Wstęp

Jest to skrypt do wykładu Algebra 1 prowadzonego w Instytucie Matematycznym Uniwersytetu Wrocławskiego. W ostatecznej formie skrypt będzie miał 15 części, które powinny odpowiadać 15 tygodniom zajęć, ale czasami materiał zrealizowany w danym tygodniu może nieco odbiegać od tego podziału.

Wykład można naturalnie podzielić tematycznie na dwie części: teorię grup (pierwsze 8 tygodni) i teorię pierścieni (kolejne 7 tygodni).

Używane oznaczenia

(1) Symbol „:=" oznacza, że lewa strona jest **definiowana** przez prawą, np.:

$$a^2 := a \cdot a.$$

(2) Symbol „□" oznacza **koniec dowodu**.

(3) Jeśli $f : A \to B$ oraz $A_0 \subseteq A, B_0 \subseteq B, b \in B$, to:
- $f(A_0)$ to **obraz** (nie używam tu nawiasów kwadratowych);
- $f^{-1}(B_0)$ to **przeciwobraz** (nie używam tu nawiasów kwadratowych);
- $f^{-1}(b) := f^{-1}(\{b\})$;
- $A \times B$ (**produkt kartezjański** A i B) to zbiór par (a, b), gdzie $a \in A$ i $b \in B$;
- $|A|$ to **moc** zbioru A.

(4) Oznaczenia zbiorów liczb:
- $\mathbb{N} := \{0, 1, 2, \ldots\}$ to zbiór liczb **naturalnych** (czyli 0 jest liczbą naturalną);
- $\mathbb{Z}$ to zbiór liczb **całkowitych**;
- $\mathbb{Q}$ to zbiór liczb **wymiernych**;
- $\mathbb{R}$ to zbiór liczb **rzeczywistych**;
- $\mathbb{N}_{>0} := \{1, 2, \ldots\}$, analogicznie np. $\mathbb{N}_{>5}$, czy też $\mathbb{R}_{>2024}$;
- $\mathbb{C}$ to zbiór liczb **zespolonych**.

TEORIA GRUP

1. Definicja grupy i pierwsze przykłady grup

Słowo **algebra** pochodzi od arabskiego **al-Jabr**:

الجبر

co oznacza przenoszenie bądź uzupełnianie. Historycznie, algebra rozpoczęła się od rozwiązywania konkretnych równań stopnia 1 oraz 2, których rozwiązywanie wymaga **przenoszenia** (na drugą stronę równania). Potem zaczęto rozważać ogólne równania, np. równanie:

$$ax^2 + bx + c = 0,$$

które ma następujące rozwiązania:

$$x_1 = \frac{-b + \sqrt{\Delta}}{2a}, \quad x_2 = \frac{-b - \sqrt{\Delta}}{2a},$$

gdzie

$$\Delta := b^2 - 4ac.$$

W tym równaniu i w jego rozwiązaniach pojawiają się operacje algebraiczne (działania): $+, -, \cdot, :, \sqrt{}$ na **literach**, o których myślimy jako o dowolnych liczbach. Taka właśnie jest algebra obecnie: zajmuje się działaniami np. na zbiorach liter, które mogą (ale nie muszą) być ogólnymi współczynnikami jakiegoś równania.

Niech teraz A będzie dowolnym niepustym zbiorem (np. $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$). Chcemy zdefiniować pojęcie **działania** na zbiorze A. Popatrzmy najpierw na bardzo naturalny przykład: działanie dodawania na $\mathbb{N}$. Dla dowolnych dwóch liczb naturalnych (np. 2 i 3) działanie dodawania produkuje ich sumę (np. $2+3=5$). Czyli działanie dodawania jest **funkcją** za zbioru par liczb naturalnych $\mathbb{N} \times \mathbb{N}$ w zbiór liczb naturalnych $\mathbb{N}$.

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \qquad (a, b) \mapsto a + b.$$

Ogólna definicja działania jest analogiczna.

Definicja 1.1. *Działaniem* na niepustym zbiorze A nazywany dowolną funkcję

$$* : A \times A \to A.$$

Konwencja 1.2. Dla $a, a' \in A$ piszemy „$a * a'$" zamiast „$*((a, a'))$".

Na razie nie mamy żadnych założeń na temat własności działania $*$, czyli działanie to może być (bardzo) „dziwne".

Przykład 1.3. Poniżej kilka przykładów działań.

(1) Na zbiorach $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ mamy zwykłe działania dodawania $(+)$ i mnożenia $(\cdot)$.

(2) Mamy też mnóstwo innych „dziwnych" działań, np. działanie:

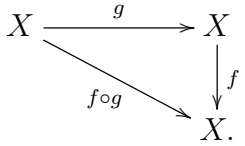
$$a * a' := (2a \cdot b) + 5a^2$$

na (np.) zbiorze $\mathbb{R}$.

(3) Teraz ważny ogólny przykład. Niech X będzie dowolnym zbiorem i niech X^X oznacza zbiór wszystkich funkcji $X \to X$ Dla $f, g \in X^X$ mamy **złożenie** funkcji $f \circ g \in X^X$:

$$\forall\, x \in X \qquad (f \circ g)(x) = f(g(x)).$$

Czyli $\circ$ jest działaniem na zbiorze X^X.



(4) Niech $\mathcal{P}(X)$ będzie zbiorem wszystkich podzbiorów zbioru X. Wtedy przekrój zbiorów ($\cap$) i suma zbiorów ($\cup$) są działaniami na zbiorze $\mathcal{P}(X)$.
(5) Rozważmy zbiór $\mathbb{R}\cup\{\infty\}$, gdzie ∞ to (nowy) formalny symbol. Definiujemy działanie $+$ na zbiorze $\mathbb{R}\cup\{\infty\}$:

$$\forall\, a, b \in \mathbb{R}\cup\{\infty\} \qquad a + \infty := \infty =: \infty + a,$$

$$\forall\, a, b \in \mathbb{R} \qquad a + b \text{ to dodawanie z } \mathbb{R}.$$

Uwaga 1.4. Mamy następujący prosty opis działań. Jeśli $*$ jest działaniem na skończonym (i nie za dużym) zbiorze $A = \{a_1, \ldots, a_n\}$, to definiujemy *tabelkę* $*$:

$*$	a_1	a_2	$\ldots$	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$	$\ldots$	$a_1 * a_n$
a_2	$a_2 * a_1$	$a_2 * a_2$	$\ldots$	$a_2 * a_n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_n	$a_n * a_1$	$a_n * a_2$	$\ldots$	$a_n * a_n$

Przykład 1.5. (1) Niech

$$A = \mathcal{P}(\{0,1\}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$$

oraz $* = \cup$. Wtedy mamy:

$\cup$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0,1\}$
$\emptyset$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0,1\}$
$\{0\}$	$\{0\}$	$\{0\}$	$\{0,1\}$	$\{0,1\}$
$\{1\}$	$\{1\}$	$\{0,1\}$	$\{1\}$	$\{0,1\}$
$\{0,1\}$	$\{0,1\}$	$\{0,1\}$	$\{0,1\}$	$\{0,1\}$

(2) Rozważmy dwa przykłady działań na $A = \{0,1\}$ dane następującymi tabelkami:

$*$	0	1
0	0	1
1	1	0

$\blacklozenge$	0	1
0	1	0
1	0	0

W związku z Przykładem 1.5(2), weźmy następującą bijekcję:

$$f : \{0,1\} \to \{2,3\}; \qquad f(0) = 2,\ f(1) = 3.$$

Używając f możemy „transportować" (np.) działanie $\blacklozenge$ ze zbioru $\{0,1\}$ do zbioru $\{2,3\}$ i otrzymać działanie, które nazwiemy $\blacksquare$. Policzmy np. $2\blacksquare 3$:

- cofamy się przez f^{-1} i dostajemy:
$$f^{-1}(2) = 0, \quad f^{-1}(3) = 1;$$
- stosujemy działanie $\blacklozenge$ i dostajemy $0\blacklozenge 1 = 0$;
- na wynik nakładamy f i dostajemy
$$2\blacksquare 3 := f(0) = 2.$$

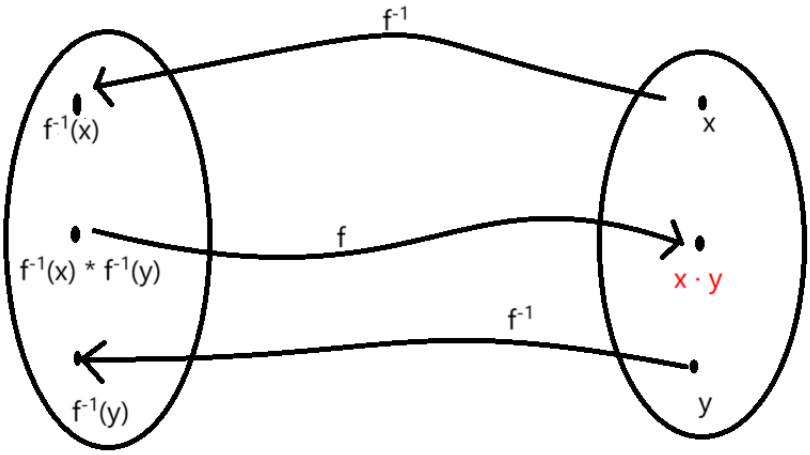
Czyli ogólny wzór jest następujący:

$$\forall\, x, y \in \{2,3\} \qquad x \blacksquare y := f\left(f^{-1}(x) \blacklozenge f^{-1}(y)\right).$$

Poniżej formalizujemy tę konstrukcję.

Definicja 1.6. Niech $f : A \to B$ będzie bijekcją i $*$ będzie działaniem na zbiorze A. Działanie $\cdot$ na zbiorze B nazywamy działaniem *indukowanym* przez działanie $*$ poprzez funkcję f (lub działaniem *transportowanym* poprzez funkcję f z działania $*$), jeśli:

$$\forall\, x, y \in B \qquad x \cdot y = f\left(f^{-1}(x) * f^{-1}(y)\right).$$



Niedługo pokażemy, że działania transportowane mają te same „własności algebraiczne" co oryginalne działania. Aby wyodrębić te własności, popatrzmy bliżej na działanie składania funkcji na zbiorze X^X.

(1) Dla $f, g, h : X \to X$ oraz $x \in X$ mamy:

$$[f \circ (g \circ h)](x) = f((g \circ h)(x)) = f(g(h)),$$

$$[(f \circ g) \circ h](x) = (f \circ g)(h(x)) = f(g(h)).$$

Tak więc dostajemy **łączność** działania $\circ$:

$$\forall\, f, g, h \in X^X \qquad f \circ (g \circ h) = (f \circ g) \circ h.$$

(2) Istnieje wyróżniona funkcja

$$\mathrm{id}_X : X \to X, \quad \mathrm{id}_X(x) := x,$$

taka że id_X jest **elementem neutralnym** działania $\circ$:

$$\forall\, f \in X^X \qquad \mathrm{id}_X \circ f = f = f \circ \mathrm{id}_X\,.$$

(3) Weźmy $f, g \in X^X$. Mówimy, że g jest **funkcją odwrotną** do f, gdy:

$$f \circ g = \mathrm{id}_X = g \circ f.$$

Jeśli funkcja odwrotna do f istnieje, to jest jedyna i oznaczamy ją przez f^{-1}. Ze Wstępu do Matematyki wiemy, że funkcja odwrotna do f istnieje wtedy i tylko wtedy, gdy f jest bijekcją.

Definicja 1.7. Niech $*$ będzie działaniem na zbiorze A.

(1) Działanie $*$ jest *łączne*, gdy:

$$\forall\, a, b, c \in A \qquad a * (b * c) = (a * b) * c.$$

(2) Element $e \in A$ nazywamy *elementem neutralnym* działania $*$, gdy:

$$\forall\, a \in A \qquad e * a = a = a * e.$$

Szybki Fakt
Jeśli e_1 i e_2 są elementami neutralnymi działania $*$, to $e_1 = e_2$.

Dowód Szybkiego Faktu. Ponieważ e_1 jest elementem neutralnym działania $*$, tak więc:

$$e_1 * e_2 = e_2.$$

Ponieważ e_2 jest elementem neutralnym działania $*$, tak więc:

$$e_1 * e_2 = e_1.$$

Stąd $e_1 = e_2$. □

Czyli jeśli element neutralny istnieje, to jest **jedyny**.

(3) Załóżmy, że $*$ ma element neutralny e (z Szybkiego Faktu wiemy, że musi on być jedyny!). Dla $a, b \in A$ mówimy, że b jest elementem *odwrotnym* do a, gdy:

$$a * b = e = b * a.$$

(4) Mówimy, że działanie $*$ jest *przemienne*, gdy:

$$\forall\, a, b \in A \qquad\qquad a * b = b * a.$$

Definicja 1.8. Niech $*$ będzie działaniem na zbiorze G. Mówimy, że para $(G, *)$ jest *grupą*, gdy działanie $*$ jest łączne, ma element neutralny i dla każdego elementu w G istnieje element odwrotny.

Grupę $(G, *)$ nazywamy *przemienną* lub *abelową*, gdy działanie $*$ jest przemiennie

Konwencja 1.9. Często zamiast „grupa $(G, *)$" piszemy „grupa G" domyślając się działania $*$.

Zanim zobaczymy przykłady, jeszcze jeden fakt zawierający istotne oznaczenie.

Fakt 1.10. *Niech $(G, \cdot)$ będzie grupą i $g \in G$. Wtedy istnieje **jedyny** element odwrotny do g w $(G, \cdot)$, który oznaczamy g^{-1}.*

Dowód. Załóżmy, że $g_1, g_2 \in G$ to elementy odwrotne do g w $(G, \cdot)$. Mamy pokazać, że $g_1 = g_2$.

Mnożymy równość:

$$g_1 \cdot g = e$$

obustronnie przez g_2 z prawej strony i otrzymujemy:

$$(g_1 \cdot g) \cdot g_2 = e \cdot g_2 = g_2.$$

Z drugiej strony, używając łączności $\cdot$ i tego, że g_2 jest elementem odwrotnym do g, otrzymujemy:

$$(g_1 \cdot g) \cdot g_2 = g_1 \cdot (g \cdot g_2) = g_1 \cdot e = g_1,$$

co daje $g_1 = (g_1 \cdot g) \cdot g_2 = g_2$. □

Udowodnimy teraz główną własność działań transportowanych.

Twierdzenie 1.11. *Niech $f : A \to B$ będzie bijekcją, $*$ będzie działaniem na A oraz $\cdot$ będzie działaniem na B indukowanym przez działanie $*$ poprzez funkcję f. Jeśli działanie $*$ jest łączne, to działanie $\cdot$ też jest łączne.*

Dowód. Weźmy $x, y, z \in B$ i oznaczmy na chwilę:

$$a := f(f^{-1}(x) * f^{-1}(y)).$$

Wtedy mamy (używając Definicji 1.6):

$$\begin{aligned}
(x \cdot y) \cdot z &= \left(f(f^{-1}(x) * f^{-1}(y))\right) \cdot z \\
&= a \cdot z \\
&= f\left(f^{-1}(a) * f^{-1}(z)\right) \\
&= f\left(f^{-1}\left(f\left[f^{-1}(x) * f^{-1}(y)\right]\right) * f^{-1}(z)\right) \\
&= f\left(\left[f^{-1}(x) * f^{-1}(y)\right] * f^{-1}(z)\right).
\end{aligned}$$

Podobnie dostajemy:

$$x \cdot (y \cdot z) = f\left(f^{-1}(x) * \left[f^{-1}(y) * f^{-1}(z)\right]\right).$$

Z łączności $*$ mamy:

$$\left[f^{-1}(x) * f^{-1}(y)\right] * f^{-1}(z) = f^{-1}(x) * \left[f^{-1}(y) * f^{-1}(z)\right]$$

i stąd w końcu dostajemy $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. □

Uwaga 1.12. Analogiczne twierdzenia są prawdziwe dla przemienności, istnienia elementów neutralnych i ogólnie każdej **algebraicznej własności** działań. W szczególności mamy następujące zadanie z ćwiczeń: jeśli powyżej $(A, *)$ jest grupą, to $(B, \cdot)$ jest też grupą.

Przykład 1.13. (1) Popatrzmy najpierw na najbardziej naturalne działania dodawania i mnożenia na zbiorach $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Działania te na każdym z tych zbiorów są łączne i przemienne. Poza tym 0 jest zawsze elementem neutralnym $+$ oraz 1 jest zawsze elementem neutralnym $\cdot$.

Popatrzmy, czy istnieją elementy odwrotne. Np. $1 \in \mathbb{N}$ nie ma elementu odwrotnego względem dodawania na zbiorze $\mathbb{N}$, Czyli $(\mathbb{N}, +)$ **nie** jest grupą. Łatwo zauważyć, że $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ są grupami przemiennymi. Jak dobrze wiemy, 0 na żadnym z tych zbiorów nie ma elementu odwrotnego względem działania $\cdot$ („nie można dzielić przez 0"). Czyli $(\mathbb{N}, \cdot), (\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot)$ **nie** są grupami.

(2) Rozważmy teraz na następujące „dziwne" działanie $*$ na $\mathbb{R}$:

$$a * b := a + b^2.$$

Dziwne działania zwykle nie są łączne. Aby udowodnić, że działanie $*$ **nie** jest łączne, należy **wskazać** konkretne elementy $a, b, c \in \mathbb{R}$, takie że zachodzi:

$$a * (b * c) \neq (a * b) * c.$$

Czyli trzeba te elementy jakoś zgadnąć. Zgadujemy, że np.:

$$a = 0,\ b = 0,\ c = 2.$$

Sprawdzamy:

$$(0 * 0) * 2 = \left(0 + 0^2\right) * 2 = 0 * 2 = 0 + 2^2 = 4,$$

$$0 * (0 * 2) = 0 * \left(0 + 2^2\right) = 0 * 4 = 0 + 4^2 = 16.$$

Czyli faktycznie to „dziwne" działanie $*$ nie jest łączne.

(3) Wiemy, że działanie składania funkcji na zbiorze X^X jest łączne i ma element neutralny id_X. Wiemy też, że jeśli $f \in X^X$ nie jest bijekcją, to f nie ma elementu odwrotnego. Rozważmy następujący podzbiór X^X:

$$S_X := \{f \in X^X \mid f \text{ jest bijekcją}\}.$$

Składanie funkcji wciąż jest działaniem na zbiorze S_X, bo złożenie bijekcji jest bijekcją oraz, oczywiście, to działanie wciąż jest łączne na zbiorze S_X. Element id_X jest bijekcją, czyli jest elementem neutralnym działania $\circ$ na zbiorze S_X. Dla każdej bijekcji $f \in S_X$, istnieje funkcja odwrotna f^{-1}, która też jest bijekcją. Czyli $(S_X, \circ)$ jest grupą.

(4) Rozważmy działanie $+$ na zbiorze $\mathbb{R} \cup \{\infty\}$ z Przykładu 1.3(5).

Udowodnimy że to działanie jest łączne. Weźmy $a, b, c \in \mathbb{R} \cup \{\infty\}$. Jeśli $a = \infty$ lub $b = \infty$ lub $c = \infty$, to:

$$(a + b) + c = \infty = a + (b + c).$$

Jeśli $a, b, c \in \mathbb{R}$, to oczywiście również mamy $(a + b) + c = a + (b + c)$. Czyli działanie $+$ na zbiorze $\mathbb{R} \cup \{\infty\}$ faktycznie jest łączne.

Łatwo zauważyć, że 0 jest elementem neutralnym działania $+$ na zbiorze $\mathbb{R} \cup \{\infty\}$. Ale element ∞ nie ma elementu odwrotnego (intuicja: $\infty - \infty$ to „symbol nieoznaczony"). Czyli $(\mathbb{R} \cup \{\infty\}, +)$ **nie** jest grupą.

(5) Rozważmy teraz dwa działania $*, \blacklozenge$ na zbiorze $\{0,1\}$ z Przykładu 1.5(2).

Łatwo sprawdzić (rozważając przypadki), że $*$ jest łączne (niedługo zrobimy to w inny sposób), 0 jest elementem neutralnym $*$ oraz:

$$0 * 0 = 0,\ 1 * 1 = 0,$$

czyli każdy element ma element odwrotny. Stąd $(\{0,1\}, *)$ jest grupą przemienną.

Popatrzmy teraz na działanie $\blacklozenge$. Mamy:

$$(0\blacklozenge 0)\blacklozenge 1 = 1\blacklozenge 1 = 0,$$

$$0\blacklozenge(0\blacklozenge 1) = 0\blacklozenge 0 = 1.$$

Czyli działanie $\blacklozenge$ **nie** jest łączne. Okaże się niedługo, że działanie $*$ jest „nieprzypadkowe" , a działanie jest „przypadkowe".

Popatrzmy teraz na nowe i ważne przykłady działań: **działania modulo** n ($n \in \mathbb{N}_{\geqslant 1}$). Niech $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$ będzie zbiorem reszt modulo n oraz

$$r_n : \mathbb{Z} \to \mathbb{Z}_n$$

będzie *funkcją n-tej reszty*, tzn. $\forall x \in \mathbb{Z}\ \forall r \in \mathbb{Z}_n$ mamy:

$$\begin{aligned} r_n(x) = r &\iff r \text{ jest resztą z dzielenia } x \text{ przez } n \\ &\iff n | x - r. \end{aligned}$$

Definiujemy działania *dodawania i mnożenia modulo* n ($+_n$ i $\cdot_n$) na zbiorze $\mathbb{Z}_n$:

$$\forall\, x, y \in \mathbb{Z}_n \qquad x +_n y := r_n(x + y), \qquad x \cdot_n y := r_n(x \cdot y).$$

Dla przykładu:

$$3 +_5 4 = r_5(7) = 2, \qquad 3 \cdot_5 4 = r_5(12) = 2.$$

Możemy napisać np. tabelkę $+_2$:

$+_2$	0	1
0	0	1
1	1	0

Widzimy, że działanie $*$ na $\{0, 1\} = \mathbb{Z}_2$ z Przykładu 1.5(2) to dokładnie działanie $+_2$, dlatego też to działanie $*$ jest „nieprzypadkowe”!

Twierdzenie 2.1. *Działanie $+_n$ jest łączne.*

Dowód. Weźmy $x, y, z \in \mathbb{Z}_n$. Pokażemy, że:

$$(x +_n y) +_n z = r_n(x + y + z) = x +_n (y +_n z).$$

Z definicji $+_n$ mamy:

$$(x +_n y) +_n z = r_n\left((x +_n y) + z\right).$$

Używając definicji r_n oraz tego, że $x +_n y = r_n(x + y)$ dostajemy:

$$n | (x +_n y) - (x + y) = (x +_n y) + z - (x + y + z).$$

Będziemy używać następującej „prostej obserwacji”:

$$\forall\, a, b \in \mathbb{Z} \qquad r_n(a) = r_n(b) \iff n | a - b.$$

Używając „prostej obserwacji” dostajemy, że:

$$r_n\left((x +_n y) + z\right) = r_n(x + y + z)$$

i stąd mamy:

$$(x +_n y) +_n z = r_n(x + y + z).$$

Analogicznie pokazuje się, że:

$$x +_n (y +_n z) = r_n(x + y + z)$$

i stąd dostajemy $(x +_n y) +_n z = x +_n (y +_n z)$, czyli działanie $+_n$ jest łączne. □

Ponadto mamy, że:

- 0 jest elementem neutralnym działania $+_n$;
- 0 jest elementem odwrotnym do samego siebie (jak każdy element neutralny);
- dla każdego $x \in \mathbb{Z}_n \setminus \{0\}$ mamy, że $n - x \in \mathbb{Z}_n$ oraz $n - x$ jest elementem odwrotnym do x.

Czyli $(\mathbb{Z}_n, +n)$ jest grupą. Działanie $+_n$ jest przemienne, czyli:

$$(\mathbb{Z}_n, +_n) \textbf{ jest grupą przemienną.}$$

Popatrzmy teraz na działanie $\cdot_n$. Podobnie jak dla $+_n$ można pokazać, że:

$$\forall\, x, y, z \in \mathbb{Z}_n \qquad (x \cdot_n y) \cdot_n z = r_n(xyz) = x \cdot_n (y \cdot_n z),$$

czyli działanie $\cdot_n$ jest łączne.

Załóżmy teraz, że $n > 1$. Oczywiście, 1 jest elementem neutralnym $\cdot_n$. Ale wciąż 0 nie ma elementu odwrotnego, czyli dla $n > 1$:

$$(\mathbb{Z}_n, \cdot_n) \textbf{ nie jest grupą.}$$

Kontynuujemy przykłady grup, opiszemy teraz (skończone) **grupy permutacji**. Dla $n > 0$ definiujemy (patrz Przykład 1.13(3)):

$$S_n := S_{\{1,2,\ldots,n\}}$$

grupę wszystkich bijekcji $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.

Dla $\sigma \in S_n$ oznaczamy:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

Przykład 2.2. Wypiszmy elementy grup S_1, S_2, S_3:

$$S_1 = \{\mathrm{id}\}, \quad S_2 = \left\{\mathrm{id}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\right\},$$

$$S_3 = \left\{\mathrm{id}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\}.$$

Jeśli oznaczmy $S_2 = \{\mathrm{id}, \sigma\}$, to wtedy tabelka S_2 wygląda następująco:

$\circ$	id	σ
id	id	σ
σ	σ	id

Pisząc kod tej tabelki w TeXu, wziąłem tabelkę działania $+_2$ i zamieniłem wszystkie wystąpienia „0" na „id" oraz „1" na „σ". Czyli tabelka $(S_2, \circ)$ jest „taka sama" jak tabelka $(\mathbb{Z}_2, +_2)$. Ogólnie, łatwo zauważyć, że jeśli $G = \{e, g\}$ jest grupą dwu-elementową, to jest tylko jedno możliwe działanie $*$ na G, takie że $(G, *)$ jest grupą.

Grupy S_1 i S_2 są przemienne. Zauważmy, że grupa S_3 nie jest przemienna:

$$\left[\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\right](1) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}(2) = 1,$$

$$\left[\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\right](1) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}(2) = 3.$$

Stąd mamy:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Podobnie dla wszystkich $n \geqslant 3$, grupa S_n nie jest przemienna.

Podsumowując, znamy już dwie serie grup skończonych dla $n \geqslant 1$:

- grupy przemienne $(\mathbb{Z}_n, +_n)$;
- grupy S_n, które nie są przemienne dla $n \geqslant 3$.

Grupy macierzy

Niech $n > 0$ i $\mathrm{GL}_n(\mathbb{R})$ będzie zbiorem macierzy $n \times n$ o wyznaczniku niezerowym. Z algebry liniowej wiemy, że:

- iloczyn macierzy o wyznaczniku niezerowym jest macierzą o wyznaczniku niezerowym, czyli mnożenie macierzy jest działaniem na $\mathrm{GL}_n(\mathbb{R})$;

- mnożenie możemy jest łączne;
- dla
$$I := \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$
macierzy identycznościowej many:
$$\forall\, A \in \mathrm{GL}_n(\mathbb{R}) \qquad A \cdot I = A = I \cdot A,$$
czyli I jest elementem neutralnym działania mnożenia macierzy na $\mathrm{GL}_n(\mathbb{R})$;
- dla każdej $A \in \mathrm{GL}_n(\mathbb{R})$ istnieje macierz odwrotna $B = A^{-1} \in \mathrm{GL}_n(\mathbb{R})$, taka że:
$$A \cdot B = I = B \cdot A.$$

Stąd $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ jest grupą.

Dla $n = 1$ mamy $\mathrm{GL}_1(\mathbb{R}) = \mathbb{R} \setminus \{0\}$, czyli
$$(\mathrm{GL}_1(\mathbb{R}), \cdot) = (\mathbb{R} \setminus \{0\}, \cdot)$$
i jest to grupa przemienna. Podobnie $(\mathbb{C} \setminus \{0\}, \cdot)$ jest grupą przemienną.

Dla $n \geqslant 2$, grupa $\mathrm{GL}_n(\mathbb{R})$ nie jest przemienna, np.:
$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \neq \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

Notacja multyplikatywna

Działanie w grupie G zwykle oznaczamy przez „$\cdot$” lub przez „nic”, tzn. dla $a, b \in G$ piszemy $a \cdot b$ lub po prostu ab. Oczywiście, jeśli mamy konkretną grupę jak np. $(\mathbb{R}, +)$ czy $(\mathbb{Z}_5, +_5)$, to już nie oznaczamy działania tam przez $\cdot$. Powyższą notację stosujemy, gdy mówimy ogólnie o grupach. Element neutralny w grupie zwykle oznaczamy przez e.

Potęgowanie w grupie

Niech $(G, \cdot)$ będzie grupą i $n > 0$. Działanie $\cdot$ jest łączne, więc dla każdego $g \in G$ element:
$$g^n := \underbrace{g \cdot \ldots \cdot g}_{n \text{ razy}}$$
jest dobrze określony. Definiujemy też:
$$g^0 := e, \qquad g^{-n} := \left(g^{-1}\right)^n.$$
Czyli dla wszystkich $m \in \mathbb{Z}, g \in G$ mamy zdefiniowany element $g^m \in G$. Na ćwiczeniach pokazujemy następujący wynik.

Twierdzenie 2.3. *Dla każdych $g, h \in G$ oraz $m, n \in \mathbb{Z}$ zachodzi:*

(1) $g^m g^n = g^{m+n}$,
(2) $(g^m)^n = g^{mn}$,
(3) *jeśli $gh = hg$, to $(gh)^n = g^n h^n$.*

Notacja addytywna

Abstrakcyjną grupę przemienną często oznaczamy przez $(A, +)$. Wtedy element neutralny oznaczamy przez 0 oraz dla $a \in A$ i $m \in \mathbb{N}$ zamiast a^m piszemy ma oraz zamiast a^{-1} piszemy $-a$.

Na ćwiczeniach rozważaliśmy dysk
$$K_r := \{z \in \mathbb{C} \mid |z| \leqslant r\}$$
i zauważyliśmy, że dla $r \leqslant 1$, K_r jest „zamknięty na $\cdot$” oraz dla $r > 1$, K_r nie jest „zamknięty na $\cdot$”. Formalizujemy teraz to pojęcie „zamkniętości”.

Definicja 2.4. Niech $(G, \cdot)$ będzie grupą i $A \subseteq G$. Mówimy, że:

(1) A jest *zamknięty na działanie* $\cdot$, gdy:

$$\forall\, a, a' \in A \qquad\qquad a \cdot a' \in A;$$

(2) A jest *podgrupą* G, co oznaczamy $A \leqslant G$, gdy:
   (i) A jest zamknięty na działanie $\cdot$,
   (ii) $e \in A$,
   (iii) dla każdego $a \in A$ mamy że $a^{-1} \in A$.

Uwaga 2.5. Jeśli $A \leqslant G$, to $(A, \cdot)$ jest grupą, gdzie tu $\cdot$ jest działaniem z G obciętym do A.

Przykład 2.6. (1) $\mathbb{R} \leqslant (\mathbb{C}, +)$, $\mathbb{Q} \leqslant (\mathbb{R}, +)$, $\mathbb{Z} \leqslant (\mathbb{Q}, +)$.
(2) $\mathbb{N}$ **nie** jest podgrupą $(\mathbb{Z}, +)$, bo choć $\mathbb{N}$ jest zamknięty na $+$ i $0 \in \mathbb{N}$, to np. $1 \in \mathbb{N}$ ale $-1 \notin \mathbb{N}$.
(3) $\mathbb{R}\setminus\{0\} \leqslant (\mathbb{C}\setminus\{0\}, \cdot)$, $\mathbb{Q}\setminus\{0\} \leqslant (\mathbb{R}\setminus\{0\}, \cdot)$.
(4) $\mathbb{R}\setminus\{0\}$ **nie** jest podgrupą $(\mathbb{R}, +)$, bo $\mathbb{R}\setminus\{0\}$ **nie** jest zamknięty na $+$, np. $1, -1 \in \mathbb{R}\setminus\{0\}$ ale $1 + (-1) = 0 \notin \mathbb{R}\setminus\{0\}$.
(5) Zadanie z ćwiczeń: jeśli $H \leqslant G$ i $N \leqslant G$, to $H \cap N \leqslant G$.

Uwaga 2.7. Teraz można sprecyzować pewne konwencje.
(1) Jak mówimy „grupa $\mathbb{R}$", to **zawsze** to znaczy „grupa $(\mathbb{R}, +)$", bo $(\mathbb{R}, \cdot)$ nie jest grupą!
(2) Jak mówimy „grupa $\mathbb{R}\setminus\{0\}$", to **zawsze** to znaczy „grupa $(\mathbb{R}\setminus\{0\}, \cdot)$", bo $+$ nie jest nawet działaniem na $\mathbb{R}\setminus\{0\}$!

Grupy izometrii

Niech $W \subseteq \mathbb{R}^2$ będzie figurą płaską (np. W to kwadrat bądź trójkąt). Definiujemy:

$$\mathrm{Izo}(W) := \{f \in S_W \mid f \text{ jest izometrią}\}.$$

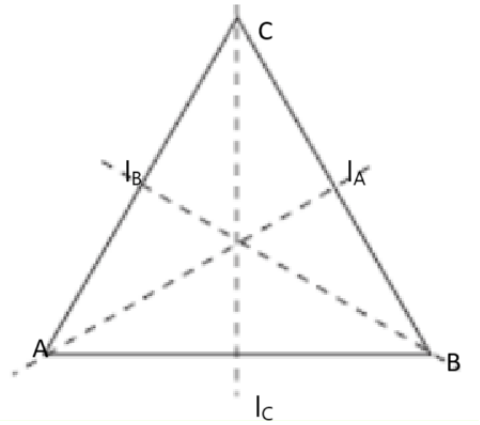
Wtedy $\mathrm{Izo}(W) \leqslant S_W$, czyli $(\mathrm{Izo}(W), \circ)$ jest grupą.

Mamy cztery typy izometrii:

- symetrie osiowe;
- obroty;
- translacje;
- złożenia translacji z symetriami osiowymi.

Jeśli figura W jest ograniczona, to rozważamy jedynie symetrie osiowe i obroty.

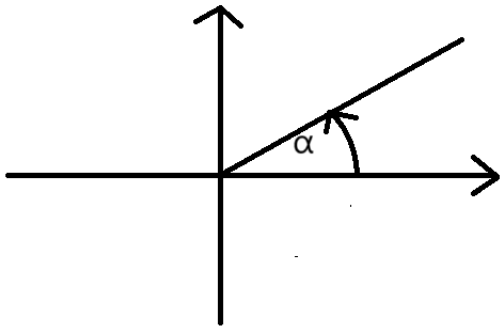
Popatrzmy dokładniej na przypadek, gdy W jest trójkątem równobocznym. Wtedy grupę izometrii oznacza się D_3 i należą do niej tylko obroty i symetrie osiowe. Ustawiamy trójkąt jak na rysunku poniżej (środek ciężkości w środku układu współrzędnych). Mamy:



$$D_3 = \left\{\mathrm{id}, O_{\frac{2\pi}{3}}, O_{\frac{4\pi}{3}}, S_A, S_B, S_C\right\},$$

gdzie S_A to symetria osiowa względem prostej l_A z rysunku, S_B to symetria osiowa względem prostej l_B, S_C to symetria osiowa względem prostej l_C i ogólnie O_α to obrót o kąt α w kierunku

przeciwnym do kierunku ruchu wskazówek zegara (środek obrotu to środek układu współrzędnych):



Izometria trójkąta równobocznego jest jednoznacznie wyznaczona przez jej wartości na wierzchołkach $\{A, B, C\}$. Czyli, aby policzyć np. $S_A \circ O_{\frac{2\pi}{3}}$ wystarczy zobaczyć na co przechodzą wierzchołki. Liczymy $S_A \circ O_{\frac{2\pi}{3}}$:

$$A \overset{O_{2\pi/3}}{\longmapsto} B \overset{S_A}{\longmapsto} C, \quad B \overset{O_{2\pi/3}}{\longmapsto} C \overset{S_A}{\longmapsto} B, \quad C \overset{O_{2\pi/3}}{\longmapsto} A \overset{S_A}{\longmapsto} A.$$

Czyli dostajemy:

$$S_A \circ O_{\frac{2\pi}{3}} = S_B.$$

Liczymy teraz $O_{\frac{2\pi}{3}} \circ S_A$:

$$A \overset{S_A}{\longmapsto} A \overset{O_{2\pi/3}}{\longmapsto} B, \quad B \overset{S_A}{\longmapsto} C \overset{O_{2\pi/3}}{\longmapsto} A, \quad C \overset{S_A}{\longmapsto} B \overset{O_{2\pi/3}}{\longmapsto} C.$$

Dostajemy:

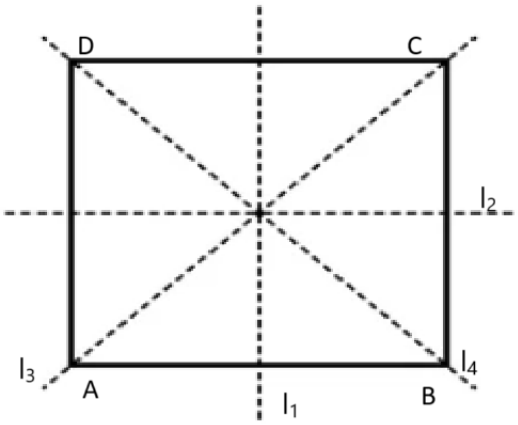
$$O_{\frac{2\pi}{3}} \circ S_A = S_C.$$

W szczególności:

$$S_A \circ O_{\frac{2\pi}{3}} \neq O_{\frac{2\pi}{3}} \circ S_A.$$

czyli grupa D_3 **nie** jest przemienna. W ten sposób można napisać całą tabelkę grupy D_3.

Ogólnie dla $n \geqslant 3$ definiujemy D_n jako grupę izometrii n-kąta foremnego. Składa się ona z n obrotów (identyczność rozumiemy jako obrót o 0 stopni) oraz n symetrii osiowych. Czyli D_n jest grupą nieprzemienną o $2n$ elementach, co daje nam kolejną serię grup skończonych. Popatrzmy na D_4:



Mamy:

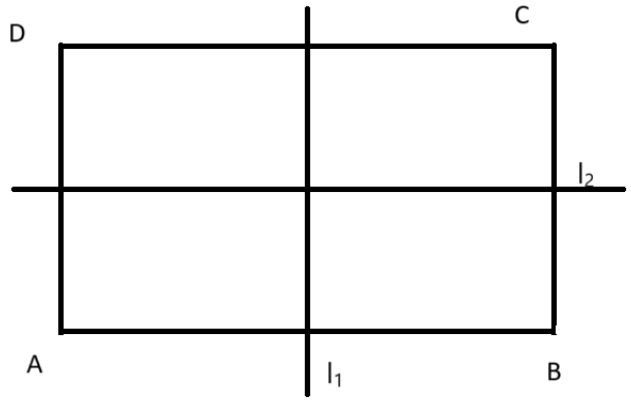
$$D_4 = \left\{ \mathrm{id}, O_{\frac{\pi}{2}}, O_\pi, O_{\frac{3\pi}{2}}, S_{l_1}, S_{l_2}, S_{l_3}, S_{l_4} \right\}.$$

Znowu wartości tych izometrii są wyznaczone na wierzchołkach $\{A, B, C, D\}$, czyli łatwo jest napisać tabelkę D_4.

Ogólne zasady

- Złożenie obrotu z obrotem jest obrotem.
- Złożenie symetrii osiowej z symetrią osiową jest obrotem.
- Złożenie obrotu z symetrią osiową (i odwrotnie) jest symetrią osiową.

Rozważmy jeszcze jedną grupę izometrii. Niech W będzie prostokątem nie będącym kwadratem:



Mamy:

$$K_4 := \mathrm{Izo}(W) = \{\mathrm{id}, O_\pi, S_{l_1}, S_{l_2}\}.$$

Napiszmy tabelkę K_4:

$\circ$	id	O_π	S_{l_1}	S_{l_2}
id	id	O_π	S_{l_1}	S_{l_2}
O_π	O_π	id	S_{l_2}	S_{l_1}
S_{l_1}	S_{l_1}	S_{l_2}	id	O_π
S_{l_2}	S_{l_2}	S_{l_1}	O_π	id

Grupę K_4 nazywamy *grupą Kleina*.

Chcemy teraz **porównywać** ze sobą grupy.

Przykład 2.8. Dwa przykłady przed ogólną definicją.

(1) Rozważmy funkcję n-tej reszty:

$$r_n : \mathbb{Z} \to \mathbb{Z}_n.$$

Dla dowolnych $a, b \in \mathbb{Z}$ mamy:

$$n|(a - r_n(a)), \quad n|(b - r_n(b)) \qquad \Rightarrow \qquad n|\left[a + b - (r_n(a) - r_n(b))\right].$$

Czyli dostajemy:

$$r_n(a + b) = r_n\left(r_n(a) + r_n(b)\right) = r_n(a) +_n r_n(b),$$

czyli funkcja r_n **przenosi** działanie z grupy $(\mathbb{Z}, +)$ na działanie w grupie $(\mathbb{Z}_n, +_n)$.

(2) Ponumerujmy wierzchołki kwadratu przez zbiór $\{1,2,3,4\}$. Definiujemy następującą funkcję:

$$\Psi : D_4 \to S_4, \qquad \Psi(f) = f|_{\{1,2,3,4\}},$$

gdzie $f|_{\{1,2,3,4\}}$ to **obcięcie** funkcji f do zbioru wierzchołków $\{1,2,3,4\}$. Wtedy dla każdych $f, g \in D_4$ mamy:

$$\Psi(f \circ g) = \Psi(f) \circ \Psi(g),$$

gdzie pierwsze „$\circ$" to składanie izometrii (działanie w grupie D_4), a drugie „$\circ$" to składanie permutacji (działanie w grupie S_4).

Definicja 2.9. Niech $(G, \cdot), (H, *)$ będą grupami i $f : G \to H$.

(1) Funkcja f jest *homomorfizmem*, gdy:

$$\forall\, g_1, g_2 \in G \qquad f(g_1 \cdot g_2) = f(g_1) * f(g_2).$$

(2) Funkcja f jest *izomorfizmem*, gdy f jest homomorfizmem i jest bijekcją.

Przykład 2.10. (1) Funkcja n-tej reszty:

$$r_n : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +_n)$$

jest homomorfizmem.

(2) Uogólniając homomorfizm obcięcia $\Psi : D_4 \to S_4$, dla każdego $n \geqslant 3$ mamy:

$$\Psi_n : D_n \to S_n$$

funkcję obcięcia izometrii n-kąta foremnego do zbioru wierzchołków $\{1, 2, \ldots, n\}$. Ponieważ każda izometria z D_n jest wyznaczona przez wartości na wierzchołkach, funkcja Ψ_n jest „1-1". Mamy:

$$|D_n| = 2n, \quad |S_n| = n! \qquad \Rightarrow \qquad |D_3| = 6 = |S_3|,$$

tak więc funkcja $\Psi_3 : D_3 \to S_3$ jest izomorfizmem.

(3) Rozważmy funkcję:

$$f : \mathbb{R} \to \mathbb{R}_{>0}, \qquad f(x) = 2^x.$$

Łatwo zauważyć, że $\mathbb{R}_{>0} \leqslant (\mathbb{R} \setminus \{0\}, \cdot)$, czyli $(\mathbb{R}_{>0}, \cdot)$ jest grupą. Mamy:

$$\forall\, x, y \in \mathbb{R} \qquad f(x + y) = 2^{x+y} = 2^x 2^y = f(x)f(y).$$

Czyli funkcja f jest homomorfizmem z grupy $(\mathbb{R}, +)$ w grupę $(\mathbb{R}_{>0}, \cdot)$. Funkcja f jest też bijekcją, czyli jest izomorfizmem.

Uwaga 2.11. Jeśli $f : (G, \cdot) \to (H, *)$ jest izomorfizmem, to działanie $*$ jest działaniem indukowanym przez działanie $\cdot$ poprzez funkcję f. Stąd algebraiczne własności działań $\cdot$ i $*$ są takie same.

Definicja 2.12. Jeśli dla grup $(G, \cdot), (H, *)$ istnieje izomorfizm

$$f : (G, \cdot) \to (H, *),$$

to mówimy, że grupy $(G, \cdot)$ i $(H, *)$ są *izomorficzne*, co oznaczamy $(G, \cdot) \cong (H, *)$ lub po prostu $G \cong H$.

Uwaga 2.13. Z Uwagi 2.11 grupy izomorficzne mają te same własności algebraiczne, np. jeśli $G \cong H$ i G jest przemienna, to H jest też przemienna.

Przykład 2.14. (1) Wiemy, że

$$D_3 \cong S_3.$$

(2) Łatwo zauważyć, że

$$S_2 \cong \mathbb{Z}_2$$

i że izomorfizmem jest funkcja:

$$S_2 \to \mathbb{Z}_2, \qquad \mathrm{id} \mapsto 0, \quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \mapsto 1,$$

co wynika np. z porównania tabelek:

$\circ$	id	σ
id	id	σ
σ	σ	id

$+_2$	0	1
0	0	1
1	1	0

(3) Wiemy też, że:

$$(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot).$$

Ten ostatni izomorfizm „przenosi dodawanie na mnożenie". Ale dodawanie jest łatwiejsze niż mnożenie! Stąd wzięła się idea działania **suwaka logarytmicznego**, gdzie dzięki dodawaniu (przesuwaniu) możemy też mnożyć używając odpowiedniej skali logarytmicznej, która odpowiada powyższemu izomorfizmowi.

Zacznijmy od opisu dwóch konkretnych sytuacji.

Przykład 3.1. (1) Niech:

$$\{0, 2, 4, 6\} \leqslant \mathbb{Z}_8$$

to będą wszystkie **wielokrotności** 2 w grupie $(\mathbb{Z}_8, +_8)$. Grupa $\mathbb{Z}_8$ jest skończona, więc jest skończenie wiele tych wielokrotności:

$$2, \quad 2 +_8 2 = 4, \quad 2 +_8 2 +_8 2 = 6, \quad 2 +_8 2 +_8 2 +_8 2 = 0.$$

(2) Niech:

$$3\,\mathbb{Z} := \{\ldots, -6, -3, 0, 3, 6, \ldots\} = \{3k \mid k \in \mathbb{Z}\}$$

to będą wszystkie wielokrotności 3 w grupie $(\mathbb{Z}, +)$. Też mamy:

$$3\,\mathbb{Z} \leqslant \mathbb{Z}\,.$$

Uogólnimy te przykłady na przypadek dowolnej grupy.

Twierdzenie 3.2. *Niech G będzie grupą i $g \in G$. Wtedy podzbiór*

$$\{g^n \mid n \in \mathbb{Z}\} \subseteq G$$

jest najmniejszą podgrupą G zawierającą element g.

Dowód. Używamy własności potęgowania w grupach (Twierdzenie 2.3).

Pokażemy najpierw, że:

$$\{g^n \mid n \in \mathbb{Z}\} \leqslant G.$$

(i) Dla każdych $i, j \in \mathbb{Z}$ mamy:

$$g^i g^j = g^{i+j} \in \{g^n \mid n \in \mathbb{Z}\},$$

czyli zbiór $\{g^n \mid n \in \mathbb{Z}\}$ jest zamknięty na działanie z grupy G.

(ii) $e = g^0 \in \{g^n \mid n \in \mathbb{Z}\}$, czyli element neutralny należy do naszego podzbioru.

(iii) Dla dowolnego $g^m \in \{g^n \mid n \in \mathbb{Z}\}$ mamy:

$$(g^m)^{-1} = g^{-m} \in \{g^n \mid n \in \mathbb{Z}\}.$$

Stąd faktycznie $\{g^n \mid n \in \mathbb{Z}\} \leqslant G$.

Pokazujemy teraz „najmniejszość" $\{g^n \mid n \in \mathbb{Z}\} \leqslant G$.
Weźmy dowolną $H \leqslant G$, taką że $g \in H$. Mamy pokazać, że:

$$\{g^n \mid n \in \mathbb{Z}\} \subseteq H.$$

Rozważamy trzy przypadki.
Jeśli $\underline{n > 0}$, to:

$$g^n := \underbrace{g \cdot \ldots \cdot g}_{n \text{ razy}} \in H,$$

ponieważ $g \in H$ i H jest podgrupą G.
Jeśli $\underline{n = 0}$, to $g^0 = e \in H$.
Jeśli $\underline{n < 0}$, to:

$$g^n := \left(g^{-n}\right)^{-1} \in H,$$

ponieważ $-n > 0$, tak więc z rozważonego powyżej przypadku mamy $g^{-n} \in H$ i wtedy (ponieważ $H \leqslant G$) dostajemy $(g^{-n})^{-1} \in H$. □

Definicja 3.3. Niech G będzie grupą i $g \in G$.

(1) Definiujemy:

$$\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}.$$

(2) Grupę G nazywamy *cykliczną*, gdy istnieje $g \in G$, takie że $G = \langle g \rangle$.

Przykład 3.4. (1) Niech $G = S_3$ i $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Wtedy:

$$\left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\rangle = \left\{ \mathrm{id}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

(2) Niech $G = \mathbb{Z}$ i $g = 3$. Wtedy:

$$\langle 3 \rangle = 3\,\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\}.$$

(3) Niech $G = \mathbb{Z}_8$ i $g = 2$. Wtedy:

$$\langle 2 \rangle = \{0, 2, 4, 6\}.$$

(4) Niech $G = \mathbb{Z}_n$ i $g = 1$. Wtedy:

$$\langle 1 \rangle = \mathbb{Z}_n\,.$$

Czyli grupa $\mathbb{Z}_n$ jest cykliczna.

(5) Niech $G = \mathbb{Z}$ i $g = 1$. Wtedy:

$$\langle 1 \rangle = \mathbb{Z}\,.$$

Czyli grupa $\mathbb{Z}$ jest cykliczna.

Zobaczymy teraz, że $\mathbb{Z}_n$ i $\mathbb{Z}$ to **jedyne** grupy cykliczne z dokładnością do izomorfizmu. Potrzebny nam jest następujący pomocniczy wynik.

Lemat 3.5. *Niech G będzie grupą, $g \in G$ i załóżmy, że $G = \langle g \rangle$ (czyli G jest cykliczna). Jeśli dla pewnego $k > 0$ mamy $g^k = e$, to wtedy $|G| \leqslant k$.*

Dowód. Wystarczy pokazać, że:

$$\langle g \rangle \subseteq \{g^0, g^1, \ldots, g^{k-1}\}$$

(przy założeniu $g^k = e$). Weźmy dowolny element $g^m \in \langle g \rangle$ ($m \in \mathbb{Z}$). Dzielimy z resztą m przez k i dostajemy $l \in \mathbb{Z}, r = r_k(m) \in \mathbb{Z}_k$, takie że:

$$m = kl + r.$$

Wtedy otrzymujemy:

$$g^m = g^{kl+r} = g^{lk} g^r = \left(g^k\right)^l g^r = e^l g^r = e g^r = g^r.$$

Ponieważ $r \in \mathbb{Z}_k = \{0, 1, \ldots, k-1\}$, dostajemy że:

$$g^m = g^r \in \{g^0, g^1, \ldots, g^{k-1}\},$$

co kończy dowód. □

Twierdzenie 3.6. *Załóżmy, że G jest grupą cykliczną. Wtedy mamy:*

(1) *jeśli G jest skończona, to $G \cong \mathbb{Z}_n$ dla pewnego $n > 0$;*
(2) *jeśli G jest nieskończona, to $G \cong \mathbb{Z}$.*

W szczególności, każda grupa cykliczna jest przemienna.

Dowód. Weźmy $g \in G$, takie że $G = \langle g \rangle$. Rozważamy dwa przypadki.

Przypadek 1: G jest skończona i $|G| = n$
Definiujemy funkcję:

$$f : \mathbb{Z}_n \to G, \qquad f(r) = g^r.$$

Udowodnimy w czterech krokach, że f jest izomorfizmem.
Krok 1: f jest „1-1"
Weźmy $i, j \in \mathbb{Z}_n$, takie że $i < j$ i załóżmy nie wprost, że $f(i) = f(j)$. Dojdziemy do sprzeczności. Mamy:

$$g^i = f(i) = f(j) = g^j.$$

Mnożąc tę równość obustronnie przez g^{-i} otrzymujemy:

$$e = g^0 = g^j g^{-i} = g^{j-i}.$$

Ale $0 < j - i < n$ oraz $G = \langle g \rangle$, tak więc z Lematu 3.5 otrzymujemy:

$$|G| \leqslant j - i < n,$$

sprzeczność, ponieważ $|G| = n$.

Krok 2: f jest „na"

f jest różnowartościową (Krok 1) funkcją ze zbioru n-elementowego w zbiór n-elementowy, tak więc f jest na, bo n jest skończone.

Krok 3: $g^n = e$

Z Kroku 2, mamy:

$$G = \{g^0, g^1, \ldots, g^{n-1}\},$$

tak więc istnieje $r \in \mathbb{Z}_n$, takie że $g^n = g^r$. Jeśli $r > 0$, to postępując jak w Kroku 1, otrzymujemy $g^{n-r} = 0$ i znowu z Lematu 3.5 mamy:

$$|G| \leqslant n - r < n,$$

sprzeczność.

Krok 4: f jest homomorfizmem

Weźmy $i, j \in \mathbb{Z}_n$. Wtedy istnieje $l \in \mathbb{Z}$, taki że:

$$i +_n j = r_n(i + j) = i + j + ln.$$

Liczymy:

$$f(i +_n j) = g^{i+_n j} = g^{i+j+ln} = g^i g^j (g^n)^l = g^i g^j e^l = g^i g^j e = g^i g^j = f(i)f(j),$$

gdzie czwarta równość wynika z Kroku 3.

Z Kroków 1–4 otrzymujemy, że f jest izomorfizmem.

Przypadek 2: G jest nieskończona

Ten przypadek jest znacznie łatwiejszy. Definiujemy funkcję:

$$f : \mathbb{Z} \to G, \qquad f(i) = g^i.$$

Udowodnimy, że f jest izomorfizmem.

Ponieważ

$$G = \langle g \rangle = \{g^i \mid i \in \mathbb{Z}\},$$

tak więc f jest „na".

Łatwo pokazujemy, że f jest homomorfizmem:

$$\forall\, i, j \in \mathbb{Z} \qquad f(i + j) = g^{i+j} = g^i g^j = f(i)f(j).$$

Pozostaje pokazać, że f jest „1-1". Weźmy $i, j \in \mathbb{Z}$, takie że $i < j$. Jeśli $f(i) = f(j)$, to tak jak w dowodzie Przypadku 1, dostajemy że $g^{j-i} = e$, czyli z Lematu 3.5, $|G| \leqslant j - i$ jest skończona, sprzeczność. □

Uwaga 3.7. Zauważmy, że z dowodu Twierdzenia 3.6, wynika że (G to grupa cykliczna):

(1) jeśli G jest skończona i $|G| = n$, to n jest **najmniejszą** liczbą dodatnią, taką że $g^n = e$;
(2) jeśli G jest nieskończona, to dla każdej $n > 0$ mamy $g^n \neq e$.

Definicja 3.8. Niech G będzie grupą i $g \in G$. Definiujemy *rząd* g, oznaczany $\mathrm{ord}_G(g)$, jako najmniejsze $n > 0$, takie że $g^n = e$. Jeśli takie $n > 0$ nie istnieje, to definiujemy $\mathrm{ord}_G(g) := \infty$.

Często piszemy „ord(g)" zamiast „ord$_G(g)$".

Z Uwagi 3.7 natychmiast wynika następujące:

Twierdzenie 3.9. *Jeśli G jest grupą i $g \in G$, to wtedy mamy:*

$$\mathrm{ord}_G(g) = |\langle g \rangle|,$$

czyli rząd elementu g, to moc najmniejszej podgrupy zawierającej g.

Wniosek 3.10. *Jeśli grupa G jest skończona i $g \in G$, to rząd g jest też skończony. Niedługo zobaczymy, że:*

$$\mathrm{ord}_G(g) \quad \textit{dzieli} \quad |G|.$$

Uwaga 3.11. Twierdzenie 3.9 mówi, że **rząd elementu** g to **moc grupy** $\langle g \rangle$. Dlatego też często na moc dowolnej grupy G mówi się *rząd* G.

Przykład 3.12. (1) Mamy $\mathrm{ord}_{\mathbb{Z}_8}(2) = 4$, ponieważ:

$$2 +_8 2 = 4 \neq 0, \quad 2 +_8 2 +_8 2 = 6 \neq 0, \quad 2 +_8 2 +_8 2 +_8 2 = 0.$$

Mamy też:

$$\underbrace{2 +_8 2 +_8 \cdots +_8 2}_{8 \text{ razy}} = 0,$$

ale $\mathrm{ord}_{\mathbb{Z}_8}(2) \neq 8$ (uwaga, to częsty błąd!), bo 8 **nie jest najmniejszą** $n > 0$, taką że:

$$\underbrace{2 +_8 2 +_8 \cdots +_8 2}_{n \text{ razy}} = 0.$$

(2) Mamy:

$$\mathrm{ord}_{S_2} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = 2.$$

(3) Mamy:

$$\mathrm{ord}_{S_3} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = 3.$$

(4) Mamy:

$$\mathrm{ord}_{\mathbb{Z}}(1) = \infty,$$

a nawet:

$$\forall\, k \in \mathbb{Z} \setminus \{0\} \qquad \mathrm{ord}_{\mathbb{Z}}(k) = \infty.$$

(5) Mamy:

$$\mathrm{ord}_{\mathbb{Z}_n}(1) = n.$$

(6) Jeśli G jest grupą i $g \in G$, to wtedy:

$$\mathrm{ord}(g) = 1 \qquad \Leftrightarrow \qquad g = e.$$

Teraz pokrótce omówimy sytuację, gdy zamiast $\{g\}$ mamy dowolny podzbiór A grupy G.

Definicja 3.13. Niech G będzie grupą i $A \subseteq G$. Wtedy $\langle A \rangle$ oznacza najmniejszą podgrupę G zawierającą A. Jeśli $\langle A \rangle = G$, to mówimy że G jest *generowana* przez A, lub że A jest zbiorem *generatorów* G. Dla $a_1, \ldots, a_n \in G$, zamiast $\langle \{g_1, \ldots, g_n\} \rangle$ piszemy $\langle g_1, \ldots, g_n \rangle$.

Pomijamy dowód następnego twierdzenia.

Twierdzenie 3.14. *Niech A, G będą jak wyżej oraz $g \in G$. Wtedy $g \in \langle A \rangle$ wtedy i tylko wtedy, gdy:*

$$\exists a_1, \ldots a_n \in A \;\; \exists k_1, \ldots k_n \in \mathbb{Z} \qquad g = a_1^{k_1} \ldots a_n^{k_n}.$$

Przykład 3.15. (1) Mamy:

$$D_3 = \left\langle O_{\frac{2\pi}{3}}, S \right\rangle,$$

gdzie S jest dowolną symetrią osiową z D_3, ponieważ:

$$O_{\frac{2\pi}{3}} \circ O_{\frac{2\pi}{3}} = O_{\frac{4\pi}{3}}, \quad O_{\frac{2\pi}{3}} \circ S = S', \quad S \circ O_{\frac{2\pi}{3}} = S'',$$

gdzie S', S'' to dwie pozostałe symetrie osiowe z D_3.

(2) Podobnie mamy dla dowolnego $n \geqslant 3$:

$$D_n = \left\langle O_{\frac{2\pi}{n}}, S \right\rangle.$$

(3) Można, pokazać że:

$$\forall\, k_1, l_1, \ldots, k_n, l_n \in \mathbb{Z}\setminus\{0\} \qquad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{k_1} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{l_1} \cdots \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{k_n} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{l_n} \neq I.$$

Czyli potrzeba wszystkich tego typu iloczynów aby dostać:

$$\left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right\rangle < \mathrm{GL}_2(\mathbb{R}).$$

Grupy permutacji

Chcemy opisać każdą permutację za pomocą pewnych prostych permutacji.

Przykład 3.16. (1) Niech:

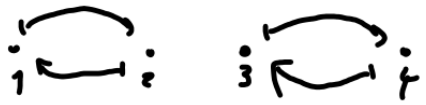
$$\sigma \in S_5, \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix}$$

Powiemy, że σ jest **cyklem** (definicja później).

(2) Niech:

$$\tau \in S_4, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Tutaj τ **nie jest cyklem**.



Aby zdefiniować pojęcie cyklu, musimy najpierw zdefiniować pojęcie **nośnika** permutacji, czyli zbioru tych "istotnych" punktów.

Definicja 3.17. Niech $\sigma \in S_n$. Wtedy *nośnik* σ to:

$$X_\sigma := \{i \in \{1, 2, \ldots, n\} \mid \sigma(i) \neq i\}.$$

W Przykładzie 3.16(1) mamy:

$$X_\sigma = \{1, 2, 3, 5\} \quad (n = 5).$$

W Przykładzie 3.16(2) mamy:

$$X_\tau = \{1, 2, 3, 4\} \quad (n = 4).$$

Definicja 3.18. (1) Niech $\sigma \in S_n$. Mówimy, że σ jest *cyklem długości* k, gdy $|X_\sigma| = k$ oraz możemy przedstawić:

$$X_\sigma = \{i_1, i_2, \ldots, i_k\},$$

tak że:

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

Taki cykl zapisujemy:

$$\sigma = (i_1, i_2, \ldots, i_k).$$

(2) Cykl długości 2 nazywamy *transpozycją*.

Uwaga 3.19. Zapis z Definicji 3.18(1) **nie** jest jednoznaczny, np. mamy:

$$(1, 2) = (2, 1).$$

Przykład 3.20. Mamy:

$$S_2 = \{\mathrm{id}, (1, 2)\}, \quad S_3 = \{\mathrm{id}, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}.$$

Czyli grupy S_2 i S_3 składają się z samych cykli! Ale wiemy, że np.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \in S_4$$

nie jest cyklem. Zauważmy, że:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1, 2) \circ (3, 4),$$

czyli ta permutacja jest złożeniem „rozłącznych" cykli.

Definicja 3.21. Niech $\sigma, \tau \in S_n$. Powiemy, że σ i τ są *rozłączne*, gdy:

$$X_\sigma \cap X_\tau = \emptyset,$$

czyli gdy nośniki σ i τ są rozłączne.

Przykład 3.22. Permutacje $(1, 2)$ i $(3, 4)$ są rozłączne. Zauważmy, że:

$$(1, 2) \circ (3, 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (3, 4) \circ (1, 2).$$

Poniżej uogólniamy obserwację z Przykładu 3.22.

Twierdzenie 3.23. *Jeśli $\sigma, \tau \in S_n$ są rozłączne, to mamy:*

$$\sigma \circ \tau = \tau \circ \sigma.$$

Dowód. Weźmy dowolne $i \in \{1, 2, \ldots, n\}$. Mamy pokazać, że:

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

Będziemy korzystali z łatwej do sprawdzenia obserwacji, że $\sigma(X_\sigma) = X_\sigma$ (czyli też $\sigma(X_\tau) = X_\tau$). Rozważamy 3 przypadki.

Przypadek 1: $\underline{i \in X_\sigma}$
Pokażemy, że:

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

Z rozłączności σ i τ dostajemy $i \notin X_\tau$, stąd $\tau(i) = i$, czyli mamy:

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

Ponieważ $i \in X_\sigma$, tak więc z powyższej obserwacji mamy $\sigma(i) \in X_\sigma$. Z rozłączności σ i τ dostajemy $\sigma(i) \notin X_\tau$. Czyli mamy:

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

Przypadek 2: $\underline{i \in X_\tau}$
Podobnie jak Przypadku 1 pokazuje się:

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

Przypadek 3: $\underline{i \notin X_\sigma \cup X_\tau}$
Podobnie jak Przypadkach 1 i 2 pokazuje się:

$$\sigma(\tau(i)) = i = \tau(\sigma(i)),$$

co kończy dowód. □

Przykład 3.24. Obliczenia na permutacjach.

(1) Weźmy:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}.$$

To jest zapis w postaci **tabularycznej** bądź **dwuwierszowej**.

(2) Mamy też zapis w postaci **iloczynu cykli rozłącznych**

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = (1,2,3) \circ (4,5),$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix} = (1,2) \circ (3,5).$$

(3) **Mnożenie permutacji**.

(a) W **postaci tabularycznej**:

$$\sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 3 & 4 \end{pmatrix},$$

$$1 \overset{\sigma_1}{\longmapsto} 2 \overset{\sigma_2}{\longmapsto} 1, \quad 2 \overset{\sigma_1}{\longmapsto} 3 \overset{\sigma_2}{\longmapsto} 5, \quad 3 \overset{\sigma_1}{\longmapsto} 1 \overset{\sigma_2}{\longmapsto} 2, \quad 4 \overset{\sigma_1}{\longmapsto} 5 \overset{\sigma_2}{\longmapsto} 3, \quad 5 \overset{\sigma_1}{\longmapsto} 4 \overset{\sigma_2}{\longmapsto} 4,$$

(b) Jako **iloczyny cykli rozłącznych**:

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

Oba wyniki się zgadzają:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 3 & 4 \end{pmatrix} = (2,5,4,3).$$

(4) **Permutacje odwrotne**.

(a) W **postaci tabularycznej** (pierwsza równość to „zamiana wierszy" a druga to „przestawienie"):

$$\sigma_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 3 & 1 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}.$$

(b) Jako **iloczyny cykli rozłącznych**:
Ogólnie dla cykli mamy:

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

Poza tym poniżej korzystamy z przemienności cykli rozłącznych:

$$\sigma_1^{-1} = ((1,2,3)(4,5))^{-1} = (1,2,3)^{-1}(4,5)^{-1} = (3,2,1)(5,4) = (1,3,2)(4,5).$$

Oba wyniki się zgadzają:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} = (1,3,2)(4,5).$$

(5) Podnoszenie do potęg.
Jest zdecydowanie łatwiej podnosić do potęg przy zapisie w postaci **iloczynu cykli rozłącznych**, np. (ponownie korzystamy z przemienności cykli rozłącznych):

$$\sigma_1^{10} = ((1,2,3)(4,5))^{10} = (1,2,3)^{10}(4,5)^{10} = (1,2,3).$$

Zauważmy tutaj, że transpozycja (cykl długości 2) ma rząd 2, cykl długości 3 ma rząd 3 i ogólnie cykl długości k ma rząd k.

Aby używać Przykładu 3.24 potrzebujemy następującego wyniku.

Twierdzenie 3.25. *Każda permutacja ma przedstawienie w postaci iloczynu cykli rozłącznych.*

Idea dowodu. Weźmy $\sigma \in S_n$ i dowolny $i \in X_\sigma$. Patrzymy na cykl:

$$\tau := \left(i, \sigma(i), \sigma^2(i), \ldots, \sigma^{k-1}(i)\right),$$

gdzie

$$k := \min\{n \mid \sigma^n(i) = i\}.$$

Jeśli $\sigma = \tau$, to twierdzenie jest już udowodnione. Jeśli nie, to bierzemy $j \in X_\sigma \setminus X_\tau$ i tworzymy kolejny cykl (rozłączny z τ) postaci:

$$\tau' := \left(j, \sigma(j), \sigma^2(j), \ldots, \sigma^{l-1}(i)\right).$$

Jeśli $\sigma = \tau \circ \tau'$, to twierdzenie jest udowodnione. Jeśli nie, to kontynuujemy... □

Twierdzenie 3.26. *Każdy cykl rozkłada się na iloczyn transpozycji.*

Dowód. Mamy:

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

□

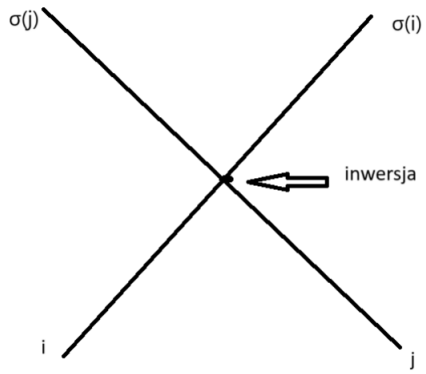
Z ostatnich dwóch twierdzeń natychmiast wynika:

Wniosek 3.27. *Każda permutacja rozkłada się na iloczyn transpozycji.*

Pozostały nam do omówienia ostatnie pojęcia dotyczące permutacji.

Definicja 3.28. Niech $\sigma \in S_n$ oraz $1 \leqslant i < j \leqslant n$.

(1) Parę (i, j) nazywamy *inwersją* σ, gdy $\sigma(i) > \sigma(j)$.

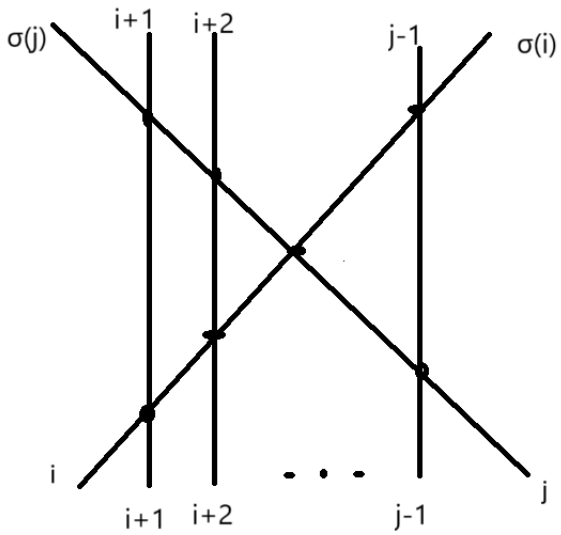


(2) *Znak* permutacji σ, oznaczany $\operatorname{sgn}(\sigma)$, to:

$$\operatorname{sgn}(\sigma) := (-1)^{\text{liczba inwersji } \sigma}.$$

(3) Mówimy, że σ jest *parzysta*, gdy $\operatorname{sgn}(\sigma) = 1$, tzn. σ ma parzyście wiele inwersji.
(4) Mówimy, że σ jest *nieparzysta*, gdy $\operatorname{sgn}(\sigma) = -1$, tzn. σ ma nieparzyście wiele inwersji.

Fakt 3.29. *Jeśli σ jest transpozycją, to σ jest nieparzysta.*



Dowód. Niech $\sigma = (i, j)$, gdzie $i < j$ oraz niech $r := j - i - 1$. Powyższy rysunek pokazuje, że σ ma $2r + 1$ inwersji, czyli nieparzyście wiele. □

Pomijamy dowód następnego wyniku.

Twierdzenie 3.30. *Dla dowolnych $\sigma, \tau \in S_n$ mamy:*

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

Z Faktu 3.29 i Twierdzenia 3.31 otrzymujemy:

Twierdzenie 3.31. *Dla dowolnej $\sigma \in S_n$ mamy, że σ jest parzysta wtedy i tylko wtedy, gdy w rozkładzie σ na transpozycje występuje parzyście wiele transpozycji.*

Z dowodu Twierdzenia 3.26 oraz z Twierdzenia 3.31 otrzymujemy:

Wniosek 3.32.
- *Cykl długości parzystej jest permutacją nieparzystą.*
- *Cykl długości nieparzystej jest permutacją parzystą.*

Uwaga 3.33. (1) Rozkład permutacji na cykle rozłączne jest **jednoznaczny** z dokładnością do permutacji czynników, np.:

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

(2) Rozkład permutacji na transpozycje jest **bardzo niejednoznaczny**, ale jednoznaczna jest (tylko) **parzystość** ilości transpozycji w rozkładzie, np.:

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

4. Warstwy, tw. Lagrange'a i zastosowania

Na początek kilka nazw.

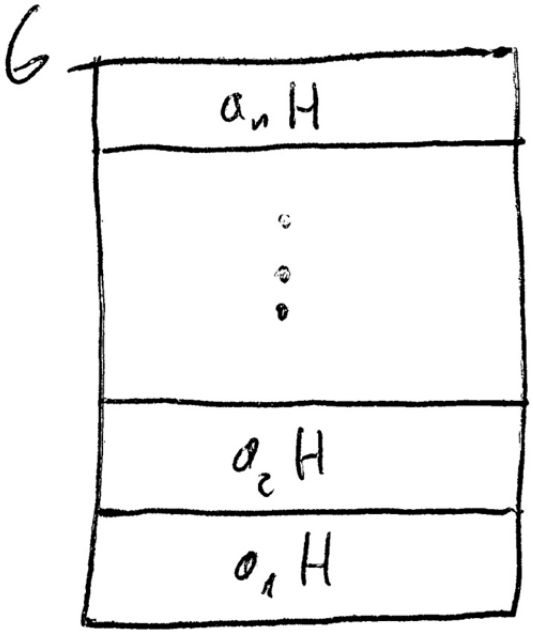
Definicja 4.1. (1) *Grupa trywialna* to grupa $G = \{e\}$ składająca się tylko z elementu neutralnego.
(2) Jeśli G to grupa, to podgrupę $\{e\} \leqslant G$ nazywamy *podgrupą trywialną*.
(3) Jeśli $A \subseteq B$ (A to podzbiór B), to podzbiór A jest *właściwy*, gdy $A \neq B$.
(4) Podobnie, jeśli $H \leqslant G$ (H to podgrupa G), to podgrupa H jest *właściwa*, gdy $H \neq G$.

Ustalmy grupę G i podgrupę $H \leqslant G$. Teraz ważne pojęcie, z którym często studenci mają kłopoty.

Definicja 4.2. Niech $a \in G$.
(1) Zbiór postaci:
$$aH := \{ah \mid h \in H\}$$
nazywamy *warstwą lewostronną* elementu a względem podgrupy H w grupie G.
(2) Zbiór postaci:
$$Ha := \{ha \mid h \in H\}$$
nazywamy *warstwą prawostronną* elementu a względem podgrupy H w grupie G.

Przykład 4.3. (1) $G = \mathbb{Z}$, $H = 3\,\mathbb{Z}$, $a = 1$.
Wtedy warstwy zapisujemy addytywnie:
$$1 + 3\,\mathbb{Z} = \{1 + 3k \mid k \in \mathbb{Z}\}.$$
Czyli powyższa warstwa lewostronna składa się z tych liczb całkowitych, które dają resztę 1 przy dzieleniu przez 3. Mamy też:
$$3\,\mathbb{Z} + 1 = \{3k + 1 \mid k \in \mathbb{Z}\} = \{1 + 3k \mid k \in \mathbb{Z}\} = 1 + 3\,\mathbb{Z}\,.$$
Czyli warstwa lewostronna 1 względem $3\,\mathbb{Z}$ w grupie $\mathbb{Z}$ pokrywa się z warstwą prawostronną 1 względem $3\,\mathbb{Z}$ w grupie $\mathbb{Z}$. Tak jest zawsze dla grup przemiennych.
Popatrzmy teraz na inne warstwy $3\,\mathbb{Z}$ w $\mathbb{Z}$:
$$0 + 3\,\mathbb{Z} = \{0 + 3k \mid k \in \mathbb{Z}\} = 3\,\mathbb{Z},$$
$$2 + 3\,\mathbb{Z} = \{2 + 3k \mid k \in \mathbb{Z}\}.$$
Czyli widzimy, że $\mathbb{Z}$ jest rozłączną sumą warstw podgrupy $3\,\mathbb{Z}$. Zobaczymy niedługo, że nie jest to przypadek.
(2) $G = \mathbb{Z}_{10}$, $H = \langle 2\rangle = \{0, 2, 4, 6, 8\}$, $a = 1$.
Wtedy mamy:
$$1 +_{10} \{0, 2, 4, 6, 8\} = \{1, 3, 5, 7, 9\}.$$
(3) $G = S_3$, $H = \langle (1,2)\rangle = \{\mathrm{id}, (1,2)\}$, $a = (1,3)$.
Wtedy mamy:
$$(1,3)\{\mathrm{id}, (1,2)\} = \{(1,3)\,\mathrm{id}, (1,3)(1,2)\} = \{(1,3), (1,2,3)\},$$
$$\{\mathrm{id}, (1,2)\}(1,3) = \{\mathrm{id}(1,3), (1,2)(1,3)\} = \{(1,3), (1,3,2)\}.$$
W tej sytuacji widzimy, że:
$$(1,3)\{\mathrm{id}, (1,2)\} \neq \{\mathrm{id}, (1,2)\}(1,3),$$
czyli warstwa lewostronna różni się od warstwy prawostronnej!

Dla $H \leqslant G$ właściwa intuicja jest wyrażona następującym rysunkiem (podobnie dla warstw prawostronnych):



Czyli G ma być rozłączną sumą warstw lewostronnych H oraz rozłączną sumą warstw prawostronnych H. Dążymy do pokazania, że ta intuicja jest właściwa cały czas zakładając $H \leqslant G$.

Twierdzenie 4.4. *Dowolne dwie warstwy lewostronne H w G są sobie równe lub są rozłączne. Analogicznie dla warstw prawostronnych.*

Dowód (dla warstw lewostronnych). Weźmy $a, b \in G$. Mamy pokazać, że

$$aH \cap bH = \emptyset \qquad \text{lub} \qquad aH = bH.$$

Załóżmy, że $aH \cap bH \neq \emptyset$. Pokażemy, że $aH = bH$. Ponieważ $aH \cap bH \neq \emptyset$, tak więc możemy wziąć $c \in aH \cap bH$. Wtedy istnieją $h_1, h_2 \in H$, takie że:

$$ah_1 = c = bh_2.$$

Pokazujemy teraz, że $aH = bH$.
Dla dowodu inkluzji „$\subseteq$”, weźmy dowolne $g \in aH$. Chcemy pokazać, że $g \in bH$. Ponieważ $g \in aH$, więc istnieje $h \in H$, takie że $g = ah$. Wtedy mamy:

$$g = ah = \underbrace{ah_1}_{c} h_1^{-1} h = \underbrace{bh_2}_{c} h_1^{-1} h \in bH,$$

bo $h_2 h_1^{-1} h \in H$ (ponieważ H jest podgrupą G).
Inkluzję „$\supseteq$” pokazujemy analogicznie zamieniając rolami a i b. □

Wniosek 4.5. *G jest sumą rozłączną warstw lewostronnych. Analogicznie dla warstw prawostronnych.*

Dowód. Ponieważ każdy $g \in G$ należy do pewnej warstwy H ($g \in gH$), tak więc dostajemy tezę dzięki Twierdzeniu 4.6. □

Musimy się teraz nauczyć rozpoznawać, czy dane dwie warstwy są równe czy też rozłączne. Służy temu następujący wynik.

Twierdzenie 4.6. *Załóżmy, że $a, b \in G$. Wtedy mamy:*

(1) $aH = bH \quad \Leftrightarrow \quad a^{-1}b \in H \quad \Leftrightarrow \quad b^{-1}a \in H;$
(2) $Ha = Hb \quad \Leftrightarrow \quad ab^{-1} \in H \quad \Leftrightarrow \quad ba^{-1} \in H.$

Dowód (tylko dla (1)*).* Z Twierdzenia 4.6 otrzymujemy (ponieważ $b \in bH$):

$$aH = bH \quad \Leftrightarrow \quad b \in aH \quad \Leftrightarrow \quad (\exists h \in H)\, b = ah \quad \Leftrightarrow \quad a^{-1}b \in H.$$

Z drugiej strony:

$$\forall\, g \in G \qquad\qquad g \in H \quad \Leftrightarrow \quad g^{-1} \in H,$$

czyli dla $g = a^{-1}b$ otrzymujemy:

$$a^{-1}b \in H \quad \Leftrightarrow \quad b^{-1}a = \left(a^{-1}b\right)^{-1} \in H,$$

co kończy dowód (1). □

Przykład 4.7. (1) Mamy:

$$1 + 3\,\mathbb{Z} = 4 + 3\,\mathbb{Z},$$

ponieważ:

$$4 - 1 = 3 \in 3\,\mathbb{Z}\,.$$

(2) Mamy:

$$1 + 3\,\mathbb{Z} \neq 2 + 3\,\mathbb{Z},$$

ponieważ:

$$2 - 1 = 1 \notin 3\,\mathbb{Z}\,.$$

Teraz idziemy krok dalej w abstrakcji.

Definicja 4.8. Niech G/H oznacza zbiór wszystkich warstw lewostronnych H w G:

$$G/H := \{gH \mid g \in G\},$$

czyli G/H to pewien **zbiór podzbiorów** G.

Podobnie $H\backslash G$ oznacza zbiór wszystkich warstw prawostronnych H w G:

$$H\backslash G := \{Hg \mid g \in G\}.$$

Będziemy się koncentrować na zbiorze G/H.

Przykład 4.9. (1) Mamy:

$$\mathbb{Z}\,/3\,\mathbb{Z} = \{\underbrace{0 + 3\,\mathbb{Z}}_{3\,\mathbb{Z}}, 1 + 3\,\mathbb{Z}, 2 + 3\,\mathbb{Z}\},$$

czyli są 3 warstwy.

(2) Mamy:

$$\mathbb{Z}_{10}\,/\{0,2,4,6,8\} = \{\{0,2,4,6,8\},\{1,3,5,7,9\}\},$$

czyli są 2 warstwy.

(3) Mamy:

$$S_3/\{\mathrm{id},(1,2)\} = \{\{\mathrm{id},(1,2)\},\{(1,3),(1,2,3)\},\{(2,3),(1,3,2)\}\},$$

czyli są 3 warstwy.

Czemu w ogóle rozważamy G/H? Idea: chcemy **wydzielić** G przez podgrupę H i dostać znowu grupę (to nie zawsze się uda, o czym niedługo). Podobnie jak mamy dwie liczby n oraz m i chcemy wydzielić n przez m i dostać $\frac{n}{m}$.

Na początek zauważmy:

Twierdzenie 4.10. *Mamy:*

$$|G/H| = |H\backslash G|,$$

czyli zbiór warstw lewostronnych H w G jest równoliczny ze zbiorem warstw prawostronnych H w G.

Szkic dowodu. Dla dowolnego podzbiorem $A \subseteq G$ definiujemy:

$$A^{-1} := \{a^{-1} \mid a \in A\}.$$

Wtedy dla $gH \in G/H$ mamy:

$$(gH)^{-1} = Hg^{-1} \in H\backslash G.$$

Definiujemy funkcję:

$$G/H \ni gH \mapsto (gH)^{-1} = Hg^{-1} \in H\backslash G$$

i łatwo zauważyć, że jest to bijekcja. □

Definicja 4.11. *Indeks H w G*, oznaczany $[G : H]$, to jest moc zbioru G/H (równoważnie moc zbioru $H\backslash G$) warstw lewostronnych H w G.

Zmierzamy do porównania: $|H|$, $|G|$ i $[G : H]$. Najpierw mamy następujące:

Twierdzenie 4.12. *Dla każdego $g \in G$ mamy:*

$$|gH| = |H| = |Hg|,$$

czyli wszystkie warstwy H w G są równoliczne.

Szkic dowodu. Mamy funkcję:

$$H \ni h \mapsto gh \in gH$$

i łatwo zauważyć, że jest to bijekcja. □

Możemy teraz udowodnić następujący, najważniejszy tutaj, wynik.

Twierdzenie 4.13 (Twierdzenie Lagrange'a)**.** *Niech G będzie grupą skończoną i $H \leqslant G$. Wtedy mamy:*

$$|G| = [G : H] \cdot |H|.$$

W szczególności dostajemy:

$$|H| \mid |G|, \qquad [G : H] \mid |G|.$$

Czyli:

- *rząd podgrupy dzieli rząd grupy;*
- *indeks podgrupy dzieli rząd grupy.*

Dowód. Niech $n := [G : H]$. Wiemy, że G jest rozłączną sumą warstw H (Wniosek 4.5), tak więc istnieją $a_1, a_2, \ldots, a_n \in G$, takie że:

$$G = a_1H \cup a_2H \cup \ldots \cup a_nH.$$

Wtedy dostajemy:

$$|G| = |a_1H| + |a_2H| + \ldots + |a_nH| = n \cdot |H| = [G : H] \cdot |H|,$$

gdzie pierwsza równość wynika z rozłączności warstw i druga równość wynika z Twierdzenia 4.12. □

Wniosek 4.14. *Niech G będzie grupą skończoną rzędu k i $a \in G$. Wtedy mamy:*

$$\mathrm{ord}(a) \mid k, \qquad a^k = e.$$

Czyli rząd elementu dzieli rząd grupy.

Dowód. Wiemy, że (Twierdzenie 3.9):

$$\mathrm{ord}(a) = |\langle a \rangle|,$$

czyli $\mathrm{ord}(a) \mid k$ z Twierdzenia Lagrange'a.

Na ćwiczeniach pokazujemy, że jeśli $\mathrm{ord}(a) \mid k$, to $a^k = e$ co daje drugą część dowodzonego wyniku. □

Potrzebujemy jeszcze jednej serii grup skończonych.

Definicja 4.15. Dla $n > 0$ definiujemy:

$$A_n := \{\sigma \in S_n \mid \sigma \text{ jest parzysta}\}.$$

Na ćwiczeniach pokazujemy, że:

$$A_n \leqslant S_n.$$

Zauważmy, że dla $n > 1$ mamy:

$$|A_n| = \frac{n!}{2},$$

czyli:

$$|A_3| = 3, \quad |A_4| = 12, \quad |A_5| = 60, \ldots$$

Uwaga 4.16. (1) Z Wniosku 4.14, wiemy że rząd elementu dzieli rząd grupy, czyli np. nie ma elementu rzędu 4 w S_3, bo

$$4 \nmid 6 = |S_3|.$$

Ale implikacja odwrotna nie jest prawdziwa, bo np.

$$4 \mid 4 = |K_4|,$$

ale w K_4 nie ma elementu rzędu 4.

(2) Z Twierdzenia Lagrange'a, wiemy że rząd podgrupy dzieli rząd grupy stąd też np. nie ma podgrupy rzędu 4 w S_3.

Ale implikacja odwrotna znowu nie jest prawdziwa, bo np.

$$6 \mid 12 = |A_4|,$$

ale można pokazać, że w A_4 nie ma podgrupy rzędu 6.

Zanim przejdziemy do zastosowań, poznamy jeszcze jedną serię przykładów grup. Dla $n \geqslant 2$, wiemy że $\cdot_n$ jest działaniem łącznym i przemiennym na $\mathbb{Z}_n$, które ma element neutralny 1, ale 0 nie ma elementu odwrotnego względem $\cdot_n$. Również np. 2 nie ma elementu odwrotnego względem $\cdot_4$. Definiujemy:

$$\mathbb{Z}_n^* := \{k \in \mathbb{Z}_n \mid \mathrm{NWD}(k, n) = 1\}.$$

Na ćwiczeniach pokazujemy, że $\cdot_n$ jest działaniem na $\mathbb{Z}_n^*$ i że $(\mathbb{Z}_n^*, \cdot_n)$ jest grupą przemienną. Jeśli p jest liczbą pierwszą, to oczywiście mamy:

$$\mathbb{Z}_p^* := \{1, 2, \ldots, p-1\}.$$

Możemy teraz udowodnić:

Twierdzenie 4.17 (Małe Twierdzenie Fermata)**.** *Załóżmy, że $a \in \mathbb{Z}$, p jest liczbą pierwszą i $p \nmid a$. Wtedy mamy:*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Dowód. Niech $r := r_p(a)$. Wtedy mamy:

$$a^{p-1} \equiv r^{p-1} \pmod{p}.$$

Czyli możemy przyjąć, że:

$$a = r \in \mathbb{Z}_p\,.$$

Ponieważ $p \nmid a$, tak więc $a \neq 0$, czyli $a \in \mathbb{Z}_p^*$.

Wiemy, że $|\,\mathbb{Z}_p^*\,| = p - 1$. Z Wniosku 4.14, dostajemy że:

$$\underbrace{a \cdot_p \ldots \cdot_p a}_{p-1 \text{ razy}} = 1 \qquad \text{w } \mathbb{Z}_p^*.$$

Czyli mamy:

$$\underbrace{a^{p-1}}_{\text{w } \mathbb{Z}} \equiv \underbrace{a \cdot_p \ldots \cdot_p a}_{p-1 \text{ razy}} \pmod{p} \equiv 1 \pmod{p},$$

co kończy dowód. □

Uwaga 4.18. Dzięki Małemu Twierdzeniu Fermata możemy łatwo liczyć reszty typu $r_p(n^m)$, gdzie p to liczba pierwsza i $m, n \in \mathbb{Z}$, ponieważ:

- n możemy zastąpić przez $r_p(n)$ (tu nic nie używamy);
- m możemy zastąpić przez $r_{p-1}(m)$ (tu używamy Małego Twierdzenia Fermata).

Przykład 4.19. Mamy:

$$r_{17}\left(172^{165}\right) = r_{17}\left(2^5\right),$$

ponieważ 17 jest liczbą pierwszą oraz:

$$r_{17}(172) = 2, \qquad r_{16}(165) = 5.$$

A potem liczymy:

$$r_{17}\left(172^{165}\right) = r_{17}\left(2^5\right) = r_{17}(32) = 15.$$

Zmierzamy do jeszcze jednego zastosowania w teorii liczb.

Twierdzenie 4.20 (Twierdzenie Wilsona)**.** *Jeśli p jest liczbą pierwszą, to mamy:*

$$(p-1)! \equiv -1 \pmod{p}.$$

Przed dowodem potrzebujemy dwóch lematów.

Lemat 4.21. *Niech $(A, +)$ (notacja addytywna!) będzie skończoną grupą przemienną. Uporządkujmy elementy A, w taki sposób że:*

$$A = \{a_1, \ldots, a_k, a_{k+1}, \ldots, a_n\},$$

gdzie $a_1, \ldots, a_k$ to wszystkie elementy $a \in A$, takie że $a + a = 0$. Wtedy mamy:

$$a_1 + \ldots + a_n = a_1 + \ldots + a_k.$$

Dowód. Mamy, że:

$$\forall\, a \in A \qquad a + a = 0 \quad \Leftrightarrow \quad a = -a.$$

Liczymy teraz:

$$a_1 + \ldots + a_n = \underbrace{a_1 + \ldots + a_k}_{a=-a} + \underbrace{a_{k+1} + \ldots + a_n}_{a\neq -a}.$$

Wtedy mamy:

$$a_{k+1} + \ldots + a_n = 0,$$

ponieważ dla każdego $a \in \{a_{k+1}, \ldots, a_n\}$ zachodzi:

$$a \neq -a \in \{a_{k+1}, \ldots, a_n\},$$

tak więc w powyższej sumie wszystkie elementy „kasują się nawzajem". □

Lemat 4.22. *Niech $p \geqslant 3$ będzie liczbą pierwszą. Wtedy $p - 1 \in \mathbb{Z}_p^*$ jest jedynym elementem rzędu 2 w $\mathbb{Z}_p^*$.*

Dowód. Ponieważ $p \geqslant 3$, tak więc mamy $p - 1 \neq 1$, czyli:

$$\mathrm{ord}_{\mathbb{Z}_p^*}(p-1) \geqslant 2.$$

Mamy też:

$$(p-1) \cdot_p (p-1) = r_p\left(p^2 - 2p + 1\right) = 1,$$

czyli faktycznie:

$$\mathrm{ord}_{\mathbb{Z}_p^*}(p-1) = 2.$$

Pozostaje pokazać, że $p-1$ jest **jedynym** elementem rzędu 2 w $\mathbb{Z}_p^*$. W tym celu weźmy $a \in \mathbb{Z}_p^*$, taki że $\mathrm{ord}_{\mathbb{Z}_p^*}(a) = 2$. Pokażemy, że $a = p - 1$. Mamy:

$$r_p\left(a^2\right) = a \cdot_p a = 1,$$

czyli:

$$p \mid a^2 - 1 = (a-1)(a+1).$$

Ponieważ $a \in \mathbb{Z}_p^* \setminus \{1\}$, dostajemy $1 \leqslant a - 1 < p$, czyli $p \nmid a - 1$. Stąd mamy:

- p to liczba pierwsza;
- $p \mid (a-1)(a+1)$;
- $p \nmid a-1$.

Z własności liczb pierwszych dostajemy, że $p \mid a+1$. Ale $0 < a+1 \leqslant p$, tak więc dostajemy, że $p = a+1$, czyli faktycznie $a = p-1$. □

Dowód Tw. Wilsona. Mamy pokazać, że:

$$(p-1)! \equiv -1 \pmod{p}.$$

Jest to prawda dla $p = 2$, załóżmy więc że $p \geqslant 3$.

Mamy, że:

$$(p-1)! \equiv 1 \cdot_p 2 \cdot_p 3 \cdot_p \ldots \cdot_p (p-1) \pmod{p},$$

gdzie po prawej stronie kongruencji jest produkt wszystkich elementów w skończonej grupie przemiennej $\mathbb{Z}_p^*$. Z Lematu 4.21 i Lematu 4.22 dostajemy:

$$(p-1)! \equiv p-1 \pmod{p} \equiv -1 \pmod{p},$$

bo $p-1$ to jedyny element rzędu 2 w grupie $\mathbb{Z}_p^*$. □

Uwaga 4.23. (1) Prawdziwa (i łatwa do pokazania) jest też implikacja przeciwna do tej w Twierdzeniu Wilsona, tzn. następujące stwierdzenie jest prawdziwe

$$\forall\, n \in \mathbb{N}_{>0} \quad (n-1)! \equiv -1 \pmod{n} \quad \Rightarrow \quad n \text{ jest liczbą pierwszą}$$

(2) Implikacja przeciwna do implikacji w Małym Twierdzeniu Fermata **nie jest prawdziwa**, tzn. jeśli sformułujemy Małe Twierdzenie Fermata jako:

$$p : \text{pierwsza} \quad \Rightarrow \quad (\forall a \in \mathbb{Z})\ a^p \equiv a \pmod{p},$$

to implikacja przeciwna nie jest prawdziwa, tzn. istnieją liczby złożone n, takie że dla każdego $a \in \mathbb{Z}$ mamy $a^n \equiv a \pmod{n}$. Liczby takie nazywają się **liczbami Carmichaela**. Najmniejszą liczbą Carmichaela jest 561. Dopiero w 1994 roku udowodniono, że istnieje nieskończenie wiele liczb Carmichaela.

Na początek trochę nazw.

Definicja 5.1. Niech $f : G \to H$ będzie homomorfizmem. Wtedy mówimy, że:

- f jest *monomorfizmem*, gdy f jest „1-1";
- f jest *epimorfizmem*, gdy f jest „na";
- f jest *endomorfizmem*, gdy $G = H$;
- f jest *automorfizmem*, gdy $G = H$ i f jest izomorfizmem.

Na ćwiczeniach udowadniamy następujący:

Fakt 5.2. *Niech G, H, N to będą grupy oraz*

$$\varphi : G \to H, \quad \psi : H \to N.$$

Wtedy mamy:

(1) *jeśli φ i ψ są homomorfizmami, to $\psi \circ \varphi$ jest też homomorfizmem;*
(2) *jeśli φ jest izomorfizmem, to $\varphi^{-1} : H \to G$ jest też izomorfizmem;*
(3) *mamy:*

$$G \cong G, \quad G \cong H \Leftrightarrow H \cong G, \quad G \cong H \text{ i } H \cong N \Rightarrow G \cong N.$$

Czyli $\cong$ „przypomina" relację równoważności.

Definicja 5.3. Niech G będzie grupą. Definiujemy:

$$\mathrm{Aut}(G) := \{\varphi \in S_G \mid \varphi \text{ jest automorfizmem}\}.$$

Na ćwiczeniach dowodzimy, że:

$$\mathrm{Aut}(G) \leqslant S_G,$$

czyli $\mathrm{Aut}(G)$ jest grupą z działaniem składania funkcji.

Przykład 5.4. (1) Na Konwersatorium pokazujemy, że dla każdego $k \in \mathbb{Z}$ funkcja:

$$\varphi_k : \mathbb{Z} \to \mathbb{Z}, \quad \varphi_k(x) = kx$$

jest endomorfizmem $\mathbb{Z}$ i że wszystkie endomorfizmy $\mathbb{Z}$ są tej postaci. Łatwo zauważyć, że:

$$\varphi_k \in \mathrm{Aut}(\mathbb{Z}) \quad \Leftrightarrow \quad k \in \{-1, 1\}.$$

Czyli mamy:

$$\mathrm{Aut}(\mathbb{Z}) = \{\underbrace{\varphi_1}_{\mathrm{id}}, \varphi_{-1}\}.$$

Łatwo napisać tabelkę $\mathrm{Aut}(\mathbb{Z})$:

$\circ$	φ_1	φ_{-1}
φ_1	φ_1	φ_{-1}
φ_{-1}	φ_{-1}	φ_1

czyli mamy:

$$\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2\,.$$

(2) Na Konwersatorium pokazujemy, że dla każdego $k \in \mathbb{Z}_n$ funkcja:

$$\varphi_k : \mathbb{Z}_n \to \mathbb{Z}_n, \quad \varphi_k(x) = k \cdot_n x$$

jest endomorfizmem $\mathbb{Z}_n$ i że wszystkie endomorfizmy $\mathbb{Z}_n$ są tej postaci. Wtedy mamy:

$$\varphi_k \in \mathrm{Aut}(\mathbb{Z}_n) \quad \Leftrightarrow \quad k \in \mathbb{Z}_n^*\,.$$

Poza tym:

$$\forall\, k, l \in \mathbb{Z}_n \qquad \varphi_k \circ \varphi_l = \varphi_{k \cdot_n l},$$

czyli funkcja:

$$\mathbb{Z}_n^* \ni k \mapsto \varphi_k \in \mathrm{Aut}(\mathbb{Z}_n)$$

jest izomorfizmem, stąd:

$$\mathrm{Aut}(\mathbb{Z}_n) \cong (\mathbb{Z}_n^*, \cdot_n)\,.$$

Dla przykładu, popatrzmy na sytuację gdy $n = 8$. Wtedy:

$$\mathrm{Aut}(\mathbb{Z}_8) \cong (\mathbb{Z}_8^*, \cdot_8)\,, \qquad \mathbb{Z}_8^* = \{1, 3, 5, 7\}.$$

Łatwo napisać tabelkę $\mathbb{Z}_8^*$:

$\cdot_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

czyli dostajemy (porównując powyższą tabelkę z tabelką grupy Kleina K_4):

$$K_4 \cong \mathbb{Z}_8^* \cong \mathrm{Aut}(\mathbb{Z}_8).$$

Teraz ważne twierdzenie o homomorfizmach i rzędach elementów.

Twierdzenie 5.5. *Niech $f : G \to H$ będzie homomorfizmem i $g \in G$. Wtedy mamy:*

(1) $f(e_G) = e_H$;
(2) $f\left(g^{-1}\right) = f(g)^{-1}$;
(3) *następujące uogólnienie* (1) *oraz* (2)*:*

$$\forall\, n \in \mathbb{Z} \qquad\qquad f\left(g^n\right) = f(g)^n;$$

(4) *jeśli f jest „1-1”, to:*

$$\mathrm{ord}_G(g) = \mathrm{ord}_H(f(g));$$

(5) *jeśli* $\mathrm{ord}_G(g)$ *jest skończony, to* $\mathrm{ord}_H(f(g))$ *jest skończony oraz:*

$$\mathrm{ord}_H(f(g)) \mid \mathrm{ord}_G(g).$$

Dowód. Punkty (3) i (4) są udowodnione na Konwersatorium. Dla dowodu (5), załóżmy że $\mathrm{ord}_G(g) = n$, tak więc $g^n = e_G$. Wtedy dostajemy:

$$f(g)^n \underbrace{=}_{(3)} f\left(g^n\right) = f\left(e_G\right) \underbrace{=}_{(1)} e_H.$$

Na Konwersatorium pokazujemy, że z $f(g)^n = e_H$ wynika:

$$\mathrm{ord}_H(f(g)) \mid n = \mathrm{ord}_G(g),$$

co kończy dowód. □

Historycznie, pojęcie grupy wzięło się z pojęcia **grupy przekształceń**, czyli (w naszej terminologii) podgrupy S_X dla pewnego zbioru X. Niedługo zobaczymy, że każdą grupę możemy traktować jako grupę przekształceń. Główny krok w tym kierunku to następujące:

Twierdzenie 5.6 (Twierdzenie Cayley'a)**.** *Dla dowolnej grupy G istnieje monomorfizm:*

$$\alpha : G \to S_G.$$

Szkic dowodu. Weźmy $g \in G$ i definiujemy:

$$F_g : G \to G, \qquad F_g(x) = gx.$$

Dla każdego $g \in G$ funkcja F_g jest bijekcją, ponieważ łatwo zauważyć, że:

$$(F_g)^{-1} = F_{g^{-1}}.$$

Możemy teraz zdefiniować naszą funkcję:

$$\alpha : G \to S_G, \qquad \alpha(g) = F_g.$$

Należy teraz sprawdzić, że:

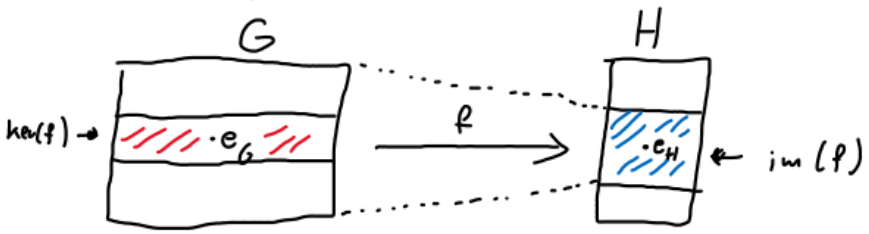
$$\forall\, g, h \in G \qquad\qquad F_{gh} = F_g \circ F_h,$$

czyli α jest homomorfizmem oraz że α jest „1-1” (co pomijamy). □

Definicja 5.7. Załóżmy, że $f : G \to H$ jest homomorfizmem. Definiujemy:

- *jądro* f jako:
$$\ker(f) := \{g \in G \mid f(g) = e_H\};$$
- *obraz* f jako:
$$\mathrm{im}(f) := \{f(g) \in H \mid g \in G\}.$$

Czyli $\ker(f) = f^{-1}(e_H)$ (przeciwobraz) oraz $\mathrm{im}(f) = f(G)$ (obraz).



Przykład 5.8. (1) Niech
$$r_5 : \mathbb{Z} \to \mathbb{Z}_5$$
będzie funkcją 5-tej reszty. Wtedy mamy:
$$\ker(r_5) = 5\,\mathbb{Z}, \qquad \mathrm{im}(f) = \mathbb{Z}_5\,.$$

(2) Niech
$$f : \mathbb{C} \to \mathbb{C}, \qquad f(x + yi) = x.$$
Wtedy mamy:
$$\ker(f) = \mathbb{R}\,i, \qquad \mathrm{im}(f) = \mathbb{R}\,.$$

Twierdzenie 5.9. *Załóżmy, że $f : G \to H$ jest homomorfizmem. Wtedy mamy:*

(1) $\mathrm{im}(f) \leqslant H$;
(2) *jeśli f jest monomorfizmem, to* $\mathrm{im}(f) \cong G$.

Dowód. Dla dowodu (1) sprawdzamy definicję bycia podgrupą.

(i) Używając Twierdzenia 5.5(1) mamy $e_H = f(e_G) \in \mathrm{im}(f)$.
(ii) Dla dowolnych $f(g_1), f(g_2) \in \mathrm{im}(f)$ mamy:
$$f(g_1)f(g_2) = f(g_1g_2) \in \mathrm{im}(f).$$
(iii) Jeśli $f(g) \in \mathrm{im}(f)$, to mamy (używając Twierdzenia 5.5(2)):
$$f(g)^{-1} = f\left(g^{-1}\right) \in \mathrm{im}(f).$$

Czyli dostaliśmy, że $\mathrm{im}(f) \leqslant H$.

Dla dowodu (2), z (1) mamy że $\mathrm{im}(f) \leqslant H$, czyli $\mathrm{im}(f)$ jest grupą. Jeśli f jest monomorfizmem, to wtedy funkcja
$$f : G \to \mathrm{im}(f)$$
jest izomorfizmem, czyli $\mathrm{im}(f) \cong G$. □

Wniosek 5.10. *Używając Twierdzenia 5.11 widzimy, że Twierdzenie Cayley'a mówi, że każda grupa G jest izomorficzna z pewną podgrupa grupy bijekcji S_G.*

Okazuje się, że jądro ma pewne dodatkowe własności, które zobaczymy poniżej.

Twierdzenie 5.11. *Załóżmy, że $f : G \to H$ jest homomorfizmem. Wtedy mamy:*

(1) $\ker(f) \leqslant G$;

(2) *dla dowolnego* $g \in G$ *mamy:*

$$g\ker(f) = \ker(f)g,$$

czyli warstwy lewostronne $\ker(f)$ *pokrywają się z warstwami prawostronnymi* $\ker(f)$.

Dowód. Dla dowodu (1) sprawdzamy definicję bycia podgrupą.

(i) Używając Twierdzenia 5.5(1) mamy $f(e_G) = e_H$, tak więc $e_G \in \ker(f)$.

(ii) Dla dowolnych $a, b \in \ker(f)$ mamy $f(a) = f(b) = e_H$, tak więc:

$$f(ab) = f(a)f(b) = e_H e_H = e_H,$$

czyli $ab \in \ker(f)$.

(iii) Jeśli $a \in \ker(f)$, to $f(a) = e_H$, stąd (używając Twierdzenia 5.5(2)) mamy :

$$f\left(a^{-1}\right) = f(a)^{-1} = e_H^{-1} = e_H,$$

tak więc $a^{-1} \in \ker(f)$.

Czyli dostaliśmy, że $\ker(f) \leqslant H$.

Dla dowodu (2) weźmy $g \in G$. Pokażemy, że:

$$g\ker(f) = \ker(f)g.$$

„$\subseteq$" Weźmy dowolne $a \in g\ker(f)$. Używając Twierdzenia 4.6 dostajemy $g^{-1}a \in \ker(f)$, tzn. $f(g^{-1}a) = e_H$. Liczymy teraz:

$$f\left(ag^{-1}\right) = f(\underbrace{gg^{-1}}_{e_G} ag^{-1}) = f(g)f\left(g^{-1}a\right) f\left(g^{-1}\right) = f(g)e_H f\left(g^{-1}\right) = e_H.$$

Stąd $ag^{-1} \in \ker(f)$, czyli (używając znowu Twierdzenia 4.6) dostajemy $a \in \ker(f)g$, tak więc:

$$g\ker(f) \subseteq \ker(f)g.$$

„$\supseteq$" Analogicznie. □

Powyższe własności jądra motywują następującą definicję.

Definicja 5.12. Podgrupę $N \leqslant G$ nazywamy *dzielnikiem normalnym* (lub *podgrupą normalną*), co oznaczamy $N \trianglelefteqslant G$, gdy:

$$\forall\, g \in G \qquad\qquad gN = Ng;$$

Intuicyjnie: dzielniki normalne to te podgrupy przez które możemy wydzielać, o czym będzie mowa wkrótce.

Przykład 5.13. Niech G będzie grupą i $H \leqslant G$.

(1) Mamy „oczywiste" dzielniki normalne:

$$\{e\} \trianglelefteqslant G, \qquad G \trianglelefteqslant G,$$

ponieważ:

$$\forall\, g \in G \qquad\qquad g\{e\} = \{e\} = \{e\}g, \qquad gG = G = Gg.$$

(2) Jeśli G jest przemienna, to $H \trianglelefteqslant G$.

(3) Zauważyliśmy, że:

$$\{\mathrm{id}, (1,2)\} \not\trianglelefteqslant S_3.$$

(4) Ale np. mamy:

$$A_3 = \{\mathrm{id}, (1,2,3), (1,3,2) \triangleleft S_3.$$

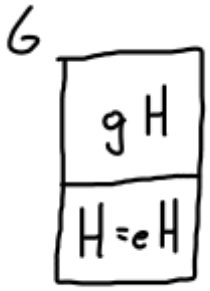
Zauważmy, że $[S_3 : A_3] = 2$.

Twierdzenie 5.14. *Jeśli* $H \leqslant G$ *oraz* $[G : H] = 2$, *to* $H \triangleleft G$.

Dowód. Weźmy $g \in G$ i rozważmy dwa przypadki.

Przypadek 1: $g \in H$
Wtedy $gH = H = Hg$.

Przypadek 2: $g \notin H$
Wtedy $gH \neq H \neq Hg$. Ale wiemy (Wniosek 4.5), że G jest rozłączna sumą warstw i w naszej sytuacji są tylko dwie warstwy, bo $[G : H] = 2$. Czyli dostajemy $gH = G \setminus H$ (dopełnienie H w G) i podobnie $Hg = G \setminus H$.



□

Teraz udowodnimy wynik, który pozwala szybko sprawdzać, czy dana podgrupa jest dzielnikiem normalnym.

Twierdzenie 5.15. *Jeśli $H \leqslant G$, to mamy:*

$$H \trianglelefteqslant G \qquad \Leftrightarrow \qquad (\forall g \in G)\ (\forall h \in H)\ ghg^{-1} \in H.$$

Dowód. „⇒” Załóżmy, że $H \trianglelefteqslant G$ i weźmy dowolne $g \in G, h \in H$. Wtedy mamy:

$$gh \in gH \underbrace{=}_{H \trianglelefteqslant G} Hg.$$

Ponieważ $gh \in Hg$, tak więc używając Twierdzenia 4.6 dostajemy $ghg^{-1} \in H$.
„⇐” Weźmy dowolny $g \in G$. Mamy pokazać, że $gH = Hg$. Dla dowodu inkluzji „$gH \subseteq Hg$”, weźmy dowolne $a \in gH$. Wtedy istnieje $h \in H$, takie że $a = gh$. Mnożąc tę równość z prawej przez g^{-1} otrzymujemy:

$$ag^{-1} = ghg^{-1} \in H$$

z założenia dowodzonej implikacji. Używając Twierdzenia 4.6 dostajemy $a \in Hg$. Inkluzję „$Hg \subseteq gH$” pokazuje się analogicznie. □

Przykład 5.16. Niech:

$$\mathrm{SL}_n(\mathbb{R}) := \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det(A) = 1\}.$$

Łatwo zauważyć, że $\mathrm{SL}_n(\mathbb{R}) < \mathrm{GL}_n(\mathbb{R})$. Pokażemy, że $\mathrm{SL}_n(\mathbb{R}) \triangleleft \mathrm{GL}_n(\mathbb{R})$ używając Twierdzenia 5.15. Weźmy dowolne $A \in \mathrm{GL}_n(\mathbb{R})$ oraz $B \in \mathrm{SL}_n(\mathbb{R})$. Liczymy:

$$\det\left(ABA^{-1}\right) = \det(A) \underbrace{\det(B)}_{1} \det(A)^{-1} = \det(A)\det(A)^{-1} = 1.$$

Czyli $ABA^{-1} \in \mathrm{SL}_n(\mathbb{R})$ i z Twierdzenia 5.15 dostajemy $\mathrm{SL}_n(\mathbb{R}) \triangleleft \mathrm{GL}_n(\mathbb{R})$.

Uwaga 5.17. Jeśli $f : G \to H$ jest homomorfizmem, to $\mathrm{im}(f) \leqslant H$ ale $\mathrm{im}(f)$ nie musi być dzielnikiem normalnym H. Np. mamy homomorfizm:

$$f : \mathbb{Z}_2 \to S_3, \qquad f(0) = \mathrm{id}, \quad f(1) = (1,2)$$

i wtedy:

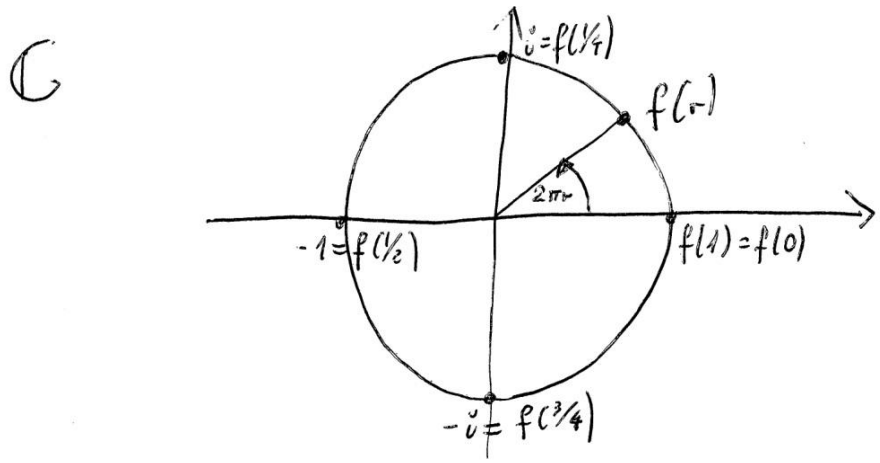
$$\mathrm{im}(f) = \{\mathrm{id}, (1,2)\} \not\trianglelefteq S_3.$$

Przykład 5.18. Rozważmy następujący homomorfizm:

$$f : (\mathbb{R}, +) \to (\mathbb{C}\setminus\{0\}, \cdot), \qquad f(r) = e^{2r\pi i} := \cos(2r\pi) + \sin(2r\pi)\, i.$$

Sprawdźmy, że to jest faktycznie homomorfizm:

$$f(r+s) = e^{2(r+s)\pi i} = e^{2r\pi i + 2s\pi i} \underbrace{=}_{\text{wzory de Moivre'a}} e^{2r\pi i} e^{2s\pi i} = f(r)f(s).$$



Weźmy dowolne $r \in \mathbb{R}$. Wtedy mamy:

$$\begin{aligned} e^{2r\pi i} = r &\iff \cos(2r\pi) + \sin(2r\pi)\, i = 1 \\ &\iff \cos(2r\pi) = 0 \text{ oraz } \sin(2r\pi) = 1 \\ &\iff r \in \mathbb{Z}\,. \end{aligned}$$

Stąd mamy:

$$\underline{\ker(f) = \mathbb{Z}}.$$

Liczymy teraz:

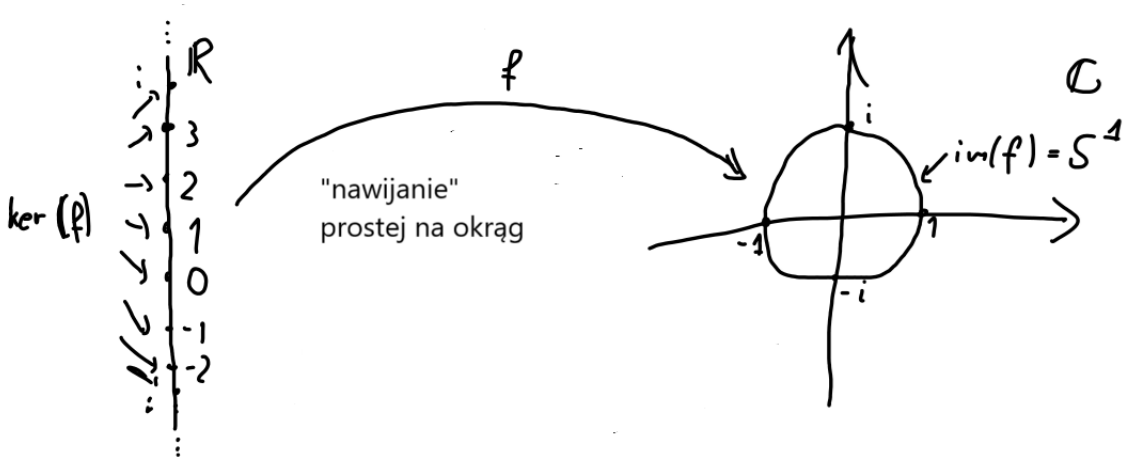
$$\operatorname{im}(f) = \{z \in \mathbb{C} \mid (\exists r \in \mathbb{R})\ e^{2r\pi i} = z\}.$$

Stąd dla dowolnego $z \in \mathbb{C}$ mamy:

$$\begin{aligned} z \in \operatorname{im}(f) &\iff (\exists r \in \mathbb{R}) \quad z = \cos(2r\pi) + \sin(2r\pi)\, i \\ &\iff |z| = 1 \\ &\iff z \in S^1, \end{aligned}$$

gdzie S^1 jest okręgiem jednostkowym. Czyli dostajemy:

$$\underline{\operatorname{im}(f) = S^1}.$$



Opiszemy teraz ogólny związek jądra z monomorfizmami.

Twierdzenie 5.19. *Niech $f : G \to H$ będzie homomorfizmem. Wtedy mamy:*

$$f \text{ jest monomorfizmem (czyli } f \text{ jest „1-1”)} \qquad \Leftrightarrow \qquad \ker(f) = \{e_G\}.$$

Dowód. „$\Rightarrow$” Załóżmy, że f jest „1-1”. Mamy pokazać, że $\ker(f) = \{e_G\}$. Inkluzja „$\{e_G\} \subseteq \ker(f)$” jest oczywista, tak więc pokazujemy tylko inkluzję „$\ker(f) \subseteq \{e_G\}$. Weźmy dowolny $a \in \ker(f)$. Wtedy mamy:

$$f(a) = e_H = f(e_G).$$

Ponieważ f jest „1-1”, otrzymujemy $a = e_G$.
„$\Leftarrow$” Załóżmy, że $\ker(f) = \{e_G\}$. Mamy pokazać, że f jest „1-1”. Weźmy $g_1, g_2 \in G$ i załóżmy, że $f(g_1) = f(g_2)$. Pokażemy, że $g_1 = g_2$. Z tego, że $f(g_1) = f(g_2)$ dostajemy:

$$e_H = f(g_1)f(g_2)^{-1} = f\left(g_1 g_2^{-1}\right).$$

Stąd mamy:

$$g_1 g_2^{-1} \in \ker(f) = \{e_G\},$$

czyli $g_1 g_2^{-1} = e_G$ i stąd $g_1 = g_2$. □

Uwaga 5.20. Jeśli chcemy sprawdzić, czy dany homomorfizm f jest monomorfizmem, to **zawsze** powinniśmy się koncentrować na pokazywaniu, że $\ker(f) = \{e\}$. Ten sposób jest **zawsze** szybszy od pokazywania bezpośrednio, że f jest „1-1”!

Przykład 5.21. Rozważmy homomorfizm α z Twierdzenia Cayley'a, czyli

$$\alpha : G \to S_G, \qquad \alpha(g) = F_g,$$

gdzie $F_g(x) = gx$. Weźmy $g \in G$ i sprawdźmy kiedy $g \in \ker(\alpha)$. Jeśli $g \in \ker(\alpha)$, to $F_g = \mathrm{id}$, czyli w szczególności:

$$e = \mathrm{id}(e) = F_g(e) = ge = g.$$

Dostajemy stąd, że $\ker(\alpha) = \{e\}$, czyli α jest faktycznie monomorfizmem.

6. Grupa ilorazowa i produkt grup

Załóżmy, że G jest grupą i $H \trianglelefteq G$. Czyli mamy:

$$\forall\, g \in G \qquad\qquad gH = Hg.$$

Wtedy:

$$G/H = \{gH \mid g \in G\} = \{Hg \mid g \in G\}.$$

Twierdzenie 6.1. *Niech $H \trianglelefteq G$. Wtedy mamy:*

(1) *Wzór*

$$aH \cdot bH := (ab)H$$

definiuje działanie w zbiorze G/H.

(2) *$(G/H, \cdot)$ jest grupą.*

(3) *Funkcja*

$$\pi : G \to G/H, \qquad \pi(g) = gH$$

jest epimorfizmem i zachodzi:

$$\ker(\pi) = H.$$

Dowód. Dla dowodu (1) trzeba sprawdzić, że powyższe działanie jest dobrze określone, czyli że nie zależy od wyboru reprezentantów warstw. Tzn. mamy pokazać, że:

$$\forall\, a, a', b, b' \in G \qquad aH = a'H,\ \ bH = b'H \qquad \Longrightarrow \qquad abH = a'b'H.$$

Używając Twierdzenia 4.6, powyższe redukuje się do pokazania:

$$\forall\, a, a', b, b' \in G \qquad a^{-1}a' \in H,\ \ b^{-1}b' \in H \qquad \Longrightarrow \qquad (ab)^{-1}a'b' = b^{-1}a^{-1}a'b' \in H.$$

Na potrzeby dowodu oznaczmy:

$$h := a^{-1}a' \in H.$$

Liczymy teraz:

$$b^{-1}\underbrace{a^{-1}a'}_{h}b' = b^{-1}\underbrace{hb'}_{\in Hb' = b'H} = b^{-1}b'h' \qquad \text{dla pewnego } h' \in H.$$

Ale $b^{-1}b' \in H$, czyli $b^{-1}b'h' \in H$, z czego wynika że:

$$abH = a'b'H,$$

co mieliśmy pokazać.

Dla dowodu (2) sprawdzamy (dość automatycznie) definicję działania grupowego.

(i) Łączność.
Weźmy $a, b, c \in G$. Wtedy mamy:

$$(aH \cdot bH) \cdot cH = (ab)H \cdot cH = ((ab)c)H = (a(bc))H = aH \cdot (bc)H = aH \cdot (bH \cdot cH).$$

(ii) Element neutralny.
Weźmy $a \in G$. Wtedy mamy:

$$aH \cdot H = aH \cdot eH = aeH = aH, \quad H \cdot aH = eH \cdot aH = eaH = aH.$$

Czyli $H = eH$ jest elementem neutralnym.

(iii) Elementy odwrotne.
Weźmy $a \in G$. Wtedy mamy:

$$aH \cdot a^{-1}H = aa^{-1}H = H, \quad a^{-1}H \cdot aH = a^{-1}aH = H.$$

Czyli $a^{-1}H$ jest elementem odwrotnym do aH.

Dla dowodu (3) sprawdzamy najpierw, że funkcja π jest homomorfizmem. Weźmy $a, b \in G$. Wtedy mamy:

$$\pi(ab) = abH = aH \cdot bH = \pi(a) \cdot \pi(b),$$

czyli funkcja π jest homomorfizmem
Następnie sprawdzamy, że π jest „na", ale to jest oczywiste, bo dla każdego $aH \in G/H$, mamy $\pi(a) = aH$.
Na koniec sprawdzamy, że $\ker(\pi) = H$. Liczymy:

$$\ker(\pi) = \{a \in G \mid \pi(a) = e_{G/H}\} = \{a \in G \mid aH = H\} = \{a \in G \mid a \in H\} = H,$$

czyli faktycznie $\ker(\pi) = H$, co kończy dowód. □

Definicja 6.2. (1) Grupę $(G/H, \cdot)$ z Twierdzenia 6.1(2) nazywamy *grupą ilorazową* G względem H.
(2) Homomorfizm $\pi : G \to G/H$ z Twierdzenia 6.1(3) nazywamy *homomorfizmem ilorazowym*.

Przykład 6.3. Weźmy $G = \mathbb{Z}$ i $H = 3\,\mathbb{Z}$. Wtedy mamy:

$$\mathbb{Z}/3\,\mathbb{Z} = \{3\,\mathbb{Z}, 1 + 3\,\mathbb{Z}, 2 + 3\,\mathbb{Z}\}.$$

Możemy policzyć np.:

$$(2 + 3\,\mathbb{Z}) + (2 + 3\,\mathbb{Z}) = (2 +_3 2) + 3\,\mathbb{Z} = 1 + 3\,\mathbb{Z}\,.$$

Dostajemy następującą tabelkę:

$+$	$3\,\mathbb{Z}$	$1 + 3\,\mathbb{Z}$	$2 + 3\,\mathbb{Z}$
$3\,\mathbb{Z}$	$3\,\mathbb{Z}$	$1 + 3\,\mathbb{Z}$	$2 + 3\,\mathbb{Z}$
$1 + 3\,\mathbb{Z}$	$1 + 3\,\mathbb{Z}$	$2 + 3\,\mathbb{Z}$	$3\,\mathbb{Z}$
$2 + 3\,\mathbb{Z}$	$2 + 3\,\mathbb{Z}$	$3\,\mathbb{Z}$	$1 + 3\,\mathbb{Z}$

Widać, że dostajemy:

$$\mathbb{Z}/3\,\mathbb{Z} \cong (\mathbb{Z}_3, +_3)$$

oraz ogólnie:

$$\mathbb{Z}/n\,\mathbb{Z} \cong (\mathbb{Z}_n, +_n).$$

Udowodnimy teraz ważne twierdzenie, które pozwala nam **zrozumieć** grupy ilorazowe i uogólnia ono obserwacje z Przykładu 6.3.

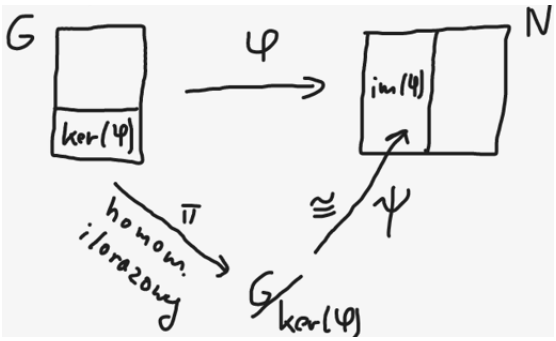
Twierdzenie 6.4 (Zasadnicze Twierdzenie o Homomorfizmach Grup)**.** *Niech $\varphi : G \to N$ będzie homomorfizmem grup. Wtedy mamy:*

$$G/\ker(\varphi) \cong \mathrm{im}(\varphi),$$

czyli ***dziedzina wydzielona przez jądro jest izomorficzna z obrazem****.*
Dokładniej: istnieje monomorfizm grup:

$$\psi : G/\ker(\varphi) \to N, \qquad \psi\,(g\ker(\varphi)) = \varphi(g),$$

taki że $\mathrm{im}(\psi) = \mathrm{im}(\varphi)$.



Dowód. Oznaczmy dla wygody $H := \ker(\varphi)$. Pokażemy najpierw, że ψ jest dobrze określone równaniem $\psi(aH) = \varphi(a)$. Weźmy $a, b \in G$, takie że $aH = bH$. Mamy pokazać, że $\varphi(a) = \varphi(b)$. Z $aH = bH$, wynika że:

$$a^{-1}b \in H = \ker(\varphi),$$

stąd dostajemy:

$$e = \varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b)$$

i ostatecznie $\varphi(a) = \varphi(b)$, co mieliśmy pokazać.

Pokażemy teraz, że ψ to homomorfizm. Weźmy $aH, bH \in G/H$. Wtedy mamy:

$$\psi(aH \cdot bH) = \psi(abH) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(aH)\psi(bH),$$

czyli ψ jest homomorfizmem.

Pokażemy teraz, że ψ jest monomorfizmem. Wystarczy pokazać, że $\ker(\psi) = \{e_{G/H}\}$ (pamiętamy, że $e_{G/H} = H$). Weźmy dowolny $gH \in \ker(\psi)$. Wtedy mamy:

$$e_N = \psi(gH) = \varphi(g),$$

czyli $g \in \ker(\varphi) = H$, co daje $gH = H$, tak więc $\ker(\psi) = \{e_{G/H}\}$.

Z definicji ψ mamy $\mathrm{im}(\psi) = \mathrm{im}(\varphi)$ i dostajemy $G/\ker(\varphi) \cong \mathrm{im}(\varphi)$. □

Przykład 6.5. Niech G będzie dowolną grupą.

(1) Mamy **homomorfizm trywialny**:

$$\varphi : G \to G, \qquad \varphi(g) = e.$$

Dostajemy, że:

$$\ker(\varphi) = G, \qquad \mathrm{im}(\varphi) = \{e\}.$$

Z Zasadniczego Twierdzenia o Homomorfizmach Grup otrzymujemy:

$$G/G \cong \{e\}.$$

(2) Mamy też:

$$\mathrm{id}_G : G \to G, \qquad \mathrm{id}_G(g) = g.$$

Dostajemy, że:

$$\ker(\varphi) = \{e\}, \qquad \mathrm{im}(\varphi) = G.$$

Z Zasadniczego Twierdzenia o Homomorfizmach Grup otrzymujemy:

$$G/\{e\} \cong G.$$

(3) Niech $n > 0$ i weźmy homomorfizm n-tej reszty:

$$r_n : \mathbb{Z} \to \mathbb{Z}_n\,.$$

Wtedy mamy:

$$\ker(f) = n\,\mathbb{Z}, \qquad \mathrm{im}(f) = \mathbb{Z}_n\,.$$

Czyli z Zasadniczego Twierdzenia o Homomorfizmach Grup otrzymujemy:

$$\mathbb{Z}\,/\,n\,\mathbb{Z} \cong \mathbb{Z}_n,$$

jak w Przykładzie 6.3.

(4) Weźmy homomorfizm z Przykładu 5.18:

$$f : (\mathbb{R}, +) \to (\mathbb{C}\setminus\{0\}, \cdot), \qquad f(r) = e^{2r\pi i} := \cos(2r\pi) + \sin(2r\pi)\,i.$$

Zauważyliśmy, że:

$$\ker(f) = \mathbb{Z}, \qquad \mathrm{im}(f) = S^1 \quad \text{(okrąg jednostkowy)}.$$

Czyli z Zasadniczego Twierdzenia o Homomorfizmach Grup otrzymujemy:

$$\mathbb{R}\,/\,\mathbb{Z} \cong S^1.$$

(5) Niech $n > 0$ i rozważmy homomorfizm zadany przez wyznacznik:

$$\det : \mathrm{GL}_n(\mathbb{R}) \to (\mathbb{R}\setminus\{0\}, \cdot).$$

Wtedy mamy:

$$\ker(\det) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det(A) = 1\} = \mathrm{SL}_n(\mathbb{R}).$$

Ponieważ $\mathrm{im}(\det) = \mathbb{R}\setminus\{0\}$, tak więc z Zasadniczego Twierdzenia o Homomorfizmach Grup otrzymujemy:

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong (\mathbb{R}\setminus\{0\}, \cdot).$$

Zmierzamy teraz do kolejnej konstrukcji algebraicznej.

Przykład 6.6. Rozważmy dwa następujące homomorfizmy:

$$\alpha : \mathbb{Z}_2 \to \mathbb{Z}_6, \qquad 0 \mapsto 0, \quad 1 \mapsto 3;$$
$$\beta : \mathbb{Z}_3 \to \mathbb{Z}_6, \qquad 0 \mapsto 0, \quad 1 \mapsto 2, \quad 2 \mapsto 4.$$

Ponieważ mamy:

$$\mathbb{Z}_6 = \{0 +_6 0, 0 +_6 2, 0 +_6 4, 1 +_6 0, 1 +_6 2, 1 +_6 4\},$$

tak więc otrzymujemy bijekcję:

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \to \mathbb{Z}_6, \qquad (i, j) \mapsto \alpha(i) +_6 \beta(j).$$

Chcemy aby bijekcja z Przykładu 6.6 była izomorfizmem, tak więc powinniśmy zdefiniować działanie grupowe na produkcie $\mathbb{Z}_2 \times \mathbb{Z}_3$. Poniżej robimy to ogólnie.

Twierdzenie 6.7. *Niech G i H będą grupami. Definiujemy następujące działanie w $G \times H$:*

$$(g, h) \cdot (g', h') := (gg', hh'),$$

gdzie na pierwszej współrzędnej jest działanie w G i na drugiej współrzędnej jest działanie w H. Wtedy $(G \times H, \cdot)$ jest grupą.

Dowód. Dla dowodu łączności $\cdot$ weźmy $(g, h), (g', h'), (g'', h'') \in G \times H$. Wtedy:

$$((g, h) \cdot (g', h')) \cdot (g'', h'') = (gg', hh') \cdot (g'', h'') =$$
$$= ((gg')g'', (hh')h'') = (g(g'g''), h(h'h'')) = (g, h) \cdot ((g', h') \cdot (g'', h'')),$$

czyli działanie $\cdot$ jest łączne.

Podobnie łatwo się sprawdza (co pomijamy), że element neutralny $\cdot$ to (e_G, e_H) oraz że dla każdego $(g, h) \in G \times H$, element odwrotny to (g^{-1}, h^{-1}). □

Definicja 6.8. Grupę z Twierdzenia 6.7 nazywamy *produktem* grup G, H i oznaczamy $G \times H$.

Przykład 6.9. (1) Rozważmy grupę:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}.$$

oraz jej tabelkę:

$\mathbb{Z}_2 \times \mathbb{Z}_2$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Widzimy, że:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \cong K_4 \quad \text{(grupa Kleina)}.$$

(2) Rozważana wcześniej funkcja:

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \to \mathbb{Z}_6, \quad (i, j) \mapsto \alpha(i) +_6 \beta(j)$$

jest izomorfizmem i mamy:

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6\,.$$

Następny wynik zawiera oba punkty z powyższego przykładu jako szczególne przypadki i daje ogólny test na to, czy dana grupa jest izomorficzna z produktem grup.

Twierdzenie 6.10 (Twierdzenie o produkcie wewnętrznym)**.** *Niech G będzie grupą i A, B będą podgrupami G, takimi że:*

(1) $A \cap B = \{e\}$;
(2) $AB = G$, *tzn. dla każdego* $g \in G$ *istnieją* $a \in A, b \in B$, *takie że* $g = ab$;
(3) *dla każdych* $a \in A, b \in B$ *mamy* $ab = ba$.

Wtedy następująca funkcja:

$$f : A \times B \to G, \qquad f(a, b) = ab$$

(zamiast „$f((a, b))$" piszemy tu „$f(a, b)$") jest izomorfizmem, czyli $A \times B \cong G$.

Dowód. Sprawdzamy, czy f jest homomorfizmem. Weźmy $(a, b), (a', b') \in A \times B$. Liczymy:

$$f((a, b) \cdot (a', b')) = f(aa', bb') = aa'bb' \underbrace{=}_{a'b = ba'} aba'b' = f(a, b)f(a', b'),$$

czyli f jest homomorfizmem.

Sprawdzamy, czy f jest „1-1". Wystarczy pokazać, że $\ker(f) = \{e_{A\times B}\}$, gdzie $e_{A\times B} = (e, e)$. Weźmy $(a, b) \in \ker(f)$. Wtedy mamy:

$$e = f(a, b) = ab,$$

czyli dostajemy

$$A \ni a^{-1} = b \in B.$$

Stąd (używając (1)) mamy:

$$a^{-1} = b \in A \cap B = \{e\},$$

czyli faktycznie $(a, b) = (e, e)$.

Sprawdzamy, czy f jest „na". Z (2) dostajemy, że dla każdego $g \in G$ istnieją $a \in A, b \in B$, takie że:

$$g = ab = f(a, b),$$

czyli faktycznie f jest „na". □

Definicja 6.11. Jeśli podgrupy A, B spełniają założenia Twierdzenia o produkcie wewnętrznym, to mówimy że G jest *produktem wewnętrznym* grup A, B.

Uwaga 6.12. (1) Twierdzenie o produkcie wewnętrznym mówi, że jeśli G jest produktem wewnętrznym grup A, B, to wtedy:

$$G \cong A \times B.$$

(2) Jeśli G jest produktem wewnętrznym grup A, B oraz istnieją grupy H, N oraz izomorfizmy:

$$\alpha : H \to A, \qquad \beta : N \to B,$$

to wtedy funkcja

$$f : H \times N \to G, \qquad f(h, n) = \alpha(h)\beta(n)$$

jest izomorfizmem i mamy:

$$G \cong H \times N.$$

Przykład 6.13. (1) Niech G będzie grupą Kleina:

$$G = K_4 = \{\mathrm{id}, S, S', O_\pi\}.$$

Weźmy:

$$A := \langle S\rangle = \{\mathrm{id}, S\}, \qquad B := \langle S'\rangle = \{\mathrm{id}, S'\}.$$

Wtedy mamy $A \cap B = \{\mathrm{id}\}$, $AB = K_4$ (bo np. $SS' = O_\pi$) oraz $SS' = S'S$ (bo cała grupa K_4 jest przemienna). Stąd K_4 jest produktem wewnętrznym A i B. Ponieważ $A \cong \mathbb{Z}_2 \cong B$, tak więc z Uwagi 6.12(2) dostajemy:

$$K_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \,.$$

(2) Grupa $\mathbb{Z}_6$ jest produktem wewnętrznym podgrup:

$$A := \{0, 3\} \cong \mathbb{Z}_2, \qquad B := \{0, 2, 4\} \cong \mathbb{Z}_3 \,.$$

z Uwagi 6.12(2) dostajemy:

$$\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \,.$$

Następny wynik uogólnia fakt, że $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

Twierdzenie 7.1. *Załóżmy, że $k, l > 0$ są względnie pierwsze. Wtedy mamy:*

$$\mathbb{Z}_{kl} \cong \mathbb{Z}_k \times \mathbb{Z}_l \,.$$

Dowód. Niech $n := kl$. Przedstawimy $\mathbb{Z}_n$ jako produkt wewnętrzny podgrup A i B, takich że:

$$A \cong \mathbb{Z}_k, \qquad B \cong \mathbb{Z}_l$$

(co wystarcza z Uwagi 6.12(2)). Weźmy:

$$A := \langle l \rangle = \{0, l, 2l, \ldots, (k-1)l\} \cong \mathbb{Z}_k,$$
$$B := \langle k \rangle = \{0, k, 2k, \ldots, (l-1)k\} \cong \mathbb{Z}_l \,.$$

Pokazujemy, że $A \cap B = \{0\}$. Weźmy $t \in A \cap B$ i pokażemy, że $t = 0$. Ponieważ $l \mid t$ i $k \mid t$, tak więc dostajemy:

$$\mathrm{NWW}(l, k) \mid t.$$

Ale $\mathrm{NWD}(l, k) = 1$, tak więc $\mathrm{NWW}(l, k) = n$. Czyli mamy $n \mid t$ oraz $t \in \mathbb{Z}_n$, stąd dostajemy $t = 0$.

Weźmy teraz dowolny $t \in \mathbb{Z}_n$. Znajdziemy $a \in A, b \in B$, takie że $a +_n b = t$. Rozważmy następujący zbiór:

$$S := \{a +_n b \mid a \in A, b \in B\}.$$

Mamy pokazać, że $S = \mathbb{Z}_n$. Rozważmy funkcję:

$$\varphi : A \times B \to S, \quad \varphi(a, b) = a +_n b.$$

Z definicji mamy, że φ jest „na". Pokażemy, że φ jest „1-1". Weźmy $(a, b), (a', b') \in A \times B$, takie że $\varphi(a, b) = \varphi(a', b')$. Wtedy mamy:

$$a +_n b = a' +_n b' \qquad \Rightarrow \qquad A \ni a -_n a' = b -'_n b \in B.$$

Stąd dostajemy:

$$a -_n a', b' -_n b \in A \cap B = \{0\}.$$

Czyli mamy:

$$a -_n a' = 0, \quad b' -_n b = 0,$$

co w końcu daje $(a, a') = (b, b')$, czyli φ jest „1-1". Podsumowując, dostajemy że powyższa funkcja $\varphi : A \times B \to S$ jest bijekcją oraz mamy:

$$|S| = |A \times B| = |A||B| = kl = n = |\,\mathbb{Z}_n\,|.$$

Stąd S_n jest podzbiorem $\mathbb{Z}_n$ mocy $n = |\,\mathbb{Z}_n\,|$, stąd faktycznie $S = \mathbb{Z}_n$, co mieliśmy pokazać.

Oczywiście, mamy też ostatni warunek z twierdzenia o produkcie wewnętrznym, bo grupa $\mathbb{Z}_n$ jest przemienna, co kończy dowód. □

Uwaga 7.2. Część „$\mathbb{Z}_n = A +_n B$" powyższego dowodu wynikała z części „$A \cap B = \{0\}$" i z faktu, że:

$$|\,\mathbb{Z}_n\,| = n = kl = |A||B|.$$

Ogólnie mamy, że jeśli:

- $H \leqslant G, K \leqslant G$ i G jest skończona;
- $H \cap K = \{e\}$;
- $|G| = |H||K|$,

to wtedy $G = HK$, czyli dla każdego $g \in G$ istnieją $x \in H, y \in K$, takie że $g = xy$. Czyli ten warunek otrzymujemy „za darmo", jeśli wiemy że $|G| = |H||K|$ oraz $H \cap K = \{e\}$.

Przyjrzymy się teraz bliżej produktom grup cyklicznych. Oczywiście, możemy brać produkty większej ilości grup, czyli dla grup $G_1, \ldots, G_n$ mamy też produkt grup $G_1 \times \ldots \times G_n$.

Twierdzenie 7.3. *Niech $k_1, \ldots, k_n > 0$. Wtedy następujące warunki są równoważne:*

(1) *Grupa* $\mathbb{Z}_{k_1} \times \ldots \times \mathbb{Z}_{k_n}$ *jest cykliczna.*
(2) *Liczby* $k_1, \ldots, k_n$ *są parami względnie pierwsze, tzn. dla* $i \neq j$ *mamy* $\mathrm{NWD}(k_i, k_j) = 1$.

Dowód. (2) $\Rightarrow$ (1)
Wiemy z Twierdzenia 7.1, że:

$$\mathrm{NWD}(k_1, k_2) = 1 \qquad \Rightarrow \qquad \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \cong \mathbb{Z}_{k_1 k_2}\,.$$

Z założenia mamy $\mathrm{NWD}(k_1 k_2, k_3) = 1$ i stąd znowu dostajemy:

$$\mathbb{Z}_{k_1 k_2 k_3} \cong \mathbb{Z}_{k_1 k_2} \times \mathbb{Z}_{k_3} \cong \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \mathbb{Z}_{k_3}\,.$$

Kontynuując tak dalej (prosta indukcja) otrzymujemy:

$$\mathbb{Z}_{k_1 \cdot \ldots \cdot k_n} \cong \mathbb{Z}_{k_1} \times \ldots \times \mathbb{Z}_{k_n},$$

czyli grupa $\mathbb{Z}_{k_1} \times \ldots \times \mathbb{Z}_{k_n}$ jest cykliczna.
(1) $\Rightarrow$ (2)
Udowodnimy, że negacja warunku (2) implikuje negację warunku (1). Załóżmy, że istnieją $i \neq j$, takie że $\mathrm{NWD}(k_i, k_j) \neq 1$. Bez zmniejszenia ogólności możemy przyjąć, że $i = 1$ oraz $j = 2$. Niech teraz:

$$k := \mathrm{NWW}(k_1, k_2) < k_1 k_2, \qquad l := k k_3 k_4 \ldots k_n < k_1 k_2 \ldots k_n.$$

Wtedy dla każdego i mamy $k_i \mid l$. Weźmy dowolny element:

$$(a_1, \ldots, a_n) \in \mathbb{Z}_{k_1} \times \ldots \times \mathbb{Z}_{k_n}\,.$$

Wtedy mamy:

$$l(a_1, \ldots, a_n) = (la_1, \ldots, la_n) = (0, \ldots, 0),$$

ponieważ dla każdego i mamy:

$$|Z_{k_i}| = k_i \mid l.$$

Stąd dla każdego $\alpha \in \mathbb{Z}_{k_1} \times \ldots \times \mathbb{Z}_{k_n}$ dostajemy:

$$\mathrm{ord}(\alpha) \leqslant l < k_1 \ldots k_n = |\,\mathbb{Z}_{k_1} \times \ldots \times \mathbb{Z}_{k_n}\,|,$$

czyli grupa $\mathbb{Z}_{k_1} \times \ldots \times \mathbb{Z}_{k_n}$ nie jest cykliczna. □

Przykład 7.4. (1) Grupa $\mathbb{Z}_6 \times \mathbb{Z}_7 \times \mathbb{Z}_{25}$ jest cykliczna.
(2) Grupa $\mathbb{Z}_6 \times \mathbb{Z}_8 \times \mathbb{Z}_1$ nie jest cykliczna.

Zauważmy, że dla każdych $k_1, \ldots, k_n > 0$ grupa $\mathbb{Z}_{k_1} \times \ldots \times \mathbb{Z}_{k_n}$ jest skończona i przemienna. Okazuje się, że zachodzi też następujące twierdzenie odwrotne, które pozostawimy bez dowodu.

Twierdzenie 7.5. *Niech* A *będzie skończoną grupa przemienną. Wtedy istnieją* $k_1, \ldots, k_n > 0$, *takie że:*

$$A \cong \mathbb{Z}_{k_1} \times \ldots \times \mathbb{Z}_{k_n}\,.$$

Czyli każda skończona grupa przemienna jest izomorficzna z produktem grup cyklicznych.

Chcemy teraz znaleźć sposób na sprawdzanie, czy dwie skończone grupy przemienne (zapisane jako produkty grup cyklicznych) są ze sobą izomorficzne.

Przykład 7.6. (1) Oczywiście, jeśli rzędy grup są różne, to grupy nie mogą być izomorficzne, dlatego będziemy rozważali jedynie sytuacje, w których rzędy rozważanych grup są takie same.
(2) Z Twierdzenia 7.3, wiemy że np.:

$$\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2, \qquad \mathbb{Z}_{20} \ncong \mathbb{Z}_{10} \times \mathbb{Z}_2\,.$$

(3) A czy np.:

$$\mathbb{Z}_6 \times \mathbb{Z}_{105} \cong \mathbb{Z}_{30} \times \mathbb{Z}_{21}?$$

Rozkładamy na produkty używając Twierdzenia 7.3:

$$\mathbb{Z}_6 \times \mathbb{Z}_{105} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7,$$
$$\mathbb{Z}_{30} \times \mathbb{Z}_{21} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_7\,.$$

Czyli dostajemy, że:

$$\mathbb{Z}_6 \times \mathbb{Z}_{105} \cong \mathbb{Z}_{30} \times \mathbb{Z}_{21}!$$

Okazuje się, że sposób z Przykładu 7.6(3) zawsze działa, o czym mówi następny wynik. Potrzebujemy najpierw pewnej notacji. Niech $n > 0$ i G będzie grupą. Wtedy oznaczamy:

$$G^n := \underbrace{G \times \ldots \times G}_{n \text{ razy}}, \qquad G^0 := \{e\}.$$

Twierdzenie 7.7. *Niech A będzie skończoną grupą przemienną.*

(1) *Istnieją $k_1, l_1, \ldots, k_n, l_n > 0$, takie że $k_1, \ldots, k_n$ to potęgi liczb pierwszych oraz*

$$A \cong (\mathbb{Z}_{k_1})^{l_1} \times \ldots \times (\mathbb{Z}_{k_n})^{l_n}\,.$$

(2) *Niech $k_1, \ldots, k_n$ to parami różne potęgi liczb pierwszych oraz $l_1, l_1', \ldots, l_n, l_n' \in \mathbb{N}$. Wtedy mamy:*

$$(\mathbb{Z}_{k_1})^{l_1} \times \ldots \times (\mathbb{Z}_{k_n})^{l_n} \cong (\mathbb{Z}_{k_1})^{l_1'} \times \ldots \times (\mathbb{Z}_{k_n})^{l_n'} \qquad \Leftrightarrow \qquad l_1 = l_1', \ldots, l_n = l_n'.$$

Dowód. Punkt (1) wynika z Twierdzenia 7.5 i Twierdzenia 7.3, ponieważ dla różnych liczb pierwszych $p_1, \ldots, p_m$ oraz $k_1, \ldots, k_m \in \mathbb{N}$ mamy:

$$\mathbb{Z}_{p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}} \cong \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_m^{k_m}}\,.$$

Punktu (2) nie będziemy dowodzić. □

Uwaga 7.8. Podsumowując, jeśli mamy dwie skończone grupy przemienne A i B, to aby sprawdzić czy $A \cong B$, należy:

(1) rozłożyć A i B na produkt grup postaci $\mathbb{Z}_{p^l}$, gdzie p jest liczbą pierwszą;
(2) policzyć ile razy występuje każde $\mathbb{Z}_{p^l}$ w rozkładzie A oraz w rozkładzie B i porównać te ilości wystąpień.

Przykład 7.9. Mamy, że:

$$\mathbb{Z}_2^2 \times \mathbb{Z}_4^3 \times \mathbb{Z}_8^2 \times \mathbb{Z}_3^5 \times \mathbb{Z}_9^7 \ncong \mathbb{Z}_2^4 \times \mathbb{Z}_4^2 \times \mathbb{Z}_8^2 \times \mathbb{Z}_3^5 \times \mathbb{Z}_9^7,$$

ponieważ:

$$(2, 3, 2, 5, 7) \neq (4, 2, 2, 5, 7).$$

Poznaliśmy już wiele przykładów grup małych rzędów. Okazuje, się że jeśli chodzi o grupy rzędu co najwyżej 8, to jest jeszcze tylko jedna grupa której nie znamy: **grupa kwaternionów**.

Na początek zauważmy, że macierze o współczynnikach zespolonych też można mnożyć (podobnie jak macierze o współczynnikach rzeczywistych) i że wtedy mamy grupę $\mathrm{GL}_n(\mathbb{C})$: grupę macierzy n na n o współczynnikach zespolonych i niezerowym wyznaczniku (z działaniem mnożenia macierzy). Wyróżniamy trzy macierze z $\mathrm{GL}_2(\mathbb{C})$:

$$\mathbf{i} := \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \qquad \mathbf{j} := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \qquad \mathbf{k} := \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

Niech teraz:

$$Q_8 := \{I, -I, \mathbf{i}, -\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\}.$$

Wtedy łatwo sprawdzić, że:

$$\mathbf{ij} = \mathbf{k}, \quad \mathbf{jk} = \mathbf{i}, \quad \mathbf{ki} = \mathbf{j}, \quad \mathbf{ji} = -\mathbf{k}, \quad \mathbf{kj} = -\mathbf{i}, \quad \mathbf{ik} = -\mathbf{j},$$
$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -I, \quad (-I)^2 = I.$$

Sprawdzamy przykładowe dwie równości:

$$\mathbf{ij} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = \mathbf{k},$$

$$\mathbf{i}^2 = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} i^2 & 0 \\ 0 & (-i)^2 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -I.$$

Czyli $Q_8 < \mathrm{GL}_2(\mathbb{C})$ i Q_8 nazywamy *grupą kwaternionów*. Poniżej tabelka Q_8:

Q_8	I	$-I$	$\mathbf{i}$	$-\mathbf{i}$	$\mathbf{j}$	$-\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$
I	I	$-I$	$\mathbf{i}$	$-\mathbf{i}$	$\mathbf{j}$	$-\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$
$-I$	$-I$	I	$-\mathbf{i}$	$\mathbf{i}$	$-\mathbf{j}$	$\mathbf{j}$	$-\mathbf{k}$	$\mathbf{k}$
$\mathbf{i}$	$\mathbf{i}$	$-\mathbf{i}$	$-I$	I	$\mathbf{k}$	$-\mathbf{k}$	$-\mathbf{j}$	$\mathbf{j}$
$-\mathbf{i}$	$-\mathbf{i}$	$\mathbf{i}$	I	$-I$	$-\mathbf{k}$	$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{j}$
$\mathbf{j}$	$\mathbf{j}$	$-\mathbf{j}$	$-\mathbf{k}$	$\mathbf{k}$	$-I$	I	$\mathbf{i}$	$-\mathbf{i}$
$-\mathbf{j}$	$-\mathbf{j}$	$\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$	I	$-I$	$-\mathbf{i}$	$\mathbf{i}$
$\mathbf{k}$	$\mathbf{k}$	$-\mathbf{k}$	$\mathbf{j}$	$-\mathbf{j}$	$-\mathbf{i}$	$\mathbf{i}$	$-I$	I
$-\mathbf{k}$	$-\mathbf{k}$	$\mathbf{k}$	$-\mathbf{j}$	$\mathbf{j}$	$\mathbf{i}$	$-\mathbf{i}$	I	$-I$

Wtedy też mamy:

- elementy rzędu 4 w Q_8 to $\mathbf{i}, -\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}$;
- element rzędu 2 w Q_8 to $-I$;
- element rzędu 1 w Q_8 to I.

8. Klasyfikacja grup małych rzędów i automorfizmy wewnętrzne

Na razie wiemy, że każda grupa cykliczna rzędu n jest izomorficzna z $\mathbb{Z}_n$. Poniżej omówimy klasyfikację (z dokładnością do izomorfizmu) grup rzędu co najwyżej 8. Na początek pierwsze twierdzenie klasyfikacyjne.

Twierdzenie 8.1. *Niech G będzie grupą rzędu p, gdzie p jest liczbą pierwszą. Wtedy mamy:*

$$G \cong \mathbb{Z}_p\,.$$

Dowód. Ponieważ rząd G jest liczbą pierwszą, tak więc $|G| \geqslant 2$, czyli istnieje $a \in G \setminus \{e\}$. Wtedy $\operatorname{ord}(a) > 1$. Z Twierdzenia Lagrange'a mamy:

$$\operatorname{ord}(a) \mid p = |G|.$$

Ponieważ $\operatorname{ord}(a) > 1$ i liczba p jest pierwsza, dostajemy że:

$$\operatorname{ord}(a) = p = |G|.$$

Czyli $G = \langle a \rangle$ i stąd $G \cong \mathbb{Z}_p$. □

Teraz klasyfikujemy grupy rzędu co najwyżej 8. Niech $|G| = n \leqslant 8$. Rozważamy przypadki.

$\underline{n = 1}$
Wtedy $G = \{e\}$ jest trywialna i np. $G \cong \mathbb{Z}_1$.

$\underline{n = 2}$
$G \cong \mathbb{Z}_2$ z Twierdzenia 8.1.

$\underline{n = 3}$
$G \cong \mathbb{Z}_3$ z Twierdzenia 8.1.

$\underline{n = 4}$
Pokażemy, że $G \cong \mathbb{Z}_4$ lub $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Dowód. Załóżmy, że $G \ncong \mathbb{Z}_4$. Pokażemy, że $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Ponieważ $G \ncong \mathbb{Z}_4$, tak więc:

$$\forall\, g \in G \qquad \operatorname{ord}(g) \neq 4.$$

Z Twierdzenia Lagrange'a (ponieważ $|G| = 4$) dostajemy:

$$\forall\, g \in G \qquad g^2 = e.$$

Na ćwiczeniach pokazaliśmy, że w tej sytuacji G jest grupą przemienną.

Weźmy teraz $a \in G$ oraz $b \in G \setminus \{a, e\}$. Definiujemy:

$$A := \langle a \rangle = \{e, a\}, \qquad B := \langle b \rangle = \{e, b\}.$$

Mamy teraz (używając przemienności G):

$$A \cap B = \{e\}, \qquad AB = G, \qquad \forall a \in A\ \forall b \in B\ ab = ba.$$

Ponieważ $A \cong \mathbb{Z}_2 \cong B$, tak więc z Uwagi 6.12(2) dostajemy, że $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. □

Uwaga 8.2. Można pokazać, że jeśli $|G| = p^2$ i p jest liczbą pierwszą, to:

$$G \cong \mathbb{Z}_{p^2} \qquad \text{lub} \qquad G \cong \mathbb{Z}_p \times \mathbb{Z}_p\,.$$

$\underline{n = 5}$
$G \cong \mathbb{Z}_5$ z Twierdzenia 8.1.

$\underline{n = 6}$
Naszkicujemy dowód tego, że $G \cong \mathbb{Z}_6$ lub $G \cong S_3$.

Idea dowodu. Rozważamy dwa przypadki, które będą miały liczne podprzypadki.

Przypadek 1: G przemienna.
Pokażemy, że $G \cong \mathbb{Z}_6$. Weźmy $a \in G \setminus \{e\}$.

Przypadek 1a: $\operatorname{ord}(a) = 6$.
Wtedy mamy:

$$G = \langle a \rangle \cong \mathbb{Z}_6 \,.$$

Przypadek 1b: $\operatorname{ord}(a) = 3$.
Zdefiniujmy:

$$A := \langle a \rangle \cong \mathbb{Z}_3$$

i weźmy $b \in G \setminus A$. Rozważamy teraz trzy „podpodprzypadki".

- Jeśli $\operatorname{ord}(b) = 6$, to j.w. $G \cong \mathbb{Z}_6$.
- Jeśli $\operatorname{ord}(b) = 2$, to bierzemy:

  $$B := \langle b \rangle \cong \mathbb{Z}_2$$

  i wtedy łatwo zauważyć, że:

  $$A \cap B = \{e\}, \qquad AB = G, \qquad \forall a \in A \; \forall b \in B \; ab = ba.$$

  Ponieważ $A \cong \mathbb{Z}_3$ i $B \cong \mathbb{Z}_2$, tak więc z Uwagi 6.12(2) i Twierdzenia 7.1 dostajemy, że

  $$G \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6 \,.$$

- Udowodnimy teraz, że $\operatorname{ord}(b) \neq 3$ (ostatni „podpodprzypadek"). Załóżmy, że $\operatorname{ord}(b) = 3$ i dojdziemy do sprzeczności. Dla $B := \langle b \rangle$ mamy że $b \in B \setminus A \cap B$ stąd:

  $$A \cap B \subsetneq B \;\text{ i }\; |A \cap B| \mid |B| = 3 \quad \Rightarrow \quad |A \cap B| = 1 \quad \Rightarrow \quad A \cap B = \{e\}.$$

  Wtedy można pokazać, że:

  $$|\{ab \mid a \in A, b \in B\}| = 9 > 6 = |G|,$$

  co daje sprzeczność.

Przypadek 1c: $\operatorname{ord}(a) = 2$.
Argument podobny do tego z Przypadku 1b.

Przypadek 2: G nie jest przemienna.
Uzasadnimy, że $G \cong S_3$. Jeśli dla każdego $a \in G$ mamy, że $a^2 = e$, to wtedy j.w. G jest przemienna, sprzeczność. Stąd istnieje $a \in G$, taki że $\operatorname{ord}(a) = 3$. Niech $H := \langle a \rangle$ i weźmy $b \in G \setminus H$. Jak w Przypadku 1 otrzymujemy, że $\operatorname{ord}(b) = 2$. Definiujemy:

$$b' := ab, \qquad b'' := ba.$$

Wtedy $b' \neq b''$, bo w przeciwnym wypadku G byłaby przemienna. Czyli mamy, że:

$$G = \{e, a, a^2, b, b', b''\}$$

i można pokazać, że następująca funkcja:

$$f : G \to S_3, \quad f(e) = \mathrm{id}, f(a) = (1,2,3), f(a^2) = (1,3,2), f(b) = (1,2), f(b') = (1,3), f(b'') = (2,3)$$

jest izomorfizmem. □

$n = 7$
$G \cong \mathbb{Z}_7$ z Twierdzenia 8.1.

$n = 8$
Wtedy mamy, że G jest izomorficzna z jedną z następujących grup:

$$Q_8, \quad D_4, \quad \mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,$$

czego już nie pokazujemy (to jest najtrudniejsze!).

Potrzebujemy jeszcze jednej definicji.

Definicja 8.3. Niech G będzie grupą. Wtedy

$$Z(G) := \{g \in G \mid \forall x \in G\ gx = xg\} \qquad (\textit{centrum} \text{ grupy } G).$$

Łatwo zauważyć, że $Z(G) \trianglelefteqslant G$.

Przykład 8.4. (1) $Z(Q_8) = \{I, -I\}$.
(2) $Z(D_3) = \{\mathrm{id}\}$.
(3) $Z(D_4) = \{\mathrm{id}, O_\pi\}$.
(4) Grupa G jest przemienna wtedy i tylko wtedy, gdy $Z(G) = G$.

TU KOŃCZY SIĘ MATERIAŁ WYMAGANY NA KOLOKWIUM 2 !!!