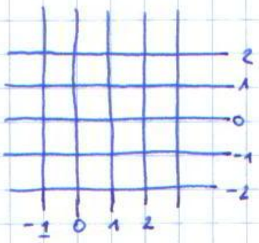
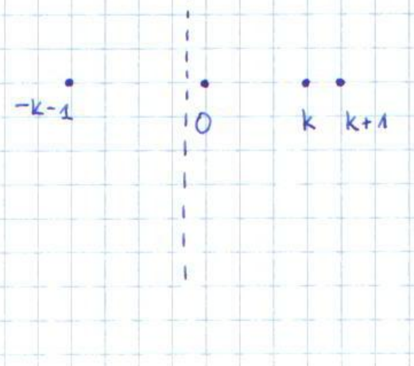
Teoria grup powstała jako skutek badania przekształceń zbiorów zachowujących jakieś struktury. Wyobraźmy sobie na przykład „nieskończoną" kartkę w kratkę. Zastanówmy



się jakie izometrie płaszczyzny zachowują taką kartkę. Na pewno są to przesunięcia o jednostkę w prawo i lewo oraz w górę i w dół. Jeśli t_x to przesunięcie w prawo, t_y to przesunięcie w górę to $(t_x)^{-1}$ daje przesunięcie w lewo, $(t_y)^{-1}$ daje przesunięcie w dół $t_y \circ t_x$ daje przesunięcie „wskos" itd. odwrotności oraz złożenia t_x i t_y dają też odwzorowanie zachowujące kratkę. Nie są to jednak wszystkie przekształcenia ~~zacho~~ zachowujące kratkę. Jest ich dużo więcej. Na przykład s_{y_0} – odbicie względem prostej $x=0$ a także wszelkie złożenia z poprzednimi, na przykład $s_{y_0} \circ t_x$: sprawdźmy co to za odwzorowanie. Jeżeli punkt o współrzędnych (k, m) poddamy t_x dostaniemy $(k+1, m)$ jeśli zastosujemy teraz s_{y_0} dostaniemy $(-k-1, m)$.



Widać, że jest to odbicie względem prostej $x = -\frac{1}{2}$. Jest to też odwzorowanie zachowujące kratkę, ale nowe – jeszcze takiego nie wymienialiśmy. Nazwijmy je $v_{-1/2}$

A co będzie jeśli zrobimy $s_{y0} \circ t_x \circ t_x$

dostajemy odbicie względem prostej $x = -1$ czyli $s_{y,-1}$

Jest jeszcze więcej symetrii - obroty wokół wierzchołków kratki, obroty względem środków kratki, odbicia względem prostych ukośnych przechodzących przez wierzchołki kratki / i \. Widać więc, że tych przekształceń jest bardzo dużo, ich składanie prowadzi do przekształceń także zachowujących kratkę. Podobnie, każde przekształcenie ma odwrotne do niego, także zachowujące kratkę. Wśród tych przekształceń jest też jedno - trywialne - identyczność, które zachowuje siatkę ponieważ nic nie robi.

Wymieniliśmy właśnie wszystkie elementy, które konstytuują grupę: działanie (składanie odwzorowań), istnienie elementów odwrotnych, istnienie elementu neutralnego

DEFINICJA: Grupą nazywamy zbiór G z działaniem $\circ : G \times G \to G$ spełniającym następujące trzy warunki

(1) działanie jest łączne tzn $g \circ (h \circ k) = (g \circ h) \circ k$

(2) W grupie G jest element neutralny e taki że dla wszystkich $g \in G$ $g \circ e = e \circ g = g$

(3) W grupie G każdy element ma element odwrotny, tzn jeśli $g \in G$ to istnieje $h \in G$ taki, że $g \circ h = h \circ g = e$ h oznaczamy g^{-1}.

Elementy odwrotne i element neutralny w naszej grupie G przykładowej już wskazaliśmy, nie wspominaliśmy jedynie o łączności składania odwzorowań.

Wiadomo, że składanie odwzorowań ma taką własność

$$\overbrace{f \circ g}^{\text{albo to najpierw}} \circ h = f \circ \underbrace{g \circ h}_{\text{możemy to najpierw}}$$

wynik się nie zmieni

Tę samą własność ma także ~~skł~~ mnożenie macierzy

$$A \cdot B \cdot C = (A \cdot B) \cdot C = A \cdot (B \cdot C)$$

Jeśli działanie jest łączne możemy nie wstawiać w ogóle nawiasów jak tu

Nasza przykładowa grupa przekształceń kratki jest duża i dość skomplikowana. Już samych przesunięć jest nieskończenie wiele, a jeszcze obroty i symetrie osiowe. Zacznijmy może od przykładów dużo prostszych grup mających skończenie wiele elementów.

Zanim zajmiemy się ciągiem dalszym teoretycznej strony zagadnienia przyjrzyjmy się przykładom. Uporządkujemy te przykłady pod względem liczby elementów:

(1) Grupa jednoelementowa jest tylko jedna – trywialna, składająca się z tylko jednego elementu neutralnego
$\{e\}$

(2) Grupa dwuelementowa jest też tylko jedna, choć można ją zrealizować na różne sposoby. Może być np.:
$\{-1, 1\}$ ze zwykłym mnożeniem

	1	-1
1	1	-1
-1	-1	1

Tabelka działania grupy

Inna reprezentacja to „grupa reszt modulo 2". Zauważmy że w $\mathbb{Z}$ mamy dwa podzbiory: liczby parzyste i liczby nieparzyste. Parzyste dzielą się przez 2 → reszta modulo 2 jest 0, nieparzyste mają resztę 1.
Suma dwóch parzystych i dwóch nieparzystych jest parzysta a suma jednej takiej i jednej takiej jest nieparzysta. To daje następujące działanie

$0+0=0 \quad 1+1=0 \quad 0+1=1 \quad 1+0=1$

W tabelce

	0	1
0	0	1
1	1	0

Te tabelki są takie same z dokładnością do nazw elementów

(3) Trójelementowa grupa też jest tylko jedna. Można ją reprezentować jako grupę reszt modulo 3

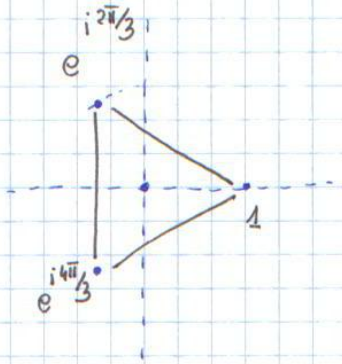
$\{0, 1, 2\}$ (z dodawaniem)

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

albo jako trójelementową podgrupę grupy obrotów płaszczyzny zawierającą id, $O(2\pi/3)$ $O(4\pi/3)$

Albo jeszcze jako zbiór $\{1, e^{i2\pi/3}, e^{i4\pi/3}\}$ z mnożeniem.

to są pierwiastki stopnia 3 z 1.



takie same tabelki

	1	$e^{\frac{2\pi}{3}i}$	$e^{\frac{4\pi}{3}i}$
1	1	$e^{2\pi/3 i}$	$e^{4\pi/3 i}$
$e^{2\pi/3 i}$	$e^{2\pi/3 i}$	$e^{4\pi/3 i}$	1
$e^{4\pi/3 i}$	$e^{4\pi/3 i}$	1	$e^{2\pi/3 i}$

Zauważmy, że w tabelkach działania mnożenia grupowego w każdym wierszu i w każdej kolumnie każdy element występuje tylko raz. Czy tak musi być? Gdyby któryś z elementów się powtórzył

	g_1	...	g_2
h	k		k

$$h \cdot g_1 = k = h \cdot g_2$$
$$h^{-1} h g_1 = h^{-1} h g_2$$
$$e g_1 = e g_2$$
$$\boxed{g_1 = g_2}$$

Podobnie byłoby w kolumnie. ~~By~~ mnożenie przez element grupy jest bijekcją grupy w siebie:

$\forall g \in G \quad \varphi_g : G \to G \quad \varphi_g(h) = gh$ jest bijekcją.

Zastanówmy się ile jest swobody w budowaniu tabelki działania

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

1. Wiadomo, że mnożenie przez element naturalny nic nie zmienia, pierwszy wiersz i pierwsza kolumna muszą więc być wypełnione w odpowiedni sposób

2. Zastanówmy się więc które z bijekcji zbioru $\{e, a, b\}$ w siebie mogą stać w wierszu 2 i 3.

e a b ← pierwszy wiersz

to ma e na miejscu 2 więc źle

e b a

b a e ← To może stać w wierszu 3

a e b ← ale b na ostatnim miejscu jest już w wierszu pierwszym

b e a

a b e

to może stać w wierszu 2, bo zaczyna się na a

Otrzymaliśmy tabelkę identyczną do tej dla reszt modulo 3 z dokładnością do nazw zmiennych. Nie było więc żadnej swobody wyboru. Pokazuje to, że jest jedna grupa rzędu 3. (tzn. mająca 3 elementy)

Podobną rzecz zrobimy dla grupy czteroelementowej. Wiemy z całą pewnością że istnieje przynajmniej jedna grupa czteroelementowa: Z_4. Jako zbiór ta grupa to ~~rze~~ liczby $\{0, 1, 2, 3\}$ a działanie to dodawanie modulo 4

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Spróbujmy tak samo jak poprzednio wymyślić inną grupę mającą 4 elementy

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

co wpisać tu?

✗ e b c (powtórzone)

e c b

✗ c b e (powt. b)

✗ b e c (powt. c)

c e b

b c e

A

c	e	b
e	c	a
b	a	e

grupa jak Z_4

B

b	c	e
c	e	a
e	a	b

grupa jak Z_4

C

e	c	b
c	e	a
b	a	e

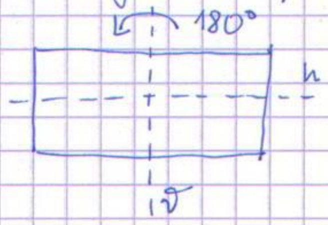
NOWA GRUPA

D

e	c	b
c	a	e
b	e	a

jak Z_4

Rozpatrzyliśmy wszystkie możliwości i tylko jeden raz otrzymaliśmy tabelkę inną niż $\mathbb{Z}_4$ (ewentualnie z poprzestawianymi kolumnami i wierszami). Jak poznać, że to inna tabelka? W $\mathbb{Z}_4$ mamy dwa elementy, które podniesione do kwadratu dają element neutralny: są to 0 i 2. Podobnie w tabelkach A (e, c), B (e, b), D (e, a). Natomiast w tabelce C każdy z elementów ma tę własność. Oznacza to, że jest to istotnie różna tabelka. Grupę z tabelką identyczną z (C) nazywamy Czwórkową grupą Kleina i oznaczamy V_4. Można ją zrealizować jako grupę symetrii prostokąta



$V_4 \simeq \{ id, O_{180°}, v, h \}$

symetria względem osi poziomej

symetria względem osi pionowej

Dla grup liczących 5 i więcej elementów nie będziemy już postępować tą samą metodą, gdyż robi się za dużo możliwości, żeby je wszystkie rozważyć. Potrzebujemy trochę więcej teorii, żeby uniknąć niepotrzebnego bałaganu.