Z}$ jest zamknięty na dodawanie i branie elementu przeciwnego, a także zawiera 0, więc $(k\mathbb{Z}, +)$ jest podgrupą $(\mathbb{Z}, +)$.

Niektóre grupy różnią się od siebie tylko tym, jak akurat w ramach konstrukcji przyjęto nazywać jej elementy. Następujące pojęcie pozwala mówić precyzyjnie, jakie grupy uważamy za takie same, tj. izomorficzne.

Definicja 3 (izomorfizmu grup)**.** Niech $(G, \circ)$, $(H, \star)$ będą grupami. Funkcję $\phi : G \to H$ nazywami *izomorfizmem*, jeśli spełnia następujące warunki.

1. Dla każdych $a, b \in G$ zachodzi $\phi(a \circ b) = \phi(a) \star \phi(b)$.
2. ϕ jest bijekcją.

Jeśli istnieje izomorfizm między $(G, \circ)$ a $(H, \star)$, to mówimy, że te grupy są izomorficzne. Przekształcenie odwrotne do izomorfizmu jest izomorfizmem.

Przekształcenie ϕ spełniające tylko warunek 1. nazywamy *homomorfizem.*

Przykłady:

- W grupie $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ pozdzbiór $H = \{0, 2\}$ jest podgrupą. Przekształcenie $\phi : H \to \mathbb{Z}_2 = \{0, 1\}$, określone jako $\phi(0) = 0$, $\phi(2) = 1$ jest izomorfizmem między $(H, +_4)$ a $(\mathbb{Z}_2, +_2)$.

- Jeśli w grupie $(G, \circ)$ element x spełnia[7] $x^i \neq e$ dla $i = 1, \ldots, n-1$, ale $x^n = e$, to mówimy, że jest rzędu n (tj. rząd x to najmniejsze $k \geqslant 2$, dla którego $x^k = e$). Wówczas zbiór $\langle x \rangle = \{e, x, \ldots, x^{n-1}\}$ jest podgrupą G, zaś przekształcenie $\phi : \mathbb{Z}_n \to \langle x \rangle$ dane jako $\phi(j) = x^j$ jest izmorfizmem z $(\mathbb{Z}_n, +_n)$ do $(\langle x \rangle, \circ)$. Np. liczba $-1 \in \mathbb{R}$ ma w grupie $(\mathbb{R} \setminus \{0\}, \cdot)$ rząd 2, więc podgrupa $\langle -1, 1 \rangle < \mathbb{R} \setminus \{0\}$ jest izomorficzna z $\mathbb{Z}_2$. Inny przykład: niech $\sigma \in \mathbb{E}_2$ będzie obrotem o kąt $\frac{2\pi}{n}$ wokół punktu $(0, 0)$. Wtedy σ jest rzędu n, a zatem grupa $\langle \sigma \rangle$ jest izomorficzna z $\mathbb{Z}_n$.

- Jeśli w grupie $(G, \circ)$ element x spełnia $x^n \neq e$ dla każdego $n \geqslant 1$, to wówczas określamy $\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$ i jest to podgrupa G. Przekształcenie $\phi : \mathbb{Z} \to \langle x \rangle$ dane jako $\phi(k) = x^k$ jest izomorfizmem. Przykładem takiego x jest $x \in \mathbb{E}_2$ wybrane jako przesunięcie o ustalony niezerowy wektor lub obrót wokół $(0, 0)$ o kąt niewspółmierny z π.

Jeśli $(G, \circ)$ jest grupą, to dla dowolnego niepustego podzbioru $A \subset G$ określamy $\langle A \rangle$ jako najmniejszą podgrupę G, która zawiera A - taka grupa w istocie istnieje i składa się ze wszystkich elementów G, które można zapisać w postaci $a_1 a_2 \ldots a_n$, gdzie każde a_i jest elementem A, lub jego odwrotnością, zaś $n \geqslant 0$ (pusty iloczyn rozumiemy jako e). $\langle A \rangle$ nazywamy podgrupą generowaną przez A. Dla elementu $x \in G$, który jest rzędu $n \geqslant 1$, zapis $\langle \{x\} \rangle$ pokrywa się z wcześniej wprowadzonym oznaczeniem $\langle x \rangle$ i używamy ich zamiennie. Ogólniej, będziemy pisać $\langle x_1, x_2, \ldots, x_k \rangle$ zamiast $\langle \{x_1, x_2, \ldots, x_k\} \rangle$.

2 Działania grup

W wymienionych przykładach większość grup była dana jako grupy pewnych przekształceń określonego zbioru (np. przestrzeni lub grafu), choć nie wszystkie (np. $\mathbb{Z}_n$). Następujące pojęcie pozwala myśleć o dosyć dowolnej grupie jak o wyznaczającej symetrie.

Definicja 4 (Działania grupy)**.** Niech X będzie zbiorem, zaś $(G, \circ)$ grupą z elementem neutralnym e. *Działaniem* G na X nazwiemy przyporządkowanie $\Theta : G \times X \to X$, spełniające warunki sformułowane w dalszym ciągu. O Θ myślimy jak o zadającym mnożenie elementów X z lewej strony przez elementy G i dla $g \in G$, $x \in X$ piszemy gx zamiast $\Theta(g, x)$. Przy tym oznaczeniu, warunki oznaczające, że Θ jest działaniem są następujące[8].

- Dla każdego $x \in X$ zachodzi $ex = x$.

- Dla każdych $a, b \in G$, $x \in X$ zachodzi $a(bx) = (ab)x$.

Przykłady:

- Grupa $\mathbb{E}_2$ działa na $\mathbb{R}^2$ w ten sposób, że dla $\phi \in \mathbb{E}_2$ oraz $x \in \mathbb{R}^2$ określamy $\phi x = \phi(x)$. Analogicznie każda grupa przekształceń pewnego zbioru X działa na X właśnie ten sposób.

- Dla $n \geqslant 1$ niech $f \in \mathbb{E}_2$ będzie obrotem wokół $(0, 0)$ o kąt $\frac{2\pi}{n}$. Wtedy $\mathbb{Z}_n$ działa na $\mathbb{R}^2$ w następujący sposób. Dla $k \in \mathbb{Z}_n$ oraz $x \in \mathbb{R}^2$ określamy[9] $kx = f^k(x)$.

[7] definiujemy potęgowanie przez warunki $x^0 = e$, $x^{j+1} = x^j \circ x$, $x^{-j} = (x^j)^{-1}$ dla $j > 0$.
[8] Przypomnijmy, że dla $a, b \in G$ używamy oznaczenia ab zamiennie z $a \circ b$.
[9] zapis ten może być mylący, ale użyjemy go tylko tutaj

3 Trochę o $\mathbb{R}^n$

Punkty $\mathbf{x} \in \mathbb{R}^n$ to ciągi postaci $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, gdzie $x_i \in \mathbb{R}$ dla każdego $i = 1, 2, \ldots, n$. Każdy punkt $\mathbf{x}$ utożsamiamy zwykle z wektorem zaczepionym w $\mathbf{0} = (0, \ldots, 0)$, mającym swój koniec w $\mathbf{x}$. Dla $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, $\alpha \in \mathbb{R}$ definiujemy

$$\mathbf{x} + \mathbf{y} = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

oraz

$$\alpha\mathbf{x} = (\alpha x_1, \alpha x_2, \ldots, \alpha x_n).$$

$(\mathbb{R}^n, +)$ jest kolejnym przykładem grupy przemiennej.

Definiujemy też iloczyn skalarny $\langle \mathbf{x}, \mathbf{y} \rangle = x_1y_1 + x_2y_2 + \ldots + x_ny_n$. Wyznacza on długość wektora $\mathbf{x}$, liczbę $\|\mathbf{x}\| = \sqrt{x_1^2 + x_2^2 + \ldots + x_n^2} = \sqrt{\langle x, x \rangle}$. Odległość między $\mathbf{x}$, a $\mathbf{y}$ to zaś $\|\mathbf{x} - \mathbf{y}\|$.

Mówimy, że $\mathbf{x}, \mathbf{y}$ są prostopadłe, jeśli $\langle \mathbf{x}, \mathbf{y} \rangle = 0$. To jest to samo, co stwierdzić, że wektory te są prostopadłe w płaszczyźnie zawierającej $\mathbf{x}$, $\mathbf{y}$, $\mathbf{0}$.

Każdy niezerowy wektor $\mathbf{v} \in \mathbb{R}^n$ wyznacza tzw. hiperpłaszczyznę
$\mathbf{v}^\perp = \{\mathbf{u} \in \mathbb{R}^n \mid (\mathbf{v}, \mathbf{u}) = 0\}$, która można utożsamić z $\mathbb{R}^{n-1}$: dla $n = 2$ jest to prosta prostopadła do $\mathbf{v}$, zaś dla $n = 3$ otrzymujemy płaszczyznę. Dla $n = 2, 3$ znana jest nam izometria $\mathbb{R}^n$, polegającą na odbiciu symetrycznym względem $\mathbf{v}^\perp$, oznaczmy ją przez $r_\mathbf{v}$ i napiszmy ogólną definicję $r_\mathbf{v}(\mathbf{u})$ dla $\mathbf{u} \in \mathbb{R}^n$ z dowolnym n.

Dane $\mathbf{u}$ zapisujemy (jednoznacznie) jako[10] $\mathbf{u} = \alpha\mathbf{v} + \mathbf{w}$, gdzie $\mathbf{w}$ jest prostopadłe do $\mathbf{v}$, tzn. $\mathbf{w} \in \mathbf{v}^\perp$, zaś $\alpha \in \mathbb{R}$. Przyjmujemy $r_\mathbf{v}(\mathbf{u}) = -\alpha\mathbf{v} + \mathbf{w}$.

4 Grupa $\mathbf{SL}_2(\mathbb{Z})$

Oznaczmy $\mathrm{SL}_2(\mathbb{Z}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z},\ ad - bc = 1\}$, zbiór macierzy 2 na 2 o współczynnikach całkowitych i wyznaczniku 1.

Mnożenie macierzy jest określone wzorem[11]

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} ax + bz & ay + bt \\ cx + dz & cy + dt \end{pmatrix}$$

$\mathrm{SL}_2(\mathbb{Z})$ staje się z tak określonym mnożeniem grupą, w której elementem neutralnym jest macierz $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, zaś macierzą odwrotną do $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ jest macierz $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, co wynika z założenia $ad - bc = 1$.

Te macierze są o tyle ciekawe, że wyznaczają izometrie tzw. płaszczyzny hiperbolicznej $\mathbb{H}^2$. O tym więcej na samych warsztatach.

Oznaczmy elementy $\mathbb{Z}^2$ w taki sposób, żeby $\mathbb{Z}^2 = \{\begin{pmatrix} a \\ b \end{pmatrix} \mid a, b \in \mathbb{Z}\}$.

Dla $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ oraz $v = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2$ określamy $Av = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$. Można sprawdzić, że to zadaje działanie[12] $\mathrm{SL}_2(\mathbb{Z})$ na $\mathbb{Z}^2$.

[10] rozkładamy wektor na składową równoległą do danego kierunku i składową prostopadłą do niego

[11] Który łatwo zapamiętać, jeśli oznaczy się *wiersze* pierwszej macierzy jako $w_1 = (a, b)$, $w_2 = (c, d)$, zaś *kolumny* drugiej jako $k_1 = (x, z)$, $k_2 = (y, t)$. Wtedy wynikiem mnożenia jest macierz $\begin{pmatrix} \langle w_1, k_1 \rangle & \langle w_1, k_2 \rangle \\ \langle w_2, k_1 \rangle & \langle w_2, k_2 \rangle \end{pmatrix}$.

[12] tj. spełnione są warunki $I_2 v = v$, $(AB)v = A(Bv)$