# Geometria z algebrą liniową I

Arkadiusz Męcel

**WYKŁAD 2, 12.10.2021 r.**

## Rola współczynników w układach równań liniowych

Do tej pory współczynnikami równania liniowego $U$ postaci

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$$

były liczby rzeczywiste, czyli $a_1, a_2, \ldots, a_n, b \in \mathbb{R}$.

Ciąg $(s_1, \ldots, s_n)$ jest rozwiązaniem $U$, gdy wykonanie **działań** dodawania i mnożenia w $\mathbb{R}$ postaci:

$$a_1 \cdot s_1 + a_2 \cdot s_2 + \ldots + a_n \cdot s_n$$

daje wynik równy $b$.

Czy zamiast $\mathbb{R}$ z operacjami $+$ oraz $\cdot$ można rozważać równania liniowe, gdzie współczynnikami są **zbiory** z **innymi działaniami** dodawania i mnożenia $\boxplus, \boxtimes$?

## Definicja 1.

Niech $X$ będzie zbiorem. Przez $X^2$ rozumieć będziemy zbiór ciągów postaci $(x_1, x_2)$, gdzie $x_1, x_2 \in X$. **Działaniem dwuargumentowym na zbiorze $X$** nazywamy każdą funkcję $\omega : X^2 \to X$.

Przykłady:

| zbiór $X$ | działanie $\omega$ |
|---|---|
| liczby rzeczywiste/wymierne/całkowite/naturalne | dodawanie/mnożenie |
| liczby rzeczywiste | $a \boxplus b = a + b + ab$ |
| zbiór podzbiorów danego zbioru | suma/częśc wspólna |
| zbiór funkcji ze zbioru $X$ na zbiór $X$ | złożenie |

Działaniem dwuargumentowym na zbiorze $\mathbb{N}$ nie jest odejmowanie, bo $1 - 3 \notin \mathbb{N}$.

## Definicja 2.

Mówimy, że działanie $* : X^2 \to X$ na zbiorze $X$ jest:

- **łączne**, jeśli dla każdych $a, b, c \in X$ mamy
$$(a * b) * c = a * (b * c),$$
- **przemienne**, jeśli dla każdych $a, b \in X$ mamy
$$a * b = b * a.$$

Przykłady:

- działanie $a \boxplus b = a^2 + b^2$ na zbiorze $\mathbb{R}$ nie jest łączne, bo: $(1 \boxplus 2) \boxplus 3 = 34$, zaś $1 \boxplus (2 \boxplus 3) = 170$.
- działanie $a \boxplus b = a + b + ab$ na zbiorze $\mathbb{R}$ jest łączne i przemienne,
- działanie $a \boxtimes b = a^b$ na zbiorze $\mathbb{R}_+$ nie jest przemienne,
- złożenie w zbiorze bijekcji (czyli 1-1 i „na”) zbioru $\mathbb{R}$ nie jest przemienne.

## Definicja 3.

**Ciałem** nazywamy piątkę $(K, \boxplus, \boxtimes, 0, 1)$, gdzie $K$ jest zbiorem przynajmniej dwuelementowym z wyróżnionymi elementami $0 \neq 1$, zwanymi zerem i jedynką, zaś $\boxplus$, $\boxtimes$ są dwuargumentowymi działaniami zwanymi dodawaniem i mnożeniem, spełniającymi następujące **aksjomaty ciała**:

| | | | |
|---|---|---|---|
| 1) | $(a \boxplus b) \boxplus c = a \boxplus (b \boxplus c)$ | $\forall_{a,b,c \in K}$ | łączność dodawania |
| 2) | $a \boxplus b = b \boxplus a$ | $\forall_{a,b \in K}$ | przemienność dodawania |
| 3) | $a \boxplus 0 = a = 0 \boxplus a$ | $\forall_{a \in K}$ | własność elementu 0 |
| 4) | $a \boxplus b = 0 = b \boxplus a$ | $\forall_{a \in K} \exists_{b \in K}$ | element przeciwny |
| 5) | $(a \boxtimes b) \boxtimes c = a \boxtimes (b \boxtimes c)$ | $\forall_{a,b,c \in K}$ | łączność mnożenia |
| 6) | $a \boxtimes b = b \boxtimes a$ | $\forall_{a,b \in K}$ | przemienność mnożenia |
| 7) | $a \boxtimes 1 = 1 \boxtimes a = a$ | $\forall_{a \in K}$ | własność elementu 1 |
| 8) | $a \boxtimes b = b \boxtimes a = 1$ | $\forall_{a \in K \setminus \{0\}} \exists_{b \in K}$ | odwrotność dla $a \neq 0$ |
| 9) | $a \boxtimes (b \boxplus c) = (a \boxtimes b) \boxplus (a \boxtimes c)$ | $\forall_{a,b,c \in K}$ | rozdzielność $\boxtimes$ wzgl. $\boxplus$ |

## Elementy: przeciwny i odwrotny.

**Fakt 1.**

Niech $K$ będzie ciałem.

- Dla każdego elementu $a \in K$ istnieje dokładnie jeden element przeciwny do $a$.
- Dla każdego niezerowego elementu $b \in K$ istnieje dokładnie jeden element odwrotny do $b$.

**Dowód** (istnienia dokładnie jednego elementu przeciwnego). Załóżmy przeciwnie, że dla pewnych elementów $x, x'$ ciała $K$ mamy $a \boxplus x = 0 = a \boxplus x'$. Mamy:

$$\begin{aligned}
x &= x \boxplus 0 && \text{(aksjomat 3 - wł. elementu 0)}\\
&= x \boxplus (a \boxplus x') && \text{(równość wyżej)}\\
&= (x \boxplus a) \boxplus x' && \text{(aksjomat 1 - łączność } \boxplus\text{)}\\
&= x' \boxplus (a \boxplus x) && \text{(aksjomat 2 - przemienność } \boxplus\text{)}\\
&= x' \boxplus 0 && \text{(równość wyżej)}\\
&= x'. && \text{(aksjomat 3 - wł. elementu 0)}
\end{aligned}$$

## Umowy odnośnie notacji

Niech $K$ będzie ciałem. W dalszym ciągu, o ile nie prowadzi to do nieporozumień, wprowadzamy następujące umowy:

- dodawanie w ciele $K$ oznaczamy jako $+$,
- mnożenie w ciele $K$ oznaczamy jako $\cdot$,
- znak mnożenia może być pomijany,
- element przeciwny do elementu $a$ oznaczamy jako $-a$,
- element odwrotny do elementu $a \neq 0$ oznaczamy jako $a^{-1}$ lub $\frac{1}{a}$,
- zamiast pisać $a + (-b)$ piszemy $a - b$, a zamiast $ab^{-1}$ piszemy $\frac{a}{b}$,
- dla liczby całkowitej dodatniej $n$ oraz $a \in K$ przyjmujemy $a^n = \underbrace{a \cdot a \cdot a \cdot \ldots \cdot a}_{n}$.

### Twierdzenie 1.

Niech $K$ będzie ciałem.

- Każdą macierz $A = M_{m \times n}(K)$ można za pomocą operacji elementarnych (1)-(2) na wierszach doprowadzić do postaci schodkowej.
- Każdą macierz $A = M_{m \times n}(K)$ można za pomocą operacji elementarnych (1)-(3) na wierszach doprowadzić do postaci zredukowanej.

Każdy niesprzeczny układ równań liniowych o współczynnikach w $K$ ma rozwiązanie ogólne. Aby je znaleźć wystarczy sprowadzić macierz tego układu do postaci schodkowej zredukowanej elementarnymi operacjami na wierszach, a następnie z otrzymanej macierzy otrzymać rozwiązanie ogólne.

Dowód jest powtórzeniem argumentów dla $K = \mathbb{R}$. Kluczowe aksjomaty:

- łączność (kolejność operacji nie ma znaczenia),
- przemienność (po której stronie zmiennej są współczynniki?),
- element przeciwny (eliminacja),
- element odwrotny (macierz schodkowa $\rightarrow$ macierz zredukowana).

## Gdy operacje nie mają istotnych własności...

- Niech $\Sigma_{a,b}$ będzie zbiorem złożonym ze wszystkich słów złożonych z liter $a$, $b$, np. $a$, $aaa$, $abaa$, $bbba$ oraz słowa pustego $\epsilon$,
- Rozważamy zbiór $P(\Sigma_{a,b})$ złożony z podzbiorów (także nieskończonych!) zbioru $\Sigma_{a,b}$, np.
$$\{\epsilon, a, ab\}, \quad \{a, aa, aaa, aaaa, \ldots\}, \quad \{ab, abab, ababab, \ldots\}.$$
- W $P(\Sigma_{a,b})$ wprowadzamy działanie $+$ oznaczające sumę mnogościową zbiorów, np.
$$\{aba, bb, ab\} + \{a, aa, bb\} = \{aba, bb, ab, a, aa\}.$$
- W $P(\Sigma_{a,b})$ wprowadzamy działanie $\cdot$ zdefiniowane w następujący sposób. Zbiór $A \cdot B$ złożony jest ze słów postaci $a \cdot b$, gdzie $a \in A$, $b \in B$. Np.
$$\{aba, bb, ab\} \cdot \{a, aa, bb\} = \{abaa, abaaa, ababb, bba, bbaa, bbbb, aba, abbb\}.$$

## Gdy operacje nie mają istotnych własności...

- Rozważamy równania liniowe o współczynnikach w $P(\Sigma_{a,b})$, np:

$$\{a, aa\} \cdot x_1 + \{bb\} \cdot x_2 = \{ab, aab, bbb, aaab\},$$

  którego **rozwiązaniem są elementy $\boldsymbol{P(\Sigma_{a,b})}$**, czyli: $x_1 = \{b, ab\}$, $x_2 = \{b\}$.

- **Problem 1.** Strona, z której piszemy współczynniki. Równania:

$$\{a\} \cdot x_1 = \{abaa\}, \quad x_1 \cdot \{a\} = \{abaa\}$$

  mają różne rozwiązania! Przyczyna – nieprzemienność działania $\cdot$.

- **Problem 2.** Brak elementów *przeciwnych* i *odwrotnych*. Mając układ:

$$\begin{cases} \{a\} \cdot x_1 = \{abaa\} \\ \{a\} \cdot x_1 = \{aba\}. \end{cases}$$

  nie sprowadzimy jego *macierzy* do postaci schodkowej lub zredukowanej!

- **Problem 3.** Układy jednorodne nie mają sensu. Trudno opisać rozwiązania.

## Twierdzenie 2.

Niech $n > 1$ będzie liczbą całkowitą. Rozważmy zbiór reszt z dzielenia przez $n$:

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

Określamy działania $+_n$, tzw. **dodawanie modulo *n***, oraz $\cdot_n$, tzw. **mnożenie modulo *n***, w zbiorze $\mathbb{Z}_n$:

- $a +_n b$ to reszta z dzielenia przez $n$ liczby całkowitej $a + b$,
- $a \cdot_n b$ to reszta z dzielenia przez $n$ liczby całkowitej $a \cdot b$.

Wówczas $(\mathbb{Z}_n, +_n, \cdot_n, 0, 1)$ jest ciałem $\iff$ $p$ jest liczbą pierwszą.

Przykłady ilustrujące powyżej zdefiniowane działania:

- $1 +_3 2 = 0$ w ciele $\mathbb{Z}_3$, więc 1 i 2 są elementami wzajemnie przeciwnymi w $\mathbb{Z}_3$,
- $3 \cdot_{23} 8 = 1$ w ciele $\mathbb{Z}_{23}$, więc 3 i 8 są elementami wzajemnie odwrotnymi w $\mathbb{Z}_{23}$,
- $2 \cdot_4 2 = 0$ w zbiorze $\mathbb{Z}_4$.

## Tabelki działań w ciałach $\mathbb{Z}_2$ i $\mathbb{Z}_3$

- ciało dwuelementowe $\mathbb{Z}_2$:

| $+_2$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| $\cdot_2$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

- ciało trzyelementowe $\mathbb{Z}_3$:

| $+_3$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

| $\cdot_3$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

## Ciało czteroelementowe? Istnieje, ale to nie $\mathbb{Z}_4$!

| $+_4$ | 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 |

**Twierdzenie**

Niech $K$ będzie ciałem i niech $a, b \in K$. Wówczas jeśli $ab = 0$, to $a = 0$ lub $b = 0$,

**Dowód.** Niech $x, y \in K$.

(i) Jeśli $x + y = x$, to $-x + (x + y) = (-x + x) + y = 0 + y = y = -x + x = 0$.

(ii) Mamy $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$. Zatem na mocy (i) mamy $0 \cdot x = 0$.

(iii) Jeśli $a \neq 0$, to na mocy (ii) mamy $0 = a^{-1} \cdot 0 = a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b = b$.

## Dlaczego $\mathbb{Z}_p$ są ciałami, gdy $p$ jest liczbą pierwszą?

Spełnianie wszystkich aksjomatów poza (8) jest rutynowym ćwiczeniem, korzystającym z dwóch faktów:

- aksjomaty ciała (1)-(7) oraz (9) są spełnione przez zbiór liczb całkowitych ze standardowymi działaniami $+$ oraz $\cdot$ oraz elementami neutralnymi 0, 1,
- jeśli przez $[x]_n$ oznaczymy resztę z dzielenia przez $n$ liczby całkowitej $x$, to dla dowolnych całkowitych $a, b$ mamy:

$$[a]_n \ +_n \ [b]_n = [a+b]_n, \qquad\qquad [a]_n \ \cdot_n \ [b]_n = [ab]_n.$$

Istnienie elementu odwrotnego do każdego elementu niezerowego w $\mathbb{Z}_n$ zagwarantowane jest jedynie, gdy $n = p$. Skorzystamy z następującego faktu.

**Lemat Bezout**

Dla niezerowej liczby całkowitej $a$ oraz dowolnej liczby całkowitej $b$ istnieją takie liczby całkowite $x, y$, że:

$$ax + by = NWD(a, b).$$

Dowodzimy, że każdy niezerowy element w $\mathbb{Z}_n$ ma odwrotność wtedy i tylko wtedy, gdy $n$ jest liczbą pierwszą.

- Jeśli $n = p$ jest liczbą pierwszą oraz $0 \neq a \in \mathbb{Z}_n$, to
$$NWD(a, p) = 1.$$
- Z Lematu Bezout istnieją liczby całkowite $x, y$, że
$$ax + py = 1.$$
Zatem $ax$ daje resztę 1 z dzielenia przez $p$. W szczególności $a^{-1} = [x]_p$ w $\mathbb{Z}_p$.
- Z drugiej strony, jeśli $n = rs$, gdzie $r, s > 1$, to nie istnieje takie $k$, że $r \cdot_n k = 1$.
- To by bowiem oznaczało, że
$$rk = qn + 1,$$
dla pewnego $q \in \mathbb{Z}$. To z kolei implikuje
$$rk - qrs = 1.$$
Jednak $r > 1$, co daje sprzeczność.

## Dowód Lematu Bezout

- Uznamy, że znane są dwa fakty:
  1. twierdzenie o dzieleniu z resztą,
  2. twierdzenie o istnieniu NWD pary liczb całkowitych.
- Ograniczymy się do przypadku, gdy $a, b$ są dodatnie (resztę łatwo uzupełnić). Rozważmy zbiór $L$ wszystkich **dodatnich** liczb postaci
$$ax + by, \quad x, y \in \mathbb{Z}.$$
- Skoro $a, b$ są dodatnie, to zbiór ten jest niepusty i **istnieje najmniejszy jego element**, który nazwiemy $d$. Twierdzimy, że $d = NWD(a, b)$.
- Jest jasne, że $NWD(a, b)$ jest dzielnikiem każdej liczby postaci $ax + by$ (bo każdy wspólny dzielnik $a, b$ jest dzielnikiem $ax + by$), więc
$$d \geq NWD(a, b).$$
- Wykażemy dalej, że $d$ to wspólny dzielnik zarówno $a$ jak i $b$.

## Dowód Lematu Bezout cd.

- Załóżmy, wbrew temu co oczekujemy, że $d$ nie jest dzielnikiem $a$. Zatem na mocy twierdzenia o dzieleniu z resztą istnieje liczba $0 < r < d$ oraz $k \geq 1$ taka, że:

$$a = kd + r.$$

- To oznacza, że $r = a - kd$. To jest niemożliwe, bo przecież:

$$r = a - kd = a - k(ax + by) = a(1 - lkx) - kby,$$

jest również (dodatnim, jako reszta!) elementem zbioru $L$, i to mniejszym niż $d$, sprzeczność.

- Stąd $d$ jest dzielnikiem $a$. Analogicznie pokazujemy, że $d$ jest dzielnikiem $b$. A zatem $d$ rzeczywiście jest wspólnym dzielnikiem $a$ oraz $b$, co oznacza, że

$$d \leq NWD(a, b).$$

- W rezultacie, $d = NWD(a, b) = ax + by$, dla pewnych całkowitych $x, y$.

Rozwiążmy układ równań liniowych o współczynnikach w ciele $\mathbb{Z}_3$:

$$\begin{cases} x_1 + x_2 = 2 \\ 2x_1 + x_2 = 1 \end{cases} \qquad \text{o macierzy} \qquad \left[\begin{array}{cc|c} 1 & 1 & 2 \\ 2 & 1 & 1 \end{array}\right] \in M_{3\times 2}(\mathbb{Z}_3).$$

Odejmujemy pierwszy wiersz przemnożony przez 2. Jest to wiersz postaci $2\,2\,|1$. A zatem po tej operacji mamy (to samo, co po dodaniu wierszy):

$$\left[\begin{array}{cc|c} 1 & 1 & 2 \\ 0 & 2 & 0 \end{array}\right].$$

Mnożymy drugi wiersz przez... odwrotność 2, czyli 2 (bo $2 \cdot_3 2 = 1$). A zatem mnożymy drugi wiersz przez 2 i odejmujemy od pierwszego. Dostajemy:

$$\left[\begin{array}{cc|c} 1 & 0 & 2 \\ 0 & 1 & 0 \end{array}\right].$$

A zatem rozwiązaniem tego układu jest para $(x_1, x_2) = (2, 0)$.

**Uwaga.** Układ $m$ równań liniowych o $n$ niewiadomych nad ciałem skończonym ma skończenie wiele rozwiązań! Np. równanie $x_1 + x_2 = 0$ ma pięć rozwiązań w $\mathbb{Z}_5$.

## Definicja 4.

**Ciało liczb zespolonych** to piątka $(\mathbb{R}^2, \oplus, \otimes, (0,0), (1,0))$, oznaczane przez $\mathbb{C}$, którego elementami są wszystkie uporządkowane pary liczb rzeczywistych, i w którym działania $\oplus, \otimes$ określone są za pomocą działań $+$ oraz $\cdot$ w $\mathbb{R}$ wzorami:

$$(a,b) \oplus (c,d) = (a+c, b+d), \quad (a,b) \otimes (c,d) = (ac-bd, ad+bc).$$

Na przykład:

- $(3,0) \oplus (4,0) = (7,0)$,
- $(0,1) \oplus (1,0) = (1,1)$,
- $(0,1) \otimes (0,1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1,0)$,
- $(2,1) \otimes (2,-1) = (2 \cdot 2 - 1 \cdot (-1), 2 \cdot (-1) + 1 \cdot 2) = (5,0)$.

### Definicja 4.

**Ciało liczb zespolonych** to piątka $(\mathbb{R}^2, \oplus, \otimes, (0,0), (1,0))$, oznaczane przez $\mathbb{C}$, którego elementami są wszystkie uporządkowane pary liczb rzeczywistych, i w którym działania $\oplus, \otimes$ określone są za pomocą działań $+$ oraz $\cdot$ w $\mathbb{R}$ wzorami:

$$(a,b) \oplus (c,d) = (a+c, b+d), \quad (a,b) \otimes (c,d) = (ac - bd, ad + bc).$$

Dowód tego, że $\mathbb{C}$ jest ciałem wynika z tego, że $\mathbb{R}$ jest ciałem.
Sprawdzenie poszczególnych aksjomatów jest uciążliwe, ale proste.

Ważne: jeśli $(a,b) \neq (0,0)$, to

$$(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right),$$

bo

$$(a,b) \otimes \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = \left(\frac{a^2+b^2}{a^2+b^2}, \frac{-ab+ab}{a^2+b^2}\right) = (1,0).$$

## Definicja 4.

**Ciało liczb zespolonych** to piątka $(\mathbb{R}^2, \oplus, \otimes, (0,0), (1,0))$, oznaczane przez $\mathbb{C}$, którego elementami są wszystkie uporządkowane pary liczb rzeczywistych, i w którym działania $\oplus, \otimes$ określone są za pomocą działań $+$ oraz $\cdot$ w $\mathbb{R}$ wzorami:

$$(a, b) \oplus (c, d) = (a + c, b + d), \quad (a, b) \otimes (c, d) = (ac - bd, ad + bc).$$

Zbiór liczb $\{(x, 0), x \in \mathbb{R}\}$ można utożsamić z liczbami rzeczywistymi:

$$(a, 0) \oplus (a', 0) = (a + a', 0), \quad (a, 0) \otimes (a', 0) = (aa' - 0, 0 + 0) = (aa', 0).$$

Liczbę postaci $(a, 0)$ będziemy zapisywać jako $a$, dla każdego $a \in \mathbb{R}$,

Liczbę $(0, 1)$ oznaczać będziemy jako $i$.

Używając tych oznaczeń mamy na przykład:

$$\begin{aligned} (a, b) &= (a, 0) \oplus (0, b) = (a, 0) \oplus (b, 0) \otimes (0, 1) = a + bi, \\ i^2 &= (0, 1) \otimes (0, 1) = (-1, 0) = -1. \end{aligned}$$

### Definicja 4.

**Ciało liczb zespolonych** to piątka $(\mathbb{R}^2, \oplus, \otimes, (0,0), (1,0))$, oznaczane przez $\mathbb{C}$, którego elementami są wszystkie uporządkowane pary liczb rzeczywistych, i w którym działania $\oplus, \otimes$ określone są za pomocą działań $+$ oraz $\cdot$ w $\mathbb{R}$ wzorami:

$$(a,b) \oplus (c,d) = (a+c, b+d), \quad (a,b) \otimes (c,d) = (ac-bd, ad+bc).$$

Liczbę $z = (a,b)$ zapisywać możemy w **postaci ogólnej** (algebraicznej)

$$z = a + bi,$$

przyjmując umowę, że

$$a + bi = c + di \quad \Rightarrow \quad a = c \quad \text{oraz} \quad b = d.$$

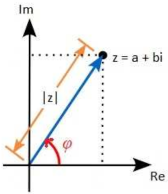
Opuszczamy oznaczenia działań $\oplus, \otimes$ i zastępujemy przez $+, \cdot$. Dodawanie i mnożenie w $\mathbb{C}$ sprowadzają się do wykonywania operacji algebraicznych, np.:

$$(a+bi)(c+di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i.$$

## Definicja 5.

Niech $z = (a, b) \in \mathbb{C}$. Wówczas:

- $a$ nazywamy **częścią rzeczywistą** liczby $z$ i oznaczamy ją przez $\mathrm{Re}(z)$,
- $b$ nazywamy **częścią urojoną** liczby $z$ i oznaczamy $\mathrm{Im}(z)$,
- liczbę $\sqrt{a^2 + b^2}$ nazywamy **modułem liczby** $z$ i oznaczamy jako $|z|$.

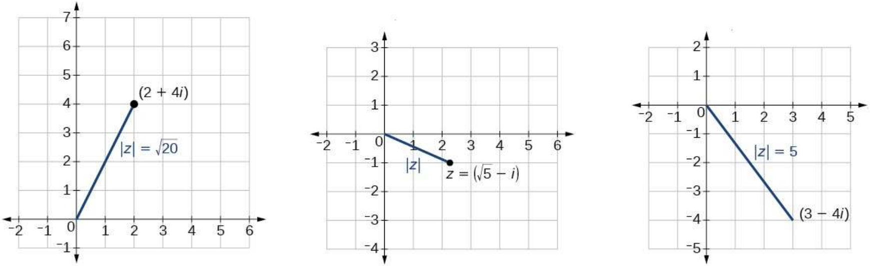



**Rys. 1.** Płaszczyzna zespolona. Moduł i argument liczby zespolonej. Źródło: Wikipedia (z modyfikacjami).

## Definicja 5.

Niech $z = (a, b) \in \mathbb{C}$. Wówczas:

- $a$ nazywamy **częścią rzeczywistą** liczby $z$ i oznaczamy ją przez $\mathrm{Re}(z)$,
- $b$ nazywamy **częścią urojoną** liczby $z$ i oznaczamy $\mathrm{Im}(z)$,
- liczbę $\sqrt{a^2 + b^2}$ nazywamy **modułem liczby** $z$ i oznaczamy jako $|z|$.




**Rys. 2.** Punkty na płaszczyźnie zespolonej. Źródło: Jay Abramson, Polar Form of Complex Numbers, math.libretexts.org

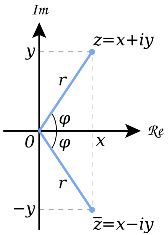
## Definicja 6.

Niech $z = a + bi$ będze liczbą zespoloną. **Sprzężeniem** liczby zespolonej $z$ nazywamy liczbę

$$\overline{z} = a - bi.$$

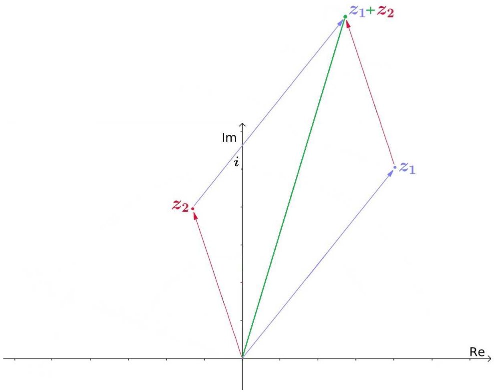
Na płaszczyźnie zespolonej punkt $\overline{z}$ jest obrazem $z$ w symetrii względem osi $\mathrm{Re}(z)$. W szczególności

$$|z| = |\overline{z}| \quad \text{oraz} \quad \arg(z) = -\arg(\overline{z}).$$




**Rys. 3.** Interpretacja geometryczna sprzężenia liczby zespolonej. Źródło: Wikipedia.

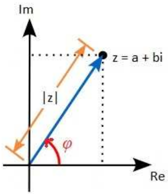
# Interpretacja geometryczna dodawania liczb zespolonych




**Rys. 4.** Interpretacja geometryczna dodawania liczb zespolonych.

$$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i.$$

## Postać trygonometryczna liczby zespolonej

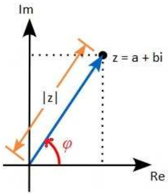



**Rys. 1.** Płaszczyzna zespolona. Moduł i argument liczby zespolonej. Źródło: Wikipedia (z modyfikacjami).

- $z = a + bi = \sqrt{a^2 + b^2}\left(\frac{a}{\sqrt{a^2+b^2}} + \frac{b}{\sqrt{a^2+b^2}}i\right).$
- Istnieje dokładnie jedno $\varphi \in [0, 2\pi)$, że:

$$\cos(\varphi) = \frac{a}{\sqrt{a^2 + b^2}}, \quad \sin(\varphi) = \frac{b}{\sqrt{a^2 + b^2}}.$$

# Postać trygonometryczna liczby zespolonej




**Rys. 1.** Płaszczyzna zespolona. Moduł i argument liczby zespolonej. Źródło: Wikipedia (z modyfikacjami).

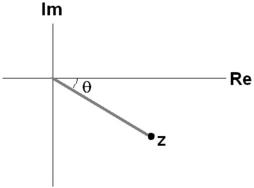
**Definicja 7.**

Niech $z \in \mathbb{C}$. Przedstawienie liczby $z$ w postaci

$$z = |z|(\cos\varphi + i\sin\varphi) \qquad (\diamondsuit).$$

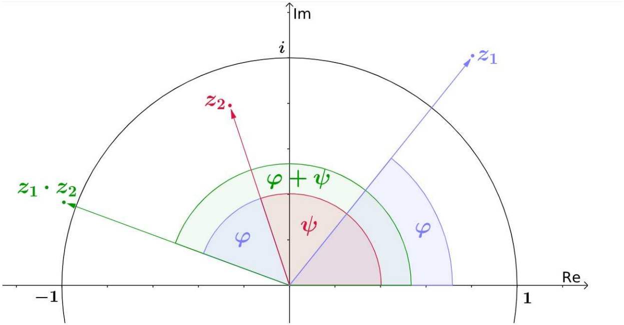
nazywamy **postacią trygonometryczna liczby** $z$. Dowolną liczbę $\varphi$ spełniającą $(\diamondsuit)$ nazywamy **argumentem** liczby $z$ i oznaczamy $\arg(z)$. Argument liczby zespolonej $z \neq 0$ jest wyznaczony z dokładnością do całkowitej wielokrotności $2\pi$. Liczbie 0 przypisujemy dowolny argument $\varphi \in \mathbb{R}$.

Przykład: $z = \sqrt{3} - i$.




- $|z| = \sqrt{\sqrt{3}^2 + (-1)^2} = 2$.
- $z = 2\left(\frac{\sqrt{3}}{2} - \frac{1}{2} \cdot i\right)$.
- $z = 2\left(\cos\frac{11\pi}{6} + i \cdot \sin\frac{11\pi}{6}\right)$.
- $z = 2\left(\cos\frac{-\pi}{6} + i \cdot \sin\frac{-\pi}{6}\right)$.

# Interpretacja geometryczna mnożenia liczb zespolonych



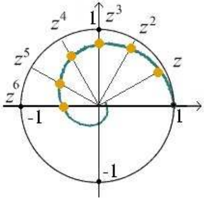

**Rys. 5.** Interpretacja geometryczna mnożenia liczb zespolonych.

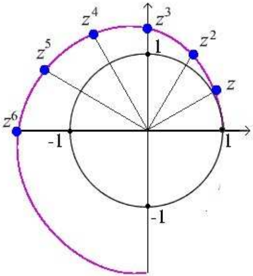
$$
\begin{aligned}
z_1 \cdot z_2 &= |z_1|(\cos\varphi + i\sin\varphi) \cdot |z_2|(\cos\psi + i\sin\psi) = \\
&= |z_1||z_2|(\cos\varphi\cos\psi - \sin\varphi\sin\psi) + i(\sin\varphi\cos\psi + \cos\varphi\sin\psi) = \\
&= |z_1 z_2|(\cos(\varphi+\psi) + i\sin(\varphi+\psi)).
\end{aligned}
$$

## Wzór Moivre'a

Niech $z = |z|(\cos\varphi + i \cdot \sin\varphi)$. Wówczas dla każdego $n$ całkowitego dodatniego mamy:

$$z^n = |z|^n(\cos(n \cdot \varphi) + i \cdot \sin(n \cdot \varphi)).$$




**Rys. 6.** Interpretacja geometryczna potęgowania liczb zespolonych. Źródło: http://www.suitcaseofdreams.net/.

**Ćwiczenie.** Pokaż, że dla dowolnych $z, z_1, z_2 \in \mathbb{C}$ mamy:

(a) $z + \overline{z} = 2\,\mathrm{Re}(z)$ oraz $z \cdot \overline{z} = |z|^2$,

(b) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ oraz $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$,

(c) $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$ oraz gdy $|z_2| \neq 0$ mamy też $\left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|}$,

(d) $|z_1 + z_2| \leq |z_1| + |z_2|$ oraz $||z_1| - |z_2|| \leq |z_1 - z_2|$.

Przykładowo: niech $z_1 = a + bi, z_2 = c + di \in \mathbb{C}$. Wówczas

$$
\begin{aligned}
|z_1 \cdot z_2| &= |(a + bi)(c + di)| = |(ac - bd) + (bc + ad)i| = \\
&= \sqrt{(ac - bd)^2 + (bc + ad)^2} = \sqrt{a^2c^2 + b^2d^2 + b^2c^2 + a^2d^2} = \\
&= \sqrt{(a^2 + b^2)(c^2 + d^2)} = |z_1| \cdot |z_2|.
\end{aligned}
$$

## Inne przykłady ciał

**Definicja 8.**

Niech $(L, +, \cdot, 0, 1)$ będzie ciałem oraz niech $K \subseteq L$. Powiemy, że $K$ jest **podciałem** ciała $L$, jeśli $0, 1 \in K$ oraz:

- dla każdych $a, b \in K$ mamy $a + b \in K$ oraz $a \cdot b \in K$,
- dla każdego $a \in K$ mamy $-a \in K$,
- dla każdego niezerowego $b \in K$ mamy $b^{-1} \in K$.

**Przykład.** Ciało liczb wymiernych $(\mathbb{Q}, +, \cdot, 0, 1)$ jest podciałem ciała $\mathbb{R}$. Ciało to ma również własność opisaną niżej (ważne ćwiczenie).

**Definicja**

Ciało $K$, które nie ma podciał właściwych, czyli różnych od siebie, nazywamy **prostym**.

## Inne przykłady ciał

**Fakt 2.**

Rozważmy podzbiór $\mathbb{Q}(\sqrt{2})$ w ciele liczb rzeczywistych złożony ze wszystkich elementów postaci

$$\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Ograniczenie działań na $\mathbb{R}$ zadaje na $\mathbb{Q}(\sqrt{2})$ strukturę podciała.

Przykłady działań w $\mathbb{Q}(\sqrt{2})$

- $(2 + \sqrt{2}) + (3 + \frac{1}{2}\sqrt{2}) = 5 + \frac{3}{2}\sqrt{2}$.
- $(1 - \sqrt{2}) \cdot (1 + \sqrt{2}) = -1 + 0 \cdot \sqrt{2}$.
- elementem odwrotnym do $3 - 2\sqrt{2}$ jest element $3 + 2\sqrt{2}$.

## Inne przykłady ciał

**Fakt 3.**

Rozważmy dowolną rodzinę podciał $K_t$ ciała $L$, gdzie $t \in T$. Wówczas część wspólna wszystkich ciał $K_t$ jest podciałem ciała $K$.

**Fakt 4.**

Dla każdego podciała $K$ ciała $L$ oraz podzbioru $S$ zbioru $L$ istnieje najmniejsze podciało $K(S)$ ciała $L$, które zawiera jednocześnie ciało $K$ oraz zbiór $S$.

**Przykłady.** Najmniejszym podciałem ciała $\mathbb{R}$ zawierającym $\mathbb{Q}$ oraz $\sqrt{2}$ jest $\mathbb{Q}(\sqrt{2})$. Inne podciała $\mathbb{R}$ to np.:

- ciała $\mathbb{Q}(\sqrt{p})$, gdzie $p$ jest liczbą pierwszą,
- ciała $\mathbb{Q}(\sqrt{p}, \sqrt{q})$, gdzie $p, q$ są liczbami pierwszymi,
- ciało liczb algebraicznych (za tydzień),
- ciała typu $\mathbb{Q}(\pi)$, $\mathbb{Q}(\sqrt{2}, \pi)$, $\mathbb{Q}(\pi, \pi^2, \pi^3, \ldots)$ itd.

Za tydzień:

- wielomiany o współczynnikach w ciele i ich pierwiastki,
- rozwiązywanie równań o współczynnikach zespolonych,
- zasadnicze twierdzenie algebry (bez dowodu),
- „całkowite liczby zespolone"(w uzupełnieniu),
- jednoznaczność rozkładu (w dodatku),
- równania wielomianowe stopni 3, 4 i wyższych (notka historyczna)