Wielomiany i funkcje wielomianowe. Równania wielomianowe

Ostatnia aktualizacja: 4.11.2021 r.

W poprzedniej części wprowadziliśmy pojęcie ciała i skupiliśmy się omówieniu dwóch istotnych przykładów: ciała reszt z dzielenia modulo p oraz ciała liczb zespolonych. Celem tego wykładu jest przedstawienie kilku uwag dotyczących funkcji o wartościach w tych ciałach. Zagadnienie to jest w ogólności niezwykle szerokie, natomiast mając na względzie program kolejnych wykładów, ograniczymy się jedynie do tzw. funkcji wielomianowych. Zacznijmy od pojęcia wielomianu o współczynnikach w ciele.

Definicja 1. ***Wielomianem*** *zmiennej x o współczynnikach w ciele K nazywamy wyrażenie:*

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

gdzie n jest 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 $K[x]$. Jeśli wszystkie współczynniki wielomianu f są równe zero, to piszemy $f = 0$, a wielomian f nazywamy wówczas* ***wielomianem zerowym****.*

Definicja 2. *Niech $f = a_0+a_1x+a_2x^2+\ldots+a_nx^n \in K[x]$, gdzie K jest ciałem.* ***Stopniem wielomianu*** *f, ozn $\deg(f)$, nazywamy:*

- *największe takie i, że $a_i \neq 0$, o ile f nie jest wielomianem zerowym.*
- *$-\infty$, jeśli f jest wielomianem zerowym.*

Jeśli $f \neq 0$ to współczynnik $a_{\deg(f)}$ nazywamy wówczas ***współczynnikiem wiodącym*** *wielomianu f.*

Na zbiorze $K[x]$ określamy naturalne operacje dodawania i mnożenia, pochodzące[1] od K. Dla dowolnych $f = a_0 + a_1x + \ldots + a_nx^n, \quad g = b_0 + b_1x + \ldots + b_mx^m$ ze zbioru $K[x]$ kładziemy:

- $f + g = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots,$
- $f \cdot g = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \ldots + a_nb_mx^{n+m}.$

Jako ćwiczenie pozostawiamy następujące własności stopnia, związane z wprowadzonymi operacjami[2]:

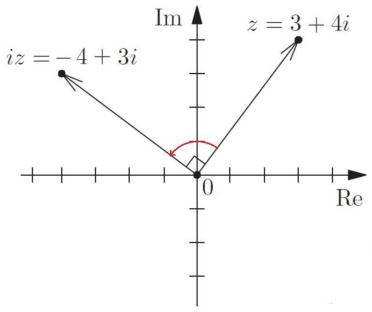
$$\deg(f + g) \leqslant \max(\deg(f), \deg(g)), \quad \deg(fg) = \deg(f) + \deg(g). \qquad (\heartsuit)$$

Definicja 3. *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 f.* ***Pierwiastkami wielomianu*** *f (inaczej: miejscami zerowymi) nazywamy wszystkie takie $s \in K$, że $f(s) = 0$.*

Uwaga. Wielomian $x^2 + x \in \mathbb{Z}_3[x]$ jest niezerowy, ale dla każdego $s \in \mathbb{Z}_2$ wyrażenie $s^2 + s$ równe jest 0. A zatem funkcja wielomianowa $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ zadana wzorem $f(x) = x^2 + x$ jest funkcją zerową[3].

Funkcje wielomianowe na $\mathbb{C}$ można interpretować jako złożenia izometrii i jednokładności. Oto przykłady.

Rozważmy funkcję $f : \mathbb{C} \to \mathbb{C}$ zadaną wzorem $f(z) = i \cdot z$ Jest to obrót płaszczyzny wokół zera o kąt $\frac{\pi}{2}$.



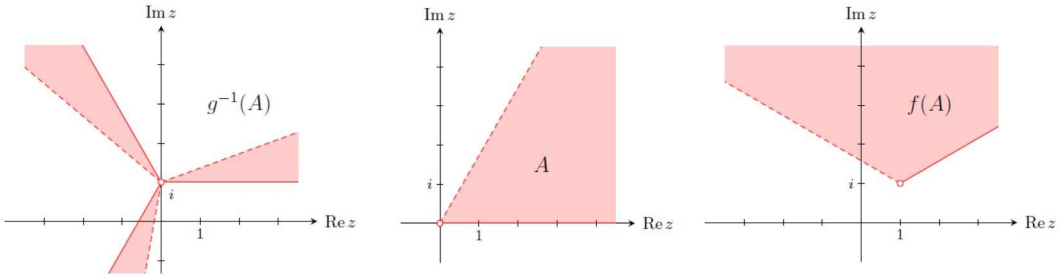
Rys. 1. Interpretacja geometryczna obrotu o kąt 90°. Źródło: E. Chen.

[1] Korzystamy z przemienności dodawania i mnożenia w K oraz z umowy, ze $x^n \cdot a = ax^n$, dla $a \in K$.

[2] Trzeba tu dodać trzy zastrzeżenia. Pierwsze – te działania mają sens także, gdy f, g są zerowe, przy naturalnych umowach typu $\max(-\infty, 1) = 1$, $-\infty + n = \infty$, $-\infty + -\infty = -\infty$. Druga – równość w pierwszej nierówności zachodzi wtedy (ale nie tylko wtedy), gdy $\deg(f) \neq \deg(g)$. Trzecia – jeśli K nie jest ciałem, wówczas tożsamość dla iloczynu trzeba zmodyfikować. Np. dla wielomianów $f, g \in \mathbb{Z}_4[x]$ postaci: $f = 2x, g = 1 + 2x$ mamy $\deg(f) = \deg(g) = 1$, ale $\deg(fg) = 1$.

[3] Morał: znając jedynie zbiór wartości f. wielomianowej $w(s)$ nie zawsze *rozpoznamy* wielomian w. Od czego to zależy?

Innym sposobem będzie rysowanie obok siebie pewnych podzbiorów płaszczyzny, ich obrazów i przeciwobrazów przy pewnych funkcjach wielomianowych. Przykłady podobne do poniższego pojawią się (wraz z odpowiednimi uzasadnieniami) na ćwiczeniach.



Rys. 2. Obraz i przeciwobraz zbioru $A = \{z \in \mathbb{C} : z \neq 0, \operatorname{Arg} z \in [0, \frac{\pi}{3})\}$ przy funkcjach $f(z) = (1 + i\sqrt{3})z^2 + 1 + i$, $g(z) = (z - i)^3$. Źródło: Ł. Kubat.

Trzeci bardzo istotny z geometrycznego punktu widzenia przykład dotyczy funkcji $f(z) = z^n$ oraz pytania dla jakich argumentów funkcja ta przyjmuje wartość $w \in \mathbb{Z}$. Odpowiedź oparta jest o wzór Movre'a

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

Zobaczmy pewne przykłady.

- 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:

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

Definicja 4. *Niech w będzie liczbą zespoloną i niech n będzie liczbą naturalną. Pierwiastki wielomianu $x^n - w \in \mathbb{C}[x]$ (czyli rozwiązania równania $x^n = w$) nazywamy **pierwiastkami stopnia n** z liczby w.*

Wnioskiem z wzoru Moivre'a są zatem również następujące formuły.

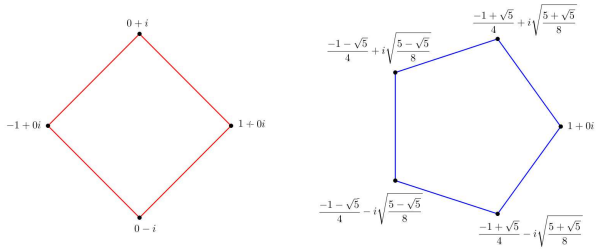
Uwaga 1. *Jeśli $w = |w|(\cos\theta + i\sin\theta) \neq 0$, to pierwiastkami stopnia n z w są liczby postaci:*

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

W szczególności pierwiastki stopnia n z 1 to liczby:

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

W interpretacji geometrycznej pierwiastki stopnia n z liczby w są wierzchołkami n-kąta foremnego.



Rys. 3. Interpretacja geometryczna pierwiastków stopnia 4 i 5 z 1. Źródło: brilliant.org.

Definicja 5. *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 $m < n$.*

Zajmiemy się teraz związkiem pomiędzy pierwiastkami wielomianu, a jego rozkładalnością na czynniki.

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:*

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

Ponadto wielomiany q, r są wyznaczone jednoznacznie.

Twierdzenie to jest skądinąd dobrze znane – choć zapewne nie dla ciał (i warto pod tym kątem obserwować dowód) – ale jest ono ważne jako fakt typu: *dla pewnych obiektów istnieją inne obiekty i są one wyznaczone jednoznacznie*. Warto dobrze zrozumieć to zagadnienie, zwłaszcza problem owej **jednoznaczności**.

Dowód. Pokażemy najpierw, że dla każdej pary $f, g \in K[x]$ takiej, że $g \neq 0$ istnieje para q, r taka, że zachodzi (1). Później wykażemy, że wielomiany q, r są wyznaczone jednoznacznie.

Niech $f, g \in K[x]$, $g \neq 0$. Zauważmy, że jeśli $\deg(g) > \deg(f)$, to za szukane wielomiany q, r można wziąć $q = 0$ oraz $r = f$. Wówczas oczywiście $\deg(r) = \deg(f) < \deg(g)$. Załóżmy dalej, że $\deg(f) \geqslant \deg(g)$. Dowód istnienia wielomianów q, r spełniających (1) jest indukcją ze względu na $\deg(f)$. Z założenia $\deg(f) \geqslant 0$, a zatem w bazowym kroku indukcji rozważamy sytuację, gdy $\deg(f) = 0$. Skoro $g \neq 0$, to $\deg(g) = 0$ i wystarczy wziąć $q = f/g$ oraz $r = 0$. Wtedy $\deg(r) < \deg(g)$. Przechodzimy wreszcie do kroku indukcyjnego. Niech $n = \deg(f)$ oraz $m = \deg(g) \leqslant n$. Niech:

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

Definiujemy **nowy wielomian** (dla niektórych tylko nowy, bo przecież Czytelnicy dodatku do wykładu pierwszego zobaczą natychmiast, że to jest właśnie S-wielomian $S(f, g)$ – tylko dla jednej zmiennej):

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

Nietrudno widzieć, że odejmujemy od siebie dwa wielomiany stopnia n o tym samym współczynniku wiodącym. Wielomian $\tilde{f}$ ma zerowy współczynnik przy x^n, a zatem $\deg(\tilde{f}) \leqslant n-1$. Z założenia indukcyjnego zastosowanego do $\tilde{f}$ wynika, że istnieją wielomiany $\tilde{q}$ oraz $\tilde{r}$ takie, że $\tilde{f} = g\tilde{q} + \tilde{r}$, $\deg(g) > \deg(\tilde{r})$ oraz:

$$b_m f - a_n x^{n-m} g = g\tilde{q} + \tilde{r}.$$

W szczególności mamy też (tu się w sposób istotny wykorzystuje założenie, że K jest ciałem!):

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

A zatem dla pary wielomianów f, g definiujemy szukane wielomiany q, r jako $q := \frac{a_n x^{n-m} + \tilde{q}}{b_m}$ oraz $r := \frac{\tilde{r}}{b_m}$. Oczywiście spełnione jest założenie $\deg(g) > \deg(r) = \deg(\tilde{r})$. Krok indukcyjny jest zatem zakończony.

Pozostaje pokazać jednoznaczność istnienia wielomianów q, r spełniających (1) dla danej pary wielomianów f, g. Będzie to (jak zwykle w takich problemach) rozumowanie nie wprost. 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

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

Wynika stąd, że:

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

Załóżmy (wbrew tezie o jednoznaczności rozkładu f), że $q \neq q'$. Mamy zatem $\deg(q - q')g \geqslant \deg(g)$. W rezultacie $\deg(r - r') \geqslant \deg(g)$. Mamy jednak $\deg(r' - r) \leqslant \max\{\deg(r'), \deg(r)\} < \deg(g)$ (założenie o stopniach r, r' i g). Otrzymaliśmy sprzeczność. A zatem musi zachodzić równość $q = q'$. Wtedy jednak zachodzi także równość $r = r'$. Dowód jednoznaczności przedstawienia (1) jest zatem zakończony. □

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. To nasz pierwszy dowód faktu typu: „*następujące warunki są równoważne*". Polegać on będzie na uzasadnieniu, że ze zdania (1) wynika zdanie (2) a następnie, że ze zdania (2) wynika zdanie (1).

Niech s będzie pierwiastkiem wielomianu f. Wykonujemy dzielenie z resztą wielomianu f przez wielomian $x - s$. 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). Implikacja z (2) do (1) jest jasna. Jeśli $f = (x - s)g$, dla pewnego $g \in K[x]$, to $f(s) = (s - s)g(s) = 0$. □

Twierdzenie Bezout jest prostym, ale niezwykle delikatnym narzędziem. Wskazuje ono bowiem na istnienie konkretnego rozkładu wielomianu na nietrywialne czynniki. Przypomnijmy, że jeśli K jest ciałem i $a, b \in K$, to warunek $ab = 0$ implikuje, że $a = 0$ lub $b = 0$. A zatem jeśli $s \in K$ jest pierwiastkiem niezerowego wielomianu $f \in K[x]$, to nie istnieją takie $g, h \in K[x]$, że s nie jest pierwiastkiem ani g, ani h oraz istnieje rozkład $f = gh$. Innymi słowy, istnienie pierwiastka s wielomianu f wymusza na **każdym** rozkładzie f na czynniki to, że jednym z nich jest $(x - s)$. Oczywiście istnieją rozkłady wielomianów na niestałe czynniki (i to jednoznaczne – co nie jest oczywiste, a o czym wspomnimy w dodatku), które nie mają pierwiastków. Np. nad $\mathbb{Q}$ mamy:

$$x^4 + 4 = (x^2 + 2)^2 - (2x)^2 = (x^2 - 2x + 2)(x^2 + 2x + 2).$$

Odnotujmy kilka obserwacji wynikających z definicji operacji na wielomianach i z twierdzenia Bezout. Są to nietrudne, ale pouczające ćwiczenia.

Wniosek 1 (Uzasadniający definicję krotności pierwiastka)**.** *Jeśli $s \in K$ nie jest pierwiastkiem wielomianów $f, g \in K[x]$ oraz dla pewnych m, n całkowitych dodatnich mamy $(x - s)^m \cdot f = (x - s)^n \cdot g$, to $m = n$ oraz $f = g$.*

Wniosek 2. *Jeśli $s \in K$ nie jest pierwiastkiem $g \in K[x]$ oraz dla pewnego $f \in K[x]$ oraz całkowitego dodatniego r mamy $f = (x - s)^r \cdot g$, to wielomian f ma o r pierwiastków więcej niż wielomian g*

Wniosek 3. *Niech $f \in K[x]$, gdzie $\deg(f) = n \geqslant 0$. Wówczas f ma co najwyżej n pierwiastków. Co więcej, jeśli f rozkłada się na iloczyn czynników stopnia 1, czyli liniowych, to rozkład ten jest jednoznaczny z dokładnością do kolejności czynników i wyrazu wiodącego.*

Druga część ostatniego wniosku jest przypadkiem szczególnym twierdzenia o jednoznaczności rozkładu wielomianów nad ciałem na tzw. czynniki nierozkładalne. Rezultat ten udowodnimy w dodatku.

Zajmiemy się teraz niezwykle ważną klasą ciał, związaną z pojęciem rozkładu na czynniki liniowe.

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. Pokażemy, że ze zdania (1) wynika zdanie (2). Zakładamy zatem, że K jest ciałem algebraicznie domkniętym. Przy pomocy dowodu indukcyjnego pokażemy, że każdy wielomian stopnia > 0 rozkłada się nad K na współczynniki liniowe. Krok bazowy indukcji jest jasny – każdy wielomian stopnia 1 da się rozłożyć na iloczyn czynników liniowych. Załóżmy prawdziwość naszego założenia dla wielomianów stopnia $n - 1$. Niech f będzie wielomianem stopnia n. Ciało K jest algebraicznie domknięte, więc f ma pierwiastek $c \in K$. Stąd $f(x) = (x - c) \cdot g(x)$, dla pewnego wielomianu $g \in K[x]$, na mocy twierdzenia Bezout. Wielomian g jest zatem stopnia $n - 1$, więc z założenia indukcyjnego g jest iloczynem czynników stopnia 1 o współczynnikach z K. Stąd f jest iloczynem czynników stopnia 1 o współczynnikach z K. Na odwrót: jeśli f jest iloczynem wielomianów stopnia 1 o współczynnikach w K, to każdy taki czynnik stopnia 1 ma pierwiastek w K, będący też pierwiastkiem wielomianu f. A zatem (2) implikuje (1). □

Z Twierdzenia Bezout wynika łatwo, że ciało algebraicznie domknięte musi być nieskończone. Okazuje się, że każde ciało jest podciałem pewnego ciała algebraicznie domkniętego. Dla przykładu, ciała $\mathbb{Q}$ oraz $\mathbb{R}$ nie są algebraicznie domknięte (np. z uwagi na wielomian $x^2 + 1$), ale jak się okazuje, są podciałami ciała liczb zespolonych, które ma tę własność. Nie jest to trywialny wynik.

Twierdzenie 4 (Zasadnicze Twierdzenie Algebry (Gauss, 1799))**.** *Ciało $\mathbb{C}$ jest algebraicznie domknięte.*

W tym momencie nie przedstawimy dowodu tego twierdzenia. Rozumowanie bazujące na argumentach czysto analitycznych będzie dla Państwa dostępne w zasadzie pod koniec semestru. Istnieje również dowód oparty o wyniki algebry liniowej, ale wymaga znajomości szeregu pojęć i faktów z drugiego semestru. Na wyższych latach studiów poznacie Państwo krótkie (m.in. algebraiczne) dowody tego rezultatu.

Wniosek 4. *Każdy wielomian w stopnia większego od 0 o współczynnikach rzeczywistych rozkłada się na iloczyn wielomianów stopnia pierwszego i stopnia drugiego o współczynnikach rzeczywistych.*

Dowód. Zaczniemy od faktu pomocniczego. Zauważmy, że jeśli $s \in \mathbb{C}$ jest pierwiastkiem wielomianu $w \in \mathbb{R}[x]$, to również $\overline{s}$ jest pierwiastkiem tego wielomianu. Istotnie, niech s będzie pierwiastkiem wielomianu

$$w = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$

gdzie $a_n, \ldots, a_0 \in \mathbb{R}$. Korzystamy z tego, że sprzężenie liczby rzeczywistej jest tą liczbą oraz z formuł $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$, $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$, prawdziwych dla dowolnych $z_1, z_2 \in \mathbb{C}$. Mamy:

$$0 = \overline{0} = \overline{a_n s^n + \ldots + a_1 s + a_0} = \overline{a_n}\overline{s^n} + \ldots + \overline{a_1 s} + \overline{a_0} = a_n(\overline{s})^n + \ldots + a_1\overline{s} + a_0.$$

Przechodzimy do dowodu wniosku. Jest to indukcja ze względu na stopień w. Dla $\deg(w) = 1$ teza jest jasna. Załóżmy, że $\deg(w) > 1$. Jeśli $r_0 \in \mathbb{R}$ jest pierwiastkiem w, to z lematu Bezout $w = (x - r_0)g$, gdzie $g \in \mathbb{R}[x]$ i teza wynika z założenia indukcyjnego zastosowanego do wielomianu g. Jeśli w nie ma pierwiastków rzeczywistych, a jedynie zespolone, to postępowanie jest następujące. Bierzemy pierwiastek z_0 wielomianu w i traktujemy w jako element $\mathbb{C}[x]$. Wówczas $\overline{z_0}$ też jest także pierwiastkiem w. 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. □

W kontekście rozwiązywania równań wielomianowych i zastosowań (także na naszym przedmiocie) warto przypomnieć/uogólnić fakt znany ze szkoły jako wzory Viete'a.

Twierdzenie 5. *Niech $x_1, x_2, x_3, \ldots, x_n$ będą pierwiastkami wielomianu $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, gdzie $a_n \neq 0$. Wówczas zachodzą równości:*

$$\begin{cases} x_1 + x_2 + \ldots + x_n = \frac{-a_{n-1}}{a_n} \\ x_1x_2 + x_1x_3 + \ldots + x_1x_n + x_2x_3 + \ldots + x_2x_n + \ldots + x_{n-1}x_n = \frac{a_{n-2}}{a_n} \\ \vdots \\ x_1x_2x_3 \ldots x_n = (-1)^n \frac{a_0}{a_n}. \end{cases}$$

Dowód. Indukcja ze względu na n. Dla n=1 dowód jest oczywisty. Załóżmy, że dla każdego wielomianu stopnia n, wzory te są prawdziwe. Rozważmy wielomian stopnia n+1, o pierwiastkach: $x_1, x_2, x_3, \ldots, x_n, x_{n+1}$. Zgodnie z twierdzeniem Bezout istnieje wielomian g(x) (którego wiodący współczynnik to 1), taki, że: $f(x) = a_{n+1} \cdot (x - x_1) \cdot g(x)$. Wielomian g jest stopnia n, i jego pierwiastkami są $x_2, x_3, \ldots, x_n, x_{n+1}$.Więcej pierwiastków, zgodnie z udowodnionym wcześniej faktem, mieć nie może. Zatem są to jego wszystkie pierwiastki. Z założenia indukcyjnego mamy zatem:

$$g(x) = x^n - (x_2 + x_3 + \ldots + x_{n+1})x^{n-1} + \ldots + (-1)^{n+1}(x_2x_3 \ldots x_{n+1}).$$

Wymnażając g w takiej postaci przez $a_{n+1} \cdot (x - x_1)$ dostajemy tezę. □

Przyjrzyjmy się przykładowemu zadaniu wykorzystującemu poznane metody.

Zadanie. Wielomian $w(x) = x^4 + ax^3 + bx^2 + cx + d$ ma współczynniki rzeczywiste oraz pierwiastki nierzeczywiste z_1, z_2, z_3, z_4. Wiadomo, że $z_1 z_2 = 13 + i$ oraz $z_3 + z_4 = 3 + 4i$. Wyznacz a, b, c, d.

Rozwiązanie. Wielomian w jest stopnia 4, a zatem z_1, z_2, z_3, z_4 są wszystkimi jego pierwiatkami. Skoro $z_1 \notin \mathbb{R}$, to jedna z liczb z_2, z_3, z_4 musi być sprzężonym do z_1 pierwiastkiem w. Jednak dla każdego $z \in \mathbb{C}$ mamy $z\overline{z} = |z|^2 \in \mathbb{R}$, a zatem $\overline{z_1} \neq z_2$, bo $z_1 z_2 \notin \mathbb{R}$. Analogicznie $\overline{z_3} \neq z_4$. Stąd $\{\overline{z_1}, \overline{z_2}\} = \{z_3, z_4\}$ (nieco dokładniej: po podzieleniu w przez $(z - z_1)(z - \overline{z_1})$ mamy wielomian, którego pierwiastkami są $z_2, \overline{z_2}$). A zatem mamy: $z_3 z_4 = \overline{z_1 z_2} = 13 - i$ oraz $z_1 + z_2 = \overline{z_3 + z_4} = 3 - 4i$. Ze wzorów Viete'a dostajemy zatem:

$$\begin{aligned} a &= -(z_1 + z_2 + z_3 + z_4) = -(3 + 4i + 3 - 4i) = -6 \\ b &= z_1z_2 + z_1z_3 + z_1z_4 + z_2z_3 + z_2z_4 + z_3z_4 = \\ &= (z_1 + z_2)(z_3 + z_4) + z_1z_2 + z_3z_4 = (3 + 4i)(3 - 4i) + (13 + i) + (13 - i) = 51 \\ c &= -(z_1z_2z_3 + z_1z_2z_4 + z_1z_3z_4 + z_2z_3z_4) = \\ &= -((z_1z_2)(z_3 + z_4) + (z_1 + z_2)(z_3z_4)) = -((13 + i)(3 + 4i) + (3 - 4i)(13 - i)) = -70 \\ d &= z_1z_2z_3z_4 = (13 + i)(13 - i) = 170. \end{aligned}$$

Uzupełnienie. O jednoznaczności rozkładu wielomianów

Jeszcze w szkole mogliśmy zauważyć podobieństwo pomiędzy teorią podzielności w zbiorze liczb całkowitych oraz w zbiorze wielomianów (o współczynnikach rzeczywistych). Mówimy bowiem o podzielności, algorytmie dzielenia z resztą, a także o największym wspólnym dzielniku czy rozkładzie na czynniki. W przyszłości, w ramach wykładu z algebry abstrakcyjnej, będziecie Państwo mogli zapoznać się dokładniej z rozmaitymi aspektami tych zagadnień i poznacie Państwo wspólny język służący do ich opisu. W ramach tego uzupełnienia ograniczymy się do kilku obserwacji, które mogą być przydatne dla osób, pragnących nieco głębiej zrozumieć znawiska, które badamy w ramach GALu.

Powiedzieliśmy już o algorytmie dzielenia z resztą i twierdzeniu Bezout. Kluczem do dalszych zagadnień jest pojęcie największego wspólnego dzielnika. W tym celu wprowadzimy kilka intuicyjnych określeń.

Definicja 7. *Niech $f = a_n x^n + \ldots + a_1 x + a_0 \in K[x]$, gdzie $\deg(f) = n \geqslant 0$.*

- *Wielomian f nazwiemy **monicznym**, jeśli $a_n = 1$.*
- *Powiemy, że $0 \neq g \in K[x]$ **dzieli** f, jeśli istnieje $h \in K[x]$ taki, że*

$$f = g \cdot h.$$

  *W takim przypadku mówimy również, że g jest **dzielnikiem** f, co zapisujemy w postaci $f \,|\, g$.*

- *Wielomian moniczny $d \in K[x]$ nazwiemy największym wspólnym dzielnikiem[4] (NWD) układu wielomianów niezerowych $p_1, \ldots, p_n$ jeśli:*
  - *$d \,|\, p_i$, dla każdego $i = 1, \ldots, n$,*
  - *jeśli dla pewnego $h \in K[x]$ mamy $h \,|\, p_i$, dla każdego i, to $h \,|\, d$.*
- *Jeśli niezerowe $p_1, \ldots, p_n \in K[x]$ spełniają $NWD(p_1, \ldots, p_n) = 1$, to nazywamy je **względnie pierwszymi**.*
- *Jeśli $\deg(f) \geqslant 1$, to wielomian f nazwiemy **nierozkładalnym**, jeśli nie istnieją (niestałe) wielomiany $g, h \in K[x]$, $\deg(f), \deg(h) \geqslant 1$ takie, że $f = g \cdot h$. Wielomian stopnia $\geqslant 1$, który nie jest nierozkładalny nazywamy r**ozkładalnym**.*

Rozkładalność wielomianu zależy oczywiście od ciała współczynników. Na wykładzie pokazaliśmy, że każdy wielomian $f \in \mathbb{R}[x]$ stopnia co najmniej 3 jest rozkładalny. Tymczasem wielomian $x^3 + 2$ nie jest rozkładalny jako element $\mathbb{Q}[x]$. Po odpowiednim rozszerzeniu współczynników, na przykład w ciele $\mathbb{Q}[\sqrt[3]{2}]$, wielomian ten można już jednak rozłożyć na czynniki stopnia $\geqslant 1$ postaci: $x - \sqrt[3]{2}$ oraz $x^2 + \sqrt[3]{2}x + \sqrt{3}(2)^2$.

Pierwszym krokiem do zrozumienia rozkładów wielomianów jest rezultat będący wersją lematu Bezout.

Lemat 1. *Niech K bedzie ciałem. Dla dowolnych niezerowych $p_1, \ldots, p_n \in K[x]$ istnieją wielomiany $q_1, \ldots, q_n \in K[x]$ takie, że*

$$q_1 p_1 + \ldots + q_n p_n = NWD(p_1, \ldots, p_n).$$

Dowód. Niech

$$I = \{q_1 p_1 + \ldots + q_n p_n \,|\, q_i \in K[x]\} \subseteq K[x].$$

Niech d będzie wielomianem monicznym najmniejszego możliwego stopnia należącym do I. Pokażemy, że jest to NWD wielomianów $p_1, p_2, \ldots, p_n$. Potrzeba zatem sprawdzić dwa warunki.

Zacznijmy od pokazania, że $d \,|\, p_i$, dla każdego i. Gdyby któryś z wielomianów p_i nie był podzielny przez d, to korzystając z twierdzenia o dzieleniu z resztą mamy $p_i = h_i d + r_i$, gdzie $\deg(r_i) < \deg(d)$. Ale skoro $d \in K$, to dla pewnych $q_1', \ldots, q_n' \in K[x]$ mamy

$$r_i = p_i - h_i d = p_i - (q_1' p_1 + \ldots + q_n' p_n),$$

zatem $r_i \in I$. Sprzeczność z wyborem d. Zatem d dzieli wszystkie p_i.

Druga część dowodu to pokazanie, że wspólny dzielnik wielomianów p_i jest dzielnikiem d. To jest jednak oczywiste. Zauważmy, że NWD układu p_i jest dzielnikiem każdego elementu I, a więc i jest dzielnikiem elementu d. Zatem d jest rzeczywiśćie NWD układu $p_1, \ldots, p_n$. □

[4] W ramach wykładów z algebry dowiecie się Państwo, ze jest to pojęcie określone z dokładnością do relacji stowarzyszenia (nie będziemy tego wyjaśniać), a więc niekoniecznie ograniczone do wielomianów monicznych

Warto odnotować, że istotne jest założenie o tym, że wielomiany mają współczynniki w ciele. W $\mathbb{Z}[x]$ największy wspólny dzielnik 2 oraz x to 1, ale nie istnieją wielomiany $f, g \in \mathbb{Z}[x]$, że $1 = 2f(x) + xg(x)$.

Twierdzenie 6 (O jednoznaczności rozkładu wielomianów o współczynnikach w ciele)**.** *Niech p będzie wielomianem stopnia $\geqslant 1$ w $K[x]$, gdzie K – ciało. Wówczas p można zapisać w postaci:*

$$p = a \cdot q_1 \cdot \ldots \cdot q_k, \qquad (\diamondsuit)$$

gdzie a jest współczynnikiem wiodącym p oraz $q_1, \ldots, q_k$ są monicznymi nierozkładalnymi wielomianami w $K[x]$. Co więcej, rozkład ów jest jednoznaczny z dokładnością do porządku występowania czynników.

Dowód. Dowód ma dwie części. Pierwsza to uzasadnienie istnienia rozkładu $(\diamondsuit)$, a druga to dowód jego jednoznaczności.

Zacznijmy od wyrazania istnienia rozkładu $(\diamondsuit)$. Rozumowanie to indukcja ze względu na stopień p. Jeśli p jest nierozkładalny, a w szczególności, jeśli p jest stopnia 1, to $p = a \cdot q$, gdzie a jest wiodącym współczynnikiem p i jest jasne, że q jest moniczny i nierozkładalny. Możemy zatem pzejść do kroku indukcyjnego i jednocześnie założyć, że p jest rozkładalny. W takim przypadku $p = p_1 p_2$, dla pewnych $p_1, p_2 \in K[x]$, przy czym $\deg(p) > \deg(p_i) \geqslant 1$ praz z założenia indukcyjnego:

$$p_1 = a_1 \cdot q_1 \ldots q_l, \quad p_2 = a_2 \cdot q_{l+1} \ldots q_k,$$

gdzie q_i są moniczne i nierozkładalne oraz a_i są współczynnikami wiodącymi w p_i. W szczególności

$$p = a_1 a_2 \cdot q_1 \ldots q_l \cdot q_{l+1} \ldots q_k,$$

jest rozkładem typu $(\diamond)$.

Aby udowodnić jednoznaczność, wykażemy najpierw pewną obserwację. Zauważmy mianowicie, że jeśli $f \in K[x]$ jest nierozkładalny oraz $f \,|\, gh$, gdzie $g, h \in K[x]$, to $f \,|\, g$, lub $f \,|\, h$,. Innymi słowy, element f jest **pierwszy** w $K[x]$. Dowód wymaga Lematu Bezout. Gdyby f nie dzielił f, to wobec nierozkładalności f mielibyśmy $NWD(f, g) = 1$. W szczególności, Lemat Bezout gwarantowałby istnienie $a, b \in K[x]$ takich, że

$$af + bg = 1 \quad \Rightarrow h = afh + bgh.$$

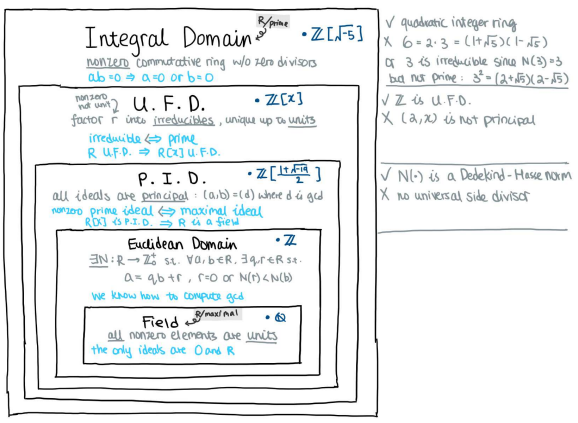
Stąd oczywiście $f \,|\, h$.

Aby pokazać jednoznaczność rozkładu $(\diamondsuit)$ niech:

$$p = a \cdot q_1 \ldots q_k = a \cdot q_1' \ldots q_r'$$

przedstawia dwa rozkłady p na czynniki nierozkładalne. Na mocy obserwacji wyżej, skoro q_1 dzieli $q_1' \ldots q_r'$, to q_1 dzieli jeden z czynników q_i'. Skoro jednak obydwa te wielomiany są moniczne i nierozkładalne, to $q_1 = q_i'$. Skracając te dwa czynniki i powtarzając en proces aż wszystkie $q_1, \ldots, q_k$ zostaną skrócone prowadzi nas do tezy. □

Uwaga. Uzyskany rezultat mówi, że $K[x]$ jest tzw. dziedziną z jednoznacznością rozkładu (UFD). Na Algebrze I pokażemy także, że $\mathbb{Z}[x]$ też jest UFD, choć droga dowodu jest tam nieco bardziej skomplikowana. Będziemy badać również inne naturalne obiekty związane z rozszerzeniami ciał i pierścieni. Problem polegać będzie na rozróżnianiu własności potrzebnych w dowodzie twierdzenia wyżej. Poniższa grafika prezentuje kilka przykładów.



Źródło: https://yiningliublog.wordpress.com/

Dodatek. Podzielność w $\mathbb{C}$ i Wielkie Twierdzenie Fermata

Rozważmy liczby zespolone $z_1 = a+bi, z_2 = c+di$ oraz $z_3 = e+fi$, gdzie $a, b, c, d, e, f \in \mathbb{Z}$ i załóżmy, że:

$$(a+bi) = (c+di)(e+fi).$$

Oczywiście mamy stąd, że $|z_1| = |z_2| \cdot |z_3|$, a więc a^2+b^2 jest wielokrotnością c^2+d^2 oraz e^2+f^2. A zatem jeśli rozważmy liczby zespolone, których części: rzeczywista i urojona są liczbami całkowitymi, wówczas zachodzić się zdają pewne związki pomiędzy rozkładem tych liczb na czynniki, a rozkładem na czynniki kwadratów ich modułów – czyli zwykłych liczb całkowitych. Ta prosta obserwacja ma, jak się okazuje, niezwykle daleko idące konsekwencje. Zacznijmy od banalnego zastosowania. Rozwiążmy zadanie.

Zadanie. Niech a, b oraz n będą liczbami naturalnymi. Udowodnić, że istnieją liczby całkowite x, y, dla których zachodzi równość

$$(a^2+b^2)^n = x^2+y^2.$$

Nie jestem pewien czy Czytelnik od razu wskazałby rozwiązanie bez użycia liczb zespolonych. Tymczasem stosując argumentację wyżej podaną równość przepisujemy do postaci:

$$(a+bi)^n(a-bi)^n = (x+yi)(x-yi).$$

A zatem rozwiązanie, to $x = \mathrm{Re}(a+bi)^n$ oraz $y = \mathrm{Im}(a+bi)^n$.
Inny, nieco bardziej „przyziemny" przykład.

Zadanie. Rozwiązać w liczbach zespolonych równanie: $z^4 - 6z^3 + 18z^2 - 30z + 25 = 0$.

W tym przypadku możliwe są różne podejścia, na przykład korzystając z twierdzenia z wykładu można argumentować, że istnieją $a, b, c, d \in \mathbb{R}$, że:

$$z^4 - 6z^3 + 18z^2 - 30z + 25 = (z^2+az+b)(z^2+cz+d).$$

Trzeba zatem rozwiązać układ równań:

$$a+c = -6, \quad b+d+ac = 18, \quad ad+bc = -30, \quad 25 = bd.$$

W tym przypadku akurat kładąc $b = d = 5$ dostajemy układ $a+c = -6, ac = 8, 5(a+c) = -30$, co daje $a^2+6a+8 = (a+4)(a+2) = 0$, czyli $a = -4, c = -2$ (lub odwrotnie). A zatem:

$$z^4 - 6z^3 + 18z^2 - 30z + 25 = (z^2-4z+5)(z^2-2z+5) = 0.$$

Widać, że te równania kwadratowe „da" się dalej rozwiązać. Udało się. Czy można było to zrobić inaczej? Może, ale będzie trzeba trochę „gdybać". Spróbujmy. „Gdyby" istniał pierwiastek postaci $z = a+bi$, gdzie a, b są **całkowite**, również $a-bi$ byłby pierwiastkiem, a więc mielibyśmy $25 = (a^2+b^2)z_3z_4$, gdzie z_3, z_4 to pozostałe pierwiastki. „Gdyby" jeszcze z_3, z_4 również miały całkowite części rzeczywiste i urojone, wówczas a^2+b^2 byłaby dzielnikiem 25. To teoretycznie nie musi się zdarzyć (nie mamy narzędzi, by stwierdzić czy tak musi być), ale niewiele jest liczb całkowitych a, b, że a^2+b^2 dzieli 25, więc warto „pogdybać". Może jednym z pierwiastków jest liczba „całkowita" $a+bi$ postaci:

$$\pm 1, \quad \pm i, \quad \pm 5, \quad \pm 5i, \quad \pm 2 \pm i, \quad \pm 1 \pm 2i, \quad \pm 5 \pm 5i.$$

Nietrudno sprawdzić, że wśród tych liczb właśnie liczby $2 \pm i$ oraz $1 \pm 2i$ są rozwiązaniami naszego równania. To rodzi rozmaite domysły: czy przypadkiem nie mamy tu do czynienia z jakąś wersją twierdzenia o pierwiastku całkowitym/wymiernym wielomianu o współczynnikach całkowitych? Tak rzeczywiście jest i wiąże się to z faktem, że $\mathbb{Z}[i] = \{a+bi \,|\, a, b \in \mathbb{Z}\}$, tzw.**pierścień liczb całkowitych Gaussa**, ma jednoznaczność rozkładu na czynniki pierwsze. Co to znaczy? Czym są te czynniki? Czytelnik zainteresowany bliższym poznaniem tych liczb i związanej z nimi teorii podzielności zechce zajrzeć do:

M. Krych: *Skąd się wzięła liczba i*, `https://smp.uph.edu.pl/msn/34/krych.pdf`.

W tekście tym znajdują się informacje nie tylko o liczbach całkowitych Gaussa, ale też o tzw. **liczbach całkowitych Eisensteina** $\mathbb{Z}[\omega_3]$, złożonych z liczb postaci $a+b\omega_3$, gdzie $a, b \in \mathbb{Z}$ oraz ω_3 jest nierzeczywistym pierwiastkiem stopnia 3 z 1. Również w tym zbiorze zachodzi teoria podzielności, a nawet twierdzenie o jednoznacznym rozkładzie... Dlaczego ten jednoznaczny rozkład jest tak istotny?

Prawie 400 lat temu Pierre de Fermat stwierdził, że znalazł „niezwykły dowód" następującego twierdzenia:

Twierdzenie. Równanie diofantyczne:

$$x^n + y^n = z^n,$$

gdzie x, y, z, n są niezerowymi liczbami całkowitymi, nie ma rozwiązań, dla $n > 2$.

Niestety, Fermat nie był w stanie przedstawić rozwiązania, ponieważ swoje odkrycie zapisał na marginesie kopii starożytnego dzieła '*Arithmetica*' Diofantosa. Stwierdził jedynie, że '*margines jest zbyt mały, by pomieścić dowód*'. Notatka Fermata stała się jedną z wielu nieudowodnionych obserwacji, zostawionych kolejnym pokoleniom. Jak się okazało, wiele przypuszczeń Fermata zostało z czasem rozstrzygniętych. Jedną z osób, która poświęciła im sporo miejsca był sam Euler. Nie był on jednak w stanie pokazać ogólnego dowodu powyższego rezultatu. Z trudem znalazł niełatwe uzasadnienie dla $n = 3$ (używając liczb zespolonych, o czym można przeczytać w tekście dr. Krycha). Problem stał się jednym z najsłynniejszych w historii matematyki, a także źródłem rozwoju licznych jej dziedzin. Twierdzenie Fermata zostało udowodnione dopiero w 1994 roku przez Andrew Wilesa, metodami dalece wykraczającymi poza elementarną teorię liczb (czy w ogóle jakąkolwiek elementarną teorię).

Twierdzenie Fermata rodzi do dziś skrajne emocje. Raz na jakiś czas na adres naszego Instytutu Matematyki lub do skrzynek poszczególnych pracowników Wydziału trafiają, nawet w obecnych czasach, „prace" mające na celu przedstawienie łatwiejszego dowodu (lub w ogóle obalenie twierdzenia Fermata). Wystarczy przejrzeć fora matematyczne, by przekonać się jak wielkim wyzwaniem jest nie tylko sam problem, ale też recepcja jego dowodu – niezwykle skomplikowanego i w zasadzie zrozumiałego dla wąskiego grona specjalistów. Nie tylko amatorzy błędnie (tak się wydaje) przypuszczają, że rozwiązanie problemu Fermata może być kilkulinijkowe. Od stuleci pojawiają się nieprawdziwe dowody. Jeden z nich wart jest jednak przypomnienia, ponieważ dał początek rozwojowi współczesnej teorii liczb (i algebry w ogóle).

Cofnijmy się do roku 1847. Problem Fermata był już wówczas jednym z największych wyzwań matematycznych. Centrum matematycznego świata wciąż jeszcze leżało w Paryżu (niedługo potem trafić miało do Getyngi, a potem za Ocean Atlantycki). Francuska Akademia Nauk oferowała (od 31 lat) złoty medal i nagrodę 3000 franków za rozwiązanie problemu Fermata. Na posiedzeniu 1 marca, z propozycją dowodu wystąpił znany matematyk Gabriel Lamé. Twierdził, że znalazł cudowne rozwiązanie, bardzo krótkie.

Idea dowodu była rzeczywiście niezwykle prosta. Przedstawmy $x^n + y^n$ jako iloczyn n czynników. Jak? Weźmy $\zeta \in \mathbb{C}$ takie, że $\zeta^n = 1$, $\zeta \neq 1$ oraz n – nieparzyste. Dostaniemy wówczas:

$$x^n + y^n = (x + y)\,(x + \zeta y)\,\left(x + \zeta^2 y\right) \cdots \left(x + \zeta^{n-1} y\right) = z \cdot z \cdot \ldots \cdot z$$

Formuła ta wynika natychmiast z rozwiązania równania $X^n - 1 = 0$, dla $X = -x/y$. Co tu widzimy? Lamé wysnuwa stąd wniosek, że $x + y$ oraz z mają wspólny dzielnik, co prowadziłoby do sprzeczności. Opiera się na względnej pierwszości czynników uzyskanego rozkładu (można się do niej ograniczyć).

Nie tylko Lamé był niezwykle przejęty zaproponowanym dowodem. Również Cauchy wystąpił i stwierdził, że od dłuższego czasu pracuje nad dowodem, w zasadzie opartym na analogicznych obserwacjach. Obydwoje część „zasługi" oddawali Josephowi Liouvillowi, który zasugerował im rozważanie liczb zespolonych w kontekście problemu Fermata. Paradoksalnie, to właśnie Liouville zwrócił uwagę na pewien problem. Zaproponowany wyżej rozkład wyrażenia $x^n + y^n$ na „czynniki względnie pierwsze" dokonuje się w zbiorze liczb $\mathbb{Z}[\zeta]$ postaci:

$$a_1 + a_2\zeta + a_3\zeta^2 + \ldots + a_{n-1}\zeta^{n-1}, a_i \in \mathbb{Z}.$$

Nie ma gwarancji, że w zbiorze tym zachodzi jednoznaczność rozkładu na czynniki. Gdyby jej nie było, wówczas wyciągnięcie wniosku, że każdy czynnik $x^n + y^n$ jest n-tą potęgą nie jest możliwe... Do tego momentu Czytelnik ma prawo być już poważnie zniecierpliwiony: ani nie powiedzieliśmy czym jest „całkowitość" w $\mathbb{C}$, ani czym są czynniki pierwsze, nierozkładalne czy względnie pierwsze w $\mathbb{Z}[\zeta]$. Jeśli tak jest, to być może osiągnąłem swój cel. Dokładny opis tego problemu przekracza ów skromny dodatek, ale jest absolutnie w zasięgu. Proszę jedynie o kontynuowanie lektury przy bardziej kompetentnym źródle: artykule prof. Balcerzyka i dr. Szurka: „*Nieco historii matematyki w wykładzie algebry*": `http://www.deltami.edu.pl/temat/matematyka/2016/05/30/1981-05-Fermat.pdf`. Tekst ma ponad 40 lat, ale zapewniam, że wyjaśnienia będą bardzo interesujące, a niektóre niejasności – rozwiane. Proszę wybaczyć, że w dodatkach nie ma zbyt wielu wyjaśnień – to Państwa zadaniem jest szukać odpowiedzi.

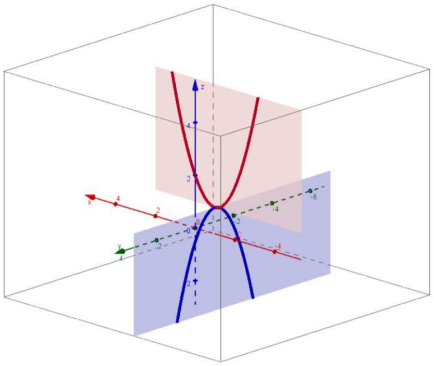
Trivia. Wykres funkcji zespolonej?

W przeciwieństwie do funkcji zmiennej rzeczywistej, której przebieg zmienności prezentujemy często graficznie na płaszczyźnie kartezjańskiej, prezentowanie „wykresów" funkcji zmiennej zespolonej nie jest czytelne z uwagi na to, że wymagałoby operowania w przestrzeni czterowymiarowej (zbiór argumentów ma dwie współrzędne i zbiór wartości ma dwie współrzędne). Z uwagi jednak na to, że często interesuje nas rozwiązanie równania $f(z) = 0$, wprowadza się różne ciekawe metody wizualizacji tego problemu. Jedną z nich są tzw. krzywe bliźniacze, wprowadzone w jednym z podręczników licealnych (!) w USA w latach 50' przez Howarda Fehra (to były początki „New Math" w nauczaniu – kto by chciał przeczytać więcej polecam artykuł: *New Thinking in School Mathematics* słynnego matematyka J. Dieudonné'a).

Rozważmy funkcję $f(z) = z^2 + 2z + 2$. Nietrudno sprawdzić, że rozwiązaniami równania $f(z) = 0$ są liczby zespolone $-1 \pm i$. Jak to zobaczyć na „wykresie"? Niech $z = x + iy$. Wówczas:

$$f(z) = f(x + iy) = (x^2 - y^2 + 2x + 2) + (2y(x + 1))i.$$

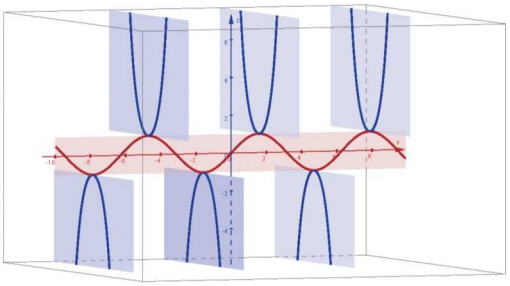
Skoro interesuje nas jedynie prezentacja warunku dotyczącego rzeczywistej wartości funkcji f (chodzi nam o wartość zero), to pomyślmy dla jakich x, y powyższa funkcja przyjmuje jedynie wartości rzeczywiste? Oczywiście dla $y = 0$ lub $x = -1$. Na płaszczyźnie $y = 0$ wartości $f(z)$ dane są przez $f(x) = x^2 + 2x + 2$, $x \in \mathbb{R}$, co reprezentowane jest przez dobrze znaną parabolę. W płaszczyźnie $x = -1$, prostopadłej do płaszczyzny $y = 0$, funkcja nasza ma postać $f(-1 + yi) = -y^2 + 1, y \in \mathbb{R}$. Oto stosowny obrazek:

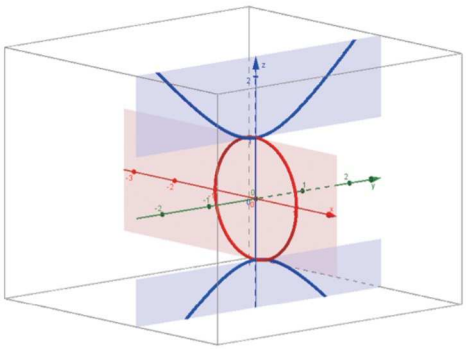


Rys. 1. Krzywe bliźniacze funkcji $f(z) = z^2 + 2z + 1$ w przestrzeni $\mathbb{R}^3$ to $x^2 + 2x + 2$ w płaszczyźnie $y = 0$ oraz $-y^2 + 1$ w płaszczyźnie $x = -1$. Źródło: Wiggins H., Harding A., Engelbrecht J.: *Visualising Complex Polynomials: A Parabola Is but a Drop in the Ocean of Quadratics*. J. Math. Research 10 (2018)

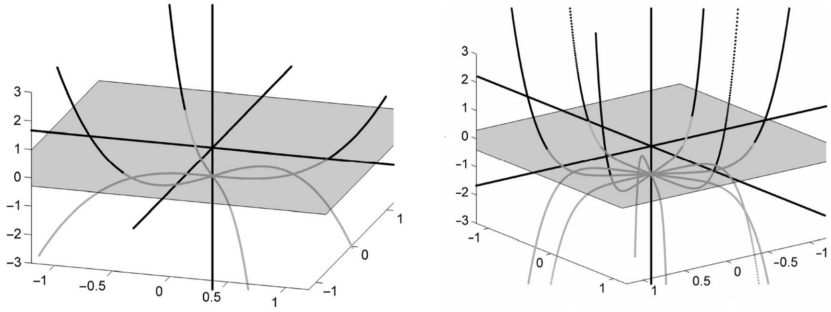
Co ten obrazek nam w zasadzie mówi? Otóż pokazuje nam on fragment czterowymiarowego wykresu funkcji $f(z)$ – ten mianowicie, na którym wartości funkcji są jedynie liczbami rzeczywistymi. Te wartości rzeczywiste reprezentowane są na osi OZ. Inaczej mówiąc: każda z powyższych dwóch krzywych ma punkty o trzech współrzędnych: (x, y, z). Pierwsze dwie współrzędne „kodują" punkt $x+iy$ z dziedziny funkcji f, zaś współrzędna z zawiera wartość rzeczywistą funkcji $f(z)$. A zatem zgodnie z intuicją: czerwona parabola nie ma punktu o współrzędnej $z = 0$, natomiast niebieska parabola – owszem: przecina płaszczyznę $z = 0$ w punktach $(-1, -1)$ oraz $(-1, 1)$. Te punkty reprezentują oczywiście liczby zespolone $-1 \pm i$.

Podobnego typu obrazki generować można dla innych funkcji, korzystając niekiedy z postaci trygonometrycznej lub wykładniczej liczb zespolonych. Ciekaw jestem czy Czytelnik potrafiłby powiedzieć jakimi równaniami opisane są krzywe bliźniacze dla funkcji $f(z) = \sin(z)$ oraz dla krzywej postaci $y^2 + z^2 = 1$?





Pouczająco wyglądają także obrazki prezentujące rozwiązania równań $z^3 = 1$ lub $z^6 = 1$.

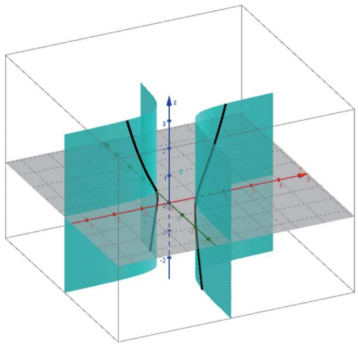


Rys. 3. Krzywe bliźniacze funkcji $f(z) = z^3 - 1$ oraz $f(z) = z^6 - 1$. Źródło: Harding A., Engelbrecht J.: *Sibling curves and complex roots 2: Looking ahead.* International Journal of Mathematical Education in Science and Technology, 38 (2017), 975-985.

Dla „funkcji kwadratowych" (zmiennej zespolonej) postaci $f(z) = az^2 + bz + c$, gdzie $a, b, c \in \mathbb{C}$, $a \neq 0$, pokazuje się, że zachodzić musi jedna z wykluczających się dwóch sytuacji:

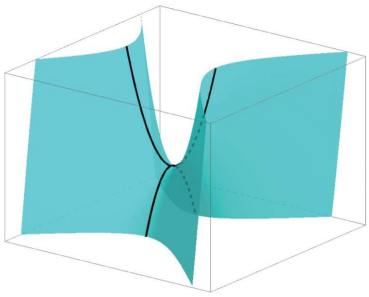
- dwie krzywe bliźniacze przecinają się – i wtedy są dwiema parabolami,
- dwie krzywe bliźniacze nie przecinają się – i stanowią gałęzie hiperboli.

Druga sytuacja zachodzi np. dla $f(z) = (z-1)(z-i)$, gdzie krzywe bliźniacze dane są wzorem $y = \frac{x-1}{2x-1}$.



Rys. 4. Krzywe bliźniacze funkcji $f(z) = (z-1)(z-i)$. Źródło jw.

Nie ma w tym rozróżnieniu, jak się okazuje, nic dziwnego. Jak pokazać, że taka klasyfikacja ma miejsce? Zasadniczo chodzi o sprowadzenie funkcji do postaci kanonicznej i rozważanie jedynie jej – jako geometrycznie „istotnej" dla kształtu krzywych bliźniaczych. Przez użycie przesunięcia, skalowania i obrotu można, bez straty ogólności, rozważać jedynie krzywe bliźniacze dla równania $f(z) = z^2 + c$, dla pewnej liczby zespolonej c. Przyjmując $z = x + iy$ dostajemy, że krzywe bliźniacze zawsze leżą, z dokładnością do skalowania, przesunięcia czy obrotu, na tak zwanej **hiperboloidzie parabolicznej** $z = x^2 - y^2$.



Rys. 5. Krzywe bliźniacze funkcji $f(z) = z^2 - 1$ na paraboloidzie hiperbolicznej $x^2 - y^2 = z$.

Należałoby, rzecz jasna, uściślić co znaczy stwierdzenie, że przesunięcie, skalowanie i obrót nie zmieniają „istoty geometrycznej" rozważanego problemu? Dlaczego wystarczyło rozważać jedynie krzywe bliźniacze równania $f(z) = z^2 + c$? Znacznie ogólniejsze i bardziej szczegółowe wyjaśnienie otrzymacie Państwo w drugim semestrze, gdy rozważać będziemy tak zwaną afiniczną klasyfikację hiperpowierzchni stopnia 2.

Animację ukazującą zmianę położenia krzywych bliźniaczych na paraboloidzie hiperbolicznej dla rodziny funkcji o równaniach $f(z)z^2 + 2z + (1 + ki)$ w zakresie $-2 \leqslant k \leqslant 2$ znajdziecie Państwo pod adresem: https://cardanogroup.files.wordpress.com/2014/08/sibling-animation.gif.

Notka historyczna. Równania wielomianowe stopnia 3, 4, 5 itd.

Już w starożytnej Mezopotamii oraz Egipcie rozwiązywano niektóre równania liniowe i kwadratowe. Inspiracją były głównie konkretne problemy praktyczne. Nie używano wtedy w zasadzie symboliki algebraicznej, ale stawiano problemy w formie tekstowej. Również rozwiązania były raczej instrukcjami słownymi wyjaśniającymi (niczym przepis kucharski) jak dojść do odpowiedzi na postawione zagadnienie. Nie korzystano z abstrakcyjnych metod czy rozumowań. Nie formułowano wzorów ogólnych. Przykładowy problem prowadzący (nas) do równania stopnia trzeciego[5] brzmiał (mniej więcej tak): jak głęboki był wykop o sześciennym kształcie, jeśli w jego wyniku usunięto określoną jednostkę objętości ziemi?

W starożytnej Grecji postawiono szereg ważnych problemów matematycznych, mających głównie (choć nie tylko) naturę geometryczną, w tym jedno zagadnienie szczególnie związane z równaniami sześciennymi: problem podwojenia sześcianu (problem delijski). W V wieku p.n.e. Hipokrates z Chios sprowadził ten problem do znalezienia, dla danych a, b, takich x, y, aby $r = \frac{a}{x} = \frac{x}{y} = \frac{y}{b}$. Wówczas bowiem $r^3 = \frac{a}{b}$. Działo się to niemal na sto lat przed czasami Euklidesa, którego „Elementy" stały się kamieniem milowym w rozwoju matematyki, punktem odniesienia i wzorcem do uczenia się prowadzenia rozumowań przez wiele stuleci[6]. Zainteresowanych tym tematem odsyłam przede wszystkim do książki „Wykłady z historii matematyki" prof. Marka Kordosa oraz do licznych artykułów Profesora w „Delcie".

Na mapie ważnych dla historii równań wielomianowych miejsc znajdują się również Indie, gdzie matematyka rozwijała się, niezależnie od Europy (choć wspomina się o wspólnych babilońskich korzeniach), od ponad 3000 lat. W roku 628 hinduski matematyk Brahmaputra podał w dziele Brahmasphuasiddhanta ogólne wzory pozwalające na rozwiązanie równania liniowego, kwadratowego (przy założeniu, że można je rozwiązać), a także opisał metodę rozwiązywania układów równań liniowych z dwiema niewiadomymi.

W średniowieczu algebrę rozwijali głównie Arabowie. Po szybkiej ekspansji imperium arabskiego w połowie VIII wieku sprowadzono z ziem podbitych i dokonano tłumaczeń klasycznych dzieł greckich, perskich oraz indyjskich, a następnie zaczęto dyskutować i rozwijać zawarte w nich idee. Czołową postacią tego okresu jest uczony, od którego imienia bierze nazwę algebra – al-Khwarizmi (780-850), astronom i kierownik biblioteki Domu Mądrości w Bagdadzie. Wielkim jego następcą był al-Khayammi (1048-1131) stosujący metody geometryczne do rozwiązywania równań stopnia 3 (niektórych).

Rozwój handlu w basenie Morza Śródziemnego sprawił, że niektórzy uczeni europejscy mieli okazję zetknąć się z matematyką arabską (a wraz z nią, ze spuścizną czasów antycznych[7]). Jednym z nich był Leonardo z Pizy, zwany Fibonaccim, którego dzieło "Liber abaci" z 1202 roku stanowiło nie tylko zebranie i podsumowanie znanej ówcześnie wiedzy matematycznej, także arabskiej, ale też w pewnych miejscach jej rozwinięcie. Dzieło to stawiało ważne dla przyszłych pokoleń pytania. Dopóki jednak nie rozwiną się uniwersytety oraz nie zostanie na szeroką skalę wykorzystany wynalazek druku, nauki ścisłe będą w stagnacji, a rozwijać się będzie w zasadzie głównie „matematyka stosowana" w handlu i bankowości. W 1494 roku franciszkanin Luca Pacioli wyda „Summa de arithmetica", w zasadzie pierwsze poważne drukowane dzieło matematyczne (uważane, nomen omen, za kamień milowy w historii rachunkowości) w którym umieści tezę o nierozwiazywalności równania stopnia trzeciego. Rozpocznie tym samym szeroką dyskusję i otworzy nowy rozdział w historii równań algebraicznych. Na czym polegać będzie przełom i jak pojawią się w nim liczby zespolone? Można tu wiele opowiadać: o rozwiązaniu zabranym do grobu, pojedynkach, oszustwie, kolejnym pojedynku i tragicznej śmierci... Chętnych zapraszam do lektury poniższych tekstów.

- Damian Wiśniewski, *O pewnym renesansowym matematycznym pojedynku i jego konsekwencjach*, Spotkania z matematyką, PTM, 12.05.2016 r.
- Paweł Gładki, *Uwagi historyczne o wzorach Cardano*: `http://www.math.us.edu.pl/~pgladki/faq/node129.html`.

Rozwiązanie problemu „(nie)istnienia wzorów" na rozwiązania równań wielomianowych stopni wyższych niż 4 uzyskano w XIX wieku. O pieknej teorii Galois i Abela będą się Państwo uczyć na Algebrze II.

[5] K. Muroi: Cubic equations of Babylonian mathematics: `https://arxiv.org/ftp/arxiv/papers/1905/1905.08034.pdf`.

[6] Zachęcam do zapoznania się z serwisem internetowym Byrne's Euclid, w ramach którego znany grafik Nicholas Rougeux, zdigitalizował przepiękne XIX-wieczne wydanie „Elementów", pięknie ilustrowane: `https://www.c82.net/euclid/#books`.

[7] Należy wspomnieć, dzieła antyczne przetrwały także w pewnej części w Europie i zachowane zostały dzięki skrupulatnej pracy zakonników i zakładanym przez nich bibliotekach (Rzym, Vivarium, Monte Cassino, Sewilla, Cluny, Tours, York). Jednym z nich był Alkuin, kierownik „Akademii"' – akwizgrańskiej szkoły pałacowej Karola Wielkiego i faktyczny współtwórca minuskuły – średniowiecznego pisma stanowiącego prototyp antykwy i łacińskiego kroju czcionki drukarskiej. Inne ważne postaci to choćby Boecjusz czy Abelard (ten ostatni do zakonu się z własnej woli nie wybrał).