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

$(\mathbb{R},+,\cdot)$

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

	$na=\underbrace{a+\ldots+a}_{n},\ n\in\mathbb{N}$	$a^n=\underbrace{a\cdot\ldots\cdot a}_{n}$
	$0\cdot a=0$	$a^0=e=e=1$
$m\in\mathbb{Z}, m<0$	$ma=\underbrace{(-a)+\ldots+(-a)}_{m}$	$a^m=\underbrace{a^{-1}\cdot\ldots\cdot a^{-1}}_{n}$

Definicja 1.3.5. Zespół $(K,\circ,*)$ złożony ze zbioru K zawierającego co najmniej dwa elementy i określonych w nim działań wewnętrznych $\circ: K\times K\to K$, $*: K\times K\to K$ nazywamy *ciałem*, jeśli

ang. FIELD

- $(K,\circ)$ 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 jedynką (różną od zera, tj. $1=e_*\neq e_\circ=0$), w którym wszystkie niezerowe (tj. różne od elementu neutralnego $e_\circ$) elementy są odwracalne.

$\neq e_\circ$

$\exists a': a'*a=1=e_*$

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 1.3.6. 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 jedynką, 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

el. neutralny

$\mathbb{Z}/4\mathbb{Z}$ 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

$\bar{0}, \bar{1}, \bar{2}, \bar{3}$

$\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$

Definicja 1.3.7. Niech $(A, +, \cdot)$ będzie pierścieniem. Elementy $a, b \in A, a \neq 0, b \neq 0$ nazywamy *dzielnikami zera*, jeśli $a \cdot b = 0$.

Uwaga 1.3.8. W ciele nie ma dzielników zera.

Dowód. Niech $(K, +, \cdot)$ będzie ciałem oraz niech $a, b \in K$. Załóżmy, że $a \cdot b = 0$ oraz $a \neq 0$. Jeśli $a \neq 0$, to istnieje $a^{-1} \in K$. Otrzymujemy

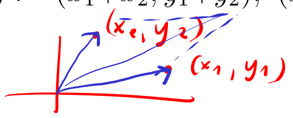
$$0 = a^{-1} \cdot 0 = a^{-1} \cdot (a \cdot b_{=}(a^{-1} \cdot a) \cdot b = 1 \cdot b = b.$$

Zatem $b = 0$. □

WAŻNE $\qquad \mathbb{R} \times \mathbb{R}$

Przykład 1.3.9. Sprawdź, że zbiór $\mathbb{R}^2$ wraz z działaniami dodawania i mnożenia zdefiniowanymi poniżej ma strukturę ciała.

$\forall (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2 \quad (x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2), \ (x_1, y_1) \cdot (x_2, y_2) := (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1).$



$(\mathbb{C}, +)$ jest grupą abelową.

Działanie $+$ jest wewnętrzne, łączne, przemienne. Elementem neutralnym jest $(0, 0) \in \mathbb{R}^2$, zaś elementem przeciwnym do $(x_1, y_1) \in \mathbb{R}^2$ jest $(-x_1, -y_1) \in \mathbb{R}^2$.

$(\mathbb{C} \setminus \{(0, 0)\}, \cdot)$ jest grupą abelową.

Działanie $\cdot$ jest wewnętrzne.

przemienność:

$(x_2, y_2) \cdot (x_1, y_1) = (x_2x_1 - y_2y_1, x_2y_1) = \ = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1) = (x_1, y_1) \cdot (x_2, y_2)$

łączność: $\quad L = P$

$$L = (a,b)\cdot[(x_1,y_1)\cdot(x_2,y_2)] = (a,b)\cdot(x_1x_2 - y_1y_2, x_1y_2 + x_2y_1) =$$
$$= (ax_1x_2 - ay_1y_2 - bx_1y_2 - bx_2y_1, ax_1y_2 + ax_2y_1 + bx_1x_2 - by_1y_2)$$
$$P = [(a,b)\cdot(x_1,y_1)]\cdot(x_2,y_2) = (ax_1 - by_1, ay_1 + bx_1)\cdot(x_2,y_2) =$$
$$= (ax_1x_2 - by_1x_2 - ay_1y_2 - bx_1y_2, ax_1y_1 - by_1y_2 + ay_1x_2 + bx_1x_2)$$

el. neutralny: $\quad e = (1,0)$

$$\forall (x_1,y_1)\in\mathbb{R}^2 \quad (1,0)\cdot(x_1,y_1) = (1\cdot x_1 - 0\cdot y_1, 1\cdot y_1 + 0\cdot x_1) = (x_1,y_1)$$

el. odwrotny do $(x_1,y_1)\neq(0,0)$:

$$(x_1,y_1)\cdot(a,b) = (1,0) \Leftrightarrow (ax_1 - by_1, ay_1 + bx_1) = (1,0) \Leftrightarrow \begin{bmatrix} x_1 & -y_1 \\ y_1 & x_1 \end{bmatrix}\cdot\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\forall (x_1,y_1)\neq(0,0) \quad a = \frac{x_1}{x_1^2+y_1^2},\ b = \frac{y_1}{x_1^2+y_1^2}$$

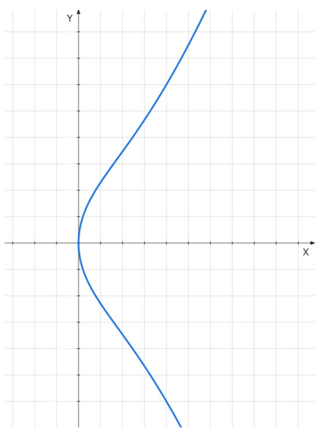
Działanie $\cdot$ jest rozdzielne względem $+$, bowiem $L = P$.

$$L = (a,b)\cdot[(x_1,y_1)+(x_2,y_2)] = (a,b)\cdot(x_1+x_2, y_1+y_2) = (ax_1+ax_2-by_1-by_2, ay_1+ay_2+bx_1+bx_2)$$
$$P = [(a,b)\cdot(x_1,y_1)] + [(a,b)\cdot(x_2,y_2)] = (ax_1 - by_1, ay_1 + bx_1) + (ax_2 - by_2, ay_2 + bx_2)$$

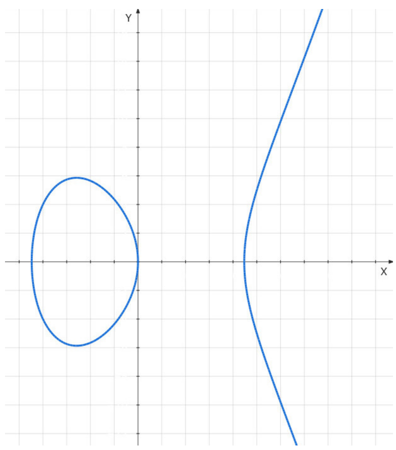
Definicja 1.3.10. Zdefiniowane powyżej ciało nazywamy *ciałem liczb zespolonych* i oznaczamy symbolem $\mathbb{C}$. Elementy tego ciała nazywamy *liczbami zespolonymi.*

NIEOBOWIĄZKOWY!

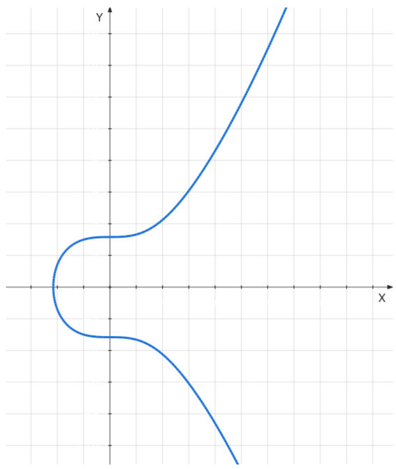
Przykład 1.3.11 (Struktura grupy na krzywej eliptycznej)**.** Niech $K = \mathbb{R}$ lub $K = \mathbb{C}$. *Krzywą eliptyczną* nad ciałem K nazywamy krzywą zdefiniowaną równaniem
$y^2 = x^3 + ax + b$, gdzie $a, b \in K$ są takie, że $4a^3 + 27b^2 \neq 0$.
Warunek ten zapewnia, iż krzywa nie ma punktów osobliwych.



$y^2 = x^3 + 20x$ nad $\mathbb{R}$



$y^2 = x^3 - 20x$ nad $\mathbb{R}$



$y^2 = x^3 + 10$ nad $\mathbb{R}$

Oznaczmy

$$E(K) = \{(x, y) \in K \times K : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\},$$

gdzie $\mathcal{O}$ jest pewnym wyróżnionym punktem, zwanym *punktem w nieskończoności*.

W zbiorze $E(K)$ można zdefiniować operację grupową + „dodawania” punktów, dla której $\mathcal{O}$ jest elementem neutralnym i taką, że $(E(K), +)$ jest grupą abelową.

Niech $A = (x_1, y_1), B = (x_2, y_2)$ to dwa punkty ze zbioru $E(K)$. Zdefinujemy dzialanie $+ : E(K) \times E(K) \to E(K)$ w opisany niżej sposób.

1. $A + \mathcal{O} = A$, $\mathcal{O} + B = B$

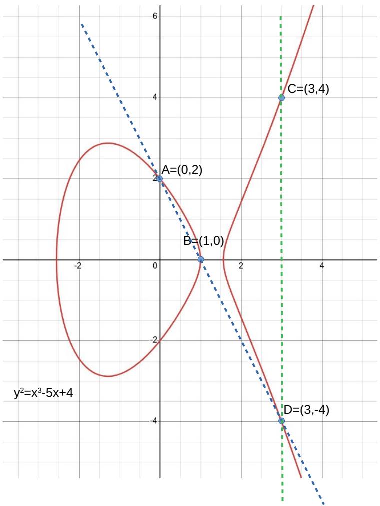
2. Jeśli $x_1 = x_2$ oraz $y_1 = -y_1$, wówczas $A + B = \mathcal{O}$.

3. W pozostałych przypadkach obliczamy $\lambda = \begin{cases} \frac{3x_1^2+a}{2y_1} & ; \quad A = B \\ \\ \frac{y_1-y_2}{x_1-x_2} & : \quad A \neq B \end{cases}$.

Wówczas $A + B = C = (x_3, y_3)$, gdzie $x_3 = \lambda^2 - x_1 - x_2$ oraz $y_3 = -\lambda x_3 - \nu$, dla $\nu = y_1 - \lambda x_1$.

W przypadku gdy $A \neq B$ oraz $x_1 \neq x_2$ dodawanie punktów można opisać geometrycznie w następujący sposób.

Wyznaczmy prostą l przechodzącą przez punkty A i B. Można wykazać, że wówczas prosta l przecina krzywą w dokładnie trzech punktach A, B oraz $D = (x_4, y_4)$, gdzie $x_3 = \lambda^2 - x_1 - x_2$ oraz $y_3 = \lambda x_3 + \nu$, dla $\nu = y_1 - \lambda x_1$. Inaczej mówiąc $x_4 = x_3$ zaś $y_4 = -y_3$.



$A+B \overset{df}{=} C$

Krzywe eliptyczne znajdują zastosowanie w kryptografii. Więcej informacji można znaleźć tutaj lub tutaj.

Elżbieta Adamus
Wydział Matematyki Stosowanej
Akademia Górniczo-Hutnicza w Krakowie

Algebra
Wykład nr 2
Data: ....

TEMAT: *Liczby zespolone*

complex numbers $\quad (\mathbb{R}\times\mathbb{R}, +, \cdot)$

2.1 Ciało liczb zespolonych

$2x-1=0$

Motywacja $\quad 2x = 1 \quad x^2-2=0 \quad \boxed{x^2+1=0} \quad i, -i \quad \mathbb{C}$

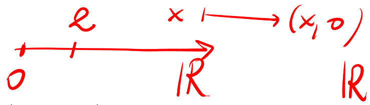
$$\mathbb{N} \underset{n\mapsto n}{\hookrightarrow} \mathbb{Z} \underset{n\mapsto \frac{n}{1}}{\hookrightarrow} \mathbb{Q} \hookrightarrow \mathbb{R} \underset{x\mapsto(x,0)}{\overset{h}{\hookrightarrow}} \mathbb{C}$$

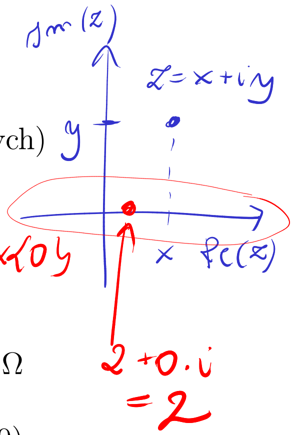
$x+1=0$

$X^2-2=0$ równanie o współczynnikach z $\mathbb{Q}$, jego rozwiązania $\pm\sqrt{2}\notin\mathbb{Q}$
Ćwiczenie: $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} : \ a,b\in\mathbb{Q}\}$ jest ciałem takim, że $\mathbb{Q}\longrightarrow\mathbb{Q}(\sqrt{2})\longrightarrow\mathbb{R}$

$X^2+1=0$ równanie o współczynnikach z $\mathbb{R}$, jego rozwiązania $\pm i$ nie należą do $\mathbb{R}$
$\mathbb{R}(i) = \{a+bi : \ a,b\in\mathbb{R}\} = \mathbb{C}$
$\mathbb{C}$ ciało *algebraicznie domknięte* - tzn. rozwiązania równań algebraicznych (wielomianowych) o współczynnikach z $\mathbb{C}$ należą do $\mathbb{C}$

$< \mathbb{R} \qquad x \longmapsto (x,0)$





Zanurzenie $\mathbb{R}$ w $\mathbb{C}$

Niech $\Omega = \mathbb{R}\times\{0\} = \{(x,0) : \ x\in\mathbb{R}\}\subset\mathbb{R}^2$. Wówczas $(\Omega,+,\cdot)$ jest ciałem.

wewnętrzność: $\quad (x_1,0)+(x_2,0) = (x_1+x_2,0)\in\Omega,\ (x_1,0)\cdot(x_2,0) = (x_1x_2,0)\in\Omega$

przemienność:
$$(x_1,0)+(x_2,0) = (x_1+x_2,0) = (x_2+x_1,0) = (x_2,0)+(x_1,0)$$
$$(x_1,0)\cdot(x_2,0) = (x_1x_2,0) = (x_2x_1,0) = (x_2,0)\cdot(x_1,0)$$

łączność:
$$[(x_1,0)+(x_2,0)]+(x_3,0) = (x_1+x_2+x_3,0) = (x_1,0)+[(x_2,0)+(x_3,0)]$$
$$[(x_1,0)\cdot(x_2,0)]\cdot x_3, 0 = (x_1x_2x_3,0) = (x_1,0)\cdot[(x_2,0)\cdot(x_3,0)]$$

el. neutralne: $(0,0)$ dla dodawania oraz $(1,0)$ dla mnożenia
el. symetryczne do $(x_1,0)$: $(-x_1,0)$ względem $+$, $(\frac{1}{x_1},0)$ względem $\cdot$

rozdzielność:
$$[(x_1,0)+(x_2,0)]\cdot(x_3,0) = (x_1+x_2,0)\cdot(x_3,0) = ((x_1+x_2)x_3,0) =$$
$$= (x_1x+3+x_2x_3,0) = [(x_1,0)\cdot(x_3,0)]+[(x_2,0)\cdot(x_3,0)]$$

Niech $h:\mathbb{R}\to\Omega$, $h(x)=(x,0)$. Jest to *zanurzenie*, czyli bijekcja taka, że $h(x_1+x_2) = h(x_1)+h(x_2)$ oraz $h(x_1\cdot x_2) = h(x_1)\cdot h(x_2)$. $\leftarrow$ zgodne z działaniami.
Utożsamiamy zbiory $\mathbb{R}$ oraz Ω i piszemy x zamiast $h(x)$.

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad = (x,0)$

$(0,1)\cdot(0,1) = (0\cdot 0 - 1\cdot 1, 0\cdot 1 + 0\cdot 1) = (-1,0) = -1$

i

$(x_1,y_1)\cdot(x_2,y_2) := (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$

Zdefiniujmy $i := (0,1)$ tzw. *jednostka urojona*. Wówczas

ćw. $e = (1,0) = 1$

$i^2 = -1$

$$i^2 = i \cdot i = (0,1)\cdot(0,1) = (-1,0) = -1$$

$i \cdot y$

$i^2 + 1 = 0$

$$\mathbb{C} \ni z = (x,y) = (x,0) + \boxed{(0,y)} = (x,0) + \boxed{(0,1)(y,0)} = x + iy$$

$(x_1,y_1)\cdot(1,0) =$

$x^2+1=0$

Postać $z = x + iy$, gdzie $x, y, \in \mathbb{R}$ to tzw. *postać kanoniczna (algebraiczna, Gaussa)* liczby zespolonej. Liczbę $x \in \mathbb{R}$ nazywamy *częścią rzeczywistą* liczby z i oznaczamy $\mathrm{Re}z$. Liczbę $y \in \mathbb{R}$ nazywamy *częścią urojoną* liczby z i oznaczamy $\mathrm{Im}z$. Liczby postaci iy, $y \in \mathbb{R}$ nazywamy *czysto urojonymi*.

$= (x_1 \cdot 1 - y_1 \cdot 0, x_1 \cdot 0 + y_1 \cdot 1)$

$h(x) + (0,1)\cdot h(y)$

$x + i \cdot y$

$= (x_1, y_1)$

$$z_1 = z_2 \Leftrightarrow \left(\mathrm{Re}z_1 = \mathrm{Re}z_1 \wedge \mathrm{Im}z_1 = \mathrm{Im}z_2\right)$$

Postać algebraiczna pozwala na dodawanie i mnożenie liczb zespolonych jak wielomianów zmiennej i, przy warunku $i^2 = -1$.

$$(x_1,y_1) + (x_2,y_2) = (x_1+x_2, y_1+y_2) \qquad (x_1+iy_1) + (x_2+iy_2) = (x_1+x_2) + i(y_1+y_2)$$
$$(x_1,y_1)\cdot(x_2,y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1) \qquad (x_1+iy_1)\cdot(x_2+iy_2) = (x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1)$$

$i^2 = -1$

Przykład 2.1.1. $(2+7i) - (4-2i) = -2 + 9i$

$+3$

$$(3-i)\cdot(2+3i) = 6 + 9i - 2i - 3i^2 = 9 + 7i$$

$i^2 y_1 y_2 = -y_1 y_2$

$$\frac{2+3i}{2-5i} = \frac{(2+3i)(2+5i)}{(2-5i)(2+5i)} = \frac{4+10i+6i+15i^2}{4-25i^2} = \frac{-11+16i}{29} = -\frac{11}{29} + \frac{16}{29}i$$

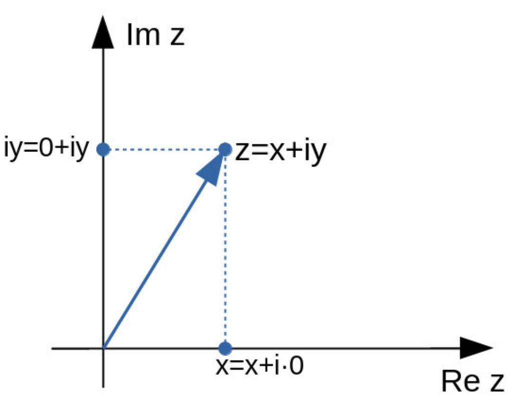
$a + b \cdot i$

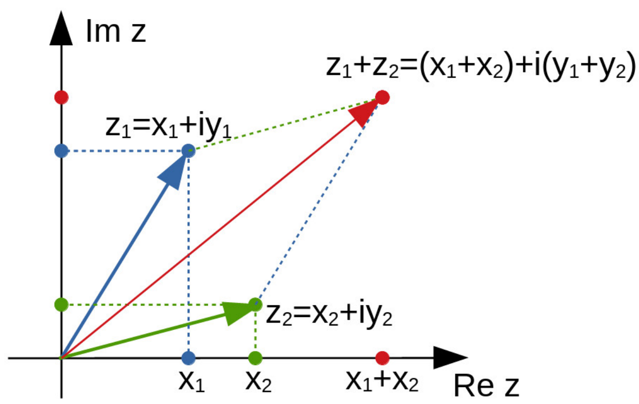
Uwaga 2.1.2. W ciele $\mathbb{C}$ nie można określić porządku liniowego.

$$-1 = i \cdot i = (-i)\cdot(-i) \qquad 1 = 1 \cdot 1 = (-1)\cdot(-1)$$

Utożsamiamy liczby zespolone z punktami na płaszczyźnie lub wektorami zaczepionymi w $(0,0)$.

Płaszczyzna zespolona - geometryczny model ciała liczb zespolonych $\mathbb{C}$





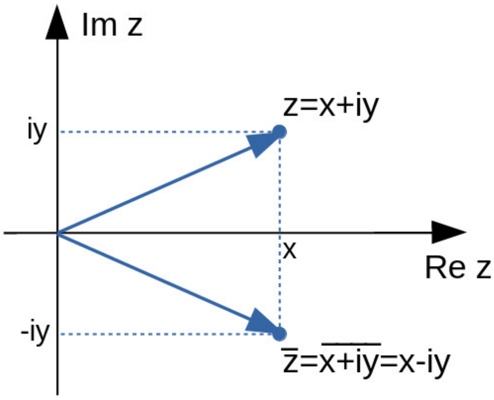
$z \cdot \bar{z} = (x+iy)(x-iy) = x^2 - i^2y^2$
$= x^2+y^2 = |z|^2$

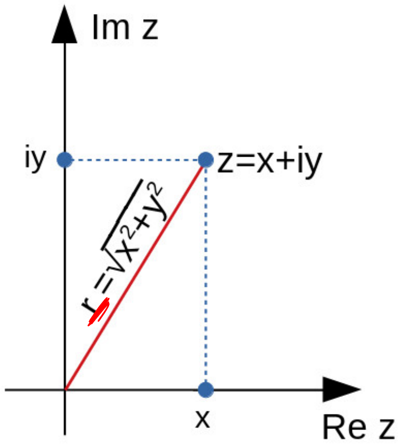
$\bar{z} = \overline{x+iy} = x-iy$

Definicja 2.1.3. Niech $z = x + iy \in \mathbb{C}$, $x, y \in \mathbb{R}$.

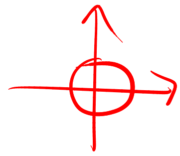
i) Liczbę zespoloną $w = x - iy$ nazywamy *liczbą sprzężoną* do liczby z. Oznaczamy ją $\bar{z}$.

i) Liczbę rzeczywistą $\sqrt{x^2+y^2}$ nazywamy modułem liczby z. Oznaczamy ją $|z|$.





$\{z \in \mathbb{C} : |z| = 1\}$



Twierdzenie 2.1.4 (Własności liczb zespolonych)**.** Niech $z, z_1, z_2 \in \mathbb{C}$. Wówczas prawdziwe są następujące równości.

i) $\mathrm{Re}(z_1 + z_2) = \mathrm{Re}z_1 + \mathrm{Re}z_2, \quad \mathrm{Im}(z_1+z_2) = \mathrm{Im}z_1 + \mathrm{Im}z_2$

ii) $\mathrm{Re}z = \frac{1}{2}(z + \bar{z}), \quad \mathrm{Im}z = \frac{1}{2i}(z - \bar{z})$

iii) $\overline{(\bar{z})} = z$

iv) $\overline{z_1+z_2} = \bar{z}_1 + \bar{z}_2, \quad \overline{z_1 - z_2} = \bar{z}_1 - \bar{z}_2, \quad \overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$

iv) $\overline{\left(\frac{z_1}{z_2}\right)} = \frac{\bar{z}_1}{\bar{z}_2}$, dla $z_2 \neq 0$

vi) $|z| = |-z| = |\bar{z}|$

vii) $z \cdot \bar{z} = |z|^2$

viii) $\mathrm{Re}z \leq |\mathrm{Re}z| \leq |z|, \quad \mathrm{Im}z \leq |\mathrm{Im}z| \leq |z|$

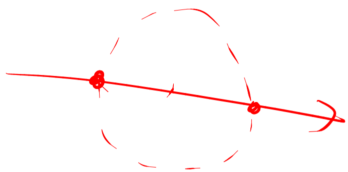
ix) $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$

x) $|z_1 + z_2| \leq |z_1| + |z_2|$ (nierówność trójkąta) $\Big||z_1| - |z_2|\Big| \leq |z_1 - z_2|$

$\mathbb{R}$

$|x| = 1$

$x = \pm 1$



Dowód. vii) $(x+iy)(x-iy) = x^2 - i^2y^2 = x^2 + y^2 = |z|^2$
viii) $\mathrm{Re}z = x \leq |x| \leq \sqrt{x^2+y^2} = |z|$
x) $1 = \mathrm{Re}1 = \mathrm{Re}\left(\frac{z_1+z_2}{z_1+z_2}\right) \overset{i)}{=} \mathrm{Re}\left(\frac{z_1}{z_1+z_2}\right) + \mathrm{Re}\left(\frac{z_2}{z_1+z_2}\right) \overset{\mathrm{def}}{\leq} \left|\frac{z_1}{z_1+z_2}\right| + \left|\frac{z_2}{z_1+z_2}\right| \overset{iv)v)}{=} \frac{|z_1|}{|z_1+z_2|} + \frac{|z_2|}{|z_1+z_2|} \Rightarrow |z_1+z_2| \leq |z_1| + |z_2|$
$|z_1| = |z_1 - z_2 + z_2| \leq |z_1 - z_2| + |z_2| \wedge |z_2| = |z_2 - z_1 + z_1| \leq |z_2 - z_1| + |z_1| \Rightarrow \Big||z_1| - |z_2|\Big| \leq |z_1 - z_2|$ □

x+iy postać algebraiczna

$z \cdot z = z^2$

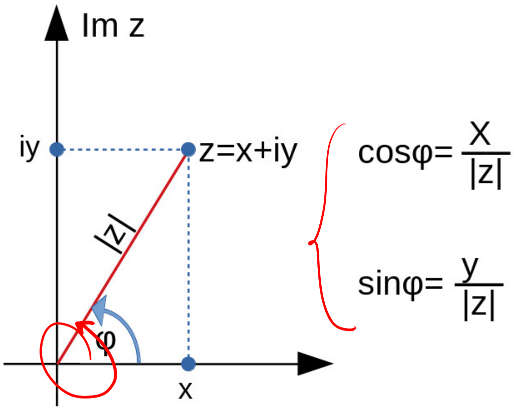
$z^{123} = (x+iy)^{123}$

2.2 Postać trygonometryczna i wykładnicza

Postać trygonometryczna liczby zespolonej

Niech $z = x + iy \neq 0$. Wówczas $z = |z|\left(\frac{x}{|z|} + i\frac{y}{|z|}\right)$. Ponieważ $\left(\frac{x}{|z|}\right)^2 + \left(\frac{y}{|z|}\right)^2 = 1$, więc istnieje kąt φ taki, że

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



$z \neq 0 \Rightarrow |z| \neq 0$

φ $\varphi + 2k\pi$ $k \in \mathbb{Z}$

Dowolny taki kąt nazywamy *argumentem* liczby z. Ten z argumentów liczby zespolonej, który leży w przedziale $[0, 2\pi)$, nazywamy *argumentem głównym* liczby z i oznaczamy $\arg z$. Zatem dowolny argument liczby z ma postać $\arg z + 2k\pi$, $k \in \mathbb{Z}$. Przyjmujemy, że argument liczby $z = 0$ jest nieokreślony. Dowolną liczbę $z \in \mathbb{C}, z \neq 0$ możemy zatem przedstawić w postaci $z = |z|(\cos\varphi + i\sin\varphi)$, gdzie φ to jeden z jej argumentów. Powyższe przedstawienie nazywamy *postacią trygonometryczną* liczby zespolonej z.

Gdy $z_1 \neq 0, z_2 \neq 0$, $z_1 = |z_1|(\cos\alpha + i\sin\alpha)$, $z_2 = |z_2|(\cos\beta + i\sin\beta)$, to wówczas $z_1 = z_2$ wtedy i tylko wtedy gdy $|z_1| = |z_2|$ oraz $\beta = \alpha + 2k\pi$ dla pewnego $k \in \mathbb{Z}$.

Przykład 2.2.1. Przedstaw podane liczby w postaci trygonometrycznej.

$z = 7$
$z = 7(1 + 0i)$

$0 + (-1)\cdot i$

$z = -i$
$|z| = \sqrt{0^2 + (-1)^2} = 1$
$z = 1\,(0 + (-1)\cdot i)$
$\begin{cases} \cos\varphi = 0 \\ \sin\varphi = -1 \end{cases}$

$z = -\sqrt{27} - 3i$
$|z| = \sqrt{27 + 9} = 6$
$z = 6\left(-\frac{\sqrt{3}}{2} - \frac{1}{2}i\right)$
$\begin{cases} \cos\varphi = -\frac{\sqrt{3}}{2} < 0 \\ \sin\varphi = -\frac{1}{2} < 0 \end{cases}$

$6\left(-\frac{\sqrt{27}}{6} + \frac{-3}{6}i\right)$

$\varphi = 0 + 2k\pi$
$\arg z = 0$

$\varphi = -\frac{\pi}{2} + 2k\pi$
$\arg z = \frac{3}{2}\pi$

$\varphi = \frac{7}{6}\pi + 2k\pi$, $\quad k \in \mathbb{Z}$ ← dowolny argument
$\arg z = \frac{7}{6}\pi$ ← argument główny

$z = 7(\cos 0 + i\sin 0)$ $\qquad -i = 1(\cos\frac{3}{2}\pi + i\sin\frac{3}{2}\pi)$ $\qquad -\sqrt{27} - 3i = 6(\cos\frac{7}{6}\pi + i\sin\frac{7}{6}\pi)$

Mnożenie i dzielenie liczb w postaci trygonometrycznej

Twierdzenie 2.2.2. Niech $z = |z|(\cos\varphi + i\sin\varphi)$,
$z_1 = |z_1|(\cos\alpha + i\sin\alpha)$, $z_2 = |z_2|(\cos\beta + i\sin\beta)$. Wówczas:

$z \cdot z$ $\quad |z||z|$ $\quad |z|^2$ $\quad \alpha+\alpha$ $\quad 2\alpha$

i) $z_1 \cdot z_2 = |z_1| \cdot |z_2| \cdot \big(\cos(\alpha+\beta) + i\sin(\alpha+\beta)\big)$,

ii) $\frac{z_1}{z_2} = \frac{|z_1|}{|z_2|} \cdot \big(\cos(\alpha-\beta) + i\sin(\alpha-\beta)\big)$,

! iii) $z^n = |z|^n \cdot \big(\cos n\varphi + i\sin n\varphi\big)$ tzw. *wzór de Moivre'a*

Dowód. i) $z_1 \cdot z_2 = |z_1| \cdot |z_2|(\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta)$
$= |z_1| \cdot |z_2|\Big(\underbrace{(\cos\alpha\cos\beta - \sin\alpha\sin\beta)}_{\cos(\alpha+\beta)} + i\underbrace{(\sin\alpha \overset{\cos\beta}{\cancel{\sin\beta}} + \cos\alpha \overset{\sin\beta}{\cancel{\cos\beta}})}_{\sin(\alpha+\beta)}\Big)$

ii) analogicznie
iii) Na mocy i) dla $n = 2$ mamy $z^2 = z \cdot z = |z|^2(\cos 2\varphi + i\sin 2\varphi)$.
Przeprowadzając dowód indukcyjny, otrzymujemy tezę. $\square$

Przykład 2.2.3. Przedstaw liczbę $z = -\sin\frac{\pi}{10} + i\cos\frac{\pi}{10}$ w postaci trygonometrycznej.

METODA I: Ponieważ $|z| = 1$, zatem $z = \cos\varphi + i\sin\varphi$ dla pewnego $\varphi \in [0, 2\pi)$.
$$\begin{cases} \cos\varphi = -\sin\frac{\pi}{10} < 0 \\ \sin\varphi = \cos\frac{\pi}{10} > 0 \end{cases} \Rightarrow \quad \varphi \text{ z II ćwiartki}$$
Na mocy wzorów redukcyjnych $\varphi = \frac{\pi}{2} + \frac{\pi}{10}$ oraz $z = \cos\left(\frac{\pi}{2} + \frac{\pi}{10}\right) + i\sin\left(\frac{\pi}{2} + \frac{\pi}{10}\right)$.

$-1 = i^2$

METODA II: $z = -\sin\frac{\pi}{10} + i\cos\frac{\pi}{10} = i^2\sin\frac{\pi}{10} + i\cos\frac{\pi}{10} = i\left(\cos\frac{\pi}{10} + i\sin\frac{\pi}{10}\right) =$
$\left(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\right)\left(\cos\frac{\pi}{10} + i\sin\frac{\pi}{10}\right) = \cos\left(\frac{\pi}{2} + \frac{\pi}{10}\right) + i\sin\left(\frac{\pi}{2} + \frac{\pi}{10}\right)$.

Przykład 2.2.4. Oblicz $\left(\frac{1+i\sqrt{3}}{1-i}\right)^{20}$.

$\sqrt{1^2+(-1)^2} = \sqrt{2}$ $\quad$ Brawo!

$\sqrt{1^2+\sqrt{3}^2} = 2$

$1+i\sqrt{3} = 2\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = 2(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3})$ $\quad 1-i = \sqrt{2}\left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right) = \sqrt{2}\left(\cos\left(-\frac{\pi}{4}\right) + i\sin\left(-\frac{\pi}{4}\right)\right)$

$\frac{\pi}{3} - \left(-\frac{\pi}{4}\right)$

$\frac{1+i\sqrt{3}}{1-i} = \frac{2}{\sqrt{2}}\left(\cos\left(\frac{\pi}{3} + \frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{3} + \frac{\pi}{4}\right)\right) = \sqrt{2}\left(\cos\left(\frac{7}{12}\pi\right) + i\sin\left(+\frac{7}{12}\pi\right)\right)$

R^{20} $\quad 20 \cdot \frac{7}{12}\pi$

wzór de Moivre'a

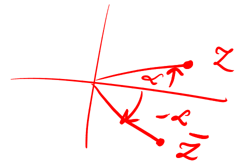
$\left(\frac{1+i\sqrt{3}}{1-i}\right)^{20} = 2^{10}\left(\cos\left(\frac{140}{12}\pi\right) + i\sin\left(\frac{140}{12}\pi\right)\right) = 2^{10}\left(\cos\left(\frac{35}{3}\pi\right) + i\sin\left(\frac{35}{3}\pi\right)\right) =$
$= 2^{10}\left(\cos\left(12\pi - \frac{\pi}{3}\right) + i\sin\left(12\pi - \frac{\pi}{3}\right)\right) = 2^{10}\left(\cos\frac{\pi}{3} - i\sin\frac{\pi}{3}\right) = 2^{10}\left(\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) =$
$= 2^9(1 - \sqrt{3}i)$

Twierdzenie 2.2.5 (Własności argumentu). Niech $z, z_1, z_2 \in \mathbb{C}$.
Wówczas prawdziwe są następujące równości.

i) $\arg(z_1 z_2) = \arg z_1 + \arg z_2 + 2k\pi$, $k \in \mathbb{Z}$ $\quad (k = 0$ lub $k = -1)$

arg
arg. główny $[0, 2\pi)$

$2\pi - \alpha$



ii) $\arg(\frac{z_1}{z_2}) = \arg z_1 - \arg z_2 + 2k\pi,\ k \in \mathbb{Z}$ $\qquad$ $(k = 0$ lub $k = -1)$

iii) $\arg(z^n) = n \cdot \arg z + 2k\pi,\ k \in \mathbb{Z}$

iv) $\arg\bar{z} = 2\pi - \arg z$, gdy $\arg z \neq 0$

Dowód. iii) Na mocy i) dla $n = 2$ mamy $\arg(z^2) = \arg(z \cdot z) = \arg z + \arg z + 2k\pi = 2\arg z + 2k\pi$. Przeprowadzając dowód indukcyjny, otrzymujemy tezę.
iv) $z \cdot \bar{z} = |z^2|$ oraz $0 = \arg(|z^2|) = \arg z + \arg\bar{z} + 2k\pi$, skąd $\arg\bar{z} = -2\pi - \arg z$ $\square$

Przykład 2.2.6. $\arg i = \frac{\pi}{2}$ $\qquad$ $\arg(-1) = \pi$ $\qquad$ $\arg(-i) = \frac{3}{2}\pi$
$i = (-1) \cdot (-i) \ \Rightarrow\ \arg i = \pi + \frac{3}{2}\pi + 2k\pi = \frac{5}{2}\pi + 2k\pi$ dla pewnego $k \in \mathbb{Z}$, tj. $k = -1$

Postać wykładnicza liczby zespolonej

$z = |z|(\cos\varphi + i\sin\varphi) = |z| e^{i\varphi}$

Dla $\varphi \in \mathbb{R}$ definiujemy $\boxed{e^{i\varphi} = \cos\varphi + i\sin\varphi.}$ Zatem dowolną liczbę zespoloną $z \neq 0$ można zapisać w postaci $z = |z|e^{i\varphi}$, gdzie φ to pewien argument liczby z.

Przykład 2.2.7. a) $e^{\frac{\pi}{2}i} = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2} = 0 + 1 \cdot i = i$

b) $e^{i\pi} = \cos\pi + i\sin\pi = \underbrace{-1 + 0 \cdot i}_{-1} \ \Rightarrow\ e^{i\pi} + 1 = 0$

najpiękniejszy wzór w matematyce

Twierdzenie 2.2.8. Niech $\alpha, \beta \in \mathbb{R}$. Wówczas:

i) $e^{i(\alpha+\beta)} = e^{i\alpha} \cdot e^{i\beta}$, $\ e^{i(\alpha-\beta)} = \frac{e^{i\alpha}}{e^{i\beta}}$,

ii) $(e^{i\alpha})^k = e^{ik\alpha}$, dla $k \in \mathbb{Z}$,

iii) $e^{i(\alpha+2k\pi)} = e^{i\alpha}$, dla $k \in \mathbb{Z}$,

iv) $e^{i\alpha} \neq 0$, $\ |e^{i\alpha}| = 1$.

Dowód. i), ii), iii) Analogiczny jak dla własności działań na liczbach w postaci trygonometrycznej.
iv) Mamy $|e^{i\alpha}| = |\cos\alpha + i\sin\alpha| = \sqrt{\cos^2\alpha + \sin^2\alpha} = 1$, zatem $e^{i\alpha} = 0 \Leftrightarrow \cos\alpha = \sin\alpha = 0$, co nie jest możliwe, gdyż gdy $\cos\alpha = 0$, to $\sin\alpha = \pm 1$. $\square$

Wniosek 2.2.9. Niech $z = re^{i\varphi}$, $z_1 = r_1 e^{i\alpha}$, $z_2 = r_2 e^{i\beta}$ będą liczbami zespolonymi w postaci wykładniczej. Wówczas:

i) $z_1 z_2 = r_1 r_2 e^{i(\alpha+\beta)}$, $\ \frac{z_1}{z_2} = \frac{r_1}{r_2} e^{i(\alpha-\beta)}$,

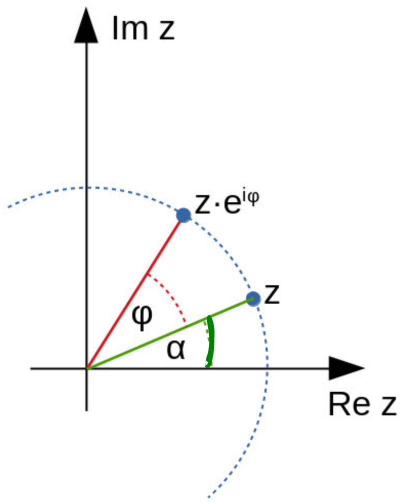
ii) $z^k = r^k e^{ik\varphi}$, dla $k \in \mathbb{Z}$,

iii) $\bar{z} = re^{-i\varphi}$.

Dowód. iii) Jeśli $\arg z = \varphi$, to $\arg\bar{z} = 2\pi - \varphi$, skąd $e^{(2\pi i - \varphi)i} = e^{2\pi}e^{-\varphi i} = e^{-\varphi i}$. $\square$

Wzory Eulera
$e^{i\varphi} = \cos\varphi + i\sin\varphi$
$e^{-i\varphi} = \cos(-\varphi) + i\sin(-\varphi) = \cos\varphi - i\sin\varphi$
Dodając lub odejmując stronami, otrzymujemy :

$$\cos\varphi = \frac{e^{i\varphi} + e^{-i\varphi}}{2}, \qquad \sin\varphi = \frac{e^{i\varphi} - e^{-i\varphi}}{2i}, \qquad \varphi \in \mathbb{R}.$$



Obrót o kąt φ
$z = re^{i\alpha}$ ← postać wykładnicza
$\underbrace{z \cdot e^{i\varphi}}_{W} = re^{i(\alpha+\varphi)}$

$r = |z|$
$z = |z| \cdot e^{i\alpha}$

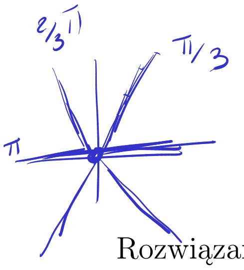
$w = 1 \cdot e^{i\varphi}$

Przykład 2.2.10. Rozwiąż równanie $z^3 = (\overline{z})^3$.

$r = |z|$

Widzimy, że $z = 0$ spełnia równanie.
Załóżmy teraz, że $z \neq 0$. Wówczas $z = re^{i\varphi}$, dla pewnych $r \in \mathbb{R}, r > 0$ oraz $\varphi \in \mathbb{R}$. Zatem

$z \neq 0 \Rightarrow |z| \neq 0$



$$\begin{aligned} z^3 &= (\overline{z})^3 \\ r^3e^{3i\varphi} &= r^3e^{-3i\varphi} \quad /: r^3 / \cdot e^{3i\varphi} \\ e^{6i\varphi} &= 1 = e^{0i} \\ 6\varphi &= 0 + 2k\pi, \quad k \in \mathbb{Z} \\ \varphi &= \tfrac{k\pi}{3}, \quad k \in \mathbb{Z} \end{aligned}$$

wystarczy te

Rozwiązaniami są punkt $z = 0$ oraz półproste $\varphi_k = \frac{k\pi}{3}, \quad k \in \{0, 1, 2, 3, 4, 5\}$.
Podsumowując, rozwiązaniami są punkty należące do prostych $y = 0$, $y = \sqrt{3}x$ oraz $y = -\sqrt{3}x$.

$z = ?\,(\cos\varphi_k + i\sin\varphi_k)$

$\cos 6 \cdot \frac{\pi}{3}$
$\cos 2\pi \qquad \cos 0$

2.3 Pierwiastkowanie, równania wielomianowe

$1 \cdot z^n - w = 0 \qquad 1 \cdot z^n - 10 = 0$

Pierwiastkowanie
Niech $n \in \mathbb{N}$, $w \in \mathbb{C}$ będą ustalone.

Definicja 2.3.1. Każdą liczbę $z \in \mathbb{C}$ spełniająca równanie $z^n = w$, nazywamy *pierwiastkiem n-tego stopnia* z liczby w.

Przykład 2.3.2. Rozwiąż równanie $z^2 = \underbrace{8 + 6i}_{W}$.

I sposób: postać wykładnicza (2)

$z = |z|e^{i\varphi}$, $w = 8 + 6i$

$|z|^2 e^{2i\varphi} = w$

$|w| = 10$

$w = 8 + 6i = 10(\frac{4}{5} + i\frac{3}{5})$

$\varphi = \arcsin \frac{3}{5} + 2k\pi$

$z^2 = |z|^2 e^{2i\varphi} = 10 \cdot e^{\alpha i}$

$|z| = \sqrt{10}$

$2\varphi = \alpha + 2k\pi$

$\varphi_k = \frac{1}{2} \arcsin \frac{3}{5} + k\pi$

$z = \sqrt{10} e^{i\varphi_k}, \ k \in \{0, 1\}$

II sposób: postać algebraiczna (1)

$z = x + iy$, $w = 8 + 6i$

$z^2 = w$

$(x + iy)^2 = 8 + 6i$

$x^2 + 2xyi - y^2 = 8 + 6i$

$$\begin{cases} x^2 - y^2 = 8 \\ 2xy = 6 \end{cases}$$

$y \neq 0$ (gdy $y = 0$, to $z = x$, $x^2 \neq 8 + 6i$)

$x = \frac{3}{y}$, $\frac{9}{y^2} - y^2 = 8$

$y^4 + 8y^2 - 9 = 0$, $\Delta = 100$

$y^2 = 1$, $y = \pm 1$

$y = 1$, $x = \frac{3}{1} = 3$ $\quad$ $y = -1$, $x = \frac{3}{-1} = -3$

$z = 3 + i \vee z = -3 - i$

$3 + 1 \cdot i$ $\quad$ $-3 + (-1) \cdot i$

III sposób: postać algebraiczna

$8 + 6i = 9 + 6i - 1 =$
$= 3^2 + 2 \cdot 3 \cdot i + i^2 =$
$= (3 + i)^2$

$z^2 = (3+i)^2$

$z = 3 + i \vee z = -3 - i$

$k = 0$ $\quad \frac{\varphi}{n}$

Twierdzenie 2.3.3. Jeśli $n \in \mathbb{N}$, $w \in \mathbb{C} \setminus \{0\}$, $w = r(\cos \varphi + i \sin \varphi)$, to wówczas równanie $z^n = w$ posiada n różnych rozwiązań. Rozwiązania te mają postać

$k = n$ $\quad$ $\frac{\varphi + 2n\pi}{n} = \frac{\varphi}{n} + 2\pi$

$z^n - w = 0$

$$z_k = \sqrt[n]{r}\left(\cos \frac{\varphi + 2k\pi}{n} + i \sin \frac{\varphi + 2k\pi}{n}\right), \quad k = 0, 1, \ldots, n - 1.$$

Dowód. Niech $z = \rho(\cos \alpha + i \sin \alpha)$, wówczas

$$z^n = w \Leftrightarrow \rho^n(\cos n\alpha + i \sin n\alpha) = r(\cos \varphi + i \sin \varphi) \Leftrightarrow \begin{cases} \rho^n = r \\ n\alpha = \varphi + 2k\pi, \ k \in \mathbb{Z} \end{cases}.$$

Otrzymujemy $z_k = \sqrt[n]{r}(\cos \alpha_k + i \sin \alpha_k)$, gdzie $\alpha_k = \frac{\varphi + 2k\pi}{n}$, $k = 0, 1, \ldots, n - 1$. □

Symbolem $\sqrt[n]{w}$ oznaczamy zbiór wszystkich rozwiązań równania. Zatem

$$\sqrt[n]{w} = \{z \in \mathbb{C} : z^n = w\} = \{z_0, z_1, \ldots, z_{n-1}\}.$$

n pierwiastków

Przykład 2.3.4. Rozwiąż równanie $z^5 = \sqrt{8} - i\sqrt{24}$.
Niech $z = \rho(\cos \alpha + i \sin \alpha)$ oraz $w = \sqrt{8} - i\sqrt{24}$.
Obliczamy $|w| = \sqrt{32} = 4\sqrt{2}$, skąd $w = 4\sqrt{2}(\frac{1}{2} - \frac{\sqrt{3}}{2}i)$. Zatem

→ 5 rozwiązań $\{z_0, z_1, z_2, z_3, z_4\}$

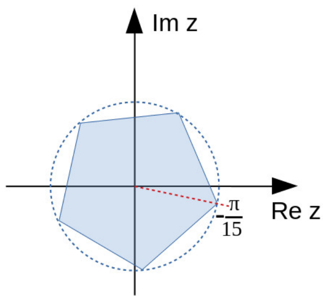
$\cos\varphi$ $\quad$ $\sin\varphi$ $\quad$ IV ćw.

$$z^5 = w \Leftrightarrow \rho^5(\cos 5\alpha + i \sin 5\alpha) = 4\sqrt{2}(\cos(-\tfrac{\pi}{3}) + i \sin(-\tfrac{\pi}{3})) \Leftrightarrow \begin{cases} \rho^5 = 4\sqrt{2} = (\sqrt{2})^5 \\ 5\alpha = -\frac{\pi}{3} + 2k\pi, \ k \in \{0, 1, 2, 3, 4\} \end{cases}.$$

Stąd $\rho = \sqrt{2}$, $\alpha_k = -\frac{\pi}{15} + \frac{2}{5}k\pi$ oraz $z_k = \sqrt{2}(\cos \alpha_k + i \sin \alpha_k)$, gdzie $k \in \{0, 1, 2, 3, 4\}$.

Interpretacja geometryczna pierwiastka z liczby zespolonej

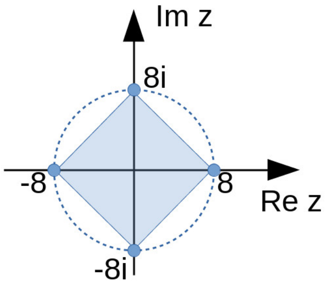
Liczby $z_0, z_1, \ldots, z_{n-1}$ będące rozwiązaniami równania $z^n = w$ stanowią wierzchołki n-kąta foremnego, wpisanego w koło o środku $z = 0$ i promieniu $\sqrt[n]{r}$.



Przykład 2.3.5. Rozwiąż równanie $z^4 = (\sqrt{3} - i)^{12}$.

Równanie ma 4 rozwiązania z_0, z_1, z_2, z_3. Będą one wierzchołkami kwadratu.

$z^4 = \left((\sqrt{3} - i)^3\right)^4$
Niech $z_0 = (\sqrt{3} - i)^3 = 3\sqrt{3} - 9i - 3\sqrt{3} + i = -8i$.
Kolejne wierzchołki kwadratu otrzymujemy przez obrót o kąt $\frac{\pi}{2}$, co odpowiada mnożeniu przez $i = e^{i\frac{\pi}{2}}$.
$z_1 = z_0 \cdot i = 8, \quad z_2 = z_1 \cdot i = 8i, \quad x_3 = z_2 \cdot i = -8$



Uwaga 2.3.6. Rozwiązywanie równań w $\mathbb{R}$ i w $\mathbb{C}$

w $\mathbb{R}$	w $\mathbb{C}$
$\sqrt{9} = 3$	$\sqrt{9} = \{-3, 3\}$
$\sqrt{-1}$ nie istnieje	$\sqrt{-1} = \{-i, i\}$
$\sqrt[4]{1} = 1$	$\sqrt[4]{1} = \{-1, 1, -i, i\}$
$\sqrt{x^2} = \|x\|$	$\sqrt{z^2} = \{-z, z\}$

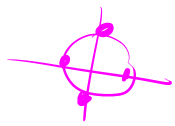
$x \in \mathbb{R} \wedge x^2 = -1$

$x \in \mathbb{R} \wedge x^4 = 1$

$z^2 = 9$

$z \in \mathbb{C} \wedge z^2 = -1$

$z \in \mathbb{C} \wedge z^4 = 1$



Równania wielomianowe

Rozważmy wielomian zmiennej zespolonej z stopnia n.
$W(z) = c_n z^n + c_{n-1} z^{n-1} + \ldots + c_1 z + c_0, \quad c_0, \ldots, c_n \in \mathbb{C}, \quad c_n \neq 0$

Definicja 2.3.7. Liczbę $z_0 \in \mathbb{C}$ nazywamy *pierwiastkiem wielomianu* W, jeżeli $W(z_0) = 0$.

Twierdzenie 2.3.8 (Bézout)**.** Liczba $z_0 \in \mathbb{C}$ jest pierwiastkiem niezerowego wielomianu W wtedy i tylko wtedy gdy istnieje wielomian P taki, że $W(z) = (z - z_0)P(z)$.

Dowód. Dzieląc przez dwumian $z - z_0$, otrzymujemy $W(z) = (z - z_0)P(z) + const$. Stąd $W(z_0) = 0 \;\Leftrightarrow\; W(z) = (z - z_0)P(z)$. $\square$

Niech $k \in \mathbb{N}$.