

TEMAT: *Metody dowodzenia twierdzeń. Działania i wybrane struktury algebraiczne*

1.1 Notacja

Parą uporządkowaną (a, b) nazywamy zbiór $\{\{a\}, \{a, b\}\}$ podzbiorów zbioru $\{a, b\}$. Dwie pary $(a, b), (c, d)$ są równe wtedy i tylko wtedy, gdy $a = c \wedge b = d$. Iloczynem kartezjańskim zbiorów A i B nazywamy zbiór

$$A \times B := \{(a, b) : a \in A \wedge b \in B\}.$$

Przykład 1.1.1. Wyznacz $A \times B, B \times A, B^2$.

i) $A = \{3, 4, 5\}, B = \{5, 7\}$

$$A \times B = \{(3, 5), (3, 7), (4, 5), (4, 7), (5, 5), (5, 7)\}$$

$$B \times A = \{(5, 3), (5, 4), (5, 5), (7, 3), (7, 4), (7, 5)\} \quad A \times B \neq B \times A$$

$$B^2 = \{(5, 5), (5, 7), (7, 5), (7, 7)\}$$

ii) przedziały $A = (0, 1) \subset \mathbb{R}, B = (1, 2) \subset \mathbb{R}$

$$A \times B = \{(x, y) : 0 < x < 1 \wedge 1 < y < 2\}$$

$$B \times A = \{(x, y) : 1 < x < 2 \wedge 0 < y < 1\}$$

iii) $A = B = \mathbb{R}$

$$A \times B = B \times A = A^2 = B^2$$

Oznaczamy $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) : x, y \in \mathbb{R}\}$ - płaszczyzna rzeczywista

Przyjmujemy następującą notację.

$\mathbb{N} = \{1, 2, 3, \dots\}$ zbiór liczb naturalnych

$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$

\mathbb{Z} zbiór liczb całkowitych

\mathbb{Q} zbiór liczb wymiernych

\mathbb{R} zbiór liczb rzeczywistych

Oznaczenia kwantyfikatorów

\forall kwantyfikator ogólny (duży) *dla każdego*

\exists kwantyfikator szczegółowy (mały) *istnieje*

$\exists!$ *istnieje dokładnie jeden*

Symbol sumy i iloczynu

Niech $n \in \mathbb{N}$ oraz niech $a_1, a_2, \dots, a_m, a_{m+1}, \dots, a_n$ to dowolny ciąg liczb.

Sumę $a_1 + a_2 + \dots + a_n$ oznaczamy symbolem $\sum_{i=1}^n a_i$. Symbol i to wskaźnik sumowania lub indeks sumowania, m to dolna granica sumowania, zaś n to górna granica sumowania.

Zauważmy że dla dowolnego $m \in \mathbb{N}$, $m < n$ oraz $c \in \mathbb{R}$ zachodzą równości $a_1 + a_2 + \dots + a_n = (a_1 + a_2 + \dots + a_m) + (a_{m+1} + a_{m+2} + \dots + a_n)$ oraz $c(a_1 + a_2 + \dots + a_n) = ca_1 + ca_2 + \dots + ca_n$, czyli

$$\sum_{i=1}^n a_i = \sum_{i=1}^m a_i + \sum_{i=m+1}^n a_i, \quad c \sum_{i=1}^n a_i = \sum_{i=1}^n ca_i.$$

Przykład 1.1.2. $\sum_{i=1}^6 i = 1 + 2 + 3 + 4 + 5 + 6 = 21$

$$\sum_{i=5}^9 \frac{i}{i+2} = \frac{5}{7} + \frac{6}{8} + \frac{7}{9} + \frac{8}{10} + \frac{9}{11}$$

$$\sum_{i=0}^n \left(\frac{1}{2}\right)^i = 1 + \frac{1}{2} + \frac{1}{4} + \dots + \left(\frac{1}{2}\right)^n = \frac{1 - \left(\frac{1}{2}\right)^{n+1}}{1 - \frac{1}{2}}$$

Iloczyn $a_1 \cdot a_2 \cdot \dots \cdot a_{n-1} \cdot a_n$ oznaczamy symbolem $\prod_{i=1}^n a_i$. Symbol i to wskaźnik iloczynu, m to dolny wskaźnik iloczynu, zaś n to górny wskaźnik iloczynu.

Przykład 1.1.3. $\prod_{i=0}^6 (9 - j) = 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3$

$$\prod_{i=1}^n i = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (-1) \cdot n = n!$$

$$\underbrace{x \cdot x \cdot \dots \cdot x}_{n \text{ razy}} = \prod_{i=1}^n x$$

1.2 Metody dowodzenia twierdzeń

Twierdzenie $\left| \begin{array}{l} \text{założenia} \Rightarrow \text{teza} \\ p \Rightarrow q, \text{ gdzie } p, q \text{ są zdaniami} \end{array} \right.$

Dowód to wykazanie prawdziwości implikacji $p \Rightarrow q$.

Dowód wprost

Przeprowadzając dowód wprost, dowodzimy prawdziwości tezy bezpośrednio poprzez dedukcję z założeń twierdzenia.

Przykład 1.2.1. Udowodnimy, że dla dowolnego $n \in \mathbb{N}$ liczba $n^5 - 5n^3 + 4n$ jest podzielna przez 5. Przekształcamy wyrażenie.

$$n^5 - 5n^3 + 4n = n(n^4 - 5n^2 + 4) = n(n^2 - 1)(n^2 - 4) = (n - 2)(n - 1)n(n + 1)(n + 2)$$

Otrzymaliśmy iloczyn pięciu kolejnych liczb naturalnych. Zatem jedna z nich jest podzielna przez 5. Stąd iloczyn jest podzielny przez 5.

Dowód nie wprost (łac. reductio ad absurdum – sprowadzenie do sprzeczności, łac. contradictio in contrarium – zaprzeczenie przeciwieństwa)

Przeprowadzając dowód nie wprost, z założenia o nieprawdziwości tezy wyprowadzamy sprzeczność z przyjętymi założeniami.

Przykład 1.2.2. Niech $a \in \mathbb{Z}$. Jeśli a^2 jest liczbą parzystą, to wówczas a również jest liczbą parzystą.

Przypuśćmy, że a jest liczbą nieparzystą. Wówczas istnieje $k \in \mathbb{Z}$ takie, że $a = 2k + 1$. Stąd $a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Zatem a^2 jest liczbą nieparzystą, co przeczy założeniu twierdzenia. To oznacza, że nasze początkowe przypuszczenie jest fałszywe i a jest liczbą parzystą.

Przykład 1.2.3. Udowodnimy, że $\sqrt{2}$ jest liczbą niewymierną.

Przypuśćmy, że $\sqrt{2}$ jest liczbą wymierną.

Wówczas istnieją $a, b \in \mathbb{Z}$, $b \neq 0$ względnie pierwsze i takie, że $\sqrt{2} = \frac{a}{b}$.

Stąd wynika, że $2 = \frac{a^2}{b^2}$ lub równoważnie $2b^2 = a^2$.

Zatem a^2 jest liczbą parzystą. Stąd wynika, że również a jest liczbą parzystą, czyli istnieje $k \in \mathbb{Z}$ takie, że $a = 2k$.

Stąd $2b^2 = 4k^2$ oraz $b^2 = 2k^2$. Zatem b^2 jest liczbą parzystą, a więc również b jest liczbą parzystą.

Ułamek $\frac{a}{b}$ nie jest nieskracalny.

Otrzymaliśmy sprzeczność. Zatem $\sqrt{2}$ jest liczbą niewymierną.

Dowód indukcyjny

Dowód indukcyjny jest to dowód w którym wykorzystujemy **zasadę indukcji matematycznej**.

Twierdzenie 1.2.4 (Zasada indukcji matematycznej). Niech $\Phi(n)$ będzie zdaniem logicznym dla $n \in \mathbb{N}_0$ oraz niech $n_0 \in \mathbb{N}_0$. Jeśli zachodzą warunki

$$\text{i) } \Phi(n_0), \quad (\Phi(n_0) \text{ jest prawdziwe})$$

$$\text{ii) } \forall n \in \mathbb{N}_0, n \geq n_0 \quad \Phi(n) \Rightarrow \Phi(n + 1), \quad (\text{prawdziwa jest implikacja})$$

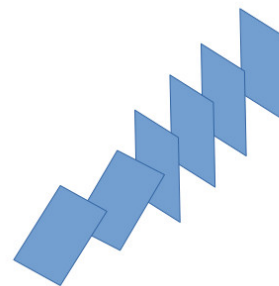
to wówczas $\forall n \in \mathbb{N}_0, n \geq n_0 \quad \Phi(n)$. $(\forall n \in \mathbb{N}_0$ zdanie $\Phi(n)$ jest prawdziwe)

Jeśli jakieś twierdzenie, w którym mowa o liczbach naturalnych, jest prawdziwe dla określonej liczby naturalnej n_0 oraz jeżeli dla każdej liczby naturalnej n z założenia, że twierdzenie jest prawdziwe dla n wynika, że jest ono prawdziwe dla liczby następnej $n + 1$, to twierdzenie jest prawdziwe dla każdej liczby naturalnej nie mniejszej niż n_0 .

Kostki domina

Czy wszystkie kostki się przewrócą?

Jeśli przewrócono pierwszą kostkę oraz kostki są ustawione tak, że upadek którejkolwiek z nich przewraca następną, to wszystkie kostki się przewrócą.



Przykład 1.2.5. Sprawdźmy poniższe równości.

$$\begin{aligned}1^3 &= \frac{1}{4} \cdot 1^2 \cdot 2^2 \\1^3 + 2^3 &= \frac{1}{4} \cdot 2^2 \cdot 3^2 \\1^3 + 2^3 + 3^3 &= \frac{1}{4} \cdot 3^2 \cdot 4^2 \\1^3 + 2^3 + 3^3 + 4^3 &= \frac{1}{4} \cdot 4^2 \cdot 5^2\end{aligned}$$

Udowodnimy, że dla dowolnej liczby naturalnej $n \in \mathbb{N}$ prawdziwa jest równość

$$\sum_{i=1}^n i^3 = 1^3 + 2^3 + 3^3 + \dots + n^3 = \frac{1}{4}n^2(n+1)^2.$$

I. Warunek początkowy

Sprawdziliśmy już, że dla $n_0 = 1$ wzór jest prawdziwy.

II. Krok indukcyjny (prawo przekazywania)

Niech n oznacza liczbę naturalną. Chcemy uzasadnić, że jeśli wzór jest prawdziwy dla n , to jest on prawdziwy dla $n+1$. Innymi słowy chcemy uzasadnić, że z założenia (tzw. założenie indukcyjne)

$$\sum_{i=1}^n i^3 = 1^3 + 2^3 + 3^3 + \dots + n^3 = \frac{1}{4}n^2(n+1)^2$$

wynika teza

$$\sum_{i=1}^{n+1} i^3 = 1^3 + 2^3 + 3^3 + \dots + n^3 + (n+1)^3 = \frac{1}{4}(n+1)^2(n+2)^2.$$

Dowód przedstawiamy poniżej.

$$\begin{aligned}L &= \sum_{i=1}^{n+1} i^3 = (n+1)^3 + \sum_{i=1}^n i^3 \stackrel{z.ind.}{=} (n+1)^3 + \frac{1}{4}n^2(n+1)^2 = \\&= (n+1)^2 \left(n+1 + \frac{1}{4}n^2 \right) = \frac{1}{4}(n+1)^2(4n+4+n^2) = \frac{1}{4}(n+1)^2(n+2)^2 = P\end{aligned}$$

Zatem $L = P$, implikacja jest prawdziwa.

III. Wniosek

Na mocy zasady indukcji matematycznej wzór jest prawdziwy dla każdej liczby naturalnej,

tj. $\forall n \in \mathbb{N} \quad \sum_{i=1}^n i^3 = \frac{1}{4}n^2(n+1)^2.$

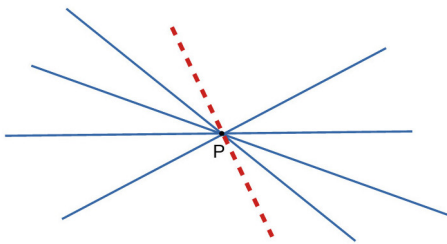
Przykład 1.2.6. Udowodnimy, że n różnych prostych na płaszczyźnie, przechodzących przez ustalony punkt P , dzieli płaszczyznę na $2n$ części.

I. Warunek początkowy, dla $n_0 = 1$

Jedna prosta dzieli płaszczyznę na $2n_0 = 2$ części.

II. Krok indukcyjny

Niech $n \in \mathbb{N}$. Załóżmy, że n prostych przechodzących przez ustalony punkt P , dzieli płaszczyznę na $2n$ części. Chcemy uzasadnić, że wówczas $n + 1$ prostych dzieli płaszczyznę na $2(n + 1) = 2n + 2$ części.



Poprowadźmy dodatkową prostą. W miejsce dwóch obszarów powstają cztery. A zatem mamy $2n + 2$ obszary.

III. Wniosek: Na mocy zasady indukcji matematycznej twierdzenie jest prawdziwe dla dowolnej liczby prostych.

Przykład błędnego rozumowania indukcyjnego można znaleźć tutaj.

1.3 Działania wewnętrzne i ich własności

Niech A będzie zbiorem niepustym.

Definicja 1.3.1. Dowolną funkcję $h : A \times A \rightarrow A$ nazywamy *działaniem wewnętrznym* w zbiorze A . Wartość funkcji $h(a, b) \in A$ nazywamy *wynikiem* działania dla pary argumentów $a, b \in A$.

Przykład 1.3.2. i) Dodawanie jest działaniem wewnętrznym w \mathbb{N} .

ii) Odejmowanie nie jest działaniem wewnętrznym w \mathbb{N} .

iii) Dodawanie nie jest działaniem wewnętrznym w $\mathbb{R} \setminus \mathbb{Q}$.

Własności działań wewnętrznych

Definicja 1.3.3. Niech $*$: $A \times A \rightarrow A$ będzie działaniem wewnętrznym.

i) Działanie $*$ nazywamy *przemienne*, jeśli $\forall a, b \in A \quad a * b = b * a$.

ii) Działanie $*$ nazywamy *łącznym*, jeśli $\forall a, b, c \in A \quad (a * b) * c = a * (b * c)$.

- iii) Element $e \in A$ nazywamy *elementem neutralnym* działania $*$, jeśli $\forall a \in A \quad a * e = e * a = a$.

Przykład 1.3.4. i) Dodawanie jest działaniem wewnętrznym łącznym i przemianym w \mathbb{R} . 0 jest elementem neutralnym.
ii) Mnożenie jest działaniem wewnętrznym łącznym i przemianym w $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. 1 jest elementem neutralnym.

Twierdzenie 1.3.5. Jeżeli element neutralny istnieje to jest jedyny.

Dowód. Przypuśćmy, że istnieją $e_1, e_2 \in A$ będące elementami neutralnymi w A . Wówczas $e_2 = e_1 * e_2 = e_1$. \square

Przykład 1.3.6. Niech X to dowolny zbiór.

- i) Zbiór pusty \emptyset jest elementem neutralnym w $(P(X), \cup)$.
ii) Zbiór X jest elementem neutralnym w $(P(X), \cap)$.

Definicja 1.3.7. Niech $*$: $A \times A \rightarrow A$ będzie działaniem wewnętrznym, posiadającym element neutralny $e \in A$. Dla dowolnego $a \in A$ każdy element $a' \in A$ taki, że $a * a' = a' * a = e$, nazywamy *elementem symetrycznym* do a względem działania $*$.

- Przykład 1.3.8.** i) W $(\mathbb{R}, +)$ elementem symetrycznym do 5 jest -5 (tzw. element przeciwny).
ii) W (\mathbb{R}^*, \cdot) elementem symetrycznym do 5 jest $\frac{1}{5}$ (tzw. element odwrotny).
iii) W (\mathbb{R}, \circ) , gdzie $x \circ y = x + y + 1$, elementem neutralnym jest -1 , zaś elementem symetrycznym do x jest $-2 - x$.

Twierdzenie 1.3.9. Jeżeli działanie wewnętrzne jest łączne oraz posiada element neutralny, to każdy element posiada co najwyżej jeden element symetryczny.

1.4 Podstawowe struktury algebraiczne

Niech G będzie zbiorem niepustym, zaś $*$: $G \times G \rightarrow G$ działaniem wewnętrznym w G .

- Definicja 1.4.1.** i) Parę $(G, *)$ nazywamy *półgrupą*, jeżeli działanie jest łączne.
ii) Parę $(G, *)$ nazywamy *grupą*, jeżeli działanie jest łączne, posiada element neutralny oraz każdy element G posiada element symetryczny względem $*$ w G .

Jeśli dodatkowo działanie $*$ jest przemienne, to mówimy o *półgrupie przemiennej*, *grupie przemiennej* (*abelowej*).

Przykład 1.4.2. Oznaczmy $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

	$(\mathbb{N}, +)$	(\mathbb{Z}, \cdot)	$(\mathbb{Q}, +)$	(\mathbb{Q}, \cdot)	$(\mathbb{R}^*, +)$	(\mathbb{R}^*, \cdot)
wewnętrzność	✓	✓	✓	✓	nie $-1 + 1 = 0$ $0 \notin \mathbb{R}^*$	✓
łączność	✓	✓	✓	✓		✓
przemienność	✓	✓	✓	✓		✓
el. neutralny	brak $0 \notin \mathbb{N}$	✓ $1 \in \mathbb{Z}$	✓ $0 \in \mathbb{Z}$	✓ $1 \in \mathbb{Z}$		✓ $1 \in \mathbb{R}^*$
el. symetryczny		brak $2 \cdot b = 1$ $b = \frac{1}{2} \notin \mathbb{Z}$	✓ $a + a' = 0$ $a' = -a \in \mathbb{Q}$	brak $a \cdot a' = 1$ $a' = \frac{1}{a}$ nie dla $a = 0$		✓ $a \cdot a' = 1$ $a' = \frac{1}{a}$ $\forall a \in \mathbb{R}^*$
	półgrupa przemienna bez el. neutr.	półrupa przemienna z el. neutr.	grupa abelowa	półrupa przemienna z el. neutr.		grupa abelowa

Przykład 1.4.3. Niech $X = \{1, 2, 4, \dots, 2^n, \dots\}$, $n \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$, zaś działanie \circ to mnożenie liczb. Czy (X, \circ) jest półgrupą/grupą (abelową)?

Jeśli $a, b, c \in X$, to istnieją $k, m, n \in \mathbb{N}_0$ takie, że $a = 2^n, b = 2^m, c = 2^k$.

wewnętrzne $a \circ b = 2^n \cdot 2^m = 2^{n+m} \in X$

przemienne $a \circ b = 2^n \cdot 2^m = 2^{n+m} = 2^{m+n} = 2^m \cdot 2^n = b \circ a$

łączne $(a \circ b) \circ c = 2^{n+m} \cdot 2^k = 2^{n+m+k} = 2^n \cdot 2^{m+k} = a \circ (b \circ c)$

el. neutralny $e = 2^s, s \in \mathbb{N}_0$ $a \circ e = a \Leftrightarrow 2^{n+s} = 2^n \Rightarrow s = 0, e = 1 \in X$

brak el. odwrotnego $a \circ b = 1 \Leftrightarrow 2^{n+m} = 2^0 \Leftrightarrow m = -n \Rightarrow m = -n \notin \mathbb{N}_0$

Wniosek: półgrupa przemienna z elementem neutralnym

Definicja 1.4.4. Zespól $(A, \circ, *)$ złożony z niepustego zbioru A i określonych w nim działań wewnętrznych $\circ : A \times A \rightarrow A$, $* : A \times A \rightarrow A$ nazywamy *pierścieniem*, jeśli (A, \circ) jest grupą abelową, zaś działanie $*$ jest łączne oraz rozdzielne względem działania \circ , tzn.

$$\forall a, b, c \in A \quad (a \circ b) * c = (a * c) \circ (b * c) \wedge c * (a \circ b) = (c * a) \circ (c * b).$$

Pierścień, w którym działanie $*$ posiada element neutralny, nazywamy *pierścieniem z jedyneką* lub *z jednością*. Pierścień, w którym działanie $*$ jest przemienne, nazywamy *pierścieniem przemiennym* lub *komutatywnym*.

Notacja addytywna		Notacja multiplikatywna	
$\circ / +$	dodawanie	$* / \cdot$	mnożenie
$a + b$	suma	$a \cdot b$	iloczyn
$e = 0$	zero	$e = 1$	jedyńska
$a' = -a$	element przeciwny	$a' = a^{-1}$	element odwrotny

$$\begin{array}{ll}
 na = \underbrace{a + \dots + a}_n, & n \in \mathbb{N} \\
 0 \cdot a = 0 \\
 m \in \mathbb{Z}, m < 0 & ma = \underbrace{(-a) + \dots + (-a)}_m \\
 \\
 a^n = \underbrace{a \cdot \dots \cdot a}_n \\
 a^0 = e = e = 1 \\
 a^m = \underbrace{a^{-1} \cdot \dots \cdot a^{-1}}_n
 \end{array}$$

Definicja 1.4.5. Zespól $(K, \circ, *)$ złożony ze zbioru K zawierającego co najmniej dwa elementy i określonych w nim działań wewnętrznych $\circ : K \times K \rightarrow K$, $* : K \times K \rightarrow K$ nazywamy *ciałem*, jeśli

- (K, \circ) jest grupą abelową (z elementem neutralnym e_\circ),
- $(K \setminus \{e_\circ\}, *)$ jest grupą abelową,
- działanie $*$ jest rozdzielne względem działania \circ .

Zatem ciało to pierścień przemienny z jedyneką (różną od zera, tj. $1 = e_* \neq e_\circ = 0$), w którym wszystkie niezerowe (tj. różne od elementu neutralnego e_\circ) elementy są odwracalne.

Zatem w ciele można zdefiniować operację *dzielenia* w sposób następujący:

$$\frac{a}{b} := a * b^{-1}, \quad a, b \in K, b \neq 0.$$

Przykład 1.4.6. i) $(\mathbb{R}, +, \cdot)$ ciało liczb rzeczywistych

$(\mathbb{R}, +)$ grupa addytywna ciała

(\mathbb{R}^*, \cdot) grupa multiplikatywna ciała

ii) $(\mathbb{Q}, +, \cdot)$ ciało liczb wymiernych

iii) $(\mathbb{Z}, +, \cdot)$ pierścień przemienny z jedyneką, ale nie ciało (bowiem np. $2^{-1} \notin \mathbb{Z}$)

iv) $(\mathbb{Z}/p\mathbb{Z}, +_p, \cdot_p)$, gdzie $p \in \mathbb{N}$, $p \geq 2$
 $+_p, \cdot_p$ dodawanie i mnożenie modulo p

Jeśli p to liczba pierwsza, to $\mathbb{Z}/p\mathbb{Z}$ jest ciałem (tzw. ciało reszt modulo p). Jeśli p nie jest liczbą pierwszą, to $\mathbb{Z}/p\mathbb{Z}$ jest pierścieniem, ale nie ciałem.

$\mathbb{Z}/5\mathbb{Z}$ to ciało	$+_5$ 0 1 2 3 4 0 0 1 2 3 4 1 1 2 3 4 0 2 2 3 4 0 1 3 3 4 0 1 2 4 4 0 1 2 3	\cdot_5 0 1 2 3 4 0 0 0 0 0 0 1 0 1 2 3 4 2 0 2 4 1 3 3 0 3 1 4 2 4 0 4 3 2 1
$\mathbb{Z}/4\mathbb{Z}$ nie jest ciałem	$+_4$ 0 1 2 3 0 0 1 2 3 1 1 2 3 0 2 2 3 0 1 3 3 0 1 2	\cdot_4 0 1 2 3 0 0 0 0 0 1 0 1 2 3 2 0 2 0 2 3 0 3 2 1

Przykład 1.4.7. Zbiór \mathbb{R}^2 wraz z działaniami dodawania i mnożenia zdefiniowanymi poniżej ma strukturę ciała.

$$\forall (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2 \quad (x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2), \quad (x_1, y_1) \cdot (x_2, y_2) := (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1).$$

Definicja 1.4.8. Zdefiniowane powyżej ciało nazywamy *ciałem liczb zespolonych* i oznaczamy symbolem \mathbb{C} . Elementy tego ciała nazywamy *liczbami zespolonymi*.