Geometria z Algebrą Liniową I

Arkadiusz Męcel

WYKŁAD 3, 3.11.2020 r.

Na ostatnim wykładzie:

- działania dwuargumentowe,
- ciała,
- podciała,
- układy równań nad ciałem,
- ciało liczb zespolonych.

Slogan dnia: liczby zespolone są ważne, bo ujawniają głębokie związki geometrii, algebry (o tym coś powiem), analizy oraz teorii liczb itd. (o tym nie powiem).

Przypomnienie

Ciało liczb zespolonych to piątka $(\mathbb{R}^2, +, \cdot, (0,0), (1,0))$, którego elementami są wszystkie uporządkowane pary liczb rzeczywistych, w którym działania $+, \cdot$ określone są wzorami:

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

a elementami neutralnymi tych działań są odpowiednio $(0,0), (1,0)$. Ciało to oznaczamy jako $\mathbb{C}$.

Notacja:

- liczbę zespoloną $(0, 1)$ oznaczamy jako i,

Przypomnienie

Ciało liczb zespolonych to piątka $(\mathbb{R}^2, +, \cdot, (0,0), (1,0))$, którego elementami są wszystkie uporządkowane pary liczb rzeczywistych, w którym działania $+, \cdot$ określone są wzorami:

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

a elementami neutralnymi tych działań są odpowiednio $(0,0), (1,0)$. Ciało to oznaczamy jako $\mathbb{C}$.

Notacja:

- liczbę zespoloną $(0, 1)$ oznaczamy jako i,
- liczbę zespoloną $(a, 0)$ zapisujemy jako a, dla $a \in \mathbb{R}$,

Przypomnienie

Ciało liczb zespolonych to piątka $(\mathbb{R}^2, +, \cdot, (0,0), (1,0))$, którego elementami są wszystkie uporządkowane pary liczb rzeczywistych, w którym działania $+, \cdot$ określone są wzorami:

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

a elementami neutralnymi tych działań są odpowiednio $(0,0), (1,0)$. Ciało to oznaczamy jako $\mathbb{C}$.

Notacja:

- liczbę zespoloną $(0,1)$ oznaczamy jako i,
- liczbę zespoloną $(a,0)$ zapisujemy jako a, dla $a \in \mathbb{R}$,
- liczbę zespoloną $z = (a,b)$ zapisujemy jako $a + bi$,

Przypomnienie

Ciało liczb zespolonych to piątka $(\mathbb{R}^2, +, \cdot, (0,0), (1,0))$, którego elementami są wszystkie uporządkowane pary liczb rzeczywistych, w którym działania $+, \cdot$ określone są wzorami:

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

a elementami neutralnymi tych działań są odpowiednio $(0,0), (1,0)$. Ciało to oznaczamy jako $\mathbb{C}$.

Notacja:

- liczbę zespoloną $(0,1)$ oznaczamy jako i,
- liczbę zespoloną $(a,0)$ zapisujemy jako a, dla $a \in \mathbb{R}$,
- liczbę zespoloną $z = (a,b)$ zapisujemy jako $a + bi$,
- $\mathrm{Re}(z) = a, \quad \mathrm{Im}(z) = b, \quad |z| = \sqrt{a^2 + b^2}, \quad \overline{z} = a - bi.$

Postać trygonometryczna liczby zespolonej

- $z = a + bi = \sqrt{a^2 + b^2}\left(\frac{a}{\sqrt{a^2+b^2}} + \frac{b}{\sqrt{a^2+b^2}}i\right).$

Postać trygonometryczna liczby zespolonej

- $z = a + bi = \sqrt{a^2 + b^2}\left(\frac{a}{\sqrt{a^2+b^2}} + \frac{b}{\sqrt{a^2+b^2}} i\right)$.
- $\left(\frac{a}{\sqrt{a^2+b^2}}\right)^2 + \left(\frac{b}{\sqrt{a^2+b^2}}\right)^2 = 1.$

Postać trygonometryczna liczby zespolonej

- $z = a + bi = \sqrt{a^2 + b^2}\left(\frac{a}{\sqrt{a^2+b^2}} + \frac{b}{\sqrt{a^2+b^2}} i\right).$
- $\left(\frac{a}{\sqrt{a^2+b^2}}\right)^2 + \left(\frac{b}{\sqrt{a^2+b^2}}\right)^2 = 1.$
- Istnieje dokładnie jedno $\varphi \in [0, 2\pi)$, że:

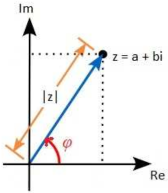
$$\cos(\varphi) = \frac{a}{\sqrt{a^2 + b^2}}, \quad \sin(\varphi) = \frac{b}{\sqrt{a^2 + b^2}}.$$

Definicja 1.

Niech $z = a + bi$ będzie liczbą zespoloną. Liczbę rzeczywistą φ taką, że

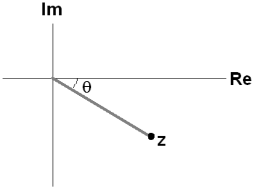
$$z = |z|(\cos(\varphi) + i \cdot \sin(\varphi))$$

nazywamy **argumentem liczby zespolonej** z i oznaczamy $\arg(z)$.

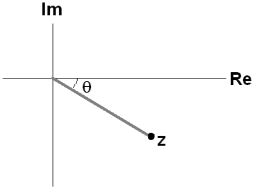


Rys. 1. Płaszczyzna zespolona. Moduł i argument liczby zespolonej. Źródło: Wikipedia (z modyfikacjami).

Przykład: $z = \sqrt{3} - i$.

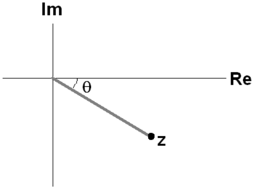


Przykład: $z = \sqrt{3} - i$.



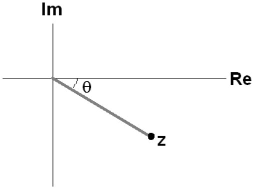
- $|z| = \sqrt{\sqrt{3}^2 + (-1)^2} = 2$.

Przykład: $z = \sqrt{3} - i$.



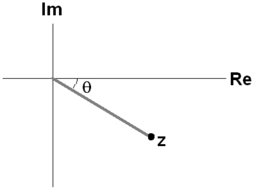
- $|z| = \sqrt{\sqrt{3}^2 + (-1)^2} = 2$.
- $z = 2\left(\frac{\sqrt{3}}{2} - \frac{1}{2} \cdot i\right)$.

Przykład: $z = \sqrt{3} - i$.



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

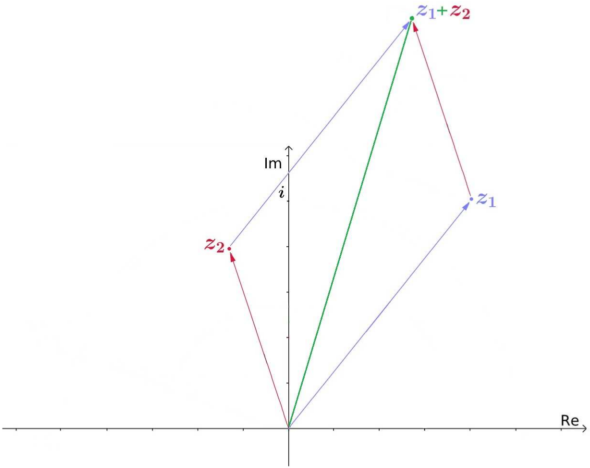
Przykład: $z = \sqrt{3} - i$.



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

Interpretacja geometryczna dodawania liczb zespolonych:

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



Rys. 2. Interpretacja geometryczna dodawania liczb zespolonych.

Interpretacja geometryczna mnożenia liczb zespolonych:

$$z_1 \cdot z_2 = |z_1|(\cos\varphi + i\sin\varphi) \cdot |z_2|(\cos\psi + i\sin\psi) =$$

Interpretacja geometryczna mnożenia liczb zespolonych:

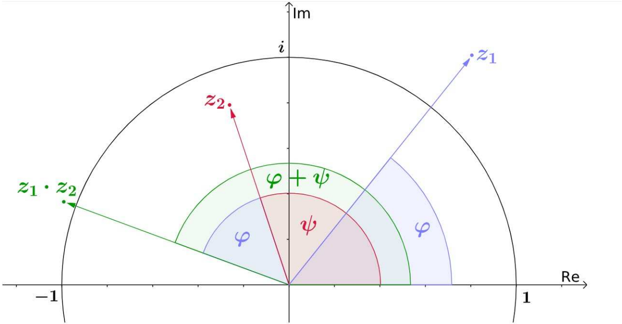
$$
\begin{aligned}
z_1 \cdot z_2 &= |z_1|(\cos \varphi + i \sin \varphi) \cdot |z_2|(\cos \psi + i \sin \psi) = \\
&= |z_1||z_2|(\cos \varphi \cos \psi - \sin \varphi \sin \psi + i(\sin \varphi \cos \psi + \cos \varphi \sin \psi) =
\end{aligned}
$$

Interpretacja geometryczna mnożenia liczb zespolonych:

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

Interpretacja geometryczna mnożenia liczb zespolonych:

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

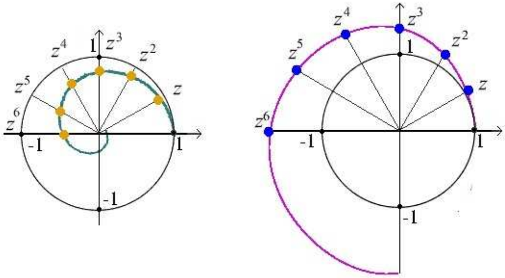


Rys. 3. Interpretacja geometryczna mnożenia liczb zespolonych.

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. 4. Interpretacja geometryczna potęgowania liczb zespolonych. Źródło: http://www.suitcaseofdreams.net/.

- Są dokładnie 3 liczby zespolone, które podniesione do potęgi 3 dają 2:

$$\sqrt[3]{2}(\cos 0 + i \sin 0), \quad \sqrt[3]{2}(\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}), \quad \sqrt[3]{2}(\cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3}).$$

- Są dokładnie 3 liczby zespolone, które podniesione do potęgi 3 dają 2:

$$\sqrt[3]{2}(\cos 0 + i \sin 0), \quad \sqrt[3]{2}(\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}), \quad \sqrt[3]{2}(\cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3}).$$

- Są dokładnie 4 liczby zespolone, które podniesione do potęgi 4 dają i:

$$\cos \frac{\pi}{8} + i \sin \frac{\pi}{8}, \quad \cos \frac{5\pi}{8} + i \sin \frac{5\pi}{8}, \quad \cos \frac{9\pi}{8} + i \sin \frac{9\pi}{8}, \quad \cos \frac{13\pi}{8} + i \sin \frac{13\pi}{8}.$$

Uwaga-Definicja

Niech n będzie liczbą całkowitą dodatnią oraz $w = |w|(\cos\theta + i\sin\theta) \neq 0$. Wówczas liczby postaci:

$$\sqrt[n]{|w|}\left(\cos\frac{\theta+2\pi k}{n} + i\sin\frac{\theta+2\pi k}{n}\right), \quad \text{dla } k = 0, 1, \ldots, n-1.$$

nazywamy **pierwiastkami stopnia** n **z** w.

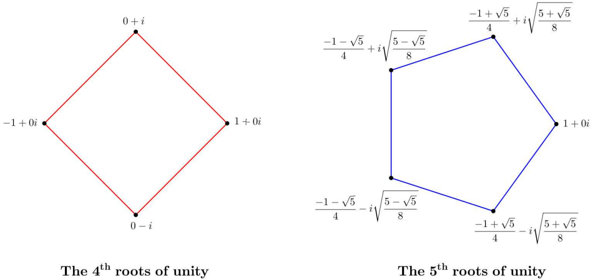
W szczególności pierwiastki stopnia n z 1 to liczby:

$$\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \quad \text{dla } k = 0, 1, \ldots, n-1.$$

Definicja 3.

Mówimy, że liczba $z \in \mathbb{C}$ jest **pierwiastkiem pierwotnym** stopnia n z 1, jeśli z jest pierwiastkiem stopnia n z 1, ale nie jest pierwiastkiem z 1 stopnia m, gdzie $m < n$.

Obserwacja geometryczna: pierwiastki stopnia *n* z liczby zespolonej $w \neq 0$ są wierzchołkami *n*-kąta foremnego, np.



Rys. 7. Interpretacja geometryczna pierwiastków stopnia 4 i 5 z 1. Źródło: brilliant.org.

Kilka (przykładowych) wniosków dotyczących geometrii płaszczyzny $\mathbb{C}$:

Kilka (przykładowych) wniosków dotyczących geometrii płaszczyzny $\mathbb{C}$:

- Liczba $|z_1 - z_2|$ oznacza standardową odległość euklidesową punktów z_1 i z_2.

Kilka (przykładowych) wniosków dotyczących geometrii płaszczyzny $\mathbb{C}$:

- Liczba $|z_1 - z_2|$ oznacza standardową odległość euklidesową punktów z_1 i z_2.
- Dla ustalonego $z_0 \in \mathbb{C}$ oraz $r \geq 0$ zbiór

  $$\{z \in \mathbb{C}\,,\ |z - z_0| = r\}$$

  jest okręgiem o środku z_0 i promieniu r.

Kilka (przykładowych) wniosków dotyczących geometrii płaszczyzny $\mathbb{C}$:

- Liczba $|z_1 - z_2|$ oznacza standardową odległość euklidesową punktów z_1 i z_2.
- Dla ustalonego $z_0 \in \mathbb{C}$ oraz $r \geq 0$ zbiór

$$\{z \in \mathbb{C}\,,\ |z - z_0| = r\}$$

  jest okręgiem o środku z_0 i promieniu r.
- Dla dwóch różnych punktów $z_1, z_2 \in \mathbb{C}$ zbiór punktów postaci:

$$\left\{z \in \mathbb{C}\,,\ \frac{z - z_1}{z_2 - z_1} \in \mathbb{R}\right\} = \{z \in \mathbb{C}\,,\ \arg(z - z_1) = \arg(z_2 - z_1)\}$$

  jest prostą przechodzącą przez punkty z_1, z_2.

Kilka (przykładowych) wniosków dotyczących geometrii płaszczyzny $\mathbb{C}$:

- Liczba $|z_1 - z_2|$ oznacza standardową odległość euklidesową punktów z_1 i z_2.
- Dla ustalonego $z_0 \in \mathbb{C}$ oraz $r \geq 0$ zbiór

  $$\{z \in \mathbb{C}\,,\ |z - z_0| = r\}$$

  jest okręgiem o środku z_0 i promieniu r.
- Dla dwóch różnych punktów $z_1, z_2 \in \mathbb{C}$ zbiór punktów postaci:

  $$\left\{z \in \mathbb{C}\,,\ \frac{z - z_1}{z_2 - z_1} \in \mathbb{R}\right\} = \{z \in \mathbb{C}\,,\ \arg(z - z_1) = \arg(z_2 - z_1)\}$$

  jest prostą przechodzącą przez punkty z_1, z_2.

  Podobnie można charakteryzować równoległość i prostopadłość odcinków, równość kątów, cykliczność czwórek punktów i wiele innych, patrz np. `https://web.evanchen.cc/handouts/cmplx/en-cmplx.pdf`.

Kilka (przykładowych) wniosków dotyczących geometrii płaszczyzny zespolonej:

- Funkcja $f : \mathbb{C} \to \mathbb{C}$ zadana wzorem

$$f(z) = z + (1 + 2 \cdot i)$$

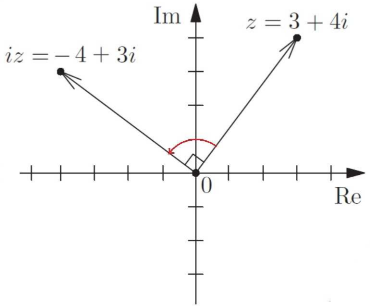
  to przesunięcie płaszczyzny o wektor $(1, 2)$.

Kilka (przykładowych) wniosków dotyczących geometrii płaszczyzny zespolonej:

- Funkcja $f : \mathbb{C} \to \mathbb{C}$ zadana wzorem

$$f(z) = i \cdot z$$

to obrót płaszczyzny wokół zera o $\frac{\pi}{2}$.



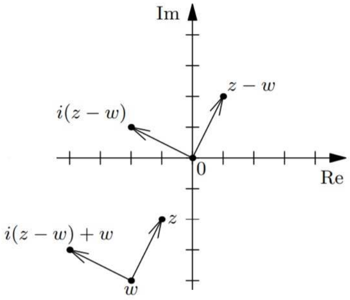
Rys. 5. Interpretacja geometryczna obrotu o kąt 90°. Źródło: Evan Chen.

Kilka (przykładowych) wniosków dotyczących geometrii płaszczyzny zespolonej:

- Funkcja $f : \mathbb{C} \to \mathbb{C}$ zadana wzorem

$$f(z) = i \cdot (z - w) + w$$

to obrót płaszczyzny wokół w o $\frac{\pi}{2}$.



Rys. 6. Interpretacja geometryczna obrotu o kąt 90° wokół w. Źródło: Evan Chen.

Definicja 4.

Wielomianem zmiennej x o współczynnikach w ciele K nazywamy wyrażenie:

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,$$

gdzie n jest dowolną liczbą całkowitą nieujemną oraz $a_0, a_1, \ldots, a_n \in K$.

Definicja 4.

Wielomianem zmiennej x o współczynnikach w ciele K nazywamy wyrażenie:

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,$$

gdzie n jest dowolną liczbą całkowitą nieujemną oraz $a_0, a_1, \ldots, a_n \in K$.

Utożsamiamy przy tym takie napisy, jeśli różnią się o składniki postaci $0 \cdot x^i$ oraz jeśli różnią się kolejnością składników.

Definicja 4.

Wielomianem zmiennej x o współczynnikach w ciele K nazywamy wyrażenie:

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,$$

gdzie n jest dowolną liczbą całkowitą nieujemną oraz $a_0, a_1, \ldots, a_n \in K$.

Utożsamiamy przy tym takie napisy, jeśli różnią się o składniki postaci $0 \cdot x^i$ oraz jeśli różnią się kolejnością składników.

Elementy a_i nazywamy **współczynnikami** wielomianu. Zbiór wielomianów o współczynnikach z ciała K oznaczamy przez $K[x]$.

Definicja 4.

Wielomianem zmiennej x o współczynnikach w ciele K nazywamy wyrażenie:

$$a_0 + a_1x + a_2x^2 + \ldots + a_nx^n,$$

gdzie n jest dowolną liczbą całkowitą nieujemną oraz $a_0, a_1, \ldots, a_n \in K$.

Utożsamiamy przy tym takie napisy, jeśli różnią się o składniki postaci $0 \cdot x^i$ oraz jeśli różnią się kolejnością składników.

Elementy a_i nazywamy **współczynnikami** wielomianu. Zbiór wielomianów o współczynnikach z ciała K oznaczamy przez $K[x]$.

Stopniem wielomianu $f = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, ozn $\deg(f)$, nazywamy

- największe takie i, że $a_i \neq 0$, jeśli istnieje (owo największe a_i nazywamy **współczynnikiem wiodącym** wielomianu f),
- $-\infty$, jeśli $a_1 = a_2 = \ldots = a_n = 0$. Wtedy wielomian nazywamy zerowym.

Definicja 5.

Niech $f = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ będzie wielomianem o współczynnikach w ciele K. Funkcję $f : K \to K$ daną wzorem $f(s) = a_0 + a_1 s + a_2 s^2 + \ldots + a_n s^n$ nazwiemy **funkcją wielomianową** odpowiadającą wielomianowi w.

Pierwiastkami wielomianu f (inaczej: miejscami zerowymi) nazywamy wszystkie takie $s \in K$, że $f(s) = 0$.

Definicja 5.

Niech $f = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ będzie wielomianem o współczynnikach w ciele K. Funkcję $f : K \to K$ daną wzorem $f(s) = a_0 + a_1s + a_2s^2 + \ldots + a_ns^n$ nazwiemy **funkcją wielomianową** odpowiadającą wielomianowi w.

Pierwiastkami wielomianu f (inaczej: miejscami zerowymi) nazywamy wszystkie takie $s \in K$, że $f(s) = 0$.

Przykłady.

- Funkcja $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ odpowiadająca $x^3 + 2x \in \mathbb{Z}_3[x]$ jest zerowa.

Definicja 5.

Niech $f = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ będzie wielomianem o współczynnikach w ciele K. Funkcję $f : K \to K$ daną wzorem $f(s) = a_0 + a_1s + a_2s^2 + \ldots + a_ns^n$ nazwiemy **funkcją wielomianową** odpowiadającą wielomianowi w.

Pierwiastkami wielomianu f (inaczej: miejscami zerowymi) nazywamy wszystkie takie $s \in K$, że $f(s) = 0$.

Przykłady.

- Funkcja $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ odpowiadająca $x^3 + 2x \in \mathbb{Z}_3[x]$ jest zerowa.
- Wielomian $w = x^2 + x + 1 \in \mathbb{R}[x]$ nie ma pierwiastków,

Definicja 5.

Niech $f = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ będzie wielomianem o współczynnikach w ciele K. Funkcję $f : K \to K$ daną wzorem $f(s) = a_0 + a_1s + a_2s^2 + \ldots + a_ns^n$ nazwiemy **funkcją wielomianową** odpowiadającą wielomianowi w.

Pierwiastkami wielomianu f (inaczej: miejscami zerowymi) nazywamy wszystkie takie $s \in K$, że $f(s) = 0$.

Przykłady.

- Funkcja $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ odpowiadająca $x^3 + 2x \in \mathbb{Z}_3[x]$ jest zerowa.
- Wielomian $w = x^2 + x + 1 \in \mathbb{R}[x]$ nie ma pierwiastków,
- Wielomian $w = x^2 + x + 1 \in \mathbb{C}[x]$ ma dwa pierwiastki.

Twierdzenie 1 (O dzieleniu z resztą).

Niech f, g będą wielomianami o współczynnikach z ciała K. Załóżmy ponadto, że g nie jest wielomianem zerowym. Wówczas istnieją wielomiany q i r takie, że:

$$f = q \cdot g + r, \quad \deg(r) < \deg(g). \tag{1}$$

Ponadto wielomiany q, r są wyznaczone jednoznacznie.

Twierdzenie 1 (O dzieleniu z resztą).

Niech f, g będą wielomianami o współczynnikach z ciała K. Załóżmy ponadto, że g nie jest wielomianem zerowym. Wówczas istnieją wielomiany q i r takie, że:

$$f = q \cdot g + r, \quad \deg(r) < \deg(g). \tag{2}$$

Ponadto wielomiany q, r są wyznaczone jednoznacznie.

Plan dowodu.

1. Wykażemy, że każdych $f, g \in K[x]$, gdzie $g \neq 0$ istnieją q, r takie, że (2).
2. Wykażemy, że wielomiany q, r są wyznaczone jednoznacznie.

Dowód *istnienia* wielomianów q, r dla pary f, g.

- Jeśli $\deg(g) > \deg(f)$, to $f = 0 \cdot g + f$.

Dowód *istnienia* wielomianów q, r dla pary f, g.

- Jeśli $\deg(g) > \deg(f)$, to $f = 0 \cdot g + f$.
- Jeśli $\deg(g) \leq \deg(f)$, to rozumowanie jest indukcją ze względu na stopień wielomianu f.

Dowód *istnienia* wielomianów q, r dla pary f, g.

- Jeśli $\deg(g) > \deg(f)$, to $f = 0 \cdot g + f$.
- Jeśli $\deg(g) \leq \deg(f)$, to rozumowanie jest indukcją ze względu na stopień wielomianu f.
- Krok bazowy: $\deg(f) = 0$.
  Z założenia $g \neq 0$, więc $\deg(g) = 0$. Wtedy $\frac{f}{g} \in K$ oraz: $f = \frac{f}{g} \cdot g + 0$.

Dowód *istnienia* wielomianów q, r dla pary f, g, cd.

- Krok indukcyjny. Niech $n = \deg(f)$ oraz $m = \deg(g) \leq n$ oraz

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

Dowód *istnienia* wielomianów q, r dla pary f, g, cd.

- Krok indukcyjny. Niech $n = \deg(f)$ oraz $m = \deg(g) \leq n$ oraz

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

- Definiujemy wielomian $\tilde{f}$ stopnia $\leq n - 1$ postaci:

$$\tilde{f} = b_m \cdot f - a_n x^{n-m} \cdot g = (b_m \cdot a_n x^n + \ldots) - (a_n b_m x^n + \ldots).$$

Dowód *istnienia* wielomianów q, r dla pary f, g, cd.

- Krok indukcyjny. Niech $n = \deg(f)$ oraz $m = \deg(g) \leq n$ oraz

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

- Definiujemy wielomian $\tilde{f}$ stopnia $\leq n - 1$ postaci:

$$\tilde{f} = b_m \cdot f - a_n x^{n-m} \cdot g = (b_m \cdot a_n x^n + \ldots) - (a_n b_m x^n + \ldots).$$

- Z założenia indukcyjnego istnieją wielomiany $\tilde{q}$ oraz $\tilde{r}$ takie, że

$$\tilde{f} = \tilde{q} \cdot g + \tilde{r}, \quad \text{gdzie} \quad \deg(g) > \deg(\tilde{r}).$$

Dowód *istnienia* wielomianów q, r dla pary f, g, cd.

- Krok indukcyjny. Niech $n = \deg(f)$ oraz $m = \deg(g) \leq n$ oraz

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

- Definiujemy wielomian $\tilde{f}$ stopnia $\leq n - 1$ postaci:

$$\tilde{f} = b_m \cdot f - a_n x^{n-m} \cdot g = (b_m \cdot a_n x^n + \ldots) - (a_n b_m x^n + \ldots).$$

- Z założenia indukcyjnego istnieją wielomiany $\tilde{q}$ oraz $\tilde{r}$ takie, że

$$\tilde{f} = \tilde{q} \cdot g + \tilde{r}, \quad \text{gdzie} \quad \deg(g) > \deg(\tilde{r}).$$

- Z definicji $\tilde{f}$ mamy $b_m f - a_n x^{n-m} g = \tilde{q} \cdot g + \tilde{r}$. Stąd wynika teza indukcji:

$$f = \left(\frac{a_n x^{n-m} + \tilde{q}}{b_m} \right) g + \frac{\tilde{r}}{b_m}.$$

Dowód *jednoznaczności* rozkładu $f = q \cdot g + r$, gdzie $\deg(g) > \deg(r)$.

- Załóżmy, że dla pewnej pary f, g wielomianów istnieją wielomiany q, q', r, r' takie, że $\deg(g) > \deg(r)$, $\deg(g) > \deg(r')$ oraz

$$f = qg + r = q'g + r'.$$

Dowód *jednoznaczności* rozkładu $f = q \cdot g + r$, gdzie $\deg(g) > \deg(r)$.

- Załóżmy, że dla pewnej pary f, g wielomianów istnieją wielomiany q, q', r, r' takie, że $\deg(g) > \deg(r)$, $\deg(g) > \deg(r')$ oraz

$$f = qg + r = q'g + r'.$$

- Zatem $(q - q')g = r' - r$.

Dowód *jednoznaczności* rozkładu $f = q \cdot g + r$, gdzie $\deg(g) > \deg(r)$.

- Załóżmy, że dla pewnej pary f, g wielomianów istnieją wielomiany q, q', r, r' takie, że $\deg(g) > \deg(r)$, $\deg(g) > \deg(r')$ oraz

$$f = qg + r = q'g + r'.$$

- Zatem $(q - q')g = r' - r$.
- Jeśli $q \neq q'$, to $\deg(q - q')g \geq \deg(g)$.

Dowód *jednoznaczności* rozkładu $f = q \cdot g + r$, gdzie $\deg(g) > \deg(r)$.

- Załóżmy, że dla pewnej pary f, g wielomianów istnieją wielomiany q, q', r, r' takie, że $\deg(g) > \deg(r)$, $\deg(g) > \deg(r')$ oraz

$$f = qg + r = q'g + r'.$$

- Zatem $(q - q')g = r' - r$.
- Jeśli $q \neq q'$, to $\deg(q - q')g \geq \deg(g)$.
- W rezultacie $\deg(r - r') \geq \deg(g)$.

Dowód *jednoznaczności* rozkładu $f = q \cdot g + r$, gdzie $\deg(g) > \deg(r)$.

- Załóżmy, że dla pewnej pary f, g wielomianów istnieją wielomiany q, q', r, r' takie, że $\deg(g) > \deg(r)$, $\deg(g) > \deg(r')$ oraz

$$f = qg + r = q'g + r'.$$

- Zatem $(q - q')g = r' - r$.
- Jeśli $q \neq q'$, to $\deg(q - q')g \geq \deg(g)$.
- W rezultacie $\deg(r - r') \geq \deg(g)$.
- Mamy zatem sprzeczność, bo na mocy założenia o stopniach r, r' i g:

$$\deg(r' - r) \leq \max\{\deg(r'), \deg(r)\} < \deg(g)$$

Dowód *jednoznaczności* rozkładu $f = q \cdot g + r$, gdzie $\deg(g) > \deg(r)$.

- Załóżmy, że dla pewnej pary f, g wielomianów istnieją wielomiany q, q', r, r' takie, że $\deg(g) > \deg(r)$, $\deg(g) > \deg(r')$ oraz

$$f = qg + r = q'g + r'.$$

- Zatem $(q - q')g = r' - r$.
- Jeśli $q \neq q'$, to $\deg(q - q')g \geq \deg(g)$.
- W rezultacie $\deg(r - r') \geq \deg(g)$.
- Mamy zatem sprzeczność, bo na mocy założenia o stopniach r, r' i g:

$$\deg(r' - r) \leq \max\{\deg(r'), \deg(r)\} < \deg(g)$$

- Zatem $q = q'$, co pociąga za sobą $r = r'$.

Twierdzenie 2 (Bezout).

Niech $f \in K[x]$. Następujące warunki są równoważne.

1. Element $s \in K$ jest pierwiastkiem wielomianu f.
2. Istnieje $g \in K[x]$ taki, że $f = (x - s)g$.

Twierdzenie 2 (Bezout).

Niech $f \in K[x]$. Następujące warunki są równoważne.

1. Element $s \in K$ jest pierwiastkiem wielomianu f.
2. Istnieje $g \in K[x]$ taki, że $f = (x - s)g$.

Dowód:

- Niech s będzie pierwiastkiem wielomianu f. Zgodnie z Twierdzeniem 1 istnieją wielomiany q, r takie, że $f = q(x - s) + r$, gdzie $\deg(r) < \deg(g) = 1$. A zatem r jest wielomianem stałym.

Twierdzenie 2 (Bezout).

Niech $f \in K[x]$. Następujące warunki są równoważne.

1. Element $s \in K$ jest pierwiastkiem wielomianu f.
2. Istnieje $g \in K[x]$ taki, że $f = (x - s)g$.

Dowód:

- Niech s będzie pierwiastkiem wielomianu f. Zgodnie z Twierdzeniem 1 istnieją wielomiany q, r takie, że $f = q(x - s) + r$, gdzie $\deg(r) < \deg(g) = 1$. A zatem r jest wielomianem stałym.
- Skoro s jest pierwiastkiem to $0 = f(s) = (s - s)q(s) + r(s) \Rightarrow 0 = r(s)$. Skoro r jest wielomianem stopnia 0, to $r = 0$. A zatem (1) implikuje (2).

Twierdzenie 2 (Bezout).

Niech $f \in K[x]$. Następujące warunki są równoważne.

1. Element $s \in K$ jest pierwiastkiem wielomianu f.
2. Istnieje $g \in K[x]$ taki, że $f = (x - s)g$.

Dowód:

- Niech s będzie pierwiastkiem wielomianu f. Zgodnie z Twierdzeniem 1 istnieją wielomiany q, r takie, że $f = q(x - s) + r$, gdzie $\deg(r) < \deg(g) = 1$. A zatem r jest wielomianem stałym.
- Skoro s jest pierwiastkiem to $0 = f(s) = (s - s)q(s) + r(s) \Rightarrow 0 = r(s)$. Skoro r jest wielomianem stopnia 0, to $r = 0$. A zatem (1) implikuje (2).
- Jeśli $f = (x - s)g$, dla pewnego $g \in K[x]$, to $f(s) = (s - s)g(s) = 0$.

Wniosek.

Niech $f \in K[x]$ będzie wielomianem stopnia n. Wówczas f ma co najwyżej n pierwiastków.

Wniosek.

Niech $f \in K[x]$ będzie wielomianem stopnia n. Wówczas f ma co najwyżej n pierwiastków.

Kluczowy przykład: wielomian $x^n - w \in \mathbb{C}[x]$, gdzie $w \in \mathbb{C}$.

Wniosek.

Niech $f \in K[x]$ będzie wielomianem stopnia n. Wówczas f ma co najwyżej n pierwiastków.

Kluczowy przykład: wielomian $x^n - w \in \mathbb{C}[x]$, gdzie $w \in \mathbb{C}$.

- Wielomian $x^3 - 2 \in \mathbb{C}[x]$ ma trzy (i nie więcej!) pierwiastki postaci:

$$\sqrt[3]{2}(\cos 0 + i \sin 0), \quad \sqrt[3]{2}(\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}), \quad \sqrt[3]{2}(\cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3}).$$

Wniosek.

Niech $f \in K[x]$ będzie wielomianem stopnia n. Wówczas f ma co najwyżej n pierwiastków.

Kluczowy przykład: wielomian $x^n - w \in \mathbb{C}[x]$, gdzie $w \in \mathbb{C}$.

- Wielomian $x^3 - 2 \in \mathbb{C}[x]$ ma trzy (i nie więcej!) pierwiastki postaci:

$$\sqrt[3]{2}(\cos 0 + i \sin 0), \quad \sqrt[3]{2}(\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}), \quad \sqrt[3]{2}(\cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3}).$$

- Wielomian $x^4 - i \in \mathbb{C}[x]$ ma cztery (i nie więcej!) pierwiastki postaci:

$$\cos \frac{\pi}{8} + i \sin \frac{\pi}{8}, \quad \cos \frac{5\pi}{8} + i \sin \frac{5\pi}{8}, \quad \cos \frac{9\pi}{8} + i \sin \frac{9\pi}{8}, \quad \cos \frac{13\pi}{8} + i \sin \frac{13\pi}{8}.$$

Definicja 6.

Jeśli każdy wielomian stopnia większego od 0 o współczynnikach z ciała K ma w ciele K pierwiastek, to K nazywamy **ciałem algebraicznie domkniętym**.

Definicja 6.

Jeśli każdy wielomian stopnia większego od 0 o współczynnikach z ciała K ma w ciele K pierwiastek, to K nazywamy **ciałem algebraicznie domkniętym**.

Twierdzenie 3.

Niech K będzie ciałem. Następujące warunki są równoważne.

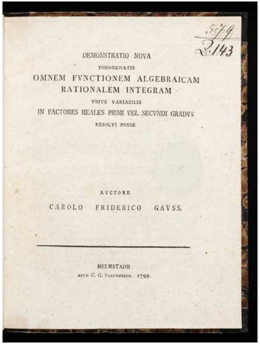
1. Ciało K jest algebraicznie domknięte.
2. Każdy wielomian stopnia > 0 o współczynnikach z K rozkłada się nad K na czynniki stopnia 1 (to znaczy: jest iloczynem wielomianów stopnia 1 o współczynnikach z K).

Dowód: ćwiczenie.

Zasadnicze Twierdzenie Algebry (Gauss, 1799)

Ciało $\mathbb{C}$ jest algebraicznie domknięte.

W przyszłości poznacie Państwo kilka dowodów.



Rys. 8. Pierwsza strona doktoratu Gaussa zawierającego (nie do końca poprawny) dowód Zasadniczego Twierdzenia Algebry.

Wniosek

Każdy wielomian $w \in \mathbb{R}[x]$ stopnia większego od 0 rozkłada się na iloczyn wielomianów stopnia pierwszego i stopnia drugiego o współczynnikach rzeczywistych.

Idea dowodu:

- Indukcja ze względu na stopień w.

Wniosek

Każdy wielomian $w \in \mathbb{R}[x]$ stopnia większego od 0 rozkłada się na iloczyn wielomianów stopnia pierwszego i stopnia drugiego o współczynnikach rzeczywistych.

Idea dowodu:

- Indukcja ze względu na stopień w.
- Dla $\deg(w) = 1$ oczywiste.

Wniosek

Każdy wielomian $w \in \mathbb{R}[x]$ stopnia większego od 0 rozkłada się na iloczyn wielomianów stopnia pierwszego i stopnia drugiego o współczynnikach rzeczywistych.

Idea dowodu:

- Indukcja ze względu na stopień w.
- Dla $\deg(w) = 1$ oczywiste.
- Jeśli $r_0 \in \mathbb{R}$ jest pierwiastkiem w, to $w = (x - r_0)g$, gdzie $g \in \mathbb{R}[x]$.

Wniosek

Każdy wielomian $w \in \mathbb{R}[x]$ stopnia większego od 0 rozkłada się na iloczyn wielomianów stopnia pierwszego i stopnia drugiego o współczynnikach rzeczywistych.

Idea dowodu:

- Indukcja ze względu na stopień w.
- Dla $\deg(w) = 1$ oczywiste.
- Jeśli $r_0 \in \mathbb{R}$ jest pierwiastkiem w, to $w = (x - r_0)g$, gdzie $g \in \mathbb{R}[x]$.
- Jeśli $z_0 \notin \mathbb{R}$ jest pierwiastkiem $w \in \mathbb{R}[x]$ traktowanego jako wielomian w $\mathbb{C}[x]$, to $\overline{z_0}$ też jest także pierwiastkiem w. Idea: dla każdych liczb zespolonych z_1, z_2 mamy $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ oraz $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$.

Wniosek

Każdy wielomian $w \in \mathbb{R}[x]$ stopnia większego od 0 rozkłada się na iloczyn wielomianów stopnia pierwszego i stopnia drugiego o współczynnikach rzeczywistych.

Idea dowodu:

- Indukcja ze względu na stopień w.
- Dla $\deg(w) = 1$ oczywiste.
- Jeśli $r_0 \in \mathbb{R}$ jest pierwiastkiem w, to $w = (x - r_0)g$, gdzie $g \in \mathbb{R}[x]$.
- Jeśli $z_0 \notin \mathbb{R}$ jest pierwiastkiem $w \in \mathbb{R}[x]$ traktowanego jako wielomian w $\mathbb{C}[x]$, to $\overline{z_0}$ też jest także pierwiastkiem w. Idea: dla każdych liczb zespolonych z_1, z_2 mamy $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ oraz $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$.
- Jeśli z_0 i $\overline{z_0}$ to pierwiastki w, wówczas

$$(x - z_0)(x - \overline{z_0}) \in \mathbb{R}[x]$$

jest dzielnikiem stopnia 2 wielomianu w.