Wstęp

Jest to skrypt do wykładu Algebra 1 prowadzonego w Instytucie Matematycznym Uniwersytetu Wrocławskiego. Skrypt ma 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.

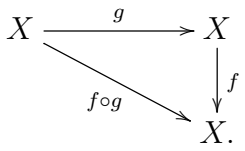
(1) Na zbiorach $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ mamy zwykłe działania dodawania $(+)$ i mnożenia $(\cdot)$.
(2) Mamy też mnóstwo innych „dziwnych" działań, np. działanie:

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

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 $\mathbb{R}\cup\{\infty\}$:

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

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

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

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

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 $\{2,3\}$ otrzymując 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
$$2\blacksquare 3 := f(0) = 2.$$

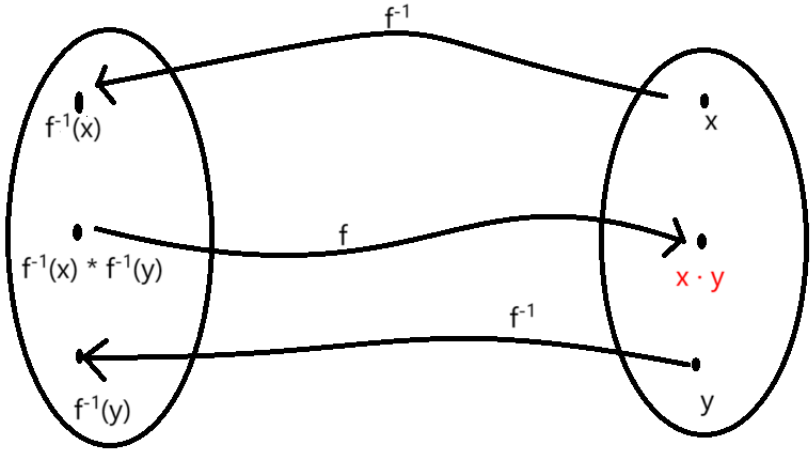
Czyli ogólny wzór jest następujący:

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

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:

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



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 $\circ$:

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

(2) Istnieje wyróżniona funkcja

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

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

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

(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:

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

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

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

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):

$$\begin{aligned}(x \cdot y) \cdot z &= \big(f(f^{-1}(x) * f^{-1}(y))\big) \cdot z \\ &= a \cdot z \\ &= f\left(f^{-1}(a) * f^{-1}(z)\right) \\ &= f(\underbrace{f^{-1}(f}_{\text{„kasują się”}}\left[f^{-1}(x) * f^{-1}(y)\right]) * f^{-1}(z)) \\ &= f\left(\left[f^{-1}(x) * f^{-1}(y)\right] * f^{-1}(z)\right).\end{aligned}$$

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 niezerowym wyznaczniku. Z algebry liniowej wiemy, że:

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

- mnożenie macierzy 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 mamy:
$$\forall\, A \in \mathrm{GL}_n(\mathbb{R}) \qquad A \cdot I = A = I \cdot A,$$
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 $(\mathbb{C} \setminus \{0\}, \cdot)$ oraz $(\mathbb{Q} \setminus \{0\}, \cdot)$ są grupami przemiennymi.

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:

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

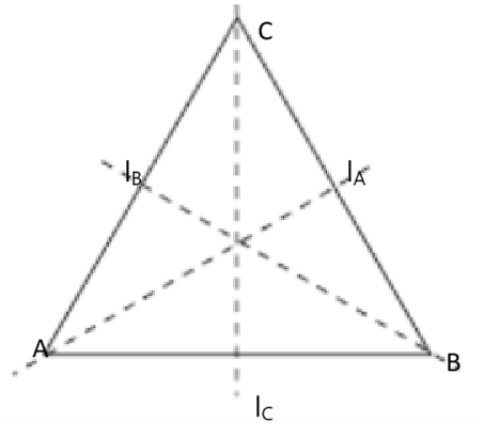
Wtedy $\mathrm{Izo}(W) \leqslant S_W$, czyli $(\mathrm{Izo}(W), \circ)$ jest grupą.

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.

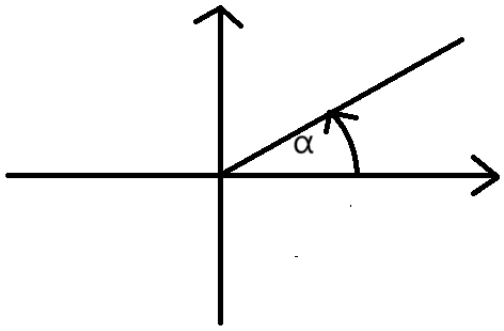
Popatrzmy dokładniej na przypadek, gdy W jest trójkątem równobocznym. Wtedy grupę izometrii oznacza się D_3 i należą do niej tylko obroty i symetrie osiowe. Ustawiamy trójkąt jak na rysunku poniżej (środek ciężkości w środku układu współrzędnych). Mamy:



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

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:

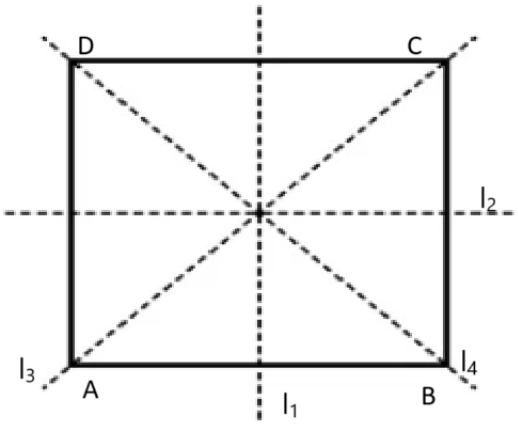
$$O_{\frac{2\pi}{3}} \circ S_A = S_C.$$

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:

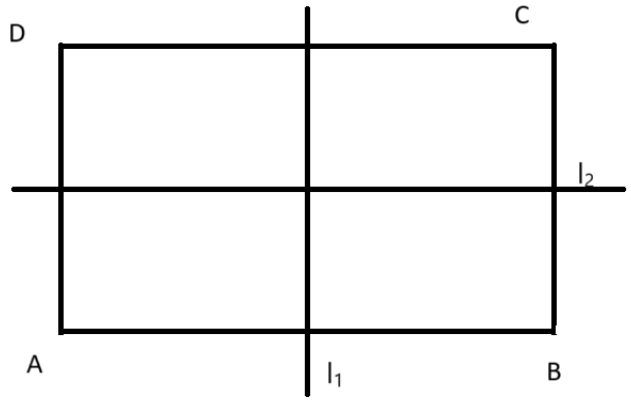
$$D_4 = \left\{ \mathrm{id}, O_{\frac{\pi}{2}}, O_\pi, O_{\frac{3\pi}{2}}, S_{l_1}, S_{l_2}, S_{l_3}, S_{l_4} \right\}.$$

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:

$$g^m = g^{kl+r} = g^{lk} g^r = \left(g^k\right)^l g^r = e^l g^r = e g^r = g^r \in \{g^0, g^1, \ldots, g^{k-1}\},$$

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

$$f(i +_n j) = g^{i+_n j} = g^{i+j+ln} = g^i g^j (g^n)^l \underbrace{=}_{\text{Krok 3}} g^i g^j e^l = g^i g^j e = g^i g^j = f(i)f(j).$$

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 dla $G = \langle g \rangle$ mamy:

(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 „$\mathrm{ord}(g)$” zamiast „$\mathrm{ord}_G(g)$”.

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 $g_1, \ldots, g_n \in G$, 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:

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

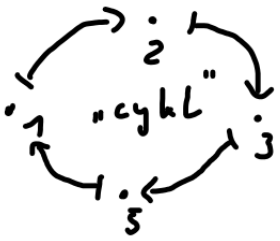
Grupy permutacji

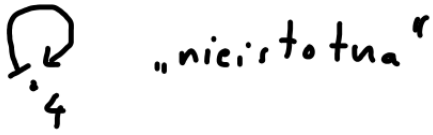
Chcemy opisać każdą permutację za pomocą pewnych prostych permutacji.

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).

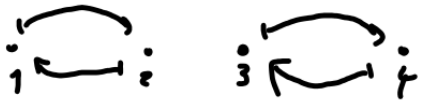




(2) Niech:

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

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:

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

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 $\tau(X_\tau) = X_\tau$). 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**
$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = (1,2,3) \circ (4,5),$$
$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix} = (1,2) \circ (3,5).$$
Będziemy zwykle pisać np. „$(1,2)(3,5)$" zamiast „$(1,2) \circ (3,5)$".

(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:

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

□

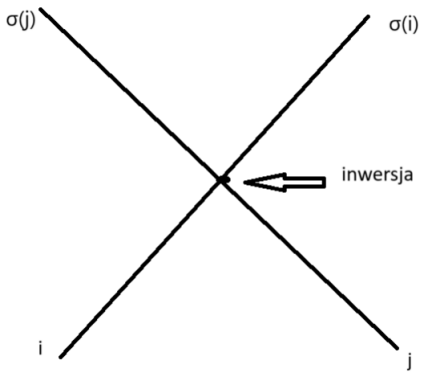
Z ostatnich dwóch twierdzeń natychmiast wynika:

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. □

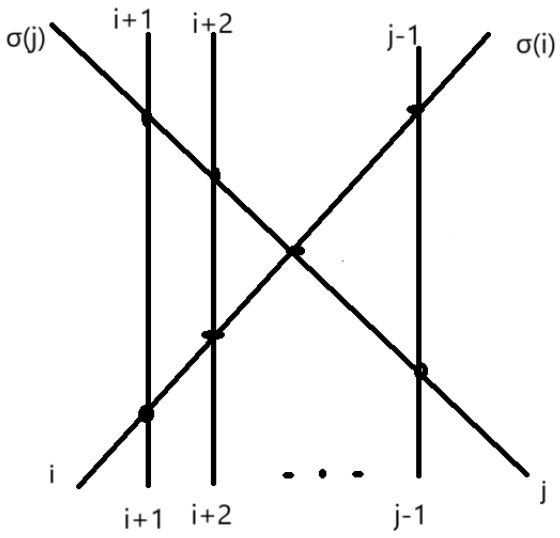
Pomijamy dowód następnego wyniku.

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 3.30 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.

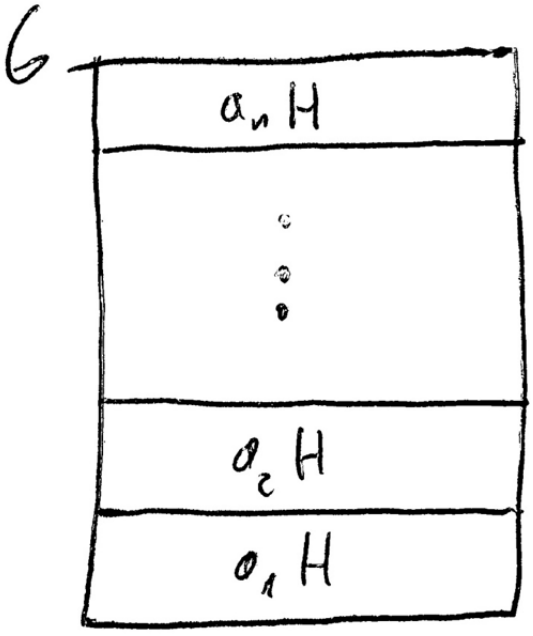
Definicja 4.1. (1) *Grupa trywialna* to grupa $G = \{e\}$ składająca się tylko z elementu neutralnego.
(2) Jeśli G to grupa, to podgrupę $\{e\} \leqslant G$ nazywamy *podgrupą trywialną*.
(3) Jeśli $A \subseteq B$ (A to podzbiór B), to podzbiór A jest *właściwy*, gdy $A \neq B$.
(4) Podobnie, jeśli $H \leqslant G$ (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 4.4. □

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 4.4 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 podzbioru $A \subseteq G$ 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 Konwersatorium 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:

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

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:

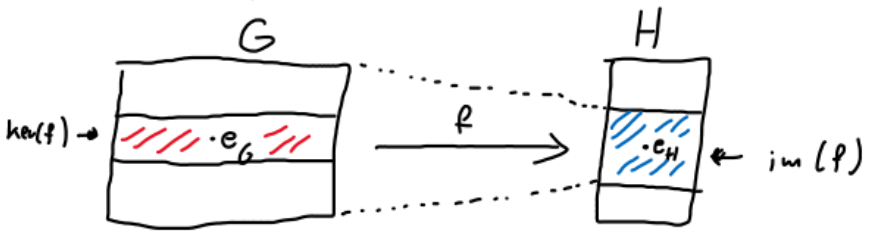
$$\forall\, g, h \in G \qquad\qquad F_{gh} = F_g \circ F_h,$$

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 5.9 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:

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

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:

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

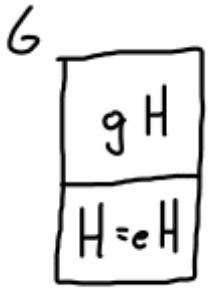
Zauważmy, że $[S_3 : A_3] = 2$.

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

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:

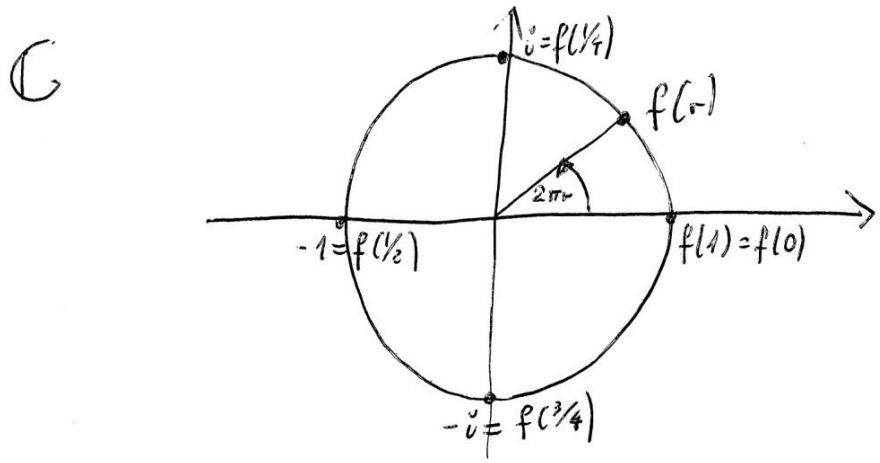
$$\mathrm{im}(f) = \{\mathrm{id}, (1,2)\} \not\trianglelefteq S_3.$$

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:

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



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

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

Stąd mamy:

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

Liczymy teraz:

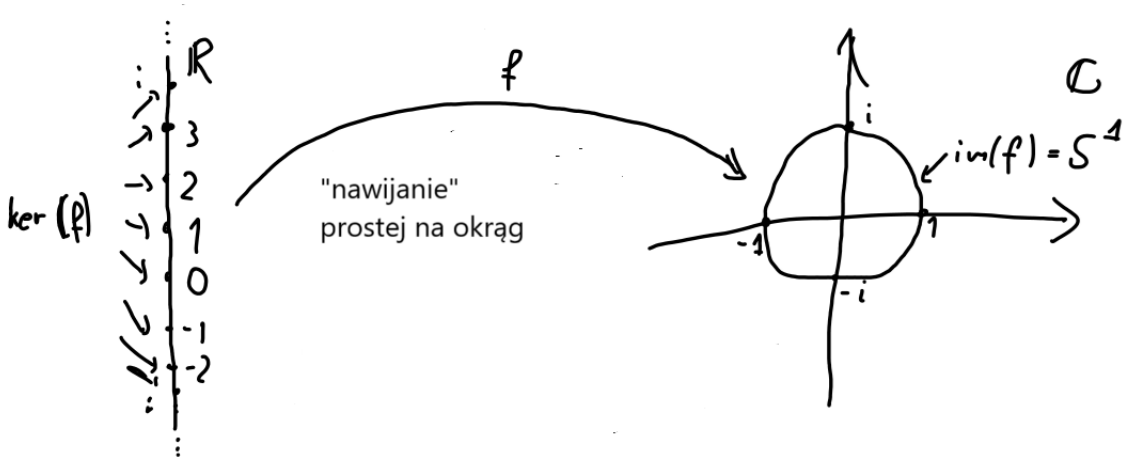
$$\operatorname{im}(f) = \{z \in \mathbb{C} \mid (\exists r \in \mathbb{R})\ e^{2r\pi i} = z\}.$$

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.

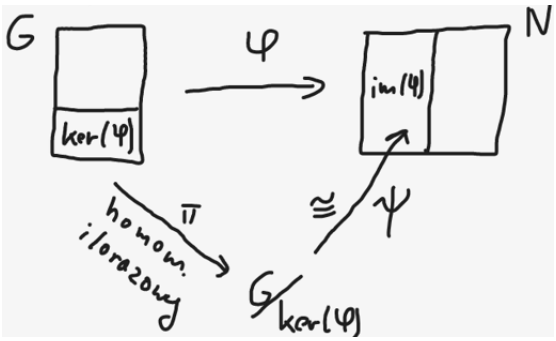
Twierdzenie 6.4 (Zasadnicze Twierdzenie o Homomorfizmach Grup)**.** *Niech $\varphi : G \to N$ będzie homomorfizmem grup. Wtedy mamy:*

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

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 jest podzbiorem $\mathbb{Z}_n$ mocy $n = |\,\mathbb{Z}_n\,|$, czyli 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 $Z(G) \trianglelefteq G$.

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 $Z(G) = G$.

Rozważmy teraz następujący motywujący przykład, który doprowadzi nas do pojęcia **automorfizmów wewnętrznych**. Weźmy niestandardową bazę przestrzeni liniowej $\mathbb{R}^2$, np.:

$$\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}.$$

Dla funkcji liniowej $f : \mathbb{R}^2 \to \mathbb{R}^2$ o macierzy A, tzn.:

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

gdzie:

$$f\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix} \right) = \begin{bmatrix} a \\ b \end{bmatrix} \quad \text{oraz} \quad f\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) = \begin{bmatrix} c \\ d \end{bmatrix},$$

chcemy policzyć macierz f w powyższej bazie niestandardowej

$$\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}.$$

Z algebry liniowej wiemy, że macierz f w tej nowej bazie to

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-1}.$$

Oznaczmy:

$$B := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Przy ustalonym B, dostajemy przekształcenie zamiany bazy:

$$\varphi_B : A \mapsto BAB^{-1}.$$

Jeśli funkcja f jest odwracalna, to mamy $A \in \mathrm{GL}_2(\mathbb{R})$ i dostajemy:

$$\varphi_B : \mathrm{GL}_2(\mathbb{R}) \to \mathrm{GL}_2(\mathbb{R}), \qquad \varphi_B(A) = BAB^{-1}.$$

Zamieniamy teraz $\mathrm{GL}_2(\mathbb{R})$ na dowolną grupę G i macierz B na dowolny element $g \in G$.

Twierdzenie 8.5. *Niech G będzie grupą i ustalmy $g \in G$. Definiujemy następującą funkcję:*

$$\varphi_g : G \to G, \qquad \varphi_g(x) = gxg^{-1}.$$

Wtedy φ_g jest automorfizmem grupy G.

Dowód. Niech $x, y \in G$. Liczymy:

$$\varphi_g(xy) = gxyg^{-1} = gx\underbrace{g^{-1}g}_{e}yg^{-1} = \varphi_g(x)\varphi_g(y),$$

czyli φ_g jest homomorfizmem. Mamy też:

$$\varphi_{g^{-1}}\left(\varphi_g(x)\right) = \varphi_{g^{-1}}\left(gxg^{-1}\right) = g^{-1}gxg^{-1}\left(g^{-1}\right)^{-1} = x.$$

Tak więc mamy:

$$\varphi_{g^{-1}} \circ \varphi_g = \mathrm{id}_G\,.$$

Podobnie otrzymujemy:

$$\varphi_g \circ \varphi_{g^{-1}} = \mathrm{id}_G\,.$$

Stąd $\varphi_g : G \to G$ jest bijekcją. Ponieważ φ_g jest też homomorfizmem, tak więc φ_g jest automorfizmem. □

Definicja 8.6. Jeśli G jest grupą oraz $g \in G$, to automorfizm postaci φ_g z Twierdzenia 8.5 nazywamy *automorfizmem wewnętrznym* grupy G wyznaczonym przez element g.

Twierdzenie 8.7. *Niech G będzie grupą. Definiujemy następującą funkcję:*

$$\varphi : G \to \mathrm{Aut}(G), \qquad \varphi(g) = \varphi_g,$$

gdzie φ_g jest automorfizmem wewnętrznym z Twierdzenia 8.5. Wtedy funkcja φ jest homomorfizmem grup.

Dowód. Weźmy $g, g' \in G$. Mamy pokazać, że:

$$\underbrace{\varphi(gg')}_{\varphi_{gg'}} = \underbrace{\varphi(g)}_{\varphi_g} \circ \underbrace{\varphi(g')}_{\varphi_{g'}}.$$

Aby to sprawdzić, weźmy dowolne $x \in G$. Liczymy:

$$\varphi_{gg'}(x) = gg'x(gg')^{-1} = gg'x\,(g')^{-1}\,g^{-1} = g\varphi_{g'}(x)g^{-1} = \varphi_g\left(\varphi_{g'}(x)\right) = \left(\varphi_g \circ \varphi_{g'}\right)(x).$$

Czyli faktycznie mamy: $\varphi_{gg'} = \varphi_g \circ \varphi_{g'}$. □

Definicja 8.8. Obraz homomorfizmu φ z Twierdzenia 8.7, czyli podgrupę $\mathrm{Aut}(G)$ składająca się z automorfizmów wewnętrznych grupy G, oznaczamy przez $\mathrm{Inn}(G)$.

Twierdzenie 8.9. *Mamy:*

$$\mathrm{Inn}(G) \cong G/Z(G).$$

Dowód. Z Twierdzenia 8.7 funkcja

$$\varphi : G \to \mathrm{Aut}(G)$$

jest homomorfizmem. Z Zasadniczego Twierdzenia o Homomorfizmach Grup otrzymujemy:

$$G/\ker(\varphi) \cong \mathrm{im}(\varphi) = \mathrm{Inn}(G).$$

Czyli wystarczy pokazać, że $\ker(\varphi) = Z(G)$. Liczymy:

$$\begin{aligned}
\ker(\varphi) &= \{g \in G \mid \varphi_g = \mathrm{id}_G\} \\
&= \{g \in G \mid \forall x \in G \;\; \varphi_g(x) = x\} \\
&= \{g \in G \mid \forall x \in G \;\; gxg^{-1} = x\} \\
&= \{g \in G \mid \forall x \in G \;\; gx = xg\} \\
&= Z(G),
\end{aligned}$$

co należało pokazać. □

Przykład 8.10. (1) Jeśli $G = \mathrm{GL}_n(\mathbb{R})$ i $B \in \mathrm{GL}_n(\mathbb{R})$, to wiemy że automorfizm wewnętrzny φ_B odpowiada zamianie bazy. Można pokazać, że:

$$Z(\mathrm{GL}_n(\mathbb{R})) = \{rI \mid r \in \mathbb{R}\setminus\{0\}\} \quad \text{(macierze skalarne)}.$$

(2) Rozważmy $G = S_4$ i popatrzmy na:

$$\varphi_{(1,2,3)}((1,2,3,4)) = (1,2,3)(1,2,3,4)(1,2,3)^{-1} = (1,2,3)(1,2,3,4)(1,3,2) =$$
$$= (1,4,2,3) = (2,3,1,4) = (\sigma(1),\sigma(2),\sigma(3),\sigma(4))$$

dla $\sigma = (1,2,3)$. Tak jest zawsze, czyli dla każdej $\sigma \in S_n$ oraz dla każdego cyklu $(k_1,\ldots,k_l) \in S_n$ mamy:

$$\sigma(k_1,\ldots,k_l)\sigma^{-1} = (\sigma(k_1),\ldots,\sigma(k_l)).$$

Czyli automorfizm wewnętrzny w S_n też można traktować jako "zamianę bazy" (bądź też "zamianę nośnika").

(3) Grupa G jest przemienna wtedy i tylko wtedy, gdy każdy automorfizm wewnętrzny w G jest identycznością.

Definicja 8.11. Niech G będzie grupą i $x, x' \in G$. Mówimy, że x i x' są *sprzężone*, gdy istnieje $g \in G$, taki że:

$$gxg^{-1} = g'.$$

Łatwo pokazać, że relacja sprzężenia w G jest relacją równoważności.

Definicja 8.12. Klasy abstrakcji relacji sprzężenia w G nazywamy *klasami sprzężoności*.

Przykład 8.13. (1) Grupa G jest przemienna wtedy i tylko wtedy, gdy klasy sprzężoności w G to singletony.

(2) Opiszemy klasy sprzężoności w grupie S_n. Z Przykładu 8.10(2) np. transpozycje tworzą klasę sprzężoności.
Podobnie: dla ustalonego $k \leqslant n$, cykle długości k tworzą klasę sprzężoności.
Ogólnie: dla każdych $\sigma, \tau \in S_n$ mamy, że σ i τ są sprzężone wtedy i tylko wtedy, gdy σ i τ mają ten sam **typ rozkładu** na cykle rozłączne.

(3) Jeśli $G = \mathrm{GL}_n(\mathbb{R})$ i $B \in \mathrm{GL}_n(\mathbb{R})$, to wiemy że automorfizm wewnętrzny φ_B odpowiada zamianie bazy. W $\mathrm{GL}_n(\mathbb{R})$ klasy sprzężoności są wyznaczone przez odwracalne funkcje liniowe

$$f : \mathbb{R}^n \to \mathbb{R}^n,$$

tzn., dla ustalonej f jak wyżej, wszystkie macierze f w różnych bazach $\mathbb{R}^n$ dają klasę sprzężoności w $\mathrm{GL}_n(\mathbb{R})$.

To koniec teorii grup na tym wykładzie, teraz zaczyna się:

TEORIA PIERŚCIENI

9. Pierścienie, elementy odwracalne i dziedziny

Rozważmy teraz **dwa** działania na ustalonym zbiorze.

Przykład 9.1. (1) Mamy działania dodawania ($+$) i mnożenia ($\cdot$) na zbiorach $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
(2) Mamy działania dodawania i mnożenia macierzy na zbiorze $M_n(\mathbb{R})$ (macierze n na n o współczynnikach z $\mathbb{R}$).
(3) Dla dowolnego zbioru X, mamy działania sumy ($\cup$) i przekroju ($\cap$) na zbiorze $\mathcal{P}(X)$ (zbiór wszystkich podzbiorów zbioru X).

Ustalmy zbiór R z dwoma działaniami, które oznaczamy przez $+$ i $\cdot$.

Definicja 9.2. (1) Trójkę $(R, +, \cdot)$ nazywamy *pierścieniem*, gdy:
(i) $(R, +)$ jest grupą przemienną.
(ii) Działanie $\cdot$ jest łączne.
(iii) Działanie $\cdot$ jest *rozdzielne* względem działania $+$, tzn. dla każdych $x, y, z \in R$ mamy:

$$(x + y) \cdot z = (x \cdot z) + (y \cdot z), \qquad z \cdot (x + y) = (z \cdot x) + (z \cdot y).$$

(2) Jeśli $(R, +, \cdot)$ jest pierścieniem i działanie $\cdot$ jest przemienne, to $(R, +, \cdot)$ nazywamy *pierścieniem przemiennym*.
(3) Jeśli $(R, +, \cdot)$ jest pierścieniem i działanie $\cdot$ ma element neutralny, to $(R, +, \cdot)$ nazywamy *pierścieniem z jedynką*.

Notacja 9.3. (1) Jeśli $(R, +, \cdot)$ jest pierścieniem, to element neutralny działania $+$ oznaczamy przez O_R lub po prostu przez 0.
(2) Jeśli $(R, +, \cdot)$ jest pierścieniem z jedynką, to element neutralny działania $\cdot$ oznaczamy przez 1_R lub po prostu przez 1 (z „Szybkiego Faktu" w Definicji 1.7(2) wiemy, że element neutralny jest jedyny).
(3) Zamiast „pierścień $(R, +, \cdot)$" często piszemy „pierścień R" (domyślając się działań).

Przykład 9.4. (1) $(\mathbb{N}, +, \cdot)$ **nie** jest pierścieniem, ponieważ $(\mathbb{N}, +)$ **nie** jest grupą.
(2) $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ są pierścieniami przemiennymi z jedynką.
(3) $(M_n(\mathbb{R}), +, \cdot)$ jest pierścieniem z jedynką ($1_{M_n(\mathbb{R})} = I$).
Jeśli $n \geqslant 2$, to $(M_n(\mathbb{R}), +, \cdot)$ nie jest pierścieniem przemiennym.
(4) Jeśli $X \neq \emptyset$, to $(\mathcal{P}(X), \cup, \cap)$ **nie** jest pierścieniem, ponieważ $(\mathcal{P}(X), \cup)$ **nie** jest grupą.
Podobnie: $(\mathcal{P}(X), \cap, \cup)$ nie jest pierścieniem, ponieważ $(\mathcal{P}(X), \cap)$ nie jest grupą.
Wciąż mamy, że:
- $\cup$ jest rozdzielne względem $\cap$,
- $\cap$ jest rozdzielne względem $\cup$.

Notacja 9.5. Niech $(R, +, \cdot)$ będzie pierścieniem.

(1) $(R, +)$ to *grupa addytywna* pierścienia R.
(2) Jeśli $a \in R$, to *elementem przeciwnym* do a nazywany element odwrotny do a w grupie $(R, +)$ i oznaczamy ten element przeciwny przez $-a$.
(3) Dla $a, b \in R$ definiujemy:

$$a - b := a + (-b).$$

(4) Dla $a, b \in R$ zamiast „$a \cdot b$" często piszemy „ab".
(5) Mnożenie wykonujemy przed dodawaniem, tzn. dla $a, b, c \in R$ zapis „$ab + c$" oznacza „$(a \cdot b) + c$".
(6) Dla $n > 0$ i $a \in R$ mamy:

$$n \cdot a := \underbrace{a + \ldots + a}_{n \text{ razy}}, \qquad 0 \cdot a := 0_R, \qquad (-n) \cdot a := -(n \cdot a).$$

Stąd dla każdego $n \in \mathbb{Z}$ i dla każdego $a \in R$ mamy zdefiniowane $n \cdot a \in R$.

(7) Dla $n > 0$ i $a \in R$ mamy:

$$a^n := \underbrace{a \cdot \ldots \cdot a}_{n \text{ razy}}.$$

Jeśli R jest pierścieniem z jedynką, to:

$$a^0 := 1_R.$$

Fakt 9.6. *Jeśli $(R, +, \cdot)$ jest pierścieniem i $a, b, c \in R$, to wtedy mamy:*

(i) $0_R \cdot a = 0_R = 0_R \cdot a$;
(ii) $-(-a) = a$;
(iii) $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$;
(iv) $(-a) \cdot (-b) = a \cdot b$;
(v) $a \cdot (b - c) = a \cdot b - a \cdot c$, $(b - c) \cdot a = b \cdot a - c \cdot a$;
(vi) *jeśli R jest pierścieniem z jedynką, to* $(-1_R) \cdot a = -a = a \cdot (-1_R)$.

Dowód. (i) Mamy:

$$0_R \cdot a = (0_R + 0_R) \cdot a \underbrace{=}_{\text{rozdzielność}} 0_R \cdot a + 0_R \cdot a.$$

Odejmując stronami $0_R \cdot a$, dostajemy $0_R \cdot a = 0_R$. Podobnie pokazuje się, że $a \cdot 0_R = 0_R$.

(ii) Wiemy, że w dowolnej grupie element odwrotny do elementu odwrotnego to wyjściowy element, co stosujemy do grupy $(R, +)$.

(iii) Mamy:

$$(-a) \cdot b + a \cdot b = (-a + a) \cdot b = 0_R \cdot b \underbrace{=}_{\text{(i)}} 0_R.$$

Stąd dostajemy $(-a) \cdot b = -(a \cdot b)$. Podobnie pokazuje się, że $a \cdot (-b) = -(a \cdot b)$.

(iv) Mamy:

$$(-a) \cdot (-b) \underbrace{=}_{\text{(iii)}} -(a \cdot (-b)) \underbrace{=}_{\text{(iii)}} -(-(a \cdot b)) \underbrace{=}_{\text{(ii)}} a \cdot b.$$

(v) Mamy:

$$a \cdot (b - c) = a \cdot ((b + (-c)) = a \cdot b + a \cdot (-c) \underbrace{=}_{\text{(iii)}} a \cdot b - a \cdot c.$$

Podobnie pokazuje się, że $(b - c) \cdot a = b \cdot a - c \cdot a$.

(vi) Mamy:

$$(-1_R) \cdot a + a = (-1_R) \cdot a + 1_R \cdot a = (-1_R + 1_R) \cdot a = 0_R \cdot a \underbrace{=}_{\text{(i)}} 0_R.$$

Stąd dostajemy, że $-a = (-1_R) \cdot a$. Podobnie pokazuje się, że $-a = (-1_R) \cdot a$.

□

Prawie zawsze zachodzi $0_R \neq 1_R$ o czym mówi następujący wynik.

Fakt 9.7. *Jeśli R jest pierścieniem z jedynką i $0_R = 1_R$, to R jest* pierścieniem zerowym, *tzn.:*

$$R = \{0_R\}, \qquad 0_R + 0_R = 0_R, \qquad 0_R \cdot 0_R = 0_R.$$

Dowód. Weźmy dowolny $a \in R$. Wtedy mamy:

$$a = a \cdot 1_R = a \cdot 0_R \underbrace{=}_{\text{9.6(i)}} 0_R,$$

czyli $R = \{0_R\}$. □

Przykład 9.8. (1) Dla każdego $n > 1$, $(n\mathbb{Z}, +, \cdot)$ jest pierścieniem przemiennym (bez jedynki!).

(2) Zobaczymy, że $(\mathbb{Z}_n, +_n, \cdot_n)$ jest pierścieniem przemiennym z jedynką. Wszystko już sprawdziliśmy wcześniej poza rozdzielnością $\cdot_n$ względem $+_n$. Weźmy $a, b, c \in \mathbb{Z}_n$. Wtedy mamy:

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

$$= r_n(ac + bc) = r_n(ac) +_n r_n(bc) = a \cdot_n c +_n b \cdot_n c.$$

Pierścień $(\mathbb{Z}_n, +_n, \cdot_n)$ nazywamy *pierścieniem reszt modulo n.*

(3) Jeśli R jest pierścieniem przemiennym z jedynką (jak np. $\mathbb{Z}_n, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$), to mamy pierścień macierzy $M_n(R)$ (z jedynką) o współczynnikach z R, gdzie działania pochodzą z pierścienia R podobnie jak działania w pierścieniu macierzy $M_n(\mathbb{R})$ pochodzą od działań w pierścieniu liczb rzeczywistych $\mathbb{R}$. Dla przykładu rozważmy pierścień $M_2(\mathbb{Z}_3)$:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} a +_3 a' & b +_3 b' \\ c +_3 c' & d +_3 d' \end{bmatrix},$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} a \cdot_3 a' +_3 b \cdot_3 c' & a \cdot_3 b' +_3 b \cdot_3 d' \\ c \cdot_3 a' +_3 d \cdot_3 c' & c \cdot_3 b' +_3 d \cdot_3 d' \end{bmatrix}.$$

(4) Niech X będzie zbiorem i R będzie pierścieniem. Przez R^X oznaczamy zbiór wszystkich funkcji $X \to R$. Wtedy R^X staje się pierścieniem z następującymi działaniami. Dla $f, g \in R^X$ oraz $x \in X$ definiujemy:

$$(f + g)(x) := f(x) +_R g(x), \qquad (f \cdot g)(x) := f(x) \cdot_R g(x)$$

(dodawanie i mnożenie funkcji).
Jeśli R jest pierścieniem przemiennym, to R^X jest też pierścieniem przemiennym.
Jeśli R jest pierścieniem z jedynką, to R^X jest też pierścieniem z jedynką, gdzie 1_{R^X} jest funkcją stałą o wartości 1_R.

(5) Definiujemy:

$$C(\mathbb{R}) := \{f \in \mathbb{R}^{\mathbb{R}} \mid f \text{ jest ciągła}\}.$$

Wtedy $C(\mathbb{R}) \subset \mathbb{R}^{\mathbb{R}}$ i $C(R)$ jest pierścieniem (przemiennym z jedynką) z działaniami dodawania i mnożenia funkcji, ponieważ (między innymi) suma/iloczyn funkcji ciągłych jest funkcją ciągłą.

(6) Niech:

$$\mathbb{Z}[i] := \{n + mi \in \mathbb{C} \mid n, m \in \mathbb{Z}\}.$$

Dla $a + bi, c + di \in \mathbb{Z}[i]$ mamy:

$$(a + bi) + (c + di) = (a + c) + (b + d)i \in \mathbb{Z}[i],$$

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i \in \mathbb{Z}[i].$$

Stąd $\mathbb{Z}[i]$ jest pierścieniem zwanym *pierścieniem Gaussa.*

W danym pierścieniu R wyróżnimy teraz pewne specjalne elementy.

Definicja 9.9. Niech R będzie pierścieniem z jedynką i $a \in R$.

(1) Element a nazywamy *elementem odwracalnym* pierścienia R, gdy istnieje $b \in R$, taki że:

$$ab = 1 = ba.$$

(2) Przez R^* oznaczamy zbiór wszystkich elementów odwracalnych pierścienia R.

Twierdzenie 9.10. *Niech R będzie pierścieniem z jedynką. Wtedy mamy:*

(1) *dla każdych $a, b \in R^*$*

$$ab \in R^*,$$

(2) *$(R^*, \cdot)$ jest grupą.*

Dowód. (1) Weźmy $a, b \in R^*$. Czyli istnieją $a', b' \in R$, takie że:

$$aa' = a'a = 1 = bb' = b'b.$$

Wtedy mamy:

$$(ab)\,(b'a') = a\underbrace{bb'}_{1}a' = aa' = 1 = b'b = b'\underbrace{a'a}_{1}b = (b'a')\,ab.$$

Stąd $ab \in R^*$, co mieliśmy pokazać.

(2) Działanie $\cdot$ jest łączne na R, czyli jest też łączne na R^*. Jedynka pierścienia R jest też elementem neutralnym $\cdot$ na R^*. Jeśli $a \in R^*$, to istnieje $b \in R$, taki że:

$$ab = 1 = ba.$$

Wtedy $b \in R^*$ i b jest elementem odwrotnym do a w $(R^*, \cdot)$.

□

Wniosek 9.11. *Jeśli $a \in R^*$, to istnieje **jedyny** $b \in R^*$, taki że $ab = 1 = ba$. Oznaczamy wtedy:*

$$a^{-1} := b.$$

Dowód. Wiemy, że jest taka własność grup (jedyność elementu odwrotnego). □

Definicja 9.12. Niech R będzie pierścieniem z jedynką. Grupę $(R^*, \cdot)$ nazywamy *grupą elementów odwracalnych* (lub *grupą multyplikatywną*) pierścienia R.

Uwaga 9.13. Niech R będzie pierścieniem.

(1) Wiemy, że:
$$0 \in R^* \quad \iff \quad R = \{0\}.$$
(2) Mamy grupę addytywną $(R, +)$.
(3) Jeśli R jest pierścieniem z jedynką, to mamy też grupę multyplikatywną $(R^*, \cdot)$.
(4) Jeśli R nie jest pierścieniem zerowym, to $(R, \cdot)$ **nie** jest grupą (0 nie ma elementu odwrotnego)!
(5) Jeśli R nie jest pierścieniem zerowym, to $+$ **nie** jest nawet działaniem na R^* ($1, -1 \in R^*$ ale $1 + (-1) = 0 \notin R^*$)!

Przykład 9.14. (1) Mamy $\mathbb{Z}^* = \{1, -1\}$, czyli $\mathbb{Z}^* \cong (\mathbb{Z}_2, +_2)$.

(2) Mamy $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. Podobnie $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ oraz $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$

(3) Dla $n > 1$ mamy:
$$(\mathbb{Z}_n)^* = \{k \in \mathbb{Z}_n \mid \mathrm{NWD}(k, n) = 1\} = \text{„stare } \mathbb{Z}_n^*\text{”}.$$
W szczególności, jeśli liczba p jest pierwsza, to mamy:
$$\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}.$$

(4) Udowodnimy, że:
$$\mathbb{Z}[i]^* = \{1, -1, i, -i\}.$$
„$\supseteq$” oczywiste: $(-1)(-1) = 1 = i(-i)$.
„$\subseteq$” Weźmy $a + bi \in \mathbb{Z}[i]^*$, tzn. $a, b \in \mathbb{Z}$ oraz istnieją $c, d \in \mathbb{Z}$, takie że:
$$(a + bi)(c + di) = 1.$$
Nakładamy na ostatnią równość $|\cdot|^2$ i korzystamy z multyplikatywności $|\cdot|^2$:
$$|(a + bi)(c + di)|^2 = |1|^2,$$
$$|(a + bi)|^2|(c + di)|^2 = 1,$$
$$\underbrace{(a^2 + b^2)}_{\in\mathbb{Z}}\underbrace{(c^2 + d^2)}_{\in\mathbb{Z}} = 1.$$
Stąd mamy:
$$a^2 + b^2 \in \mathbb{Z}^* = \{-1, 1\} \quad \text{oraz} \quad a^2 + b^2 \geqslant 0.$$

Czyli dostajemy, że:

$$a^2 + b^2 = 1 \quad \text{oraz} \quad a, b \in \mathbb{Z}\,.$$

Tak więc mamy:

$$(a = \pm 1 \ \text{ i } \ b = 0) \quad \text{lub} \quad (a = 0 \ \text{ i } \ b = \pm 1).$$

Stąd dostajemy cztery możliwości, które dokładnie dają, że $a + bi \in \{1, -1, i, -i\}$.

(5) Z definicji grupy $\mathrm{GL}_n(\mathbb{R})$ dostajemy, że:

$$M_n(\mathbb{R})^* = \mathrm{GL}_n(\mathbb{R}).$$

(6) Niech R będzie pierścieniem przemiennym z jedynką i X będzie zbiorem. Wtedy mamy:

$$\left(R^X\right)^* = \left\{f \in R^X \mid \forall x \in X \ \ f(x) \in R^*\right\} = \left(R^*\right)^X.$$

Teraz zajmiemy się elementami zupełnie innego typu (niż elementy odwracalne).

Definicja 9.15. Niech R będzie pierścieniem przemiennym i $a \in R$. Mówimy, że a jest *dzielnikiem zera*, gdy:

(i) $a \neq 0$,
(ii) istnieje $b \in R \setminus \{0\}$, taki że $ab = 0$.

Twierdzenie 9.16. *Niech R będzie pierścieniem przemiennym z jedynką i $a \in R^*$. Wtedy a **nie** jest dzielnikiem zera.*

Dowód. Załóżmy nie wprost, że $a \in R^*$ i że a jest dzielnikiem zera, tzn. istnieje $b \in R \setminus \{0\}$, taki że $ab = 0$. Mnożąc obustronnie ostatnią równość przez a^{-1} dostajemy:

$$b = a^{-1}ab = a^{-1} \cdot 0 = 0.$$

Stąd $b = 0$, co daje sprzeczność. □

Definicja 9.17. Niezerowy pierścień przemienny z jedynką w którym nie ma dzielników zera nazywamy *dziedziną*.

Przykład 9.18. (1) Pierścienie $\mathbb{Z}, \mathbb{Z}[i], \mathbb{Q}, \mathbb{R}, \mathbb{C}$ są dziedzinami.
(2) Pierścień $\mathbb{Z}_{10}$ nie jest dziedziną, ponieważ $2, 5 \in \mathbb{Z}_{10} \setminus \{0\}$ oraz $2 \cdot_{10} 5 = 0$.
(3) Jeśli p jest liczbą pierwszą, to pierścień $\mathbb{Z}_p$ jest dziedziną, bo wiemy że każdy niezerowy element $\mathbb{Z}_p$ jest odwracalny, czyli (używając Twierdzenia 9.16) tenże niezerowy element $\mathbb{Z}_p$ nie może być dzielnikiem zera.

Następny wynik zawiera implikację odwrotną do tej w Przykładzie 9.18(3).

Twierdzenie 9.19. *Niech $n > 1$. Wtedy mamy:*

$$\mathbb{Z}_n \textit{ jest dziedziną} \qquad \Leftrightarrow \qquad n \textit{ jest liczbą pierwszą.}$$

Dowód. Implikacja "$\Leftarrow$" to dokładnie Przykład 9.18(3).
Implikację "$\Rightarrow$" pokazujemy przez **kontrapozycję**, tzn. zakładamy że n **nie** jest liczbą pierwszą i pokazujemy, że pierścień $\mathbb{Z}_n$ **nie** jest dziedziną. Skoro n nie jest liczbą pierwszą, to istnieją $k, l > 1$, takie że $n = kl$. Wtedy $k, l \in \mathbb{Z}_n \setminus \{0\}$ oraz

$$k \cdot_n l = 0,$$

czyli faktycznie pierścień $\mathbb{Z}_n$ nie jest dziedziną. □

Następny wynik uogólnia Twierdzenie 9.19.

Twierdzenie 9.20. *Niech R będzie skończonym pierścieniem przemiennym z jedynką oraz $a \in R \setminus \{0\}$. Wtedy następujące warunki są równoważne.*

(1) $a \in R^*$,
(2) *a nie jest dzielnikiem zera,*
(3) *istnieje $m \geqslant 1$, takie że $a^m = 1$.*

Dowód. Implikacja "(1) $\Rightarrow$ (2)" zachodzi dla dowolnych pierścieni przemiennych z jedynką na mocy Twierdzenia 9.16.
Dla dowodu implikacji "(2) $\Rightarrow$ (3)", używając zasady szufladkowej oraz skończoności R, dostajemy że istnieją $n, m > 0$, takie że:

$$a^{n+m} = a^n.$$

Stąd mamy:

$$a^n(a^m - 1) = 0 \qquad \Rightarrow \qquad aa^{n-1}(a^m - 1) = 0.$$

Ponieważ R jest dziedziną oraz $a \neq 0$, ostatnia równość implikuje:

$$a^{n-1}(a^m - 1) = 0.$$

Podobnie dostajemy:

$$a^{n-2}(a^m - 1) = 0$$

oraz poprzez indukcję mamy:

$$a^m - 1 = 0.$$

Czyli $a^m = 1$, co należało pokazać.
Dla dowodu implikacji "(3) $\Rightarrow$ (1)", zauważmy że:

$$a^m = 1 \qquad \Rightarrow \qquad aa^{m-1} = 1,$$

czyli $a \in R^*$. □

W poprzednim dowodzie pojawiła się:

Zasada skracania dla dziedzin.
Jeśli R jest dziedziną, $a, b, c \in R$, $a \neq 0$ i $ab = ac$, to wtedy $b = c$.

Dowód. Ponieważ $ab = ac$, tak więc dostajemy:

$$a(b - c) = 0.$$

Ponieważ $a \neq 0$ i R jest dziedziną, dostajemy że $b - c = 0$, czyli $b = c$. □

Uwaga 9.21. W powyższej zasadzie wystarczy założenie, że $a \neq 0$ i a nie jest dzielnikiem zera.

10. Ciała, homomorfizmy pierścieni i pierścienie wielomianów

Teraz zobaczymy kolejną definicję, która wyróżnia „najlepsze" pierścienie, takie jak $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Definicja 10.1. *Ciało* K to pierścień przemienny z jedynką, taki że:

$$K^* = K \setminus \{0\}$$

(niezerowe elementy są odwracalne).

Przykład 10.2. (1) Pierścienie $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ są ciałami.

(2) Jeśli p jest liczbą pierwszą, to pierścień $\mathbb{Z}_p$ jest ciałem.

(3) Wiemy, że pierścień $\mathbb{Z}_4$ **nie** jest ciałem. Ale wciąż istnieje ciało $K = \{0, 1, a, b\}$ mocy 4. Napiszemy tabelki $+$ i $\cdot$ w tym ciele.

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Wtedy mamy:

$$(K, +) \cong \underbrace{K_4}_{\text{grupa Kleina}} \cong (\mathbb{Z}_2, +_2) \times (\mathbb{Z}_2, +_2), \qquad K^* \cong (\mathbb{Z}_3, +_3).$$

Twierdzenie 10.3. *Niech R będzie pierścieniem przemiennym z jedynką. Wtedy mamy:*

(1) *jeśli R jest ciałem, to R jest dziedziną;*

(2) *jeśli R jest skończony i jest dziedziną, to R jest ciałem.*

Dowód. (1) Niech R będzie ciałem i $a \in R \setminus \{0\}$. Wtedy $a \in R^*$, czyli (na mocy Twierdzenia 9.16) a nie jest dziennikiem zera. Stąd w R nie ma dzielników zera, tzn. R jest dziedziną.

(2) Załóżmy, że R jest skończony i że jest dziedziną. Weźmy $a \in R \setminus \{0\}$. Ponieważ R jest dziedziną, tak więc a nie jest dzielnikiem zera. Z Twierdzenia 9.20 (implikacja „(2) $\Rightarrow$ (1)") otrzymujemy, że $a \in R^*$. Stąd R jest ciałem.

□

Wniosek 10.4. *Niech $n \geqslant 2$. Wtedy następujące warunki są równoważne:*

(1) *liczba n jest pierwsza,*

(2) *pierścień $\mathbb{Z}_n$ jest dziedziną,*

(3) *pierścień $\mathbb{Z}_n$ jest ciałem.*

Przykład 10.5. Założenie skończoności jest niezbędne w Twierdzeniu 10.3(2), bo np. pierścień $\mathbb{Z}$ jest dziedziną, ale nie jest ciałem.

Podobnie jak dla grup, mamy też pojęcie homomorfizmów pierścieni.

Definicja 10.6. Niech R i S będą pierścieniami.

(1) Funkcja $f : R \to S$ jest *homomorfizmem pierścieni*, gdy dla każdych $x, y \in R$ mamy:

$$f(x +_R y) = f(x) +_S f(y), \qquad f(x \cdot_R y) = f(x) \cdot_S f(y).$$

(2) Jeśli R, S są pierścieniami z jedynką, to dodatkowo wymagamy, że:

$$f(1_R) = 1_S.$$

Przykład 10.7. (1) Funkcja $r_n : \mathbb{Z} \to \mathbb{Z}_n$ jest homomorfizmem pierścieni, bo dla każdych $x, y \in \mathbb{Z}$ mamy:

$$r_n(x + y) = r_n(x) +_n r_n(y), \qquad r_n(x \cdot y) = r_n(x) \cdot_n r_n(y), \qquad r_n(1) = 1.$$

(2) Naturalne funkcje inkluzji:

$$\mathbb{Z} \to \mathbb{Q}, \qquad \mathbb{Q} \to \mathbb{R}, \qquad \mathbb{R} \to \mathbb{C}$$

są homomorfizmami pierścieni.

Uwaga 10.8. Podobnie jak w przypadku grup, mamy pojęcie *izomorfizmu* pierścieni, tzn. bijektywnego homomorfizmu pierścieni. Jeśli istnieje izomorfizm pierścieni $R \to S$, to mówimy że pierścienie R i S są *izomorficzne* i piszemy $R \cong S$. Podobnie jak w przypadku grup, izomorficzne pierścienie mają te same własności algebraiczne, tzn. np. jeśli R jest dziedziną i $R \cong S$, to wtedy S jest też dziedziną.

Podobnie jak dla grup mamy pojęcie produktu pierścieni.

Definicja 10.9. Niech R i S będą pierścieniami. Definiujemy działania $+$ i $\cdot$ na $R \times S$:

$$(r,s) + (r',s') := (r +_R r', s +_S s'), \qquad (r,s) \cdot (r',s') := (r \cdot_R r', s \cdot_S s').$$

Wtedy trójka $(R \times S, +, \cdot)$ jest pierścieniem zwanym *produktem* pierścieni R i S, np. mamy:

$$0_{R\times S} = (0_R, 0_S).$$

Twierdzenie 10.10. *Niech R, S będą pierścieniami.*

(1) *Jeśli R, S są pierścieniami z jedynką, to $R \times S$ jest pierścieniem z jedynką.*
(2) *Jeśli R, S są pierścieniami przemiennymi, to $R \times S$ jest pierścieniem przemiennym.*
(3) *Mamy:*

$$(R \times S)^* = R^* \times S^*.$$

Dowód. Łatwe dowody punktów (1) i (2) pomijamy. Dla dowodu (3) weźmy $(r,s) \in R \times S$. Wtedy mamy:

$$\begin{aligned} (r,s) \in (R\times S)^* &\Leftrightarrow \exists\, (r',s') \in R \times S \qquad (r,s)\cdot(r',s') = (1_R,1_S) = (r',s')\cdot(r,s) \\ &\Leftrightarrow \exists r' \in R\ \exists s' \in S \qquad\quad rr' = 1_R = r'r, \quad ss' = 1_S = s's \\ &\Leftrightarrow (r,s) \in R^* \times S^*. \end{aligned}$$

Czyli faktycznie: $(R \times S)^* = R^* \times S^*$. □

Uwaga 10.11. Produkt pierścieni $R \times S$ prawie nigdy **nie jest dziedziną** (chyba, że np. R jest dziedziną i $S = \{0\}$), bo mamy:

$$(r,0)\cdot(0,s) = (0,0).$$

Twierdzenie 10.12. *Załóżmy, że liczby $n, m > 1$ są względnie pierwsze. Wtedy następująca funkcja:*

$$f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, \qquad f(x) = (r_m(x), r_n(x))$$

jest izomorfizmem pierścieni.

Dowód. Wiemy, że jeśli $k \mid l$, to wtedy funkcja

$$r_k : (\mathbb{Z}_l, +_l) \to (\mathbb{Z}_k, +_k)$$

jest homomorfizmem grup, tzn.

$$\forall\, x,y \in \mathbb{Z}_l \qquad\qquad r_k(x +_l y) = r_k(x) +_k r_k(y).$$

Podobnie można pokazać, że:

$$\forall\, x,y \in \mathbb{Z}_l \qquad\qquad r_k(x \cdot_l y) = r_k(x) \cdot_k r_k(y).$$

Czyli funkcja $r_k : \mathbb{Z}_l \to \mathbb{Z}_k$ jest homomorfizmem pierścieni (gdy $k \mid l$). W szczególności, funkcje:

$$r_n : \mathbb{Z}_{mn} \to \mathbb{Z}_n, \qquad r_m : \mathbb{Z}_{mn} \to \mathbb{Z}_m$$

są homomorfizmami pierścieni. Weźmy $x, y \in \mathbb{Z}_{mn}$. Wtedy mamy:

$$\begin{aligned} f(x +_{mn} y) &= (r_m(x +_{mn} y), r_n(x +_{mn} y)) \\ &= (r_m(x) +_m r_m(y), r_n(x) +_n r_n(y)) \\ &= (r_m(x), r_n(x)) + (r_m(y), r_n(y)) \\ &= f(x) + f(y). \end{aligned}$$

Podobnie pokazuje się, że:

$$f\left(x \cdot_{mn} y\right) = f(x) \cdot f(y).$$

Czyli funkcja f jest homomorfizmem pierścieni. Pozostaje pokazać, że f jest bijekcją. Mamy:

$$|\,\mathbb{Z}_{mn}\,| = mn = |\,\mathbb{Z}_m \times \mathbb{Z}_n\,|,$$

czyli wystarczy pokazać, że f jest „1-1". Na mocy Twierdzenia 5.19 (traktując f jako homomorfizm grup addytywnych), wystarczy pokazać, że $\ker(f) = \{0\}$. Mamy:

$$\ker(f) = \left\{x \in \mathbb{Z}_{mn} \;\middle|\; f(x) = 0_{\mathbb{Z}_m \times \mathbb{Z}_n}\right\}.$$

Dla każdego $x \in \ker(f)$ mamy:

$$(0,0) = 0_{\mathbb{Z}_m \times \mathbb{Z}_n} = f(x) = \left(r_m(x), r_n(x)\right).$$

Stąd dostajemy $r_m(x) = 0$ oraz $r_n(x) = 0$, czyli:

$$m \mid x \qquad \text{oraz} \qquad n \mid x.$$

Ponieważ m i n są względnie pierwsze, otrzymujemy że $mn \mid x$, tak więc $x = 0$, ponieważ $x \in \mathbb{Z}_{mn}$. Stąd $\ker(f) = \{0\}$, co należało pokazać. □

Definiujemy ogólnie jądro homomorfizmów pierścieni w ten sam sposób, jak było ono użyte w powyższym dowodzie.

Definicja 10.13. Jeśli $f : R \to S$ jest homomorfizmem pierścieni, to *jądro* f definiujemy jako:

$$\ker(f) := \{x \in R \mid f(x) = 0_S\}.$$

Kolejna definicja jest związana z pierścieniami reszt.

Definicja 10.14. *Funkcja Eulera*, oznaczana:

$$\varphi : \mathbb{N}_{>1} \to \mathbb{N}_{>0}$$

jest zdefiniowana w następujący sposób:

$$\varphi(n) := |\{k \in \{1, 2, \ldots, n-1\} \;:\; \mathrm{NWD}(k,n) = 1\}|.$$

Uwaga 10.15. Wiemy, że:

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

Stąd mamy:

$$\varphi(n) = |\,\mathbb{Z}_n^*\,|.$$

Powyższa uwaga ma związek z następującym twierdzeniem, które uogólnia Małe Twierdzenie Fermata.

Twierdzenie 10.16 (Twierdzenie Eulera)**.** *Niech $k, n > 0$ będą względnie pierwsze. Wtedy mamy:*

$$n^{\varphi(k)} \equiv 1 \pmod{k}.$$

Dowód. Wystarczy pokazać, że:

$$r_k(n)^{\varphi(k)} = 1$$

w grupie $\mathbb{Z}_k^*$.

Element $r_k(n)$ należy do $\mathbb{Z}_k^*$, ponieważ:

$$\mathrm{NWD}(k,n) = 1 \qquad \Rightarrow \qquad \mathrm{NWD}\left(k, r_k(n)\right) = 1.$$

Ponieważ $|\,\mathbb{Z}_k^*\,| = \varphi(k)$, tak więc na mocy Wniosku 4.14 dostajemy, że $r_k(n)^{\varphi(k)} = 1$ (w grupie $\mathbb{Z}_k^*$), co należało pokazać. □

Uwaga 10.17. Ponieważ dla liczby pierwszej p mamy:

$$\varphi(p) = |\,\mathbb{Z}_p^*\,| = p - 1,$$

tak więc faktycznie Twierdzenie Eulera uogólnia Małe Twierdzenie Fermata.

Teraz chcemy policzyć wartość $\varphi(n)$ dla dowolnego $n > 1$. Okazuje się, że jest to możliwe jeśli tylko umiemy rozłożyć n na czynniki pierwsze. Potrzebujemy dwóch lematów.

Lemat 10.18. *Jeśli p jest liczbą pierwszą i $m \geqslant 1$, to wtedy:*

$$\varphi\left(p^m\right) = p^m - p^{m-1}.$$

Dowód. Liczba $k \in \mathbb{N}$ **nie** jest względnie pierwsza z p^m wtedy i tylko wtedy, gdy k jest wielokrotnością p. Wielokrotności p w zniorze $\mathbb{Z}_{p^m} = \{0, 1, \ldots, p^m - 1\}$ to dokładnie:

$$0 \cdot p, 1 \cdot p, 2 \cdot p, \ldots, \left(p^{m-1} - 1\right) \cdot p$$

i jest ich p^{m-1}. Stąd mamy:

$$\varphi\left(p^m\right) = |\, \mathbb{Z}_{p^m}^* \,| = p^m - p^{m-1},$$

co należało pokazać. □

Lemat 10.19. *Jeśli $k, l > 1$ są względnie pierwsze, to wtedy:*

$$\varphi(kl) = \varphi(k)\varphi(l).$$

Dowód. Wiemy, że:

$$\varphi\left(kl\right) = |\, \mathbb{Z}_{kl}^* \,|.$$

Ponieważ k i 1 są względnie pierwsze, to z Twierdzenia 10.12 dostajemy, że:

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

(izomorfizm pierścieni). Stąd mamy, że:

$$\mathbb{Z}_{kl}^* \cong \left(\mathbb{Z}_k \times \mathbb{Z}_l\right)^* = \mathbb{Z}_k^* \times \mathbb{Z}_l^*,$$

gdzie równość wynika z Twierdzenia 10.10(3). Czyli mamy:

$$\varphi\left(kl\right) = |\, \mathbb{Z}_{kl}^* \,| = |\, \mathbb{Z}_k^* \times \mathbb{Z}_l^* \,| = |\, \mathbb{Z}_k^* \,| \cdot |\, \mathbb{Z}_l^* \,| = \varphi(k)\varphi(l),$$

co należało pokazać. □

Twierdzenie 10.20. *Załóżmy, że*

$$n = p_1^{k_1} \cdot \ldots \cdot p_l^{k_l},$$

gdzie $p_1, \ldots, p_l$ to parami różne liczby pierwsze i $k_1, \ldots, k_l > 0$. Wtedy mamy:

$$\varphi(n) = \left(p_1^{k_1} - p_1^{k_1 - 1}\right) \cdot \ldots \cdot \left(p_l^{k_l} - p_l^{k_l - 1}\right).$$

Dowód. Liczby $p_1^{k_1}, \ldots, p_l^{k_l}$ są względnie pierwsze. Używając Lematu 12.6 (i prostej indukcji) dostajemy:

$$\varphi(n) = \varphi\left(p_1^{k_1} \cdot \ldots \cdot p_l^{k_l}\right) = \varphi\left(p_1^{k_1}\right) \cdot \ldots \cdot \varphi\left(p_l^{k_l}\right).$$

Z Lematu 12.5 dostajemy, że dla każdego $i \leqslant l$ mamy:

$$\varphi\left(p_i^{k_i}\right) = p_i^{k_i} - p_i^{k_i - 1},$$

co daje tezę. □

Przykład 10.21. Obliczmy $\varphi(100)$ i $\varphi(315)$.

$$\varphi(100) = \varphi\left(2^2 \cdot 5^2\right) = \left(2^2 - 2^1\right)\left(5^2 - 5^1\right) = 2 \cdot 20 = 40,$$

$$\varphi(315) = \varphi\left(3^2 \cdot 5 \cdot 7\right) = \left(3^2 - 3^1\right)(5 - 1)(7 - 1) = 6 \cdot 4 \cdot 6 = 144.$$

Niech R będzie pierścieniem przemiennym z jedynką. Chcemy zdefiniować pojęcie **wielomianu** o współczynnikach z R. W analizie, wielomian (o współczynnikach rzeczywistych) jest rozumiany jako funkcja $f : \mathbb{R} \to \mathbb{R}$ postaci:

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

dla pewnego $n \in \mathbb{N}$ i pewnych $a_0, a_1, \ldots, a_n \in \mathbb{R}$.

Jednak np. nad ciałem skończonym $\mathbb{Z}_2$ mamy trzy **różne wielomiany**:

$$f(x) = 1 + x, \qquad h(x) = 1 + x^2, \qquad g(x) = 1 + x^3$$

dające **te same funkcje**:

$$f(0) = 1,\ f(1) = 1 +_2 1 = 0, \quad h(0) = 1,\ h(1) = 1 +_2 1 \cdot_2 1 = 0, \quad g(0) = 1,\ g(1) = 1 +_2 1 \cdot_2 1 \cdot_2 1 = 0.$$

Czyli f, g, h powyżej to te same funkcje, ale różne wielomiany! To jest dobry moment, aby wreszcie formalnie zdefiniować czym jest wielomian.

Definicja 10.22. *Wielomian* o współczynnikach z pierścienia przemiennego z jedynką R definiujemy jako nieskończony ciąg $(a_0, a_1, a_2, \ldots)$ elementów R (czyli dla każdego i mamy $a_i \in R$), taki że:

$$\exists n \quad \forall k \geqslant n \qquad a_k = 0,$$

tzn. nasz ciąg jest postaci:

$$(a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots).$$

Taki wielomian (czyli powyższy ciąg) oznaczamy przez:

$$a_0 + a_1 X + \ldots + a_n X^n \qquad \text{lub przez} \qquad \sum_{i=0}^{n} a_i X^i.$$

Uwaga 10.23. Pokrótce: wielomian jest zdefiniowany jako ciąg jego współczynników.

Poniżej kolejne definicje związane z wielomianami.

Definicja 10.24. Niech $f = a_0 + a_1 X + \ldots + a_n X^n$ będzie wielomianem.

(1) Element a_0 nazywamy *wyrazem wolnym* wielomianu f.
(2) Wielomian $(0, 0, \ldots)$ nazywamy *wielomianem zerowym*.
(3) Wielomian postaci $(a_0, 0, 0, \ldots)$ nazywamy *wielomianem stałym*.
(4) Jeśli $a_n \neq 0$, to:
   (i) liczbę n nazywamy *stopniem* wielomianu f;
   (ii) współczynnik a_n nazywamy *współczynnikiem wiodącym* wielomianu f;
   (iii) jeśli $a_n = 1$, to mówimy że f jest *wielomianem unormowanym*;
   (iv) wielomian zerowy **nie ma stopnia**.

Przykład 10.25. Niech $R = \mathbb{Z}$. Wtedy

$$3 + 5X + 1X^2$$

to unormowany wielomian stopnia 2 o wyrazie wolnym równym 3. Powyższy wielomian zapisujemy po prostu jako $3 + 5X + X^2$.

Definicja 10.26. Zbiór wielomianów o współczynnikach z pierścienia przemiennego z jedynką R oznaczamy przez $R[X]$.

Wiemy, że wielomiany o współczynnikach z R **nie są funkcjami** $R \to R$, ale wciąż takie wielomiany **wyznaczają funkcje** $R \to R$.

Definicja 10.27. Niech

$$f = a_0 + a_1 X + \ldots + a_n X^n \in R[X].$$

Wielomian f wyznacza następującą *funkcję wielomianową*:

$$F : R \to R, \qquad F(r) := a_0 + a_1 r + \ldots + a_n r^n.$$

Uwaga 10.28. Każda funkcja wielomianowa jest elementem **pierścienia funkcji** R^R jak w Przykładzie 9.8(4) (dla $X = R$).

Teraz chcemy aby sam zbiór wielomianów $R[X]$ stał się pierścieniem. Czyli definiujemy działania $+, \cdot$ na zbiorze $R[X]$ w „sensowny sposób", czyli tak aby były zgodne z działaniami w pierścieniu funkcji R^R.

Definicja 10.29. Weźmy

$$f = (a_0, a_1, a_2, \ldots) \in R[X], \qquad g = (b_0, b_1, b_2, \ldots) \in R[X].$$

Definiujemy:

$$f + g := (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots),$$
$$f \cdot g := (c_0, c_1, c_2, \ldots),$$

gdzie dla każdego $k \in \mathbb{N}$ mamy:

$$c_k := a_0 b_k + a_1 b_{k-1} + \ldots + a_{k-1} b_1 + a_k b_0 = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i+j=k} a_i b_j.$$

Przykład 10.30. Niech:

$$f = 1 + X \in \mathbb{Z}[X], \qquad g = 1 + 2X + X^2 \in \mathbb{Z}[X].$$

Wtedy mamy:

$$f + g = (1 + X) + \left(1 + 2X + X^2\right) = 2 + 3X + X^2,$$
$$f \cdot g = (1+X) \cdot \left(1 + 2X + X^2\right) = 1 \cdot 1 + (1 \cdot 2 + 1 \cdot 1)X + (1 \cdot 1 + 1 \cdot 2)X^2 + (1 \cdot 1)X^3 = 1 + 3X + 3X^2 + X^3.$$

Trzeba jeszcze się upewnić, że zbiór wielomianów jest zamknięty na działania z Definicji 10.29, tzn. że otrzymane w tej definicji ciągi są faktycznie wielomianami. Do tego służy następujący wynik.

Twierdzenie 10.31. *Niech $f, g \in R[X]$. Wtedy $f + g, f \cdot g \in R[X]$ oraz jeśli*

$$f + g \neq 0 \neq f \cdot g,$$

to mamy:

$$\deg(f + g) \leqslant \max\left(\deg(f), \deg(g)\right), \qquad \deg(f \cdot g) \leqslant \deg(f) + \deg(g).$$

Dowód. Niech:

$$f = a_0 + a_1 X + \ldots a_n X^n, \qquad g = b_0 + b_1 X + \ldots + b_m X^m,$$

gdzie $a_n \neq 0 \neq b_m$, tzn.:

$$\deg(f) = n, \qquad \deg(g) = m.$$

Bez zmniejszenia ogólności możemy przyjąć, że $n \geqslant m$, czyli zachodzi:

$$n = \max\left(\deg(f), \deg(g)\right).$$

Wtedy mamy:

$$f + g = (a_0 + b_0) + (a_1 + b_1)X + \ldots + (a_m + b_m)X^m + a_{m+1}X^{m+1} + \ldots + a_n X^n,$$

czyli faktycznie:

$$\deg(f + g) \leqslant n = \max\left(\deg(f), \deg(g)\right).$$

Podobnie mamy:

$$fg = a_0 b_0 + (a_1 b_0 + a_0 b_1)X + \ldots + a_m b_m X^{n+m},$$

czyli $\deg(f \cdot g) \leqslant \deg(f) + \deg(g)$. □

Stąd działania z Definicji 10.29 są działaniami na zbiorze $R[X]$.

Twierdzenie 10.32. *Jeśli R jest pierścieniem przemiennym z jedynką, to $R[X]$ jest też pierścieniem przemiennym z jedynką.*

Dowód. Wprost z definicji działania $+, \cdot$ na $R[X]$ są przemienne. Łatwo zauważyć, że $(R[X], +)$ jest grupą, gdzie $0_{R[X]}$ to wielomian zerowy. Widać też, że elementem neutralnym $\cdot$ jest wielomian stały o wyrazie wolnym równym 1. Pozostaje do pokazania rozdzielność $\cdot$ względem $+$ oraz łączność $\cdot$. Weźmy $f, g, h \in R[X]$, takie że:

$$f = \sum_i a_i X^i, \qquad g = \sum_j b_j X^j, \qquad h = \sum_k c_k X^k.$$

rozdzielność $\cdot$ względem $+$
Mamy $(f+g) \cdot h = \sum_l d_l X^l$, gdzie:

$$d_l = \sum_{i=0}^{l} (a_i + b_i) c_{l-i} = \underbrace{\sum_{i=0}^{l} a_i c_{l-i}}_{d'_l} + \underbrace{\sum_{i=0}^{l} b_i c_{l-i}}_{d''_l}.$$

Ale zachodzi:

$$f \cdot h = \sum_i d'_i X^i, \qquad g \cdot h = \sum_i d''_i X^i.$$

Czyli faktycznie:

$$(f+g) \cdot h = f \cdot h + g \cdot h.$$

łączność $\cdot$
Można policzyć, że $(f \cdot g) \cdot h = \sum_l d_l X^l$, gdzie:

$$d_l = \sum_{i+j+k=l} a_i b_j c_k.$$

Podobnie dostajemy $f \cdot (g \cdot h) = \sum_l d_l X^l$, co daje łączność $\cdot$. □

Zobaczymy teraz co się dzieje w sytuacji gdy R jest dziedziną.

Twierdzenie 10.33. *Załóżmy, że R jest dziedziną i $f, g \in R[X] \setminus \{0\}$. Wtedy zachodzi:*

(1) $\deg(fg) = \deg(f) + \deg(g)$ *(w szczególności: $fg \in R[X] \setminus \{0\}$);*
(2) $R[X]$ *jest dziedziną.*

Dowód. Niech:

$$f = a_0 + a_1 X + \ldots + a_n X^n, \quad g = b_0 + b_1 X + \ldots + b_m X^m,$$

gdzie $a_n \neq 0 \neq b_n$. Wtedy mamy:

$$\deg(f) = n, \qquad \deg(g) = m.$$

Wiemy, że:

$$fg = a_0 b_0 + (a_1 b_0 + a_0 b_1) X + \ldots + a_m b_m X^{n+m}.$$

Ponieważ R jest dziedziną oraz $a_n \neq 0 \neq b_n$, tak więc $a_n b_n \neq 0$ oraz $\deg(fg) = n + m$, co daje punkt (1).

Punkt (2) wynika natychmiast z (1). □

Uwaga 10.34. Można podać (ćwiczenia) przykład np. $f, g \in \mathbb{Z}_4[X]$, takich że:

$$\deg(fg) < \deg(f) + \deg(g).$$

Definicja 10.35. Niech R będzie pierścieniem przemiennym z jedynką, $f \in R[X]$ oraz $r \in R$.

(i) Przez $f(r)$ oznaczamy wartość na r funkcji wielomianowej pochodzącej od f.
(ii) Definiujemy:

$$\mathrm{ev}_r : R[X] \to R, \qquad \mathrm{ev}_r(f) := f(r)$$

i funkcję ev_r nazywamy *funkcją ewaluacji* (w r).

Uwaga 10.36. (1) Działania dodawania i mnożenia wielomianów sa tak zdefiniowane aby dla każdego $r \in R$ funkcja $\mathrm{ev}_r : R[X] \to R$ była homomorfizmem pierścieni, tzn. mamy:

$$\forall\, f, g \in R[X] \qquad \underbrace{(f+g)(r)}_{\text{dodawanie w } R[X]} = \underbrace{f(r) + g(r)}_{\text{dodawanie w } R}.$$

Podobnie dla mnożenia.

(2) Cała „duża" funkcja

$$\Psi : R[X] \to R^R, \qquad \Psi(f) = F,$$

gdzie F jest funkcją wielomianową wyznaczoną przez f, jest też homomorfizmem pierścieni.

(3) Mamy też następujący monomorfizm pierścieni:

$$\alpha : R \to R[X], \qquad \alpha(r) = (r, 0, 0, \ldots),$$

gdzie $(r, 0, 0, \ldots)$ jest wielomianem stałym o wyrazie wolnym r.

Poniżej definiujemy pojęcie analogiczne do pojęcia podgrupy.

Definicja 10.37. Niech R będzie pierścieniem i $S \subseteq R$. Podzbiór S nazywamy *podpierścieniem* R, gdy:

(i) S jest podgrupą $(R, +)$;

(ii) dla każdego $x, y \in S$ mamy:

$$x \cdot y \in S.$$

Jeśli R jest pierścieniem z jedynką, to S nazywamy *podpierścieniem z jedynką*, gdy S dodatkowo spełnia:

(iii) $1_R \in S$.

Uwaga 10.38. Tak jak w przypadku grup i podgrup mamy:

(1) jeśli S jest podpierścieniem R, to S jest pierścieniem z działaniami z R obciętymi do S;

(2) jeśli S jest podpierścieniem z jedynką R, to S jest pierścieniem z jedynką z działaniami z R obciętymi do S.

Przykład 10.39. (1) $\mathbb{Z}$ jest podpierścieniem z jedynką $\mathbb{Q}$, $\mathbb{Q}$ jest podpierścieniem z jedynką $\mathbb{R}$ i $\mathbb{R}$ jest podpierścieniem z jedynką $\mathbb{C}$.

(2) $2\,\mathbb{Z}$ jest podpierścieniem $\mathbb{Z}$, ale **nie jest** podpierścieniem z jedynką.

(3) Teraz dość nietypowy przykład: $\mathbb{R} \times \{0\}$ jest podpierścieniem $\mathbb{R} \times \mathbb{R}$, ale nie jest podpierścieniem z jedynką. Pomimo tego, $\mathbb{R} \times \{0\}$ **jest** pierścieniem z jedynką! Mamy:

$$1_{\mathbb{R}\times\{0\}} = (1, 0) \neq (1, 1) = 1_{\mathbb{R}\times\mathbb{R}}.$$

Również pierścień zerowy jest zawsze podpierścieniem i jeśli jest podzbiorem właściwym, to nie jest podpierścieniem z jedynką. Jednak sam w sobie pierścień zerowy jest pierścieniem z jedynką, która też jest zerem tego pierścienia.

(4) $M_n(\mathbb{Q})$ jest podpierścieniem z jedynką $M_n(\mathbb{R})$ i $M_n(\mathbb{R})$ jest podpierścieniem z jedynką $M_n(\mathbb{C})$.

(5) $\mathbb{Z}_2$ **nie jest** podpierścieniem $\mathbb{Z}_4$.

(6) $\mathbb{Z}[i]$ jest podpierścieniem $\mathbb{C}$.

Uwaga 10.40. Jeśli $f : R_1 \to R_2$ jest homomorfizmem pierścieni, to $f(R_1)$ jest podpierścieniem R_2. Jeśli f jest monomorfizmem, to mamy:

$$R_1 \cong f(R_1).$$

Przykład 10.41. Rozważmy monomorfizm $\alpha : R \to R[X]$ z Uwagi 10.36(3). Czyli mamy:

$$R \cong \alpha(R),$$

gdzie $\alpha(R)$ jest podpierścieniem R składającym się z wielomianów stałych. Często **utożsamiamy** R z powyższym $\alpha(R)$ i piszemy $R \subset R[X]$ uznając R za podpierścień pierścienia wielomianów $R[X]$.

Definicja 10.42. Pierścień wielomianów dwóch zmiennych to:

$$R[X, Y] := R[X][Y].$$

Analogicznie przez prostą indukcję można zdefiniować pierścień wielomianów n zmiennych dla dowolnego $n > 0$:

$$R[X_1, \ldots, X_n] := R[X_1, \ldots, X_{n-1}][X_n].$$

11. Ciało ułamków i pierścienie euklidesowe

Wiemy, że z **dziedziny** $\mathbb{Z}$ można dostać **ciało** $\mathbb{Q}$, tzn.:

(i) $\mathbb{Z}$ jest podpierścieniem $\mathbb{Q}$;

(ii) Dla każdego $x \in \mathbb{Q}$ istnieją $m, n \in \mathbb{Z}$, takie że:

$$x = \frac{n}{m}.$$

Chcemy zrobić coś podobnego dla dowolnej dziedziny R, tzn. chcemy otrzymać ciało K, takie że (i)–(ii) powyżej będą spełnione dla "R" zamiast "$\mathbb{Z}$" oraz "K" zamiast "$\mathbb{Q}$".

Ustalmy dziedzinę R. Definiujemy następującą relację $\sim$ na zbiorze $R \times (R \setminus \{0\})$:

$$(r_1, s_1) \sim (r_2, s_2) \qquad \Leftrightarrow \qquad r_1 s_2 = r_2 s_1.$$

Twierdzenie 11.1. *Powyższa relacja $\sim$ jest relacją równoważności.*

Dowód. Zwrotność i symetryczność relacji $\sim$ są oczywiste. Dla dowodu tranzytywności weźmy $r_1, r_2, r_3 \in R$ oraz $s_1, s_2, s_3 \in R \setminus \{0\}$, takie że:

$$(r_1, s_1) \sim (r_2, s_2), \qquad (r_2, s_2) \sim (r_3, s_3).$$

Pokażemy, że $(r_1, s_1) \sim (r_3, s_3)$. Z założenia mamy, że:

$$r_1 s_2 = r_2 s_1, \qquad r_2 s_3 = r_3 s_2.$$

Mnożąc pierwszą z tych równości obustronnie przez s_3 dostajemy (używając drugiej równości):

$$r_1 s_2 s_3 = s_1 r_2 s_3 = s_1 r_3 s_2.$$

Czyli mamy:

$$r_1 s_3 s_2 = r_3 s_1 s_2.$$

Używając Prawa Skracania dla Dziedzin (i założenia: $s_2 \neq 0$), mamy że $r_1 s_3 = r_3 s_1$, czyli $(r_1, s_1) \sim (r_3, s_3)$, co mieliśmy pokazać. □

Definicja 11.2. Jeśli R i $\sim$ są j.w., to dla $(r, s) \in R \times (R \setminus \{0\})$ klasę abstrakcji $[(r, s)]_\sim$ nazywamy *ułamkiem* o *liczniku* r oraz *mianowniku* s i oznaczamy ją przez:

$$\frac{r}{s} := [(r, s)]_\sim.$$

Widać, że faktycznie ciało $\mathbb{Q}$ powstaje z dziedziny $\mathbb{Z}$ w opisany powyżej sposób. Definiujemy teraz działania $+$ i $\cdot$ na zbiorze ułamków pochodzących od naszej ustalonej dziedziny R:

$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} := \frac{r_1 r_2}{s_1 s_2}, \qquad \frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}.$$

Twierdzenie 11.3. (1) *Powyższe działania są dobrze określone, tzn. nie zależą od wyboru liczników i mianowników.*

(2) *Zbiór ułamków z powyższymi działaniami jest ciałem, które oznaczamy przez K.*

(3) *Następująca funkcja:*

$$\varphi : R \to K, \qquad \varphi(r) = \frac{r}{1}$$

jest monomorfizmem pierścieni.

Dowód. (1) Weźmy $r_1, r_1', r_2, r_2' \in R$ oraz $s_1, s_1', s_2, s_2' \in R \setminus \{0\}$, takie że:

$$\frac{r_1}{s_1} = \frac{r_1'}{s_1'}, \qquad \frac{r_2}{s_2} = \frac{r_2'}{s_2'}.$$

Czyli mamy:

$$r_1 s_1' = r_1' s_1, \qquad r_2 s_2' = r_2' s_2.$$

Wtedy dostajemy:

$$r_1 r_2 s_1' s_2' = r_1' r_2' s_1 s_2 \qquad \Rightarrow \qquad \frac{r_1 r_2}{s_1 s_2} = \frac{r_1' r_2'}{s_1' s_2'},$$

czyli mnożenie ułamków jest dobrze określone.

Z dodawaniem jest trudniej, co nie powinno dziwić w przypadku ułamków. Liczymy:

$$\begin{aligned} 0 &= \underbrace{(r_1 s_1' - r_1' s_1)}_{0} s_2 s_2' - \underbrace{(r_2 s_2' - r_2' s_2)}_{0} s_1 s_1' \\ &= r_1 s_2 s_1' s_2' - r_1' s_2' s_1 s_2 - r_2 s_1 s_1' s_2' + r_2' s_1' s_1 s_2 \\ &= (r_1 s_2 + r_2 s_1)\, s_1' s_2' - (r_1' s_2' + r_2' s_1')\, s_1 s_2. \end{aligned}$$

Stąd dostajemy:

$$\frac{r_1 s_2 - r_2 s_1}{s_1 s_2} = \frac{r_1' s_2' - r_2' s_1'}{s_1' s_2'},$$

czyli dodawanie ułamków jest również dobrze określone.

(2) Warunki z Definicji 9.2 łatwo się sprawdza. Zobaczmy np. łączność dodawania:

$$\begin{aligned} \left(\frac{r_1}{s_1} + \frac{r_2}{s_2}\right) + \frac{r_3}{s_3} &= \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} + \frac{r_3}{s_3} \\ &= \frac{(r_1 s_2 + r_2 s_1)\, s_3 + r_3 s_1 s_2}{s_1 s_2 s_3} \\ &= \frac{r_1 s_2 s_3 + r_2 s_1 s_3 + r_3 s_1 s_2}{s_1 s_2 s_3}. \end{aligned}$$

Podobnie sprawdza się, że:

$$\frac{r_1}{s_1} + \left(\frac{r_2}{s_2} + \frac{r_3}{s_3}\right) = \frac{r_1 s_2 s_3 + r_2 s_1 s_3 + r_3 s_1 s_2}{s_1 s_2 s_3}.$$

Mamy też:

$$O_K = \frac{0}{1}, \qquad 1_K = \frac{1}{1}.$$

Udowodnimy teraz, że K jest ciałem. Weźmy:

$$\frac{r}{s} \in K \setminus \{0_K\}.$$

Mamy:

$$\frac{r}{s} \neq 0_K = \frac{0}{1},$$

stąd dostajemy:

$$r = r \cdot 1 \neq 0 \cdot s = 0.$$

Czyli $r \neq 0$ i stąd:

$$\frac{s}{r} \in K \qquad \text{oraz} \qquad \frac{r}{s} \cdot \frac{s}{r} = \frac{1}{1} = 1_K,$$

czyli K jest ciałem.

(3) Weźmy funkcję:

$$\varphi : R \to K, \qquad \varphi(r) = \frac{r}{1}.$$

Mamy wtedy:

$$\begin{aligned} \varphi(r_1 + r_2) &= \frac{r_1 + r_2}{1} = \frac{r_1}{1} + \frac{r_2}{1} = \varphi(r_1) + \varphi(r_2), \\ \varphi(r_1 r_2) &= \frac{r_1 r_2}{1} = \frac{r_1}{1} \cdot \frac{r_2}{1} = \varphi(r_1) + \cdot\varphi(r_2), \\ \varphi(1) &= \frac{1}{1} = 1_K, \end{aligned}$$

czyli φ jest homomorfizmem pierścieni.

Aby sprawdzić, że φ jest monomorfizmem liczymy jądro:

$$\ker(\varphi) = \left\{ r \in R \mid \frac{r}{1} = 0_K = \frac{1}{1} \right\} = \{r \in R \mid r \cdot 1 = 0 \cdot 1\} = \{0\}.$$

Stąd $\ker(\varphi) = \{0\}$, czyli φ jest monomorfizmem.

□

Definicja 11.4. Ciało K z Twierdzenia 11.3 nazywamy *ciałem ułamków* R.

Uwaga 11.5. Często utożsamiamy R z $\varphi(R)$ (z Twierdzenia 11.3(3)) i piszemy $R \subseteq K$.

Przykład 11.6. Jeśli F jest ciałem to przez $F(X)$ oznaczamy ciało ułamków pierścienia wielomianów $F[X]$, które to ciało nazywamy *ciałem funkcji wymiernych* (o współczynnikach z ciała F).

Zmierzamy teraz do ogólnego pojęcia **dzielenia z resztą** w pierścieniach. Na początek, sformalizujmy pojęcia dzielenia z resztą w pierścieniu $\mathbb{Z}$.

Dla każdych $a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}$ *istnieją* $q, r \in \mathbb{Z}$, *takie że:*

$$a = b\underbrace{q}_{iloraz} + \underbrace{r}_{reszta} \qquad oraz \qquad |r| < |b|.$$

Czyli w celu sformalizowania pojęcia dzielenia z resztą w pierścieniu $\mathbb{Z}$ istotna była funkcja wartości bezwzględnej:

$$|\cdot| : \mathbb{Z} \to \mathbb{N}\,.$$

Teraz ogólna definicja.

Definicja 11.7. Pierścień R jest *euklidesowy*, gdy R jest dziedziną oraz istnieje funkcja

$$\delta : R \setminus \{0\} \to \mathbb{N},$$

zwana *normą euklidesową*, taka że:
dla każdych $a \in R, b \in R \setminus \{0\}$ istnieją $q, r \in R$ spełniające:

$$a = bq + r \qquad \text{oraz} \qquad (\delta(r) < \delta(b) \quad \text{lub} \quad r = 0)\,.$$

Przykład 11.8. Ponieważ dla każdego $n \in \mathbb{Z}$ mamy:

$$|n| = 0 \qquad \Leftrightarrow \qquad n = 0,$$

tak więc funkcja

$$|\cdot| : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$$

jest normą euklidesową na pierścieniu $\mathbb{Z}$ i pierścień $\mathbb{Z}$ jest euklidesowy.

Zobaczymy jeszcze dwa przykłady pierścieni euklidesowych.

Twierdzenie 11.9. *Pierścień Gaussa* $\mathbb{Z}[i]$ *jest euklidesowy z następującą normą euklidesową:*

$$\delta : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}, \qquad \delta(n + mi) := |n + mi|^2 = n^2 + m^2.$$

Dowód. Weźmy:

$$a = a_1 + a_2 i \in \mathbb{Z}[i], \qquad b = b_1 + b_2 i \in \mathbb{Z}[i] \setminus \{0\}.$$

Na początek dzielimy a przez b w ciele $\mathbb{C}$, czyli bierzemy $\alpha, \beta \in \mathbb{R}$, takie że:

$$\alpha + \beta i = \frac{a}{b}$$

(na konwersatorium zobaczymy, że $\alpha, \beta \in \mathbb{Q}$). Teraz weźmy $q_1, q_2 \in \mathbb{Z}$, takie że:

$$|\alpha - q_1| \leqslant \frac{1}{2}, \qquad |\beta - q_2| \leqslant \frac{1}{2}.$$

Definiujemy:

$$q := q_1 + q_2 i \in \mathbb{Z}[i], \qquad r := a - bq \in \mathbb{Z}[i].$$

Oczywiście zachodzi warunek $a = bq + r$, tak więc musimy tylko sprawdzić, czy $|r|^2 < |b|^2$ (ponieważ dla każdego $z \in \mathbb{C}$ mamy $|z| = 0 \Leftrightarrow z = 0$, więc, podobnie jak w przypadku

pierścienia $\mathbb{Z}$, nie musimy się przejmować bardziej skomplikowanym warunkiem). Zauważmy, że:

$$|r|^2 < |b|^2 \qquad \Leftrightarrow \qquad \frac{|r|^2}{|b|^2} < 1 \qquad \Leftrightarrow \qquad \left|\frac{r}{b}\right|^2 < 1.$$

Sprawdzimy ten ostatni warunek. Mamy, że:

$$r = a - bq \qquad \Rightarrow \qquad \frac{r}{b} = \frac{a}{b} - q.$$

Stąd dostajemy:

$$\begin{aligned}\left|\frac{r}{b}\right|^2 &= \left|\frac{a}{b} - q\right|^2 \\ &= |(\alpha + \beta i) - (q_1 + q_2 i)\,|^2 \\ &= |\,(\alpha - q_1) + (\beta - q_2)\,i|^2 \\ &= (\alpha - q_1)^2 + (\beta - q_2)^2 \\ &\leqslant \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1,\end{aligned}$$

co należało pokazać. □

Wiemy już, że pierścienie $\mathbb{Z}$ oraz $\mathbb{Z}[i]$ są euklidesowe. Zobaczymy teraz jeszcze jeden typ przykładów pierścieni euklidesowych. Wielomiany można dzielić z resztą, tzn. mamy poniższe.

Dla każdych $F \in \mathbb{R}[X], H \in \mathbb{R}[X] \setminus \{0\}$ *istnieją* $Q, R \in \mathbb{R}$*, takie że:*

$$F = HQ + R \qquad \textit{oraz} \qquad (\deg(R) < \deg(H) \quad \textit{lub} \quad R = 0)\,.$$

Powyższe pozostaje prawdą, gdy zastąpimy $\mathbb{R}$ przez dowolne ciało (dowód pomijamy, bo jest analogiczny jak w przypadku ciała $\mathbb{R}$).

Twierdzenie 11.10. *Niech K będzie ciałem. Wtedy pierścień wielomianów $K[X]$ jest euklidesowy, gdzie normą euklidesową jest funkcja stopnia wielomianu:*

$$\deg : K[X] \setminus \{0\} \to \mathbb{N}\,.$$

Zajmiemy się teraz **największym wspólnym dzielnikiem** (NWD). Aby wyznaczyć $\mathrm{NWD}(n, m)$ dla $n, m > 0$ używamy dzielenia z resztą w **algorytmie Euklidesa**.

Przykład 11.11. Zastosujemy algorytm Euklidesa dla $n = 854$ i $m = 350$.

Krok 1 Dzielimy z resztą 854 przez 350:

$$854 = 350 \cdot 2 + 154.$$

Krok 2 Dzielimy z resztą 350 przez 154:

$$350 = 154 \cdot 2 + 42.$$

Krok 3 Dzielimy z resztą 154 przez 42:

$$154 = 42 \cdot 3 + 28.$$

Krok 4 Dzielimy z resztą 42 przez 28:

$$42 = 28 \cdot 1 + 14.$$

Krok 5 Dzielimy z resztą 28 przez 14:

$$28 = 14 \cdot 2 + 0.$$

Ostatnia reszta to 0, czyli w tym momencie algorytm się zatrzymuje i dostajemy:

$$\mathrm{NWD}(854, 350) = 14.$$

Analizując powyższy przykład, ogólna procedura znajdowania $\mathrm{NWD}(n,m)$ dla $n,m>0$ jest następująca:

- dzielimy z resztą n przez m:
$$n = mq_1 + r_1, \qquad |r_1| < |m|;$$
- dzielimy z resztą m przez r_1:
$$m = r_1q_2 + r_2, \qquad |r_2| < |r_1|;$$
- dzielimy z resztą r_1 przez r_2:
$$r_1 = r_2q_3 + r_3, \qquad |r_2| < |r_3|$$

i tak dalej... W końcu dostajemy następującą sytuację:

$$r_{k-1} = r_kq_{k+1} + 0, \qquad r_k \neq 0.$$

Wtedy algorytm Euklidesa daje, że:

$$\mathrm{NWD}(n,m) = r_k.$$

Możemy powyższą procedurę przeprowadzić w dowolnym pierścieniu euklidesowym, ale aby wiedzieć do czego ta procedura ma prowadzić musimy najpierw zdefiniować pojęcie największego wspólnego dzielnika (w dowolnym pierścieniu przemiennym z jedynką). Na początek zdefiniujemy pojęcie dzielnika.

Definicja 11.12. Niech R będzie pierścieniem przemiennym z jedynką oraz $x,y \in R$.

(1) Mówimy, że x *dzieli* y (w pierścieniu R), co oznaczamy $x \mid y$, gdy istnieje $r \in R$, taki że $y = rx$.
(2) Mówimy, że x jest *stowarzyszony* z y (w pierścieniu R), co oznaczamy $x \sim y$, gdy $x \mid y$ oraz $y \mid x$.

Przykład 11.13. (1) Jeśli $x,y \in \mathbb{Z}$, to mamy:

$$x \sim y \qquad \Leftrightarrow \qquad x = y \ \text{ lub } \ x = -y.$$

(2) Jeśli $F,W \in \mathbb{R}[X]$, to mamy:

$$F \sim W \qquad \Leftrightarrow \qquad \exists r \in \mathbb{R}\setminus\{0\} \quad F = rW.$$

Analogicznie, jeśli zamiast $\mathbb{R}$ mamy dowolne ciało.

Uwaga 11.14. Łatwo zauważyć, że:

(i) relacja podzielności $\mid$ jest zwrotna i przechodnia, tzn.
$$x \mid x \qquad \text{oraz} \qquad x \mid y \ \text{ i } \ y \mid z \quad \Rightarrow \quad x \mid z;$$
(ii) relacja stowarzyszenia $\sim$ jest relacją równoważności.

Definicja 11.15. Niech R będzie pierścieniem przemiennym z jedynką oraz $x,y,z \in R$. Mówimy, że z jest *największym wspólnym dzielnikiem* (*n.w.d.*) x i y (w pierścieniu R), gdy:

(i) $z \mid x$ i $z \mid y$;
(ii) dla każdego $z' \in R$ mamy:
$$z' \mid x \quad \text{oraz} \quad z' \mid y \qquad \Rightarrow \qquad z' \mid z.$$

Uwaga 11.16. (1) W Definicji 11.15:
- punkt (i), mówi że z jest wspólnym dzielnikiem x i y;
- punkt (ii), mówi że z dzieli każdy wspólny dzielnik x i y.

(2) Słowo „największy” w Definicji 11.15 odnosi się do relacji podzielności $\mid$, a nie do innych możliwych relacji na R. Np. **nie** odnosi się ono do relacji porządku $\leqslant$ na $\mathbb{Z}$!

(3) Dla $R = \mathbb{Z}$ mamy zawsze **dwa** największe wspólne dzielniki (w sensie Definicji 11.15), np. największe wspólne dzielniki 4 i 6 to 2 oraz -2. Jeśli z tych dwóch największych wspólnych dzielników, wybierzemy ten dodatni, to otrzymujemy „klasyczny" największy wspólny dzielnik (oznaczany NWD), który jest też największy w sensie relacji porządku $\leqslant$ na $\mathbb{Z}$.

(4) Jak widać w punkcie (3), n.w.d. nie jest wyznaczony jednoznacznie, tzn. mamy:
   (i) jeśli z oraz z' są n.w.d. x i y, to $z \sim z'$;
   (ii) jeśli z jest n.w.d. x i y oraz $z \sim z'$, to z' jest również n.w.d. x i y.

(5) Są przykłady pierścieni i elementów w nich, dla których n.w.d. **nie istnieje**.

Zobaczymy teraz, że w pierścieniach euklidesowych n.w.d. istnieją i że można je wyznaczać używając algorytmu Euklidesa.

Twierdzenie 11.17. *Niech*

$$\delta : R \setminus \{0\} \to \mathbb{N}$$

będzie normą euklidesową w dziedzinie R oraz $a, b \in R \setminus \{0\}$. Bierzemy teraz $q_i, r_i \in R$, takie że

$$\begin{aligned} a &= bq_1 + r_1 && \delta(r_1) < \delta(b), \\ b &= r_1 q_2 + r_2 && \delta(r_2) < \delta(r_1), \\ r_1 &= r_2 q_2 + r_3 && \delta(r_3) < \delta(r_2) \end{aligned}$$

i tak dalej ... Ta procedura musi się urwać po skończenie wielu krokach, tzn. dla pewnego $k > 0$ mamy (przyjmując $r_0 := b, r_{-1} := a$):

$$\begin{aligned} r_{k-2} &= r_{k-1} q_k + r_k && \delta(r_k) < \delta(r_{k-1}), \\ r_{k-1} &= r_k q_{k+1} && \text{tzn. } r_k \mid r_{k-1}. \end{aligned}$$

Wtedy r_k jest n.w.d. a i b.

Dowód. Mamy pokazać, że:

(i) $r_k \mid a$ oraz $r_k \mid b$,

(ii) dla każdego $d \in R$ zachodzi:

$$d \mid a \quad \text{oraz} \quad d \mid b \qquad \Rightarrow \qquad d \mid r_k.$$

Dla dowodu (i) zauważmy, że:

$$r_{k-1} = r_k q_{k+1} \qquad \Rightarrow \qquad \underline{r_k \mid r_{k-1}}.$$

Tak więc, używając następującej oczywistej implikacji:

$$x \mid y \quad \text{oraz} \quad x \mid z \qquad \Rightarrow \qquad x \mid y \pm z$$

dostajemy, że:

$$r_{k-2} = r_{k-1} q_k + r_k \quad \text{oraz} \quad r_k \mid r_{k-1} \qquad \Rightarrow \qquad \underline{r_k \mid r_{k-2}}.$$

Postępując tak dalej (indukcyjnie) otrzymujemy:

$$r_k \mid r_{k-1},\ r_k \mid r_{k-2}, \ldots, r_k \mid r_1,\ r_k \mid \underbrace{r_0}_{b},\ r_k \mid \underbrace{r_{-1}}_{a},$$

co pokazuje (i).

Dla dowodu (ii) załóżmy, że $d \mid a$ oraz $d \mid b$. Wtedy mamy:

$$a = bq_1 + r_1 \qquad \Rightarrow \qquad r_1 = a - bq_1 \qquad \underbrace{\Rightarrow}_{d|a, d|b} \qquad \underline{d \mid r_1},$$

$$b = r_1 q_2 + r_2 \qquad \Rightarrow \qquad r_2 = b - r_1 q_2 \qquad \underbrace{\Rightarrow}_{d|b, d|r_1} \qquad \underline{d \mid r_2}$$

i tak dalej ... Indukcyjnie dostajemy, że $d \mid r_k$, co należało pokazać. □

Przykład 11.18. (1) Weźmy $R = \mathbb{Z}[i]$. Wtedy norma euklidesowa to:

$$\delta : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}, \qquad \delta(n+mi) := |n+mi|^2 = n^2 + m^2.$$

Wyznaczymy n.w.d. $a = -24 + 2i$ oraz $b = -1 + 13i$.

Krok 1 Dzielimy z resztą $-24 + 2i$ przez $-1 + 13i$.

$$\underbrace{-24+2i}_{a} = \underbrace{(-1+13i)}_{b} \cdot \underbrace{2i}_{q_1} + \underbrace{2+4i}_{r_1}$$

(procedura dzielenia z resztą w pierścieniu $\mathbb{Z}[i]$ była opisana w dowodzie Twierdzenia 11.9). Upewniamy się, że na pewno podzieliliśmy z resztą, ponieważ mamy:

$$20 = 2^2 + 4^2 = \delta(2+4i) < \delta(-1+13i) = (-1)^2 + 13^2 = 170.$$

Krok 2 Dzielimy z resztą $-1 + 13i$ przez $2 + 4i$.

$$\underbrace{-1+13i}_{b} = \underbrace{(2+4i)}_{r_1} \cdot \underbrace{(2+i)}_{q_2} + \underbrace{-1+3i}_{r_2}.$$

Upewniamy się, że na pewno podzieliliśmy z resztą:

$$10 = (-1)^2 + 3^2 = \delta(-1+3i) < \delta(2+4i) = 20.$$

Krok 3 Dzielimy z resztą $2 + 4i$ przez $-1 + 3i$.

$$\underbrace{2+4i}_{r_1} = \underbrace{(-1+3i)}_{r_2} \cdot \underbrace{(1-i)}_{q_3} + \underbrace{0}_{r_3}.$$

Czyli ostatnia niezerowa reszta $r_2 = -1 + 3i$ jest n.w.d. $-24 + 2i, -1 + 13i$.

(2) Weźmy $R = \mathbb{Q}[X]$. Wtedy norma euklidesowa to:

$$\delta : \mathbb{Q}[X] \setminus \{0\} \to \mathbb{N}, \qquad \delta(F) := \deg(F).$$

Wyznaczymy n.w.d. $a = X^2 + 7X + 6$ oraz $b = X^2 - 5X - 6$.

Krok 1 Dzielimy z resztą $X^2 + 7X + 6$ przez $X^2 - 5X - 6$.

$$\underbrace{X^2+7X+6}_{a} = \underbrace{(X^2-5X-6)}_{b} \cdot \underbrace{1}_{q_1} + \underbrace{12X+12}_{r_1}.$$

Upewniamy się, że na pewno podzieliliśmy z resztą:

$$1 = \deg(12X+12) < \delta(X^2-5X-6) = 2.$$

Krok 2 Dzielimy z resztą $X^2 - 5X - 6$ przez $12X + 12$.

$$\underbrace{X^2-5X-6}_{b} = \underbrace{(12X+12)}_{r_1} \cdot \underbrace{\left(\frac{1}{12}X - \frac{1}{2}\right)}_{q_2} + \underbrace{0}_{r_2}.$$

Czyli ostatnia niezerowa reszta $r_1 = 12X + 12$ jest n.w.d. $X^2 + 7X + 6, X^2 - 5X - 6$. Ponieważ $12X + 12 \sim X + 1$ (Przykład 11.13(2)), tak więc $X + 1$ jest również n.w.d. $X^2 + 7X + 6, X^2 - 5X - 6$, na mocy Uwagi 11.16(4(ii)), i tenże $X + 1$ jest w pewnym sensie „najładniejszym" n.w.d. $X^2 + 7X + 6, X^2 - 5X - 6$.

Teraz ogólna obserwacja.

Twierdzenie 11.19. *Niech R będzie dziedziną oraz $r, r' \in R \setminus \{0\}$. Wtedy mamy:*

$$r \sim r' \qquad \Leftrightarrow \qquad \exists u \in R \;\; r' = ur.$$

Dowód. „⇐” (ta implikacja jest prawdziwa w dowolnym pierścieniu przemiennym z jedynką)
Załóżmy, że $r' = ur$, gdzie $u \in R^*$. Wtedy mamy, że $r \mid r'$. Ponadto mamy $r = u^{-1}r'$ $(u \in R)$, czyli mamy też $r' \mid r$. Stąd dostajemy $r \sim r'$, co należało pokazać.
„⇒” (tu używamy założenia, że R jest dziedziną)
Ponieważ $r \sim r'$, tak więc $r \mid r'$ oraz $r' \mid r$, czyli istnieją $a, b \in R$, takie że:

$$r' = ar \qquad \text{oraz} \qquad r = br',$$

co daje:

$$r = bar.$$

Ponieważ (z założenia) $r \neq 0$, z Prawa Skracania dla Dziedzin dostajemy, że:

$$1 = ba.$$

Czyli $a \in R^*$ oraz $r' = ar$, co należało pokazać. □

Wniosek 11.20. *Jeśli R jest dziedziną, $a, b, r \in R$ oraz r to n.w.d. a, b, to* ***dowolny n.w.d.*** *a, b jest postaci ur dla pewnego $u \in R^*$.*

Przykład 11.21. Wiemy, że:

$$\mathbb{Z}[i]^* = \{1, -1, i, -i\}$$

i wiemy też, że $\underline{-1+3i}$ to n.w.d. $-24+2i, -1+13i$. Stąd pozostałe n.w.d. $-24+2i, -1+13i$ to:

$$-(-1+3i) = \underline{1-3i}, \qquad i(-1+3i) = \underline{-3-i}, \qquad (-i)(-1+3i) = \underline{3+i}.$$

Wracamy do obliczeń prowadzących do NWD$(350, 824)$. Mamy:

$$854 = 350 \cdot 2 + 154, \quad 350 = 154 \cdot 2 + 42, \quad 154 = 42 \cdot 3 + 28,$$

$$42 = 28 + 14, \quad 28 = 14 \cdot 2, \quad \text{NWD}(350, 824) = 14.$$

Teraz „cofamy się”:

$$14 = -28 + 42 \qquad \text{oraz} \qquad 28 = 154 - 42 \cdot 3$$

implikuje:

$$14 = 42 - (154 - 3 \cdot 42) = 154 + 4 \cdot 42.$$

Ostatnia równość wraz z równością $42 = 350 - 2 \cdot 154$ implikuje:

$$14 = -154 + 4 \cdot (350 - 2 \cdot 154) = 4 \cdot 350 - 9 \cdot 154.$$

Ostatnia równość wraz z równością $154 = 854 - 2 \cdot 350$ implikuje:

$$\underline{14} = 4 \cdot 350 - 9 \cdot (854 - 2 \cdot 350) = \underline{22 \cdot 350 + (-9) \cdot 854}.$$

Stąd zapisaliśmy 14 (czyli NWD$(350, 824)$) jako „$\mathbb{Z}$-liniową kombinację” liczb 350 i 824. Podobnie możemy zrobić w dowolnym pierścieniu euklidesowym zastępując NWD przez n.w.d.

Twierdzenie 11.22 (Rozszerzony algorytm Euklidesa)**.** *Niech R będzie pierścieniem euklidesowym, $x, y, r \in R$ oraz r to n.w.d. x, y. Wtedy istnieją $a, b \in R$, takie że:*

$$r = ax + by.$$

Idea dowodu. „Odwracamy” algorytm Euklidesa jak w przykładzie powyżej. □

Dualnie do pojęcia największego wspólnego dzielnika możemy też zdefiniować pojęcie **najmniejszej wspólnej wielokrotności**.

Definicja 11.23. Niech R będzie pierścieniem przemiennym z jedynką oraz $x, y, z \in R$. Mówimy, że z jest *najmniejszą wspólną wielokrotnością* x i y (w pierścieniu R), gdy:

(i) $x \mid z$ i $y \mid z$;
(ii) dla każdego $z' \in R$ mamy:

$$x \mid z' \quad \text{oraz} \quad y \mid z' \qquad \Rightarrow \qquad z \mid z'.$$

Uwaga 11.24. Podobnie jak dla największego wspólnego dzielnika, najmniejsza wspólna wielokrotność jest wyznaczona z dokładnością do relacji stowarzyszenia oraz najmniejsza wspólna wielokrotność może nie istnieć.

Przykład 11.25. Wiemy, że dla $m, n > 0$ mamy:

$$\mathrm{NWD}(m,n) \cdot \mathrm{NWW}(m,n) = m \cdot n.$$

Stąd np. dostajemy:

$$\mathrm{NWW}(350, 854) = \frac{350 \cdot 854}{\mathrm{NWD}(350, 854)} = \frac{196420}{14} = 14030.$$

Podobnie jest w dowolnym pierścieniu euklidesowym (dowód pomijamy).

Twierdzenie 11.26. *Niech R będzie pierścieniem euklidesowym oraz $x, y \in R$. Wtedy najmniejsza wspólna wielokrotność x, y istnieje i jest postaci:*

$$\frac{xy}{r},$$

gdzie r to n.w.d. x, y.

Przykład 11.27. Z Twierdzenia 11.26 najmniejsza wspólna wielokrotność wielomianów:

$$X^2 + 7X + 6, \quad X^2 - 5X - 6$$

w pierścieniu $\mathbb{Q}[X]$ to (używając Przykładu 11.18(2)):

$$\frac{(X^2 + 7X + 6) \cdot (X^2 - 5X - 6)}{X + 1} = X^3 - 2X^2 + 29X - 30.$$

Dowód następnego wyniku stosuje teorię pierścieni euklidesowych.

Twierdzenie 11.28 (Twierdzenie Bézout)**.** *Załóżmy, że K jest ciałem, $F \in K[X]$ oraz $\alpha \in K$. Wtedy mamy:*

$$F(\alpha) = 0 \qquad \Leftrightarrow \qquad (X - \alpha) \mid F.$$

Dowód. "$\Leftarrow$"
Ponieważ $(X - \alpha) \mid F$, tak więc istnieje $Q \in K[X]$, taki że:

$$F = (X - \alpha)Q.$$

Wtedy mamy:

$$F(\alpha) = ((X - \alpha)Q)(\alpha) = (\alpha - \alpha)Q(\alpha) = 0 \cdot Q(\alpha) = 0.$$

"$\Rightarrow$"
Załóżmy, że $F(\alpha) = 0$. Dzielimy z resztą F przez $X - \alpha$ w pierścieniu euklidesowym $K[X]$ i otrzymujemy $Q, R \in K[X]$, takie że:

$$F = (X - \alpha)Q + R, \qquad \text{oraz} \qquad R = 0 \ \text{ lub } \ \deg(R) < \deg(X - \alpha) = 1.$$

Jeśli $R = 0$, to $(X - \alpha) \mid F$, co należało pokazać.
Załóżmy, że $R \neq 0$ i dojdziemy do sprzeczności, która zakończy dowód. Mamy, że:

$$\deg(R) < 1 \qquad \Rightarrow \qquad \deg(R) = 0 \qquad \Rightarrow \qquad R \in K \setminus \{0\}.$$

Wtedy mamy:

$$0 = F(\alpha) = ((X - \alpha)Q + R)(\alpha) = R \neq 0,$$

sprzeczność. □

Definicja 11.29. Niech R będzie pierścieniem przemiennym z jedynką, $F \in R[X]$ i $r \in R$. Mówimy, że r jest *pierwiastkiem* F, gdy

$$F(r) = 0.$$

Przykład 11.30. Weźmy:

$$F := 1 + X + X^2 + X^3 \in \mathbb{Q}[X].$$

Wtedy mamy $F(-1) = 0$, czyli z Twierdzenia Bézout dostajemy:

$$X + 1 \mid 1 + X + X^2 + X^3.$$

Widać też, że:

$$1 + X + X^2 + X^3 = (1 + X) + X^2(1 + X) = (1 + X)\left(1 + X^2\right),$$

czyli faktycznie $X + 1 \mid 1 + X + X^2 + X^3$.

Mamy następujące klasyczne twierdzenie:

Twierdzenie 12.1 (Podstawowe Twierdzenie Arytmetyki)**.** *Każda liczba naturalna $n > 1$ jest iloczynem liczb pierwszych. Składniki tego iloczynu są jedyne z dokładnością do kolejności.*

Chcemy to twierdzenie uogólnić do przypadku dowolnych pierścieni euklidesowych. Na początek potrzebujemy ogólnego odpowiednika liczb pierwszych.

Definicja 12.2. Niech R będzie dziedziną i $p \in R\backslash(R^* \cup \{0\})$. Mówimy, że p jest *nierozkładalny*, gdy:

$$\forall\, a, b \in R \qquad p = a \cdot b \qquad \Rightarrow \qquad a \in R^* \quad \text{lub} \quad b \in R^*.$$

Uwaga 12.3. Każdy element $x \in R$ ma „rozkład”:

$$x = x \cdot 1$$

i ogólniej dla dowolnego $u \in R^*$ mamy też „rozkład”:

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

Element x jest nierozkładalny, gdy takie trywialne rozkłady jak powyżej to **jedyne** rozkłady x na iloczyny elementów R.

Przykład 12.4. Weźmy $n \in \mathbb{Z}$. Wtedy mamy:

$$n \text{ jest nierozkładalny} \qquad \Leftrightarrow \qquad n = p \ \text{ lub } \ n = -p, \ \text{ gdzie } p \text{ to liczba pierwsza.}$$

Dla dowodu twierdzenia uogólniającego Podstawowe Twierdzenie Arytmetyki do dowolnego pierścienia euklidesowego potrzebujemy trzech lematów.

Lemat 12.5. *Załóżmy, że:*

- *R jest pierścieniem euklidesowym;*
- *$x, y, z \in R$;*
- *1 to n.w.d. x, y;*
- *$x \mid yz$.*

Wtedy $x \mid z$.

Dowód. Z tego, że R jest pierścieniem euklidesowym oraz 1 to n.w.d. x, y otrzymujemy (na mocy Twierdzenia 11.22), że istnieją $s, t \in R$, takie że:

$$1 = sx + ty.$$

Mnożąc ostatnią równość obustronnie przez z otrzymujemy:

$$z = sxz + tyz.$$

Ponieważ $x \mid yz$, tak więc $x \mid tyz$. Czyli mamy:

$$x \mid sxz \quad \text{oraz} \quad x \mid tyz \qquad \Rightarrow \qquad x \mid sxz + tyz = z,$$

co należało pokazać. □

Kolejny wynik mówi o drugiej własności (pierwsza jest zawarta w Definicji 12.2), która wyróżnia liczby pierwsze.

Lemat 12.6. *Załóżmy, że:*

- *R jest pierścieniem euklidesowym;*
- *$a, b, p \in R$;*
- *p jest nierozkładalny;*
- *$p \mid ab$.*

Wtedy $p \mid a$ lub $p \mid b$.

Dowód. Niech $d \in R$ będzie n.w.d. a, p. W szczególności $d \mid p$, czyli istnieje $h \in R$, taki że $p = dh$. Mamy wtedy:

$$p = dh \quad \text{oraz} \quad p \text{ jest nierozkładalny} \qquad \Rightarrow \qquad d \in R^* \ \text{ lub } \ h \in R^*.$$

Rozważamy dwa przypadki.

Przypadek 1: $\underline{d \in R^*}$.
Ponieważ $d \in R^*$, tak więc $d \sim 1$ (przypominam, że $\sim$ to relacja stowarzyszenia). Czyli mamy:

$$d \text{ to n.w.d. } a, p \quad \text{oraz} \quad d \sim 1 \qquad \Rightarrow \qquad 1 \text{ to n.w.d. } a, p.$$

Z Lematu 12.5 (dla $x = p, y = a, z = b$) otrzymujemy, że $p \mid b$, co wystarczało pokazać.

Przypadek 2: $\underline{h \in R^*}$.
Ponieważ $p = dh$ oraz $h \in R^*$, tak więc $d = ph^{-1}$, czyli $p \mid a$. Wtedy mamy:

$$p \mid d \quad \text{oraz} \quad d \mid a \qquad \Rightarrow \qquad p \mid a,$$

co również wystarczało pokazać. □

Kolejny wynik mówi, że w pierścieniu euklidesowym nie istnieje nieskończony i istotnie zstępujący ciąg w sensie relacji podzielności. Dowód będzie szkicowy.

Lemat 12.7. *Niech*

$$\delta : R \setminus \{0\} \to \mathbb{N}$$

*będzie normą euklidesową na R. Wtedy **nie** istnieje nieskończony ciąg $a_0, a_1, a_2, \ldots \in R$, taki że:*

$$\forall\, n \in \mathbb{N} \qquad a_n \nsim a_{n+1} \qquad \textit{oraz} \qquad a_{n+1} \mid a_n.$$

Szkic dowodu. Załóżmy nie wprost, że powyższy ciąg istnieje. Definiujemy:

$$I := \{r_0 a_0 + r_1 a_1 + \ldots + r_n a_n \mid n \in \mathbb{N},\ r_0, r_1, \ldots, r_n \in R\} \subseteq R.$$

Weźmy $g \in I \setminus \{0\}$, taki że $\delta(g)$ jest minimalna. Wtedy mamy:

$$\exists N \in \mathbb{N} \quad \exists a_0, a_1, \ldots, a_N \in R \qquad g = r_0 a_0 + r_1 a_1 + \ldots + r_N a_N.$$

Dzieląc z resztą w pierścieniu euklidesowym R oraz używając minimalności $\delta(g)$ otrzymujemy:

$$\forall\, n \in \mathbb{N} \qquad g \mid a_n$$

(użyjemy tylko tego, że $g \mid a_{N+1}$).
Z drugiej strony mamy, że:

$$a_N \mid a_0,\ a_N \mid a_1, \ldots, a_N \mid a_N \qquad \Rightarrow \qquad a_N \mid g = r_0 a_0 + r_1 a_1 + \ldots + r_N a_N.$$

Tak więc dostajemy:

$$a_N \mid g \quad \text{oraz} \quad g \mid a_{N+1} \qquad \Rightarrow \qquad a_N \mid a_{N+1}.$$

Ponieważ z założenia mamy, że $a_{N+1} \mid a_N$, tak więc dostajemy $a_N \sim a_{N+1}$, co daje sprzeczność z założeniem i kończy dowód. □

Teraz już możemy sformułować i udowodnić (szkicowo) twierdzenie o jednoznaczności rozkładu w pierścieniach euklidesowych.

Twierdzenie 12.8. *Załóżmy, że R jest pierścieniem euklidesowym i $a \in R \setminus (R^* \cup \{0\})$. Wtedy istnieją elementy nierozkładalne $p_1, \ldots, p_n \in R$, takie że:*

$$a = p_1 \cdot \ldots \cdot p_n$$

oraz rozkład ten jest jednoznaczny z dokładnością do kolejności czynników i stowarzyszenia, tzn. jeśli mamy elementy nierozkładalne $q_1, \ldots, q_m \in R$, takie że $a = q_1 \cdot \ldots \cdot q_m$, to wtedy:

(i) $n = m$,

(ii) *istnieje* $\sigma \in S_n$, *taka że:*

$$p_1 \sim q_{\sigma(1)}, \ldots, p_n \sim q_{\sigma(n)}.$$

Szkic dowodu. Istnienie rozkładu
Jeśli a nie ma takiego rozkładu, to (nieco przewrotnie) element a **jest rozkładalny** i to w taki sposób, że:

$$\exists a_0, a_1 \in R \setminus R^* : \qquad a = a_0 a_1$$

i np. a_1 nie ma takiego rozkładu, tzn.

$$\exists a_{10}, a_{11} \in R \setminus R^* : \qquad a_1 = a_{10} a_{11}$$

i np. a_{11} nie ma takiego rozkładu, tzn.

$$\exists a_{110}, a_{111} \in R \setminus R^* : \qquad a_{11} = a_{110} a_{111} ...$$

Wtedy mamy:

$$a_1 \mid a,\ a_{11} \mid a_1,\ a_{111} \mid a_{11}, \ldots \qquad a_1 \nsim a,\ a_{11} \nsim a_1,\ a_{111} \nsim a_{11}, \ldots$$

co przeczy Lematowi 12.7 i pokazuje istnienie rozkładu.
Jednoznaczność rozkładu
Załóżmy, że:

$$p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_m,$$

gdzie wszystkie elementy $p_i, q_j \in R$ są nierozkładalne. Wtedy dzięki Lematowi 12.6 i prostej indukcji dostajemy:

$$p_1 \mid q_1 \cdot \ldots \cdot q_m \qquad \Rightarrow \qquad \exists i \quad p_1 \mid q_i.$$

Stąd istnieje $t \in R$, taki że $q_i = p_1 t$. Ponieważ q_i jest nierozkładalny, tak więc:

$$q_i = p_1 t \qquad \Rightarrow \qquad p_1 \in R^* \quad \text{lub} \quad t \in R^*.$$

Ale p_1 jest nierozkładalny, tak więc $p_1 \notin R^*$, czyli mamy, że $t \in R^*$. Stąd dostajemy, że $p_1 \sim q_i$. Definiujemy teraz $\sigma(1) := i$, wydzielamy obie strony równości

$$p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_m$$

przez p_1 i indukcyjnie kończymy dowód. □

Przykład 12.9. Twierdzenie 12.8 specjalizuje się do następujących sytuacji.

(1) $R = \mathbb{Z}$: Podstawowe Twierdzenie Arytmetyki.
(2) $R = K[X]$, gdzie K jest ciałem: jednoznaczność rozkładu na wielomiany nierozkładalne.
(3) $R = \mathbb{Z}[i]$: jednoznaczność rozkładu w pierścieniu Gaussa.

Uwaga 12.10 (Uwaga historyczna: związek z Wielkim Twierdzeniem Fermata)**.** Wielkie Twierdzenie Fermata (WTF) można sformułować w następujący sposób. Niech $p > 2$ będzie liczbą pierwszą. Wtedy równanie:

$$X^p + Y^p = Z^p$$

nie ma nietrywialnych rozwiązań całkowitych.

W XIX wieku pojawiły się „dowody" WTF używające rozkładów w pierścieniu $\mathbb{Z}[\zeta_p]$, gdzie $\zeta_p \in \mathbb{C} \setminus \{1\}$, takim że $\zeta_p^p = 1$ i $\mathbb{Z}[\zeta_p]$ jest najmniejszym podpierścieniem z jedynką $\mathbb{C}$ zawierającym ζ_p. Powyższe „dowody" byłyby dobre, gdyby pierścienie $\mathbb{Z}[\zeta_p]$ miały własność jednoznacznego rozkładu, np. gdyby pierścienie $\mathbb{Z}[\zeta_p]$ były euklidesowe. Jednak okazało się, że jeśli $p \geqslant 23$, to wtedy pierścień $\mathbb{Z}[\zeta_p]$ **nie ma** własności jednoznacznego rozkładu.

Poprawny dowód WTF został podany dopiero w 1994 roku przez Andrew Wilesa.

Przykład 12.11. Uzasadnimy szkicowo, że pierścień

$$\mathbb{Z}\left[\sqrt{-3}\right] := \left\{n + m\sqrt{-3} \mid n, m \in \mathbb{Z}\right\}$$

nie ma własności jednoznacznego rozkładu. Rozważmy następujące dwa rozkłady elementu 4 w pierścieniu $\mathbb{Z}[\sqrt{-3}]$:

$$2 \cdot 2 = \left(1 + \sqrt{-3}\right) \cdot \left(1 - \sqrt{-3}\right).$$

Aby udowodnić, że własność jednoznacznego rozkładu **nie** zachodzi należy pokazać, że:

(i) elementy

$$2,\ 1 + \sqrt{-3},\ 1 - \sqrt{-3}$$

są nierozkładalne w pierścieniu $\mathbb{Z}\left[\sqrt{-3}\right]$;

(ii) mamy:

$$1 + \sqrt{-3} \nsim 2 \nsim 1 - \sqrt{-3}$$

w pierścieniu $\mathbb{Z}\left[\sqrt{-3}\right]$.

Aby pokazać powyższe (i) oraz (ii) używamy następującej funkcji „normy" (**nie jest** to norma euklidesowa!):

$$d : \mathbb{Z}\left[\sqrt{-3}\right] \to \mathbb{N}, \qquad d\left(n + m\sqrt{-3}\right) = n^2 + 3m^2.$$

Mamy następujące własności funkcji d, których dowody pomijamy ($x, y \in \mathbb{Z}\left[\sqrt{-3}\right]$):

(1) $d(xy) = d(x)d(y)$;

(2) $x \in \mathbb{Z}\left[\sqrt{-3}\right]^* \quad \Leftrightarrow \quad d(x) = 1.$

Ponieważ mamy:

$$d(x) = 1 \qquad \Leftrightarrow \qquad x = \pm 1,$$

tak więc z (2) otrzymujemy, że:

$$\mathbb{Z}\left[\sqrt{-3}\right]^* = \{-1, 1\}.$$

Stąd dostajemy od razu (ii) używając Twierdzenia 11.19.

Jeśli chodzi o (i), to dla przykładu pokażemy że 2 jest elementem nierozkładalnym w pierścieniu $\mathbb{Z}\left[\sqrt{-3}\right]$. Weźmy $x, y \in \mathbb{Z}\left[\sqrt{-3}\right]$, takie że $2 = xy$. Mamy pokazać, że:

$$x \in \mathbb{Z}\left[\sqrt{-3}\right]^* \qquad \text{lub} \qquad y \in \mathbb{Z}\left[\sqrt{-3}\right]^*.$$

Używając (1) liczymy:

$$4 = d(2) = d(xy) = d(x)d(y).$$

Czyli mamy:

$$d(x), d(y) \in \mathbb{N} \quad \text{oraz} \quad d(x)d(y) = 4 \qquad \Rightarrow \qquad d(x) = 1 \ \text{ lub } \ d(y) = 1 \ \text{ lub } \ d(x) = 2 = d(y).$$

Zauważmy, że dla każdych $n, m \in \mathbb{N}$ mamy:

$$n^2 + 3m^2 \neq 2 \qquad \Rightarrow \qquad d(x) = 1 \quad \text{lub} \quad d(y) = 1.$$

Ponownie z (3) powyżej otrzymujemy, że $x \in \mathbb{Z}\left[\sqrt{-3}\right]^*$ lub $y \in \mathbb{Z}\left[\sqrt{-3}\right]^*$, co należało pokazać.

Zauważmy najpierw następującą prostą własność pierścieni wielomianów.

Fakt 13.1. *Niech S będzie dziedziną. Wtedy mamy:*

$$S[X]^* = S^*.$$

Dowód. Dowodzona równość wynika natychmiast z Twierdzenia 10.33(1). □

Dla wygody wprowadzamy następującą definicję.

Definicja 13.2. Niech R będzie pierścieniem przemiennym z jedynką i $r \in R$. Mówimy, że r jest *rozkładalny*, gdy:

(i) $r \neq 0$ oraz $r \notin R^*$,
(ii) r **nie jest** nierozkładalny, tzn. istnieją $x, y \in R \setminus R^*$, takie że:

$$r = xy.$$

Niech K będzie ciałem. Z Faktu 13.1, wiemy że:

$$K[X]^* = K^* = K \setminus \{0\}.$$

Czyli dla $F \in K[X]$ warunek (i) z Definicji 13.2 jest równoważny temu, że $F \in K[X] \setminus K$, tzn. F **nie** jest wielomianem stałym, czyli $\deg(F) \geqslant 1$.

Teraz będzie seria twierdzeń o rozkładalności wielomianów. Ustalmy K j.w. oraz $F \in K[X]$.

Twierdzenie 13.3. *Jeśli* $\deg(F) > 1$ *i F ma pierwiastek, to wtedy F jest rozkładalny.*

Dowód. Niech $a \in K$, takie że $F(a) = 0$. Z Twierdzenia Bezout $(X - a) \mid F$, czyli istnieje $W \in K[X]$, taki że:

$$F = (X - a)W.$$

Wtedy mamy:

$$2 \leqslant \deg(F) = \deg((X - a)W) = \deg(X - a) + \deg(W) = 1 + \deg(W).$$

Stąd $\deg(W) \geqslant 1$, czyli $W \notin K[X]^*$. Podobnie $X - a \notin K[X]^*$, stąd F jest rozkładalny. □

Uwaga 13.4. F i K j.w.

(1) Jeśli $\deg(F) = 1$, to oczywiście F jest nierozkładalny.
(2) Odwrotna implikacja do tej w Twierdzeniu 13.3 **nie** jest prawdziwa, bo np.

$$F := (X^2 + 1)(X^2 + 2) \in \mathbb{R}[X]$$

jest rozkładalny w $\mathbb{R}[X]$, ale wciąż **nie ma** pierwiastków w $\mathbb{R}$.

Twierdzenie 13.5. *Załóżmy, że* $\deg(F) \in \{2, 3\}$. *Wtedy mamy:*

$$F \text{ jest nierozkładalny} \quad \Leftrightarrow \quad F \text{ nie ma pierwiastków.}$$

Dowód. Obie implikacje pokażemy poprzez kontrapozycję.
„⇒” Ta implikacja jest prawdziwa nawet przy założeniu $\deg(F) > 1$ używając Twierdzenia 13.3.
„⇐” Załóżmy, że F jest rozkładalny i że $\deg(F) \in \{2, 3\}$. Pokażemy, że F ma pierwiastek.

Ponieważ F jest rozkładalny, tak więc istnieją $H, W \in K[X]$, takie że:

$$\deg(H) > 0 \quad \text{oraz} \quad \deg(W) > 0 \quad \text{oraz} \quad F = HW.$$

Stąd dostajemy:

$$\{2, 3\} \ni \deg(F) = \deg(H) + \deg(W) > 0 \quad \text{oraz} \quad \deg(H) \geqslant 1 \quad \text{oraz} \quad \deg(W) \geqslant 1.$$

Czyli ostatecznie:

$$\deg(H) = 1 \quad \text{lub} \quad \deg(W) = 1.$$

Ponieważ K jest ciałem, tak więc dostajemy że:

$$H \text{ ma pierwiastek w } K \qquad \text{lub} \qquad W \text{ ma pierwiastek w } K.$$

Stąd $F = HW$ ma również pierwiastek w K, co należało pokazać. □

Przykład 13.6. Następujący wielomian:

$$F = 1 + X^2 + X^3 \in \mathbb{Z}_2[X]$$

jest nierozkładalny z Twierdzenia 13.5, ponieważ $\deg(F) = 3$ oraz:

$$F(0) = 1 \neq 0, \qquad F(1) = 1 +_2 1 +_2 1 = 1 \neq 0,$$

czyli F nie ma pierwiastków (w $\mathbb{Z}_2$).

Dowody dwóch kolejnych twierdzeń pomijamy. Dowód pierwszego z nich jest dość trudny i (standardowy dowód) ma charakter analityczny. Dowód drugiego z tych twierdzeń jest łatwiejszy.

Twierdzenie 13.7 (Gauss 1799, Zasadnicze Twierdzenie Algebry (liczb zespolonych))**.** *Jeśli $F \in \mathbb{C}[X] \setminus \mathbb{C}$, to F ma pierwiastek w $\mathbb{C}$ (tzn. $\mathbb{C}$ jest ciałem „algebraicznie domkniętym").*

Twierdzenie 13.8. *Jeśli $W \in \mathbb{R}[X]$ oraz $a, b \in \mathbb{R}$ są takie, że:*

$$z := a + bi \notin \mathbb{R} \qquad \textit{oraz} \qquad W(z) = 0,$$

to $W(\bar{z}) = 0$, gdzie $\bar{z} = a - bi$, oraz następujący wielomian o współczynnikach rzeczywistych:

$$(X - z)(X - \bar{z}) = X^2 - 2aX + \left(a^2 + b^2\right)$$

dzieli W w $\mathbb{R}[X]$.

Wniosek 13.9. (1) *Niech $W \in \mathbb{C}[X]$. Wtedy mamy:*

$$W \textit{ jest nierozkładalny} \qquad \Leftrightarrow \qquad \deg(W) = 1.$$

(2) *Niech $W \in \mathbb{R}[X]$. Wtedy następujące warunki są równoważne:*
- (i) *W jest nierozkładalny;*
- (ii) $\deg(W) = 1$ ***lub*** $\deg(W) = 2$ *oraz* $\Delta := b^2 - 4ac < 0$.

Dowód. Punkt (1) wynika od razu z Twierdzeń 13.3 i 13.7.

Dla dowodu punktu (2) pokazujemy dwie implikacje.
„⇐" Jeśli $\deg(W) = 1$, to wiemy że W jest nierozkładalny.
Jeśli $W = aX^2 + bX + c$ i $\Delta < 0$, to wiemy (szkoła średnia), że W nie ma pierwiastków. Z Twierdzenia 13.5 wynika (ponieważ $\deg(W) = 2$), że W jest nierozkładalny.
„⇒" Załóżmy, że W jest nierozkładalny. Wtedy z Twierdzenia 13.3 dostajemy, że $\deg(W) = 1$ lub W nie ma pierwiastków. Możemy założyć, że $\deg(W) > 1$, czyli dostajemy, że W nie ma pierwiastków rzeczywistych. Z Twierdzenia 13.7 dostajemy, że W ma pierwiastek zespolony $z \in \mathbb{C} \setminus \mathbb{R}$. Z Twierdzenia 13.8 wiemy, że:

$$H := (X - z)(X - \bar{z}) \in \mathbb{R}[X] \qquad \text{oraz} \qquad H \mid W \quad (\text{w } \mathbb{R}[X]).$$

Czyli istnieje $T \in \mathbb{R}[X]$, taki że $W = HT$. Mamy teraz:

$$W \text{ jest nierozkładalny} \quad \text{oraz} \quad W = HT \quad \text{oraz} \quad \deg(H) = 2 > 0 \qquad \Rightarrow \qquad \deg(T) = 0.$$

Stąd

$$\deg(W) = \deg(HT) = \deg(H) + \deg(T) = 2 + 0 = 2$$

do czego dążyliśmy. Ponieważ W nie ma pierwiastków, tak więc (ponownie szkoła średnia) $\Delta < 0$, co należało pokazać. □

Zobaczymy teraz jakie liczby wymierne mogą być pierwiastkami wielomianów o współczynnikach całkowitych.

Twierdzenie 13.10 (Twierdzenie o pierwiastkach wymiernych)**.** *Niech:*

$$W = a_n X^n + \ldots + a_1 X + a_0 \in \mathbb{Z}[X]$$

oraz $k, l \in \mathbb{Z}$ będą względnie pierwsze, takie że $W(k/l) = 0$. Wtedy $k \mid a_0$ oraz $l \mid a_n$ (w pierścieniu $\mathbb{Z}$).

Dowód. Mamy, że:

$$0 = W\left(\frac{k}{l}\right) = a_n \frac{k^n}{l^n} + \ldots + a_1 \frac{k}{l} + a_0.$$

Mnożąc ostatnią równość obustronnie przez l^n dostajemy:

$$0 = a_n k^n + a_{n-1} l k^{n-1} + \ldots + a_1 k l^{n-1} + a_0 l^n,$$

$$k\left(a_n k^{n-1} + a_{n-1} l k^{n-2} + \ldots + a_1 l^{n-1}\right) = -a_0 l^n.$$

Ostatnia równość implikuje, że $k \mid a_0 l^n$.

Ponieważ k, l są względnie pierwsze, tak więc również k, l^n są względnie pierwsze. Czyli mamy:

$$\text{NWD}\,(k, l^n) = 1 \qquad \text{oraz} \qquad k \mid a_0 l^n \qquad \Rightarrow \qquad k \mid a_0,$$

co mieliśmy pokazać. Analogicznie pokazuje się, że $l \mid a_n$. □

Przykład 13.11. Niech:

$$W = 2X^3 + X^2 + 4X + 2 \in \mathbb{Z}[X].$$

Z Twierdzenia o pierwiastkach wymiernych, jedyne możliwe pierwiastki wymierne W to:

$$2,\ -2,\ 1,\ -1,\ \frac{1}{2},\ -\frac{1}{2}.$$

Łatwo sprawdzić, że $W(-1/2) = 0$. W szczególności W jest wielomianem rozkładalnym w pierścieniu $\mathbb{Q}[X]$. Wciąż nie wiemy czy ten wielomian jest rozkładalny w pierścieniu $\mathbb{Z}[X]$. W tym celu stosuje się następujący wynik, którego dowód pomijamy.

Twierdzenie 13.12 (Lemat Gaussa)**.** *Niech:*

$$W = a_n X^n + \ldots + a_1 X + a_0 \in \mathbb{Z}[X] \setminus \mathbb{Z}\,.$$

Wtedy następujące warunki są równoważne.

(1) *W jest wielomianem nierozkładalnym w pierścieniu $\mathbb{Z}[X]$.*
(2) *W jest wielomianem nierozkładalnym w pierścieniu $\mathbb{Q}[X]$* ***oraz*** *żadna liczba pierwsza nie dzieli wszystkich współczynników $a_0, a_1, \ldots, a_n$.*

W szczególności dla wielomianów z $\mathbb{Z}[X]$ mamy:

$$\text{nierozkładalny w } \mathbb{Z}[X] \qquad \Rightarrow \qquad \text{nierozkładalny w } \mathbb{Q}[X],$$

$$\text{rozkładalny w } \mathbb{Q}[X] \qquad \Rightarrow \qquad \text{rozkładalny w } \mathbb{Z}[X].$$

Tak więc, wielomian W z Przykładu 13.11 jest rozkładalny w $\mathbb{Z}[X]$.

Teraz ostatnie kryterium, które jest bardzo użyteczne (jeśli się stosuje).

Twierdzenie 13.13 (Kryterium Eisensteina)**.** *Niech:*

$$W = a_n X^n + \ldots + a_1 X + a_0 \in \mathbb{Z}[X]$$

i załóżmy, że istnieje liczba pierwsza p, taka że:

(i) $p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1}$;
(ii) $p \nmid a_n$;
(iii) $p^2 \nmid a_0$.

Wtedy wielomian W jest nierozkładalny ***w pierścieniu*** *$\mathbb{Q}[X]$.*

Dowód. Dzieląc przez NWD$(a_0, a_1, \ldots, a_n)$ (w pierścieniu $\mathbb{Z}[X]$) możemy przyjąć, że $a_0, a_1, \ldots, a_n$ nie mają żadnego wspólnego dzielnika pierwszego.

Załóżmy nie wprost, że W jest rozkładalny w pierścieniu $\mathbb{Q}[X]$. Z Lematu Gaussa dostajemy, że W jest rozkładalny w pierścieniu $\mathbb{Z}[X]$. Weźmy więc $G, H \in \mathbb{Z}[X] \setminus \mathbb{Z}[X]^*$, takie że $W = GH$. Ponieważ $a_0, a_1, \ldots, a_n$ nie mają żadnego wspólnego dzielnika pierwszego, tak więc dostajemy że $\deg(G) > 0$ oraz $\deg(H) > 0$. Niech:

$$G = b_d X^d + \ldots + b_1 X + b_0, \quad H = c_n X^n + \ldots + c_1 X + c_0, \quad b_d \neq 0 \neq d, \quad c_m \neq 0 \neq m.$$

Ponieważ $W = GH$, tak więc dostajemy $a_0 = b_0 c_0$. Czyli mamy:

$$a_0 = b_0 c_0 \ \text{ i } \ p \mid a_0 \ \text{ i } \ p^2 \nmid a_0 \qquad \Rightarrow \qquad (p \nmid b_0 \ \text{ i } \ p \mid c_0) \quad \textbf{lub} \quad (p \nmid c_0 \ \text{ i } \ p \mid b_0)\,.$$

Przyjmijmy, że $\underline{p \nmid b_0}$ i $\underline{p \mid c_0}$ (jeśli $p \nmid c_0$ i $p \mid b_0$, to dowód jest analogiczny).
Weźmy teraz:

$$r := \min\{i \leqslant m \mid p \nmid c_i\}.$$

Wtedy mamy:

$$p \mid c_0 \quad \text{oraz} \quad p \nmid c_m \qquad \Rightarrow \qquad 0 < r \leqslant m < n (= d + m).$$

Z minimalności r otrzymujemy, że:

$$p \mid c_0, p \mid c_1, \ldots, p \mid c_{r-1}, p \nmid c_r.$$

W szczególności:

$$p \mid b_1 c_{r-1} + \ldots + b_{r-1} c_1 + b_r c_0.$$

Używając tego, że p jest liczbą pierwszą dostajemy:

$$p \nmid c_r \quad \text{oraz} \quad p \nmid b_0 \qquad \Rightarrow \qquad p \nmid b_0 c_r.$$

Łącznie otrzymujemy:

$$p \mid b_1 c_{r-1} + \ldots + b_{r-1} c_1 + b_r c_0 \ \text{ oraz } \ p \nmid b_0 c_r \qquad \Rightarrow \qquad p \nmid a_r = b_0 c_r + b_1 c_{r-1} + \ldots + b_{r-1} c_1 + b_r c_0,$$

co daje sprzeczność, ponieważ $r < n$. □

Przykład 13.14. (1) Weźmy:

$$W = 3X^4 + 15X^2 + 10, \quad p = 5.$$

Wtedy mamy:
(i) $5 \mid 10, 5 \mid 15$;
(ii) $5 \nmid 3$;
(iii) $5^2 \nmid 10$.
Czyli z Kryterium Eisensteina, W jest nierozkładalny w pierścieniu $\mathbb{Q}[X]$.
Z Lematu Gaussa (ponieważ współczynniki W nie mają żadnego wspólnego dzielnika pierwszego), W jest nierozkładalny w pierścieniu $\mathbb{Z}[X]$.

(2) Weźmy:

$$W = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1.$$

Zauważmy, że ogólnie (dla dowolnych wielomianów o współczynnikach z dowolnych pierścieni przemiennych z jedynką) mamy:

$$W \text{ jest nierozkładalny} \qquad \Leftrightarrow \qquad W(X+1) \text{ jest nierozkładalny.}$$

Używając przedstawienia:

$$W = \frac{X^7 - 1}{X - 1}$$

możemy policzyć, że:

$$W(X+1) = X^6 + \binom{7}{6} X^5 + \binom{7}{5} X^4 + \binom{7}{4} X^3 + \binom{7}{3} X^2 + \binom{7}{2} X + \binom{7}{1}.$$

Wtedy dla $p = 7$ z Kryterium Eisensteina otrzymujemy, że wielomian $W(X+1)$ jest nierozkładalny w pierścieniu $\mathbb{Q}[X]$. Stąd wielomian W jest nierozkładalny w pierścieniu

$\mathbb{Q}[X]$. Z Lematu Gaussa dostajemy też, że wielomiany W i $W(X+1)$ są nierozkładalne w pierścieniu $\mathbb{Z}[X]$.

Podobnie dla każdej liczby pierwszej p, wielomian:

$$X^{p-1} + \ldots + X + 1$$

jest nierozkładalny w pierścieniu $\mathbb{Q}[X]$ oraz w pierścieniu $\mathbb{Z}[X]$.

Uwaga 13.15. Lemat Gaussa i Kryterium Eisensteina zachodzą

- ogólniej: dla dowolnego pierścienia euklidesowego R zamiast $\mathbb{Z}$ oraz ciała ułamków K pierścienia R zamiast $\mathbb{Q}$;
- jeszcze ogólniej: dla dowolnej dziedziny z **własnością jednoznacznego rozkładu** R (i ciała ułamków K).

14. Chińskie twierdzenie o resztach i ideały

Sunzi Suanjing, czyli „podręcznik arytmetyczny Mistrza Sun" to traktat matematyczny napisany pomiędzy trzecim a piątym wiekiem naszej ery. Rozdział trzeci tegoż traktatu zawiera następujący akapit:

Mamy pewne rzeczy, których ilość jest nieznana. Jeśli liczymy te rzeczy po trzy, to zostaną dwie; jeśli liczymy te rzeczy po pięć, to zostaną trzy i jeśli liczymy te rzeczy po siedem, to zostaną dwie. Ile jest tych rzeczy?

Mistrz Sun otrzymał rozwiązanie: $x = 23$.

Powyższe pytanie jest równoważne pytaniu o rozwiązanie następującego układu kongruencji:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

Następujące twierdzenie wyjaśnia te rozważania.

Twierdzenie 14.1 (Chińskie Twierdzenie o Resztach)**.** *Weźmy $n_1, \ldots, n_k > 1$ parami względnie pierwsze i niech:*

$$N := n_1 \cdot \ldots \cdot n_k.$$

Wtedy dla dowolnych $a_1, \ldots, a_k \in \mathbb{Z}$ istnieje $x \in \mathbb{Z}$, które jest rozwiązaniem następującego układu kongruencji:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\ldots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

Ponadto, jeśli $x' \in \mathbb{Z}$ jest również rozwiązaniem tego układu kongruencji, to mamy:

$$x \equiv x' \pmod N.$$

Dowód. Pokazujemy najpierw (nieco nietypowo) **jedyność** (czyli część „Ponadto...") rozwiązania rozważanego układu kongruencji, w sytuacji gdy jeszcze nie wiemy czy jakiekolwiek rozwiązania istnieją. Jedyności tej użyjemy później do dowodu istnienia rozwiązania.

Jeśli x oraz x' są rozwiązaniami rozważanego układu kongruencji, to mamy:

$$x \equiv a_1 \pmod{n_1}, \qquad x' \equiv a_1 \pmod{n_1},$$

czyli dostajemy:

$$x \equiv x' \pmod{n_1} \qquad \Rightarrow \qquad n_1 \mid x - x'.$$

Podobnie otrzymujemy:

$$n_1 \mid x - x', \quad n_2 \mid x - x', \ldots, n_k \mid x - x'.$$

Ponieważ $n_1, \ldots, n_k > 1$ są parami względnie pierwsze, otrzymujemy że:

$$N = n_1 \cdot \ldots \cdot n_k \mid x - x',$$

co znaczy, że $x \equiv x' \pmod N$.

Dla dowodu **istnienia** rozwiązania rozważanego układu kongruencji bierzemy następującą funkcję:

$$\varphi : \mathbb{Z}_N \to \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}, \qquad \varphi(x) = \left(r_{n_1}(x), \ldots, r_{n_k}(x)\right).$$

Z udowodnionej **jedyności** powyżej, funkcja φ jest „1-1". Zauważmy, że:

$$|\,\mathbb{Z}_N\,| = N = n_1 \cdot \ldots \cdot n_k = |\,\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}\,|.$$

Czyli funkcja φ jest funkcją różnowartościową pomiędzy dwoma skończonymi zbiorami tej samej mocy, tak więc φ jest również „na". W szczególności, istnieje $x \in \mathbb{Z}_N$ taki że:

$$r_{n_1}(x) = r_{n_1}(a_1), \quad r_{n_2}(x) = r_{n_2}(a_2), \ldots, r_{n_k}(x) = r_{n_k}(a_k),$$

czyli x jest rozwiązaniem rozważanego układu kongruencji. □

Uwaga 14.2. Powyższy dowód nie jest **konstruktywny**, tzn. nie podaje sposobu jak **znaleźć** powyższe rozwiązanie x. Nietrudno jest jednak podać taki sposób. Jeśli chcemy rozwiązać następujący układu kongruencji:

$$x \equiv a_1 \pmod{n_1}, \qquad x \equiv a_2 \pmod{n_2},$$

gdzie $\mathrm{NWD}(n_1, n_2) = 1$ (czyli $k = 2$), to (ponieważ $\mathrm{NWD}(n_1, n_2) = 1$) używając Twierdzenia 11.22 dostajemy $m_1, m_2 \in \mathbb{Z}$, takie że:

$$m_1 n_1 + m_2 n_2 = 1.$$

Wtedy nasze rozwiązanie to:

$$x := a_1 m_2 n_2 + a_2 m_1 n_1,$$

ponieważ liczymy, że:

$$x = a_1 m_2 n_2 + a_2 m_1 n_1 = a_1 (1 - m_1 n_1) + a_2 m_1 n_1 = a_1 + (a_2 - a_1) m_1 n_1 \equiv a_1 \pmod{n_1}.$$

Podobnie dostajemy, że:

$$x \equiv a_2 \pmod{n_2}.$$

Istnieją też analogiczne wzory w sytuacji, gdy $k > 2$ i znał je już Mistrz Sun.

Pojęcie kongruencji można uogólnić do dowolnego pierścienia przemiennego z jedynką (podobnie można też uogólnić Chińskie Twierdzenie o Resztach) używając pojęcia **ideału**. Intuicyjnie: ideały w teorii pierścieni grają rolę dzielników normalnych w teorii grup.

Definicja 14.3. Niech R będzie pierścieniem przemiennym z jedynką oraz $I \subseteq R$. Wtedy I nazywamy *ideałem* pierścienia R, co oznaczamy $I \trianglelefteq R$, jeśli:

(i) $I \leqslant (R, +)$;
(ii) zachodzi

$$\forall\, r \in R \ \ \forall\, x \in I \qquad\qquad rx \in I.$$

Czyli I jest podgrupą grupy addytywnej pierścienia R oraz I jest zamknięty na mnożenie przez elementy R.

Przykład 14.4. (1) Zawsze mamy ideał zerowy:

$$\{0\} \trianglelefteq R,$$

oraz ideał niewłaściwy:

$$R \trianglelefteq R.$$

(2) Mamy

$$2\,\mathbb{Z} \triangleleft \mathbb{Z}$$

i ogólniej dla dowolnego $n \in \mathbb{Z}$:

$$n\,\mathbb{Z} \trianglelefteq \mathbb{Z}\,.$$

(3) Niech:

$$I := \{F \in \mathbb{R}[X] \mid F(i) = 0\}$$

(np. $X^2 + 1 \in I$). Wtedy łatwo pokazać, że $I \triangleleft \mathbb{R}[X]$.

(4) Niech:

$$I := \{a_n X^n + \ldots + a_1 X + a_0 \in \mathbb{Z}[X] \ : \ 2 \mid a_0\}.$$

Wtedy nietrudno zauważyć, że $I \triangleleft \mathbb{R}[X]$.

Uwaga 14.5. (1) Jeśli $I \trianglelefteq R$ oraz $1 \in I$, to $I = R$, ponieważ dla każdego $r \in R$ mamy:

$$r = r \cdot 1 \in I.$$

Czyli ideał:
(i) **zawsze** jest podpierścieniem;
(ii) **prawie nigdy** nie jest podpierścieniem z jedynką.

(2) Jeśli $I \cap R^* \neq \emptyset$, to również $I = R$, ponieważ jeśli $u \in I \cap R^*$, to dla każdego $r \in R$ mamy:

$$r = ru^{-1} \cdot u \in I.$$

Definicja 14.6. Niech R będzie pierścieniem przemiennym z jedynką oraz $x_1, \ldots, x_n \in R$. Przez $(x_1, \ldots, x_n)$ oznaczamy ideał *generowany* przez $x_1, \ldots, x_n$, tzn.:

$$(x_1, \ldots, x_n) := \{r_1x_1 + \ldots + r_nx_n \mid r_1, \ldots, r_n \in R\}$$

(wszystkie „R-liniowe kombinacje" elementów $x_1, \ldots, x_n$).

Uwaga 14.7. Łatwo zauważyć, że:

(i) $(x_1, \ldots, x_n)$ jest faktycznie ideałem pierścienia R;
(ii) $(x_1, \ldots, x_n)$ jest **najmniejszym** ideałem pierścienia R zawierającym elementy $x_1, \ldots, x_n$.

Definicja 14.8. Ideał $I \trianglelefteq R$ nazywamy *głównym*, gdy istnieje $x \in I$, taki że:

$$I = (x).$$

Uwaga 14.9. Ideały główne to dokładnie te ideały, które mogą być generowane przez jeden element.

Przykład 14.10. (1) Mamy:

$$\{0\} = (0), \qquad R = (1),$$

czyli są to ideały główne.

(2) Mamy:

$$n\,\mathbb{Z} = (n),$$

czyli są też to ideały główne.

(3) Wkrótce (Przykład 14.13(2)) zauważymy, że

$$\{F \in \mathbb{R}[X] \mid F(i) = 0\} = \left(X^2 + 1\right),$$

czyli to jest też ideał główny.

(4) Można pokazać, że:

$$\{a_nX^n + \ldots + a_1X + a_0 \in \mathbb{Z}[X] \ : \ 2 \mid a_0\} = (2, X)$$

oraz że ideał $(2, X) \lhd \mathbb{Z}[X]$ **nie** jest ideałem głównym.

Definicja 14.11. Dziedzinę R, w której każdy ideał jest główny nazywamy *dziedziną ideałów głównych.*

Teraz ogólny wynik, który np. daje Przykład 14.13(2).

Twierdzenie 14.12. *Każdy pierścień euklidesowy R jest dziedziną ideałów głównych.*
Dokładniej, jeśli I jest niezerowym ideałem R oraz

$$\delta : R \setminus \{0\} \to \mathbb{N}$$

jest normą euklidesową na R, to mamy $I = (a)$, gdzie:

$$\delta(a) = \min\{\delta(x) \mid x \in I \setminus \{0\}\}.$$

Dowód. Niech R, δ, I, a będą j.w. Pokazujemy, że:

$$I = (a).$$

„$\supseteq$" Dowolny element ideału (a) ma postać qa dla pewnego $q \in R$. Ponieważ $a \in I$ oraz I jest ideałem R, tak więc $qa \in I$, czyli dostajemy $I \supseteq (a)$.
„$\subseteq$" Weźmy dowolny $x \in I$. Chcemy pokazać, że $x \in (a)$, tzn. że $a \mid x$ w R. Aby to pokazać postępujemy jak zwykle w pierścieniach euklidesowych, tzn. dzielimy z resztą x przez a dostając $q, r \in R$, takie że:

$$x = aq + r \qquad \text{oraz} \qquad (\delta(r) < \delta(a) \quad \text{lub} \quad r = 0)\,.$$

Jeśli $r = 0$, to $a \mid x$ i twierdzenie jest udowodnione.
Jeśli $r \neq 0$, to $\delta(r) < \delta(a)$ i dążymy do otrzymania sprzeczności. Mamy:

$$r = \underbrace{x}_{\in I} - \underbrace{a}_{\in I}\underbrace{q}_{\in R} \in I.$$

Ale $r \neq 0$ oraz $\delta(r) < \delta(a)$, co przeczy minimalności $\delta(a)$. □

Przykład 14.13. (1) W ideale $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ element n (jeśli $n \neq 0$) jest niezerowym elementem o najmniejszej wartości bezwzględnej (norma euklidesowa na $\mathbb{Z}$), tak więc z Twierdzenia 14.12 mamy:

$$n\mathbb{Z} = (n),$$

co jest też oczywiste bez używania Twierdzenia 14.12.

(2) Jeśli K jest ciałem, to $K[X]$ jest pierścieniem euklidesowym, gdzie normą euklidesową jest stopień wielomianu. Stąd, jeśli I jest niezerowym ideałem w $K[X]$, to mamy $I = (F)$, gdzie:

$$\deg(F) = \min\{\deg(W) \mid W \in I \setminus \{0\}\}.$$

W szczególności, jeśli $K = \mathbb{R}$ oraz

$$I := \{F \in \mathbb{R}[X] \mid F(i) = 0\},$$

to $X^2 + 1$ jest wielomianem najmniejszego stopnia z I (w I nie ma wielomianów stopnia 1, ponieważ $i \notin \mathbb{C}$), tak więc mamy:

$$\{F \in \mathbb{R}[X] \mid F(i) = 0\} = \left(X^2 + 1\right).$$

(3) W pierścieniu $\mathbb{Z}[X]$ mamy ideał $(2, X)$, który **nie** jest ideałem głównym. Czyli $\mathbb{Z}[X]$ **nie** jest dziedziną ideałów głównych. Używając Twierdzenia 14.12 dostajemy, że $\mathbb{Z}[X]$ **nie** jest pierścieniem euklidesowym.

Na ćwiczeniach zauważyliśmy, że stopień **nie** jest normą euklidesową na pierścieniu $\mathbb{Z}[X]$. Teraz widzimy, że na pierścieniu $\mathbb{Z}[X]$ **nie istnieje żadna** norma euklidesowa.

Uwaga 14.14. Wiemy, że pierścień euklidesowy ma własność jednoznacznego rozkładu (Twierdzenie 12.8). Można pokazać ogólniejsze twierdzenie (w praktyce jest to ten sam dowód, co dowód Twierdzenia 12.8) mówiące, że każda dziedzina ideałów głównych ma własność jednoznacznego rozkładu.

Jeśli mamy dzielnik normalny N w grupie G, to możemy skonstruować grupę ilorazową G/N. Zobaczymy teraz, że podobnie jest w przypadku ideałów w pierścieniach.

Definicja 14.15. Niech $I \trianglelefteq R$. Wtedy R/I definiujemy jako zbiór warstw **addytywnych** I w R, tzn.:

$$R/I := \{r + I \mid r \in R\}.$$

Twierdzenie 14.16. *Niech $I \trianglelefteq R$. Definiujemy działania $+, \cdot$ na zbiorze R/I:*

$$(a + I) + (b + I) := a + b + I, \qquad (a + I) \cdot (b + I) := ab + I.$$

Wtedy mamy:

(1) *powyższe działania są dobrze określone;*

(2) $(R/I, +, \cdot)$ *jest pierścieniem przemiennym z jedynką zwanym* pierścieniem ilorazowym*;*
(3) *funkcja*

$$\pi : R \to R/I, \qquad \pi(r) = r + I$$

jest homomorfizmem pierścieni, który jest „na" oraz $\ker(\pi) = I$.

Szkic dowodu. Pokażemy tylko, że mnożenie jest dobrze określone, co jest tu najtrudniejsze (ale wciąż łatwe). Weźmy $a, a', b, b' \in R$, takie że:

$$a + I = a' + I, \qquad b + I = b' + I.$$

Mamy pokazać, że $ab + I = a'b' + I$.

Z założenia mamy:

$$a - a' \in I \quad \text{oraz} \quad b - b' \in I \qquad \Rightarrow \qquad (a - a')b \in I \quad \text{oraz} \quad (b - b')a \in I.$$

Czyli dostajemy, że:

$$ab - a'b' = \underbrace{ab - a'b}_{(a-a')b} + \underbrace{ba' - b'a'}_{(b-b')a} \in I.$$

Stąd dostajemy, że $ab + I = a'b' + I$, co należało pokazać. □

Przykład 14.17. (1) Warstwy i kongruencje

Niech $I = n\,\mathbb{Z} \trianglelefteqslant \mathbb{Z}$ oraz $a, b \in \mathbb{Z}$. Wtedy mamy:

$$n \mid a - b \quad \Leftrightarrow \quad a \equiv b \pmod{n} \quad \Leftrightarrow \quad a - b \in n\,\mathbb{Z} \quad \Leftrightarrow \quad a + n\,\mathbb{Z} = b + n\,\mathbb{Z}\,.$$

Uogólniamy (notacyjnie) równoważność:

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad a + n\,\mathbb{Z} = b + n\,\mathbb{Z}$$

do dowolnego pierścienia przemiennego z jedynką R oraz dowolnego $I \trianglelefteqslant R$. Dla każdego $a, b \in R$ piszemy:

$$a \equiv b \pmod{I},$$

jeśli $a + I = b + I$ (czyli $b - a \in I$) i mówimy wtedy, że a *przystaje do* b *modulo* I.

(2) Pierścienie ilorazowe

Łatwo zauważyć, że mamy następujący izomorfizm pierścieni ($n > 0$):

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

Niedługo będzie ogólne twierdzenie na ten temat (Twierdzenie 14.19).

Zobaczymy teraz, że ideały mają kolejną cechę dzielników normalnych, tzn. że są to dokładnie jądra homomorfizmów pierścieni.

Twierdzenie 14.18. *Niech* $f : R \to S$ *będzie homomorfizmem pierścieni przemiennych z jedynką. Wtedy:*

(1) $\ker(f) \trianglelefteqslant R$,
(2) $\mathrm{im}(f)$ *jest podpierścieniem z jedynką pierścienia* R.

Dowód. Sprawdzimy tylko, że $\ker(f)$ jest zamknięty na mnożenie przez elementy R. Weźmy $x \in \ker(f)$ oraz $r \in R$. Wtedy mamy:

$$f(x) = 0 \qquad \Rightarrow \qquad f(rx) = f(r)f(x) = f(r) \cdot 0 = 0.$$

Czyli $rx \in \ker(f)$, co należało sprawdzić. □

Następne twierdzenie jest analogiczne do Zasadniczego Twierdzenia o Homomorfizmach Grup. Analogiczny dowód pomijamy.

Twierdzenie 14.19 (Zasadnicze Twierdzenie o Homomorfizmach Pierścieni)**.** *Niech* $f : R \to S$ *będzie homomorfizmem pierścieni przemiennych z jedynką. Wtedy mamy następujący izomorfizm pierścieni:*

$$R/\ker(f) \cong \mathrm{im}(f).$$

Przykład 14.20. (1) Funkcja n-tej reszty $r_n : \mathbb{Z} \to \mathbb{Z}_n$ jest homomorfizmem pierścieni i mamy:

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

Czyli z Zasadniczego Twierdzenia o Homomorfizmach Pierścieni otrzymujemy:

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

(2) Rozważmy następującą funkcję ewaluacji:

$$\mathrm{ev}_i : \mathbb{R}[X] \to \mathbb{C}, \qquad \mathrm{ev}_i(F) = F(i).$$

Ponieważ $i \notin \mathbb{R}$, tak więc powyższa funkcja nie jest specjalnym przypadkiem funkcji ewaluacji z Definicji 10.35, ale wciąż ta funkcja jest homomorfizmem pierścieni analogicznie do Uwagi 10.36(1). Mamy:

$$\ker\left(\mathrm{ev}_i\right) = \{F \in \mathbb{R}[X] \mid F(i) = 0\} = \left(X^2 + 1\right).$$

Łatwo zauważyć, że $\operatorname{im}(\mathrm{ev}_i) = \mathbb{C}$ ($\mathrm{ev}_i(aX + b) = ai + b$), tak więc z Zasadniczego Twierdzenia o Homomorfizmach Pierścieni otrzymujemy:

$$\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}\,.$$

(3) Rozważmy następującą funkcję ewaluacji:

$$\mathrm{ev}_{\sqrt{2}} : \mathbb{Q}[X] \to \mathbb{Q}[\sqrt{2}], \qquad \mathrm{ev}_{\sqrt{2}}(F) = F\left(\sqrt{2}\right).$$

Podobnie jak w punkcie (2) powyżej, mamy $\operatorname{im}(\mathrm{ev}_{\sqrt{2}}) = \mathbb{Q}[\sqrt{2}]$. Mamy też:

$$\ker\left(\mathrm{ev}_{\sqrt{2}}\right) = \left\{F \in \mathbb{Q}[X] \mid F\left(\sqrt{2}\right) = 0\right\} \lhd \mathbb{Q}[X].$$

Dzięki Twierdzeniu 14.12 wiemy, że:

$$\ker\left(\mathrm{ev}_{\sqrt{2}}\right) = (F),$$

gdzie $F \in \ker(\mathrm{ev}_{\sqrt{2}})$ jest wielomianem minimalnego stopnia. Ponieważ $\sqrt{2} \notin \mathbb{Q}$, tak więc w $\ker(\mathrm{ev}_{\sqrt{2}})$ nie ma wielomianów stopnia 1 i dostajemy:

$$\ker\left(\mathrm{ev}_{\sqrt{2}}\right) = \left(X^2 - 2\right).$$

Z Zasadniczego Twierdzenia o Homomorfizmach Pierścieni otrzymujemy:

$$\mathbb{Q}[X]/(X^2 - 2) \cong \mathbb{Q}[\sqrt{2}].$$

(4) Niech:

$$\mathbb{Z}\,[1/2] := \left\{\frac{n}{2^m} \in \mathbb{Q} \;\middle|\; n \in \mathbb{Z},\ m \in \mathbb{N}\right\}$$

będzie najmniejszym podpierścieniem $\mathbb{Q}$ zawierającym $\mathbb{Z}$ oraz $1/2$. Rozważmy następującą funkcję ewaluacji:

$$\mathrm{ev}_{1/2} : \mathbb{Z}[X] \to \mathbb{Z}[1/2], \qquad \mathrm{ev}_{1/2}(F) = F\,(1/2)\,.$$

Wtedy można pokazać, że:

$$\ker\left(\mathrm{ev}_{1/2}\right) = (2X - 1), \qquad \operatorname{im}(f) = \mathbb{Z}[1/2].$$

Czyli z Zasadniczego Twierdzenia o Homomorfizmach Pierścieni otrzymujemy:

$$\mathbb{Z}[X]/(2X - 1) \cong \mathbb{Z}[1/2].$$

(5) Rozważmy:

$$r_7 : \mathbb{Z}_{14} \to \mathbb{Z}_7\,.$$

Ponieważ $7 \mid 14$, tak więc jest to homomorfizm pierścieni. Mamy:

$$\ker\left(r_7\right) = \{0, 7\}, \qquad \operatorname{im}\left(r_7\right) = \mathbb{Z}_7\,.$$

Czyli z Zasadniczego Twierdzenia o Homomorfizmach Pierścieni otrzymujemy:

$$\mathbb{Z}_{14}\,/\{0, 7\} \cong \mathbb{Z}_7\,.$$

W powyższych przykładach pojawiły się pierścienie typu $R[X]/(W)$ dla $W \in R[X]$. Przyjrzymy się bliżej tej sytuacji gdy $R = K$ jest ciałem. Dowód następującego twierdzenia pomijamy.

Twierdzenie 14.21. *Niech K będzie ciałem oraz $W \in K[X]$, takim że $\deg(W) = n > 0$. Wtedy każdy element $\alpha \in K[X]/(W)$ ma jednoznaczne przedstawienie jako:*

$$\alpha = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} + (W)$$

dla pewnych (dla tego ustalonego α jedynych!) $a_0, a_1, \ldots, a_{n-1} \in K$.

Uwaga 14.22. Niech K i W będą jak w Twierdzeniu 14.21.

(1) Przedstawienie α jak w Twierdzeniu 14.21 nazywamy *przedstawieniem w postaci normalnej.*

(2) Twierdzenie 14.21 można wyrazić mówiąc, że $K[X]/(W)$ jest przestrzenią liniową nad ciałem K o wymiarze n i bazie:

$$\left\{1 + (W), X + (W), \ldots, X^{n-1} + (W)\right\}.$$

Przykład 14.23. Niech

$$W := 1 + X + X^2 + X^3 + X^4 \in \mathbb{Q}[X]$$

i rozważmy pierścień $R := \mathbb{Q}[X]/(W)$. Weźmy:

$$\alpha := X^2 + 1 + (W) \in R, \qquad \beta := X^3 + 5X^2 + 1 + (W) \in R.$$

Przedstawimy $\alpha\beta \in R$ w postaci normalnej. Postać „nienormalna" to:

$$\alpha\beta = \left(X^2 + 1\right)\left(X^3 + 5X^2 + 1\right) + (W) = X^5 + 5X^4 + X^3 + 6X^2 + 1 + (W).$$

Aby przedstawić $\alpha\beta$ w postaci normalnej musimy podzielić z resztą $X^5 + 5X^4 + X^3 + 6X^2 + 1$ przez $1 + X + X^2 + X^3 + X^4$ w pierścieniu $\mathbb{Q}[X]$. Robimy to i dostajemy:

$$X^5 + 5X^4 + X^3 + 6X^2 + 1 = \underbrace{(X+4)}_{q}\left(1 + X + X^2 + X^3 + X^4\right) + \underbrace{\left(-4X^3 + X^2 - 5X - 3\right)}_{r}.$$

Stąd postać normalna jest następująca:

$$\alpha\beta = -4X^3 + X^2 - 5X - 3 + (W).$$

Udowodnimy teraz, że pierścień

$$R = \mathbb{Q}[X]/(W) = \mathbb{Q}[X]/(1 + X + X^2 + X^3 + X^4)$$

jest ciałem. Weźmy $\alpha \in R \setminus \{0\}$. Pokażemy, że $\alpha \in R^*$. Ponieważ $\alpha \neq 0$, tak więc

$$\alpha = F + (W)$$

dla pewnego $F \in \mathbb{Q}[X] \setminus (W)$. Skoro $F \notin (W)$, to $W \nmid F$. Z Przykładu 13.14(2), wielomian $W = 1 + X + X^2 + X^3 + X^4$ jest nierozkładalny w pierścieniu $\mathbb{Q}[X]$. Na ćwiczeniach pokazujemy ogólnie, że:

jeśli $a, b \in R$, R jest dziedziną, a nie dzieli b oraz element a jest nierozkładalny, to wtedy największy wspólny dzielnik a i b to 1.

Czyli w naszej sytuacji dostajemy:

$$W \nmid F \quad \text{oraz} \quad W \text{ jest nierozkładalny} \qquad \Rightarrow \qquad \text{n.w.d. } W, F \text{ to } 1.$$

Ponieważ pierścień $\mathbb{Q}[X]$ jest euklidesowy oraz n.w.d. W, F to 1, tak więc z Twierdzenia 11.22 istnieją $A, B \in \mathbb{Q}[X]$, takie że:

$$AF + BW = 1.$$

Stąd dostajemy, że:

$$AF + (W) = 1 + (W) = 1_R.$$

Czyli dla $\beta = X^3 + 5X^2 + 1 + (W) \in R$ mamy:

$$\alpha\beta = (F + (W))(A + (W)) = AF + (W) = 1_R.$$

Stąd $\alpha \in R^*$ i R jest ciałem.

Podobnie dowodzi się następujący ogólny wynik.

Twierdzenie 14.24. *Niech K będzie ciałem i wielomian $W \in K[X]$ będzie nierozkładalny. Wtedy pierścień $K[X]/(W)$ jest ciałem.*

15. Ideały maksymalne i ciała

Wyodrębnimy teraz abstrakcyjną własność ideałów postaci (W) jak w Twierdzeniu 14.24, która zapewnia, że iloraz jest ciałem.

Definicja 15.1. Ideał $I \trianglelefteq R$ nazywamy *ideałem maksymalnym*, gdy:

(i) $I \neq R$;
(ii) dla każdego $J \trianglelefteq R$ mamy:

$$I \subseteq J \qquad \Rightarrow \qquad J = I \quad \text{lub} \quad J = R.$$

Uwaga 15.2. Powyższa definicja mówi, że ideały maksymalne R to **elementy maksymalne** zbioru ideałów właściwych R względem porządku danego przez inkluzję.

Twierdzenie 15.3. *Niech R będzie pierścieniem euklidesowym oraz $r \in R$ będzie elementem nierozkładalnym. Wtedy ideał główny (r) jest maksymalny.*

Dowód. Udowodnimy najpierw, że $(r) \neq R$. Załóżmy nie wprost, że $(r) = R$. Wtedy w szczególności mamy, że $1 \in R$, tzn. istnieje $s \in S$, taki że $rs = 1$. Ale to znaczy, że $r \in R^*$, co przeczy nierozkładalności r.

Weźmy teraz $J \trianglelefteq R$, taki że $(r) \subsetneqq J$. Mamy pokazać, że $J = R$. Z Twierdzenia 14.12, R jest dziedziną ideałów głównych, czyli istnieje $r' \in R$, taki że $(r') = J$. Pokażemy najpierw, że $r' \nmid r$. Załóżmy nie wprost, że $r' \mid r$, czyli istnieje $a \in R$, taki że $r' = ar$. Wtedy dla każdego $b \in R$ mamy:

$$br' = bar \in (r).$$

Ponieważ dowolny element $J = (r')$ jest postaci br' dla pewnego $b \in R$, dostajemy $J \subseteq (r)$. Ponieważ z założenia mamy, że $(r) \subseteq J$, tak więc dostajemy $(r) = J$, co przeczy założeniu $(r) \subsetneqq J$ i pokazuje, że $r' \nmid r$. Przypominamy teraz zadanie z ćwiczeń, które pojawiło się w Przykładzie 14.23:

jeśli $a, b \in R$, R jest dziedziną, a nie dzieli b oraz element a jest nierozkładalny, to wtedy największy wspólny dzielnik a i b to 1.

Używając powyższego wnioskujemy:

$$r \text{ jest nierozkładalny} \quad \text{oraz} \quad r' \nmid r \qquad \Rightarrow \qquad \text{n.w.d. } r, r' \text{ to } 1.$$

Tak więc używając Twierdzenia 11.22 istnieją $x, y \in R$, takie że:

$$xr + yr' = 1.$$

Czyli mamy:

$$r \in (r) \subset J \quad \text{oraz} \quad r' \in J \qquad \Rightarrow \qquad 1 = xr + yr' \in J.$$

Z Uwagi 14.5(1) otrzymujemy, że $J = R$, co należało pokazać. □

Uwaga 15.4. Twierdzenie 15.3 jest też prawdziwe (ten sam dowód) w ogólniejszej wersji, jeśli zastąpimy „pierścień euklidesowy" przez „dziedzina ideałów głównych".

Przykład 15.5.
(1) Jeśli K jest ciałem, to wtedy pierścień $K[X]$ jest euklidesowy. Stąd, jeśli wielomian $W \in K[X]$ jest nierozkładalny, to ideał $(W) \lhd K[X]$ jest maksymalny.
(2) Jeśli p jest liczbą pierwszą, to ideał $p\mathbb{Z} \lhd \mathbb{Z}$ jest maksymalny.
(3) Pierścień $\mathbb{Z}[i]$ jest euklidesowy i np. wiemy że element $1 + i \in \mathbb{Z}[i]$ jest nierozkładalny. Stąd ideał $(1 + i) \lhd \mathbb{Z}[i]$ jest maksymalny.

Udowodnimy teraz ogólny wynik, z którego (oraz z Przykładu 15.5(1)) wynika Twierdzenie 14.24.

Twierdzenie 15.6. *Niech R będzie pierścieniem przemiennym z jedynką oraz $I \trianglelefteq R$. Wtedy mamy:*

$$I \text{ jest ideałem maksymalnym} \qquad \Leftrightarrow \qquad R/I \text{ jest ciałem.}$$

Dowód. Pierścień jest ciałem wtedy i tylko wtedy, gdy $0 \neq 1$ oraz każdy niezerowy element jest odwracalny. Łatwo zauważyć, że:

$$I \neq R \quad \Leftrightarrow \quad R/I \neq \{0\} \quad \Leftrightarrow \quad 0_{R/I} \neq 1_{R/I}.$$

Czyli możemy założyć, że $I \neq R$.
„$\Rightarrow$" Załóżmy, że I jest ideałem maksymalnym i weźmy $\alpha \in R/I$, takie że $\alpha \neq 0$. Mamy pokazać, że $\alpha \in (R/I)^*$. Niech $r \in R$ będzie, taki że $\alpha = r + I$. Ponieważ $\alpha \neq 0$, tak więc $r \notin I$. Rozważmy zbiór:

$$J := \{x + y \mid x \in I,\ y \in (r)\}.$$

Łatwo zauważyć, że:

$$J \trianglelefteq R \qquad \text{oraz} \qquad I \subseteq J.$$

Ponieważ $r \in J \setminus I$, tak więc $I \subsetneqq J$. Ponieważ I jest ideałem maksymalnym dostajemy, że $J = R$ oraz:

$$1 \in J \qquad \Rightarrow \qquad \exists x \in I\ \exists y \in (r) \quad 1 = x + y.$$

Ponieważ $y \in (r)$, tak więc istnieje $a \in R$, takie że $y = ar$ i dostajemy:

$$1 = x + ar.$$

Liczymy teraz:

$$\alpha \cdot (a + I) = (r + I)(a + I) = ar + I \underbrace{=}_{x \in I} 1 + I = 1_{R/I}.$$

Stąd $\alpha \in (R/I)^*$, co należało pokazać.
„$\Leftarrow$" Załóżmy, że R/I jest ciałem i weźmy $J \trianglelefteq R$, taki że $I \subsetneqq J$. Mamy pokazać, że $J = R$. Używając Uwagi 14.5(1) wystarczy pokazać, że $1 \in R$. Weźmy $a \in J \setminus I$. Wtedy mamy:

$$a + I \neq I = 0_{R/I} \qquad \underbrace{\Rightarrow}_{R/I \text{ jest ciałem}} \qquad a + I \in (R/I)^*.$$

Tak więc istnieje $b \in R$, takie że:

$$1 + I = (a + I)(b + I) = ab + I.$$

Czyli mamy:

$$r := 1 - ab \in I,$$

tak więc dostajemy:

$$1 = \underbrace{r}_{\in I \subset J} + \underbrace{ab}_{\in J} \in J,$$

co mieliśmy pokazać. □

Przykład 15.7. Wiemy, że wielomiany:

$$X^2 + X + 1 \in \mathbb{Z}_2[X], \qquad X^2 + 1 \in \mathbb{Z}_3[X]$$

są nierozkładalne, ponieważ są stopnia 2 i nie mają pierwiastków (Twierdzenie 13.5). Tak więc z Twierdzenia 15.3 dostajemy, że ideały:

$$(X^2 + X + 1) \lhd \mathbb{Z}_2[X], \qquad (X^2 + 1) \lhd \mathbb{Z}_3[X]$$

są maksymalne i z Twierdzenia 15.6 wynika, że pierścienie:

$$\mathbb{Z}_2[X]/(X^2 + X + 1), \qquad \mathbb{Z}_3[X]/(X^2 + 1)$$

są ciałami. Z Twierdzenia 14.21 (o postaci normalnej) otrzymujemy, że

$$|\,\mathbb{Z}_2[X]/(X^2 + X + 1)| = 4, \qquad |\,\mathbb{Z}_3[X]/(X^2 + 1)| = 9,$$

czyli otrzymaliśmy ciała mocy 4 i 9. Można pokazać, że powyższe ciało mocy 4 jest izomorficzne z ciałem z Przykładu 10.2(3).

Wiemy, że ideały maksymalne można otrzymać z elementów nierozkładalnych. Następujące twierdzenie, którego dowód pomijamy, pokazuje że ideałów maksymalnych jest bardzo dużo.

Twierdzenie 15.8. *Każdy ideał właściwy rozszerza się do ideału maksymalnego.*

Uwaga 15.9. (1) Dzięki Twierdzeniu 15.8 wiemy, że w każdym pierścieniu R jest dużo ideałów maksymalnych, tak więc używając Twierdzenia 15.6 otrzymujemy też dużo homomorfizmów ilorazowych $R \to R/I$, gdzie pierścień ilorazowy R/I jest ciałem.
(2) Dowód Twierdzenia 15.8 korzysta z aksjomatu wyboru, czyli wiemy że ideały maksymalne istnieją, ale być może nie jesteśmy w stanie ich konkretnie wskazać.

Na koniec tego wykładu koncentrujemy się na ciałach. Niech K będzie ciałem. Zauważmy, że jeśli $K = \mathbb{Z}_2$, to mamy:

$$1 +_2 1 = 0,$$

a jeśli $K = \mathbb{Q}$, to mamy:

$$\forall\, n > 0 \qquad \underbrace{1 + \ldots + 1}_{n \text{ razy}} \neq 0.$$

Interesuje nas ile razy trzeba dodać do siebie 1 w K aby otrzymać 0 i czy to w ogóle może się zdarzyć.

Definicja 15.10. Weźmy $n > 0$. Mówimy, że *charakterystyka* ciała K to n, co oznaczamy $\underline{\text{char}(K) = n}$, gdy n jest **najmniejszą** liczbą dodatnią, taką że:

$$\underbrace{1 + \ldots + 1}_{n \text{ razy}} = 0.$$

Jeśli takie n nie istnieje, to przyjmujemy że $\text{char}(K) = 0$.

Przykład 15.11. Niech p będzie liczbą pierwszą.
(1) $\text{char}(\mathbb{Z}_p) = p$.
(2) $\text{char}(\mathbb{Q}) = 0$.
(3) $\text{char}(\mathbb{Z}_p(X)) = p$.
(4) $\text{char}(\mathbb{Q}(X)) = 0$.
(5) $\text{char}(\mathbb{C}) = 0$.

W Przykładzie 15.11 charakterystyka danego ciało to zawsze liczba pierwsza lub 0. Zobaczymy teraz, że tak jest zawsze.

Twierdzenie 15.12. *Niech K będzie ciałem. Wtedy charakterystyka K to liczba pierwsza lub 0.*

Dowód. Załóżmy, że $n := \text{char}(K) \neq 0$. Pokażemy, że n jest liczbą pierwszą. Wiemy, że n jest najmniejszą liczbą dodatnią, taką że:

$$\underbrace{1 + \ldots + 1}_{n \text{ razy}} = 0.$$

Ponieważ $1 \neq 0$, tak więc $n \geqslant 2$. Niech p będzie dowolnym dzielnikiem pierwszym n. Pokażemy, że $n = p$. Załóżmy nie wprost, że $n \neq p$ i niech:

$$m := \frac{n}{p}.$$

Wtedy $1 < m, p < n$ i mamy:

$$\underbrace{(1 + \ldots + 1)}_{p \text{ razy}} \cdot \underbrace{(1 + \ldots + 1)}_{m \text{ razy}} = \underbrace{1 \cdot 1 + \ldots + 1 \cdot 1}_{pm = n \text{ razy}} = \underbrace{1 + \ldots + 1}_{n \text{ razy}} = 0.$$

Definiujemy teraz:

$$a := \underbrace{1 + \ldots + 1}_{p \text{ razy}}, \qquad b := \underbrace{1 + \ldots + 1}_{m \text{ razy}}.$$

Ponieważ $m, n < p$, tak więc $a \neq 0 \neq b$. Ale $ab = 0$, czyli np. a jest dzielnikiem zera, co przeczy temu, że każde ciało jest dziedziną. $\square$

Często spotykaliśmy się z sytuacją, że mieliśmy podpierścień R ciała K, taki że R też był ciałem np.:

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}\,.$$

Poniżej ogólna definicja.

Definicja 15.13. Niech K będzie ciałem i $F \subseteq K$. Mówimy, że F jest *podciałem* K, gdy:

(i) F jest podpierścieniem z jedynką ciała K;
(ii) dla każdego $a \in F \setminus \{0\}$ mamy $a^{-1} \in F$.

Uwaga 15.14. Następujące obserwacje są oczywiste.

(1) Podciała ciała K to dokładnie te podpierścienie K, które są ciałami.
(2) Jeśli F jest podciałem ciała K, to mamy:

$$\mathrm{char}(F) = \mathrm{char}(K).$$

Definicja 15.15. Jeśli F jest podciałem ciała K, to mówimy też, że inkluzja $F \subseteq K$ jest *rozszerzeniem ciał*.

Zauważmy, że często spotykamy się z sytuacją, gdy wielomian $F \in F[X]$ nie ma pierwiastków w ciele F, ale istnieje rozszerzenie ciał $F \subseteq K$, takie że F ma pierwiastki w K.

Przykład 15.16. (1) Wielomian $X^2 - 2$ nie ma pierwiastków w ciele $\mathbb{Q}$, ale ma pierwiastki w ciele $\mathbb{R}$.
(2) Wielomian $X^2 + 1$ nie ma pierwiastków w ciele $\mathbb{R}$, ale ma pierwiastki w ciele $\mathbb{C}$.

Twierdzenie 15.17. *Niech F będzie ciałem oraz $W \in F[X] \setminus F$. Wtedy istnieje rozszerzenie ciał $F \subseteq K$, takie że W ma pierwiastek w K.*

Dowód. Ponieważ $F[X]$ jest pierścieniem euklidesowym i $W \in F[X] \setminus F$, tak więc (z Twierdzenia 12.8) W rozkłada się na iloczyn wielomianów nierozkładalnych w pierścieniu $F[X]$. W szczególności istnieje wielomian nierozkładalny $W_0 \in F[X]$, taki że $W_0 \mid W$. Niech:

$$K := F[X]/(W_0).$$

Z Twierdzenia 14.24, K jest ciałem. Rozważmy homomorfizm $\alpha : F \to K$, który jest złożeniem następujących homomorfizmów:

$$F \xrightarrow{\subseteq} F[X] \xrightarrow[\text{ilorazowy}]{\text{homomorfizm}} K = F[X]/(W_0).$$

Z ćwiczeń wiemy, że dowolny homomorfizm pomiędzy ciałami jest „1-1”, czyli α jest „1-1”. Dlatego można przyjąć, że α to inkluzja i że mamy rozszerzenie ciał $F \subseteq K$.

Niech teraz:

$$x := X + (W_0) \in K.$$

Wtedy mamy:

$$W(x) = W\left(X + (W_0)\right) = W(X) + (W_0) = W + (W_0) = (W_0) = 0_K,$$

ponieważ $W_0 \mid W$, czyli $W \in (W_0)$. Stąd x jest pierwiastkiem W w ciele K. $\square$

Przykład 15.18. Weźmy:

$$F = \mathbb{R}, \qquad W = W_0 = X^2 + 1 \in \mathbb{R}[X].$$

Wtedy wiemy, że:

$$\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}\,.$$

Przy powyższym izomorfiźmie element $x := X + (X^2+1) \in \mathbb{R}[X]/(X^2+1)$ z dowodu Twierdzenia 15.17 przechodzi na jednostkę urojoną $i \in \mathbb{C}$ oraz mamy $W(i) = 0$.

Definicja 15.19. Ciało K nazywamy *algebraicznie domkniętym*, gdy każdy niestały wielomian $W \in K[X]$ ma pierwiastek w K.

Przykład 15.20 (Zasadnicze Twierdzenie Algebry)**.** Ciało $\mathbb{C}$ jest algebraicznie domknięte.

Można się spytać, czy istnieją jakieś inne (niż $\mathbb{C}$) ciała algebraicznie domknięte. Ponownie jest ich bardzo dużo, ale nie można ich konkretnie wskazać, o czym mówi poniższe twierdzenie, którego dowód pomijamy.

Twierdzenie 15.21. *Niech F będzie ciałem. Wtedy istnieje rozszerzenie ciał $F \subseteq K$, takie że K jest algebraicznie domknięte.*

Idea dowodu. Używając Twierdzenia 15.17 znajdujemy rozszerzenia, w których istnieją pierwiastki wielomianów i robimy to wiele, wiele razy ... (indukcja pozaskończona). □

Uwaga 15.22. Ciała algebraicznie domknięte są nieskończone.

Dowód. Jeśli ciało $F = \{a_1, \ldots, a_n\}$ jest skończone, to wielomian

$$F := (X - a_1) \cdot \ldots \cdot (X - a_n) + 1 \in F[X]$$

nie ma pierwiastków w F. □

Ciała algebraicznie domknięte są „duże". Zajmiemy się teraz „najmniejszymi" ciałami.

Fakt 15.23. *Ciało $\mathbb{Q}$ nie ma żadnych podciał właściwych.*

Dowód. Niech K będzie podciałem $\mathbb{Q}$. Mamy pokazać, że $K = \mathbb{Q}$. Ponieważ K jest podciałem, tak więc $1 \in K$. Weźmy dowolny $x \in \mathbb{Q}$. Wtedy istnieją $n \in \mathbb{Z}, m \in \mathbb{N}_{>0}$, takie że:

$$x = \frac{n}{m} \qquad \Rightarrow \qquad x = \frac{\pm(\overbrace{1 + \ldots + 1}^{|n| \text{ razy}})}{\underbrace{1 + \ldots + 1}_{m \text{ razy}}}.$$

Ponieważ K jest podciałem $\mathbb{Q}$ oraz $1 \in K$, tak więc $x \in K$. Czyli dostajemy, że $K = \mathbb{Q}$, co należało pokazać. □

Definicja 15.24. Ciało F nazywamy *ciałem prostym*, gdy F nie ma żadnych podciał właściwych.

Przykład 15.25. (1) $\mathbb{Q}$ jest ciałem prostym.

(2) Jeśli p jest liczbą pierwszą, to $\mathbb{Z}_p$ jest ciałem prostym, bo dla każdego $r \in \mathbb{Z}_p$ mamy:

$$r = \underbrace{1 +_p \ldots +_p 1}_{r \text{ razy}}.$$

Twierdzenie 15.26. *Jeśli F jest ciałem prostym, to wtedy $F \cong \mathbb{Q}$ lub $F \cong \mathbb{Z}_p$ dla pewnej liczby pierwszej p.*

Dowód. Rozważamy dwa przypadki.
$\underline{\text{char}(F) = 0.}$
Pokażemy, że $F \cong \mathbb{Q}$. Niech:

$$F_0 := \left\{ \frac{\pm(\overbrace{1 + \ldots + 1}^{n \text{ razy}})}{\underbrace{1 + \ldots + 1}_{m \text{ razy}}} \in F \mid n, m > 0 \right\} \cup \{0\}.$$

Łatwo sprawdzić (używając założenia o charakterystyce F), że:

- F_0 jest podciałem F,
- $F_0 \cong \mathbb{Q}$.

Ponieważ F jest ciałem prostym, dostajemy że $F = F_0$, czyli $F \cong \mathbb{Q}$.
$\underline{\text{char}(F) \neq 0}$.
Z Twierdzenia 15.12, wiemy że $\text{char}(F) = p$, gdzie p jest liczbą pierwszą. Pokażemy, że $F \cong \mathbb{Z}_p$. Niech:

$$F_0 := \left\{ \underbrace{1 + \ldots + 1}_{n \text{ razy}} \in F \mid 0 < n < p \right\} \cup \{0\}.$$

Łatwo sprawdzić (używając założenia o charakterystyce F), że:

- F_0 jest podciałem F,
- $F_0 \cong \mathbb{Z}_p$.

Ponieważ F jest ciałem prostym, dostajemy że $F = F_0$, czyli $F \cong \mathbb{Z}_p$. □

Wniosek 15.27. *Z dowodu Twierdzenia 15.26 wynika też, że jeśli F jest dowolnym ciałem, to istnieje **jedyne** podciało $F_0 \subseteq F$, takie że F_0 jest ciałem prostym. To podciało F_0 nazywamy* podciałem prostym *ciała F.*

Uwaga 15.28. (1) Jeśli $\text{char}(F) = 0$, to podciało proste F jest izomorficzne z $\mathbb{Q}$.
(2) Jeśli $\text{char}(F) = p > 0$, to podciało proste F jest izomorficzne z $\mathbb{Z}_p$.

Na koniec zajmiemy się ciałami skończonymi. Zauważmy, że nie pojawiło się dotychczas ciało mocy 6. Poniższe twierdzenie mówi, że nie jest to przypadek.

Twierdzenie 15.29. *Jeśli F jest ciałem skończonym, to $|F|$ jest potęgą liczby pierwszej.*

Dowód. Niech F_0 będzie podciałem prostym ciała F. Ponieważ ciało F jest skończone, tak więc ciało F_0 jest również skończone. Z Twierdzenia 15.26 dostajemy, że $F_0 \cong \mathbb{Z}_p$ dla pewnej liczby pierwszej p. Wtedy F staje się przestrzenią liniową nad F_0 i niech:

$$n := \dim_{F_0}(F).$$

Ponieważ F jest skończone, tak więc n jest liczbą naturalną i dostajemy że

$$|F| = |F_0|^n = p^n,$$

czyli $|F|$ jest potęgą liczby pierwszej. □

Wniosek 15.30. *Nie istnieją ciała mocy 6, ponieważ 6 nie jest potęgą liczby pierwszej.*

Dowody dwóch kolejnych twierdzeń pomijamy.

Twierdzenie 15.31. *Dla każdej liczby pierwszej p i każdego $n > 0$ istnieje ciało F, takie że:*

$$|F| = p^n.$$

Twierdzenie 15.32. *Jeśli F_1, F_2 to ciała skończone oraz $|F_1| = |F_2|$, to wtedy*

$$F_1 \cong F_2.$$

Wniosek 15.33. *Widzimy, że dla każdej liczby pierwszej p i każdego $n > 0$ istnieje **jedyne** (z dokładnością do izomorfizmu) ciało F, takie że $|F| = p^n$. Ciało to oznaczane jest przez $\mathbb{F}_{p^n}$.*

KONIEC WYKŁADU