

1 Liczby zespolone

1.1 Dlaczego nie wystarczają liczby rzeczywiste

W dziejach systemów liczbowych, niejednokrotnie trzeba było rozszerzać istniejące – wynikało to z naturalnych zapotrzebowań.

- Liczby naturalne $\mathbb{N} = \{1, 2, 3, \dots\}$ z działaniami dodawania i mnożenia; są one zawsze wykonalne. Natomiast działanie odwrotne do dodawania, tzn. odejmowanie, jest *nie zawsze* wykonalne w zbiorze \mathbb{N} , np. równanie: $x + 3 = 1$ nie ma rozwiązań w \mathbb{N} . Można jednak sprawić, by odejmowanie stało się wykonalne, *rozszerzając* zbiór \mathbb{N} o wszystkie rozwiązania równań postaci $x + a = 0$, $a \in \mathbb{N}$.
- W zbiorze $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ jest już wykonalne odejmowanie, natomiast nie zawsze jest wykonalna operacja odwrotna do mnożenia, tzn. dzielenie; innymi słowy, równanie postaci: $ax = 1$, $a \neq 0$, nie zawsze ma rozwiązanie w liczbach całkowitych. I znów można zapewnić wykonalność dzielenia, dołączając do \mathbb{Z} rozwiązania równań postaci $ax = 1$, $a \neq 0$. Wynikiem jest zbiór liczb *wymiernych* \mathbb{Q} jako zbioru ułamków nieskracalnych $\frac{p}{q}$, $p, q \in \mathbb{Z}$.
- W zbiorze \mathbb{Q} (tzn. liczb postaci $\frac{p}{q}$, gdzie $p, q \in \mathbb{Z}$) są już wykonalne dodawanie, odejmowanie, mnożenie i dzielenie. Można jednak wprowadzić jeszcze operację *potęgowania* (wywodzącą się z mnożenia): $a^n = a \cdot a \cdot \dots \cdot a$ (n razy). I znów okazuje się, że operacja odwrotna do potęgowania, tzn. *pierwiastkowanie* (tzn. szukanie, dla danej liczby $a \in \mathbb{Q}$, takiej liczby x , że $x^n = a$), *nie zawsze* jest wykonalne (np. $\sqrt{2} \notin \mathbb{Q}$; czy Czytelnik pamięta /może zrekonstruować dowód?)
Zbiór liczb wymiernych można rozszerzać na różne sposoby; najważniejszy z nich to dołączenie do \mathbb{Q} wszystkich *granic ciągów zbieżnych* o wyrazach wymiernych; prowadzi to do zbioru liczb rzeczywistych. W zbiorze liczb rzeczywistych wyciąganie pierwiastków jest już wykonalne (jeśli są to pierwiastki parzyste, to można je wyciągać jedynie z liczb nieujemnych).

Jednak w zbiorze liczb rzeczywistych mamy jeszcze jeden problem z pierwiastkami: Pierwiastki (parzystych stopni) z liczb *ujemnych*.

Rozpatrzmy podnoszenie do kwadratu i wyciąganie pierwiastka drugiego stopnia. To pierwsze jest zawsze wykonalne i jego wynikiem jest liczba *nieujemna*. Powoduje to, że wyciąganie pierwiastka jest wykonalne tylko dla liczby *nieujemnej*. Tak więc, pozostając w obrębie liczb rzeczywistych, nie ma sensu wyrażenie

$$\sqrt{-1}, \tag{1}$$

gdyż nie istnieje taka liczba rzeczywista, która podniesiona do kwadratu dałaby liczbę ujemną (tu: -1).

Tym niemniej, taki “bezsensowny” czy “nieistniejący” obiekt jak $\sqrt{-1}$ pojawiał się kilkakrotnie w dziejach (średniowiecznej i renesansowej) matematyki i nie można go było ignorować. Problem nabrzmiał w *XVI* wieku, kiedy odkryto metodę rozwiązywania równań trzeciego stopnia:

$$ax^3 + bx^2 + cx + d = 0,$$

gdzie a, b, c, d są liczbami rzeczywistymi. Dla $a \neq 0$, zawsze istnieje przynajmniej jeden pierwiastek tego równania, będący liczbą rzeczywistą.

W XVI w. znaleziono metodę znajdowania rozwiązań (pierwiastków) takich równań dla dowolnych parametrów a, b, c, d , zwaną *metodą Cardano* (choć wcześniej metodę rozwiązywania znaleźli też Tartaglia i Scipio del Ferro). Cechą charakterystyczną tej metody był jednak fakt, że – mimo iż rozwiązanie było rzeczywiste – aby je otrzymać, trzeba było użyć “nieistniejącej” liczby $\sqrt{-1}$.

Pokażemy to na przykładzie.

Weźmy równanie:

$$x^3 - 3\sqrt[3]{2}x + 2 = 0.$$

Metoda Cardano daje rozwiązanie w postaci: $x = a + b$, gdzie $a = \sqrt[3]{-1 + \sqrt{-1}}$, $b = \sqrt[3]{-1 - \sqrt{-1}}$. Wygląda – zapewne – strasznie; ale nie taki diabeł straszny! Sprawdźmy najspierw, że x spełnia nasze równanie. Mamy:

$$\begin{aligned} x^3 &= (a + b)^3 = a^3 + b^3 + 3ab(a + b) = -1 + \sqrt{-1} + (-1) - \sqrt{-1} + 3ab \cdot x = \\ &= -2 + 3x\sqrt[3]{(-1)^2 - (\sqrt{-1})^2} = -2 + 3x\sqrt[3]{1 - (-1)} = -2 + 3x\sqrt[3]{2}; \end{aligned}$$

zatem $x^3 - 3x\sqrt[3]{2}x + 2 = 0$ – tak więc x spełnia wyjściowe równanie.

A ile “tak naprawdę” wynosi x ? (“Tak naprawdę” czyli jako liczba rzeczywista). Otóż mamy:

$$(1 + \sqrt{-1})^3 = -2 + 2\sqrt{-1}, \quad (1 - \sqrt{-1})^3 = -2 - 2\sqrt{-1};$$

tak więc, wyciągając pierwiastek trzeciego stopnia, możemy napisać:

$$\sqrt[3]{(-1)^2 + (\sqrt{-1})^2} = \frac{1 + \sqrt{-1}}{\sqrt[3]{2}}, \quad \sqrt[3]{(-1)^2 - (\sqrt{-1})^2} = \frac{1 - \sqrt{-1}}{\sqrt[3]{2}},$$

zatem

$$x = \frac{1 + \sqrt{-1}}{\sqrt[3]{2}} + \frac{1 - \sqrt{-1}}{\sqrt[3]{2}} = \frac{2}{\sqrt[3]{2}} = \sqrt[3]{4};$$

sprawdźmy, że liczba x zapisana w tej postaci spełnia wyjściowe równanie: $4 - 3\sqrt[3]{2}\sqrt[3]{4} + 2 = 0$.

Można by zapytać, czemu używaliśmy “zakazanych” obiektów, takich jak $\sqrt{-1}$, skoro koniec końców i tak otrzymaliśmy rozwiązanie rzeczywiste? Otóż nie udawało się znaleźć metody, która by pozwalała otrzymać rozwiązanie i operowała *wyłącznie* na liczbach rzeczywistych.

Morał z tej całej sytuacji jest taki, że aby otrzymać rozwiązanie rzeczywiste, trzeba było przejść przez “zakazany obszar”, gdzie pojawia się “nieistniejący” (urojony) obiekt $\sqrt{-1}$.

Skoro więc taki obiekt, jak $\sqrt{-1}$, okazuje swoją użyteczność, to może nie brońmy się przed nim i pozwólmy mu zaistnieć? Oczywiście, nie jest wyjściem z sytuacji przyjęcie go za liczbę rzeczywistą. Ale gdyby spróbować rozszerzyć pojęcie liczby rzeczywistej, tak by to – ogólniejsze – pojęcie dopuszczało też takie byty jak $\sqrt{-1}$.

Czy można tak rozszerzyć zbiór liczb rzeczywistych, aby to rozszerzenie zawierało też takie byty jak $\sqrt{-1}$? Odpowiedź jest pozytywna; zanim jednak o tym powiemy, wyliczmy najpierw własności dodawania i mnożenia, co doprowadzi do pojęcia *ciała*; oraz sprecyzujmy co rozumiemy przez “rozszerzenie”.

1.2 Ciała

W zbiorach takich, jak \mathbb{Q} oraz \mathbb{R} , wykonalne są działania dodawania i mnożenia oraz ich odwrotności. Bardziej precyzyjnie można powiedzieć, że \mathbb{Q} oraz \mathbb{R} są przykładami *ciał*.

Definicja. *Ciałem* nazywamy zbiór \mathbb{K} , w którym można wykonywać działania dodawania: “+” i mnożenia “·”, takie, że \mathbb{K} jest zamknięty względem tych działań (tzn. nie wyprowadzają one poza zbiór \mathbb{K}). “+” i “·” spełniają warunki:

- *łączność*: $(a + b) + c = a + (b + c)$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- *przemienność*: $a + b = b + a$, $a \cdot b = b \cdot a$.
- *istnienie elementu neutralnego* (dla “+” i “·”): $a + 0 = a$, $a \cdot 1 = a$, przy czym $1 \neq 0$.
- *istnienie elementu przeciwnego (odwrotnego) do danego*: $a + (-a) = 0$, $a \cdot a^{-1} = 1$ (dla $a \neq 0$).
- *rozdzielność mnożenia względem dodawania*: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Definicja. *Rozszerzeniem* ciała \mathbb{K}_0 przez ciało \mathbb{K} nazywamy takie ciało \mathbb{K} , że $\mathbb{K}_0 \subset \mathbb{K}$ oraz działania w \mathbb{K} stosowane do elementów \mathbb{K}_0 pokrywają się z działaniami w \mathbb{K}_0 . Mówimy też wtedy, że ciało \mathbb{K}_0 jest *podciałem* ciała \mathbb{K} .

Dwa przykłady ciał, które już znamy, to liczby wymierne \mathbb{Q} i rzeczywiste \mathbb{R} . Tutaj \mathbb{R} jest rozszerzeniem \mathbb{Q} . **Inne przykłady:**

1. Ciało Z_2 , tzn. zbiór $\{0, 1\}$ z działaniami: $0 + 0 = 0, 0 + 1 = 1 + 0 = 1, 1 + 1 = 0, 0 \cdot 0 = 0, 0 \cdot 1 = 1 + 0 = 0, 1 \cdot 1 = 1$, jest ciałem (proszę sprawdzić!). Elementami neutralnymi są: 0 dla dodawania oraz 1 dla mnożenia. Ciało Z_2 jest podzbiorem \mathbb{R} , natomiast *nie jest* podciałem \mathbb{R} .
2. Zbiór liczb postaci: $a + b\sqrt{2}$, gdzie a, b są liczbami wymiernymi, jest ciałem liczbowym. Oznaczamy je $Q(\sqrt{2})$; jest ono rozszerzeniem ciała liczb wymiernych. (Proszę sprawdzić te stwierdzenia!)
3. Zbiór liczb postaci: $a + b\sqrt[3]{2}$, gdzie a, b są liczbami wymiernymi, *nie jest* ciałem liczbowym (dlaczego?).
4. Natomiast zbiór liczb postaci: $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, gdzie a, b, c są liczbami wymiernymi, jest już ciałem liczbowym. (proszę sprawdzić!)

Nasz problem rozszerzenia ciała R możemy więc doprecyzować tak: *Znaleźć rozszerzenie ciała \mathbb{R} zawierające element, którego kwadrat jest równy -1 .*

Stwierdzenie. Jeśli $\tilde{\mathbb{K}}$ jest takim rozszerzeniem, zaś i jest elementem takim, że $i^2 = -1$, to podzbiór $\hat{\mathbb{C}} \in \tilde{\mathbb{K}}$

$$\hat{\mathbb{C}} := \{a + bi : a, b \in \mathbb{R}\} \quad (2)$$

jest zamknięty ze względu na dodawanie, mnożenie i branie elementu odwrotnego, więc jest podciałem $\tilde{\mathbb{K}}$, w szczególności jest też ciałem.

Dowód: Operacje dodawania, mnożenia i brania elementu odwrotnego, stosowane do elementów $\hat{\mathbb{C}}$, nie wyprowadzają poza ten podzbiór (własność *zamkniętości*). Wynika to z wzorów:

$$(a + bi) + (c + di) = (a + c) + (b + d)i; \quad (3)$$

$$(a + bi) \cdot (c + di) = a \cdot c - b \cdot d + (ad + bc)i; \quad (4)$$

$$-(a + bi) = (-a) + (-b)i; \quad (5)$$

$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i \quad (6)$$

Operacje te określają w podzbiorku $\hat{\mathbb{C}}$ strukturę podciała.

Ponadto widać, że wszystkie działania na elementach postaci $a + bi$ nie zależą od rozszerzenia; są one dane wzorami (3)–(6), które nie odwołują się w żaden sposób do rozszerzenia.

1.3 Konstrukcja ciała liczb zespolonych

Wprowadźmy w zbiorze $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ par liczb rzeczywistych działanie dodawania i mnożenia w następujący sposób:

$$(a, b) + (c, d) = (a + b, c + d), \quad (7)$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc). \quad (8)$$

Można sprawdzić bezpośrednimi rachunkami, że tak określona struktura jest ciałem. Zerem jest tu para $(0, 0)$; jedyneką: $(1, 0)$; elementem przeciwnym do (a, b) jest $(-a, -b)$, zaś element odwrotny do (a, b) to $(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$.

Tak zdefiniowane ciało nazywamy *ciałem liczb zespolonych* i oznaczamy jako \mathbb{C} . Daje ono rozwiązanie naszego problemu (tzn. rozszerzenia ciała liczb rzeczywistych). Zawieranie się ciała liczb rzeczywistych w \mathbb{C} jako podciała dane jest przez utożsamienie $a \in \mathbb{R}$ z liczbą zespoloną $(a, 0) \in \mathbb{C}$, natomiast elementem takim, że $i^2 = -1$, można wziąć $i := (0, 1)$. Mając to utożsamienie, dostajemy prostszą do rachunków postać liczby zespolonej:

$$(a, b) = (a, 0) + (b, 0)(0, 1) = a + bi. \quad (9)$$

(W ten sposób dokonaliśmy utożsamienia \mathbb{C} z $\hat{\mathbb{C}}$). Postać liczby zespolonej jako pary jest mniej wygodna do rachunków, ale prowadzi do wygodnej interpretacji liczby zespolonej jako *punktu na płaszczyźnie*. Bowiem na iloczyn kartezjański $\mathbb{R} \times \mathbb{R}$ można patrzeć jako na płaszczyznę właśnie; w ten sposób liczba zespolona (a, b) będzie wektorem o składowej “ x ”-owej równej a oraz składowej “ y ” równej b . Taki sposób patrzenia na liczby zespolone podał Gauss na przełomie XVIII i XIX w.

1.4 Sprzężenie zespolone

Ważną operacją w ciele liczb zespolonych jest *sprzężenie zespolone*, określane jako:

$$z = a + bi \rightarrow \bar{z} := a - bi. \quad (10)$$

Łatwo sprawdzić (bezpośrednim rachunkiem) następujące własności operacji sprzężenia zespolonego:

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2, \quad \overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2; \quad \frac{\bar{z}_1}{z_2} = \frac{\bar{z}_1}{\bar{z}_2}; \quad \overline{\bar{z}} = z.$$

Niech $z = a + bi$. Wprowadźmy oznaczenia:

$$\Re z := a, \quad \Im z := b; \quad (11)$$

nazywamy je odpowiednio: częścią *rzeczywistą* i *urojoną* liczby z . Mamy:

$$\Re z = \frac{z + \bar{z}}{2}, \quad \Im z = \frac{z - \bar{z}}{2i}.$$

1.5 Postać trygonometryczna

Liczbę zespoloną $a + bi$ można przedstawić jako punkt na płaszczyźnie \mathbb{R}^2 o współrzędnych kartezjańskich (a, b) lub jako wektor o tych składowych. Dodawanie liczb zespolonych odpowiada dodawaniu wektorów.

Punkty na płaszczyźnie możemy też opisywać innymi współrzędnymi- *biegunowymi*: (r, ϕ) . Przejście od współrzędnych kartezjańskich do biegunowych dane jest przez wyrażenia:

$$r = \sqrt{a^2 + b^2}; \quad \cos \phi = \frac{a}{\sqrt{a^2 + b^2}}; \quad \sin \phi = \frac{b}{\sqrt{a^2 + b^2}}$$

Definicja. Jeśli $z \neq 0$, to $\phi \in \mathbb{R}$ takie, że

$$\cos \phi = \frac{a}{\sqrt{a^2 + b^2}}; \quad \sin \phi = \frac{b}{\sqrt{a^2 + b^2}}$$

nazywamy *argumentem* liczby z i oznaczamy przez $\arg z$.

Zauważmy, że argument liczby zespolonej wyznaczony jest z dokładnością do wielokrotności 2π . Argument ϕ liczby z spełniającej nierówność $0 \leq \phi < 2\pi$ nazywamy *argumentem głównym* i oznaczamy $\text{Arg } z$.

Przejście od współrzędnych biegunowych do kartezjańskich dane jest wyrażeniami:

$$a = r \cos \phi; \quad b = r \sin \phi$$

Liczbę zespoloną $z = a + bi$ można więc równoważnie przedstawić w postaci

$$z = r(\cos \phi + i \sin \phi),$$

nazywanej *reprezentacją trygonometryczną* liczby zespolonej z .

Przykład. Niech $z_1 = 1 + i$; mamy: $z_1 = \sqrt{2}(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i) = \sqrt{2}(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4})$; promień dla liczby z_1 jest równy $\sqrt{2}$, zaś argument $\text{Arg } z_1 = \frac{\pi}{4}$.

1.6 Moduł i jego własności

Definicja. *Modułem* $|z|$ liczby zespolonej $z = a + bi$ nazywamy

$$|z| = \sqrt{a^2 + b^2} \tag{12}$$

Bezpośrednio z definicji i z postaci trygonometrycznej liczby zespolonej $z = a + bi = r(\cos \phi + i \sin \phi)$ wynikają własności

- $|z| \in \mathbb{R} \cup \{0\}$,
- $|z| = r$.

Stwierdzenie. Zachodzą związki:

1. $|z|^2 = z\bar{z}$,
2. $|z_1 z_2| = |z_1| \cdot |z_2|$,
3. $|\bar{z}| = |z|$,
4. $|\text{Re } z| \leq |z|$, $|\text{Im } z| \leq |z|$; tym bardziej: $\text{Re } z \leq |z|$, $\text{Im } z \leq |z|$.
5. $\frac{|z_1|}{|z_2|} = \left| \frac{z_1}{z_2} \right|$,

$$6. \arg(z_1 z_2) = \arg z_1 + \arg z_2,$$

$$7. \arg \bar{z} = -\arg z.$$

Dowód:

1. Niech $z = a + ib$, gdzie $a, b \in \mathbb{R}$. Z bezpośredniego rachunku mamy:

$$z\bar{z} = (a + ib)(a - ib) = a^2 + b^2 = |z|^2.$$

2. Udowodniona właśnie równość mówi że $z\bar{z} = |z|^2$; zastosujmy ją do $z = z_1 z_2$:

$$|z_1 z_2|^2 = z_1 z_2 \overline{z_1 z_2} = z_1 \bar{z}_1 z_2 \bar{z}_2 = |z_1|^2 |z_2|^2.$$

3. Oczywiście.

4. Niech $z = a + bi$. Mamy: $|\operatorname{Re} z| = |a| \leq \sqrt{a^2 + b^2} = |z|$. Drugą nierówność pokazujemy analogicznie.

5. Mamy $1 = z \frac{1}{z}$. Biorąc moduły obu stron i korzystając z 2) mamy: $1 = |z| \left| \frac{1}{z} \right|$. Zatem $\frac{1}{|z|} = \left| \frac{1}{z} \right|$. Stąd i z 2) wynika 4).

6. Niech $z_i = r_i(\cos \phi_i + i \sin \phi_i)$, $i = 1, 2$. Mamy:

$$\begin{aligned} z_1 z_2 &= r_1(\cos \phi_1 + i \sin \phi_1) \cdot r_2(\cos \phi_2 + i \sin \phi_2) \\ &= r_1 r_2 [(\cos \phi_1 \cos \phi_2 - \sin \phi_1 \sin \phi_2) + i(\cos \phi_1 \sin \phi_2 + \cos \phi_2 \sin \phi_1)] \\ &= r_1 r_2 [\cos(\phi_1 + \phi_2) + i \sin(\phi_1 + \phi_2)] \end{aligned}$$

skąd wynika 5). Powyższą równość można też wypowiedzieć słowami: "Przy mnożeniu liczb zespolonych promienie się mnożą a argumenty dodają".

7. W reprezentacji biegunowej:

$$\bar{z} = r(\cos \phi - i \sin \phi) = r(\cos(-\phi) + i \sin(-\phi))$$

Wniosek (wzór de Moivre'a). Jeżeli $z = r(\cos \phi + i \sin \phi)$, to dla $n \in \mathbb{N}$

$$z^n = r^n [\cos(n\phi) + i \sin(n\phi)].$$

Uwaga. Wygodne jest zastosowanie następującego skrótowego zapisu liczby postaci $(\cos \phi + i \sin \phi)$:

$$\cos \phi + i \sin \phi = e^{i\phi}.$$

Mamy:

$$e^{i(\phi+\psi)} = e^{i\phi} e^{i\psi}, \quad \overline{e^{i\phi}} = e^{-i\phi}.$$

W chwili obecnej, symbol $e^{i\phi}$ jest jedynie wygodnym *oznaczeniem* i nie ma on żadnego związku z liczbą e i funkcją wykładniczą. Związek ten pojawi się dopiero na analizie, stając się *twierdzeniem*.

Stwierdzenie. Dla dowolnych $z_1, z_2 \in \mathbb{R}$ zachodzą nierówności:

1. $|z_1 + z_2| \leq |z_1| + |z_2|$,
- 1'. $|z_1 + z_2 + \dots + z_n| \leq |z_1| + |z_2| + \dots + |z_n|$
2. $||z_1| - |z_2|| \leq |z_1 - z_2|$.

Dowód:

1. Weźmy kwadrat lewej strony nierówności:

$$\begin{aligned}
 |z_1 + z_2|^2 &= (z_1 + z_2) \cdot \overline{(z_1 + z_2)} = z_1\bar{z}_1 + z_2\bar{z}_1 + z_1\bar{z}_2 + z_2\bar{z}_2 \\
 &= |z_1|^2 + z_2\bar{z}_1 + z_1\bar{z}_2 + |z_2|^2 = |z_1|^2 + z_2\bar{z}_1 + \overline{z_1\bar{z}_2} + |z_2|^2 \\
 &= |z_1|^2 + 2\operatorname{Re}(z_1\bar{z}_2) + |z_2|^2 \leq |z_1|^2 + 2|\operatorname{Re}(z_1\bar{z}_2)| + |z_2|^2 \\
 &\leq |z_1|^2 + 2|(z_1\bar{z}_2)| + |z_2|^2 = |z_1|^2 + 2|z_1| \cdot |z_2| + |z_2|^2 = (|z_1| + |z_2|)^2
 \end{aligned}$$

(wykorzystaliśmy tu p. 4) poprzedniego stwierdzenia).

- 1'. Dowód indukcyjny, którego pierwszy krok stanowi powyższa nierówność.
2. Z udowodnionej właśnie nierówności 1. wynika

$$|z_1| = |z_1 - z_2 + z_2| \leq |z_1 - z_2| + |z_2|,$$

$$|z_2| = |z_2 - z_1 + z_1| \leq |z_2 - z_1| + |z_1|,$$

skąd

$$|z_1| - |z_2| \leq |z_1 - z_2|,$$

$$|z_2| - |z_1| \leq |z_1 - z_2|,$$

i teza.

1.7 Pierwiastkowanie liczb zespolonych

Definicja. Niech $w \in \mathbb{R}$. *Pierwiastkiem* stopnia n z liczby w nazywamy taką liczbę zespoloną z , że $z^n = w$.

Stwierdzenie. Niech $n \in \mathbb{N}$. Każda niezerowa liczba zespolona posiada $w \in \mathbb{R}$ dokładnie n różnych pierwiastków n -tego stopnia. Jeśli $w = r(\cos \phi + i \sin \phi)$, to są one dane wzorami

$$z_k = \sqrt[n]{r} \left(\cos \frac{\phi + 2k\pi}{n} + i \sin \frac{\phi + 2k\pi}{n} \right) = \sqrt[n]{r} e^{i \frac{\phi + 2k\pi}{n}}, \quad k = 0, 1, \dots, n-1 \quad (13)$$

gdzie $\sqrt[n]{r}$ – pierwiastek arytmetyczny.

Dowód: Liczba $z = |z|(\cos \alpha + i \sin \alpha)$ jest takim pierwiastkiem

$$\iff |z| = \sqrt[n]{r} \text{ oraz } n\alpha = \phi + 2k\pi \text{ dla pewnego } k \in \mathbb{Z}$$

$$\iff |z| = \sqrt[n]{r} \text{ oraz } \alpha = \frac{\phi + 2k\pi}{n} \text{ dla pewnego } k \in \mathbb{Z}.$$

Dwie liczby całkowite k i k' dają równoważne argumenty $\alpha = \frac{\phi + 2k\pi}{n}$ i $\alpha' = \frac{\phi + 2k'\pi}{n}$

$$\iff \frac{\phi + 2k\pi}{n} - \frac{\phi + 2k'\pi}{n} \text{ jest wielokrotnością } 2\pi$$

$$\iff k - k' \text{ jest wielokrotnością } n.$$

Stąd wynika, że wszystkie różne pierwiastki otrzymamy dla $k = 0, 1, \dots, n-1$.

Przykład. Weźmy $w = -4$ i obliczmy $\sqrt[4]{-4}$. Mamy: $w = (\sqrt{2})^4(-1+0i) = (\sqrt{2})^4(\cos \pi + i \sin \pi)$. Istnieją cztery pierwiastki:

$$k = 0 : \quad z_0 = (\sqrt{2}) \left[\cos \left(\frac{\pi + 0 \cdot 2\pi}{4} \right) + i \sin \left(\frac{\pi + 0 \cdot 2\pi}{4} \right) \right] = 1 + i$$

$$k = 1 : \quad z_0 = (\sqrt{2}) \left[\cos \left(\frac{\pi + 1 \cdot 2\pi}{4} \right) + i \sin \left(\frac{\pi + 1 \cdot 2\pi}{4} \right) \right] = -1 + i$$

$$k = 2 : \quad z_0 = (\sqrt{2}) \left[\cos \left(\frac{\pi + 2 \cdot 2\pi}{4} \right) + i \sin \left(\frac{\pi + 2 \cdot 2\pi}{4} \right) \right] = -1 - i$$

$$k = 3 : \quad z_0 = (\sqrt{2}) \left[\cos \left(\frac{\pi + 3 \cdot 2\pi}{4} \right) + i \sin \left(\frac{\pi + 3 \cdot 2\pi}{4} \right) \right] = 1 - i$$

Przykład. Obliczmy pierwiastki n -tego stopnia z 1. Promień liczby 1 jest równy 1, a argument $\text{Arg}=0$. Mamy więc n pierwiastków, danych wyrażeniami:

$$\epsilon_k = \left[\cos \left(\frac{2k\pi}{n} \right) + i \sin \left(\frac{2k\pi}{n} \right) \right], \quad k = 0, 1, \dots, n-1.$$

Wszystkie te pierwiastki leżą na okręgu jednostkowym o środku w punkcie $(0, 0)$ układu współrzędnych, w wierzchołkach n -kąta foremnego.

Uwaga. Mamy: $\epsilon_k = (\epsilon_1)^k$.

Uwaga. Jeśli z jest *którymkolwiek* pierwiastkiem z liczby zespolonej $w \neq 0$, to **wszystkie** pierwiastki n -tego stopnia można otrzymać z z mnożąc ją przez wszystkie ϵ_k . Mamy więc wszystkie te pierwiastki dane wzorem równoważnym z (13)

$$z, z\epsilon_1, z\epsilon_2, \dots, z\epsilon_{n-1}.$$

1.8 Zasadnicze twierdzenie algebry

Twierdzenie. Każde równanie n -tego stopnia

$$q(z) = z^n + c_{n-1}z^{n-1} + \dots + c_1z + c_0 = 0 \quad (14)$$

gdzie $n \in \mathbb{N}$, $c_j \in \mathbb{C}$ ($j = 0, \dots, n-1$) ma rozwiązanie w \mathbb{C} .

Dygresja. Ideę dowodu zilustrujemy najpierw w prostszym przypadku wersji rzeczywistej powyższego twierdzenia:

Każde równanie nieparzystego stopnia $n = 2k + 1$

$$p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$$

gdzie $k \geq 0$, $a_j \in \mathbb{R}$ ($j = 0, \dots, n-1$) ma rozwiązanie w \mathbb{R} .

Tu idea dowodu jest następująca: Dla $x \rightarrow +\infty$, również $p(x) \rightarrow +\infty$, tak więc istnieje x_+ takie, że dla dowolnego $x > x_+$, $p(x) > 0$. Analogicznie, dla $x \rightarrow -\infty$ zachodzi: $p(x) \rightarrow -\infty$, tak więc istnieje x_- takie, że dla dowolnego $x < x_-$, $p(x) < 0$. Ponieważ funkcja $p(x)$ jest ciągła, to na odcinku $[x_-, x_+]$ funkcja $p(x)$ przyjmuje wszystkie wartości pośrednie, a w szczególności istnieje takie x_0 , że $f(x_0) = 0$.

W przypadku równania (14) zarówno argument jak i wartość funkcji są liczbami zespolonymi, więc nie można użyć powyższego rozumowania bezpośrednio; jednak uogólnienie jest naturalne i wtedy dowód "idzie".

Idea dowodu. (Nie będzie to dowód jako taki, gdyż argumentacja odwołuje się do kilku faktów z analizy, prawdopodobnie nie znany w tej chwili Czytelnikowi. W tej chwili znajomość tych faktów musi zastąpić Jego/Jej intuicja.)

1) Rozpatrzmy najspierw odwzorowanie $\mathbb{C} \rightarrow \mathbb{C} : z \rightarrow z^n$. Weźmy w przestrzeni argumentów okrąg $\gamma_1 = C_0^R$ (okrąg o środku w punkcie 0 i promieniu R); jego obrazem jest również okrąg $C_0^{R^n}$. Obiegnijmy naokoło okrąg γ_1 . Zmiana argumentu w *przeciwobrazie* wynosi 2π , zaś w *obrazie* wynosi $2n\pi$.

2) Pokażemy, że podobna sytuacja ma miejsce, gdy rozpatrujemy dowolne odwzorowanie $\mathbb{C} \rightarrow \mathbb{C} : z \rightarrow q(z)$ dla dostatecznie dużego R . Rozpatrzmy znów obraz okręgu $\gamma_1 = C_0^R : \gamma_2 = q(\gamma_1)$. Obraz ten jest pewną zamkniętą krzywą *ciągłą*. Obiegnijmy znów naokoło okrąg γ_1 . Ile będzie wynosił przyrost argumentu w *obrazie*? Obliczmy argument $q(z)$:

$$\arg(q(z)) = \arg(z^n + c_{n-1}z^{n-1} + \dots + c_1z + c_0) = \arg(z^n) + \arg\left(1 + \frac{c_{n-1}}{z} + \dots + \frac{c_1}{z^{n-1}} + \frac{c_0}{z^n}\right)$$

Przyrost argumentu $\Delta(q(z))$, gdy z obiega okrąg γ_1 , wynosi:

$$\Delta(q(z)) = 2\pi n + \Delta \arg\left(1 + \frac{c_{n-1}}{z} + \dots + \frac{c_1}{z^{n-1}} + \frac{c_0}{z^n}\right)$$

Mamy oszacowanie (pamiętajmy że $z = Re^{i\phi}$):

$$\begin{aligned} \left|1 + \frac{c_{n-1}}{z} + \dots + \frac{c_1}{z^{n-1}} + \frac{c_0}{z^n}\right| &\leq 1 + \left|\frac{c_{n-1}}{z}\right| + \dots + \left|\frac{c_1}{z^{n-1}}\right| + \left|\frac{c_0}{z^n}\right| \\ &= 1 + \frac{|c_{n-1}|}{R} + \dots + \frac{|c_1|}{R^{n-1}} + \frac{|c_0|}{R^n} \end{aligned}$$

Biorąc teraz R dostatecznie duże, otrzymujemy, że dla dowolnego $z = Re^{i\phi}$ liczby: $\left(1 + \frac{c_{n-1}}{z} + \dots + \frac{c_1}{z^{n-1}} + \frac{c_0}{z^n}\right)$ leżą wewnątrz okręgu o środku w punkcie 1 i promieniu $\frac{1}{2}$. Tak więc zmiana argumentu tej liczby wynosi zero, gdy obiegamy okrąg γ_1 w przeciwobrazie.

Sytuację możemy podsumować mówiąc, że: *Przyrost argumentu $q(z)$, gdy z obiega okrąg γ_1 , wynosi $2\pi n$.*

3) Z drugiej strony, mamy: $q(0) = c_0$, zakładamy zaś, że $c_0 \neq 0$, gdyż w innym przypadku dowód jest skończony.

4) Weźmy teraz rodzinę okręgów o promieniu malejącym od R do zera i rozpatrujemy obrazy tych okręgów. Zmiana obrazu okręgu o promieniu r jest *ciągła*, gdy zmieniamy promień. Z 2) i 3) wnioskujemy, że gdzieś po drodze, gdy deformujemy okręgi, przechodząc od promienia R do zera, obraz pewnego okręgu “zahaczy” o zero.

Uwaga. Pokazaliśmy, że dowolne równanie algebraiczne n -tego stopnia posiada przynajmniej jeden pierwiastek. A co z możliwością jego *obliczenia*? Innymi słowy, czy dla dowolnego równania algebraicznego da się napisać wzory na jego pierwiastki, analogiczne do wzorów Cardana dla $n = 3$?

Okazuje się, że odpowiedź jest *negatywna*. Wzory na pierwiastki daje się jeszcze napisać dla równania 4. stopnia (znalazł je L. Ferrari w XVI w.) Rozwiązań dla równań wyższych stopni bezskutecznie poszukiwano przez następne dwa wieki, aż na początku XIX w. niezależnie N. Abel oraz E. Galois odkryli, że *dla równań stopnia wyższego niż czwarty, w ogólnym przypadku pierwiastki nie wyrażają się za pomocą skończonej kombinacji działań arytmetycznych i operacji wyciągania pierwiastka.*

Później okazało się, że *można* napisać wyrażenia na pierwiastki równania dowolnego stopnia, jeśli rozszerzy się “asortyment” funkcji, które dopuszczamy w wyrażeniach na pierwiastki. Pierwiastki dowolnego równania można wyrazić przez tzw. *funkcje modularne* (do ich zdefiniowania i zbadania konieczna jest dość zaawansowana analiza zespolona). Pokazano to pod koniec XIX wieku (Ch. Hermite, F. Klein, F. Lindemann, C. Jordan).