Algebra obliczeniowa - kilka wprowadzeń

Damian Orlef

1 Liczby zespolone

1.1 Czym one są?

Liczby zespolone (ozn. $\mathbb{C}$) to pewne uogólnienie pojęcia liczb rzeczywistych i działań na nich. Możemy je dodawać, odejmować, mnożyć, dzielić (byle nie przez 0), otrzymując nowe liczby zespolone. Zachowane są wszystkie prawa arytmetyki liczb rzeczywistych (łączność, przemienność, rozdzielność mnożenia względem dodawania) oraz dawne wyniki działań na liczbach rzeczywistych (bo nowe działania są rozszerzeniem starych).

Przez i oznaczamy pewną wyróżnioną liczbę zespoloną, która spełnia $i^2 = -1$. Jest ona o tyle ważna, że każda liczba zespolona daje się zapisać jako $a + bi$ dla pewnych $a, b \in \mathbb{R}$ (oczywiście każde takie wyrażenie jest liczbą zespoloną).

Skoro i nie jest rzeczywiste, to liczby $a + bi$ są parami różne dla różnych par (a, b), czyli dla $z \in \mathbb{C}$ mamy jednoznacznie wyznaczone $a, b \in \mathbb{R}$, które dają nam $z = a + bi$. Nazywamy a i b odpowiednio częścią rzeczywistą i urojoną liczby z, zaś oznaczamy je $\Re(z) = a$ i $\Im(z) = b$.

Wiedząc, że spełnione są prawa przemienności i łączności, możemy łatwo wyrazić w tej postaci sumę i iloczyn liczb $a + bi$ oraz $c + di$ $(a, b, c, d \in \mathbb{R})$:

$$(a + bi) + (c + di) = (a + c) + (bi + di) = (a + c) + (b + d)i$$

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

Jednym ze sposobów na zdefiniowanie liczb zespolonych jest określenie, że są to pary liczb rzeczywistych (a, b), zapisywane jako $a + bi$, a działania mnożenia i dodawania dane są przez uzyskane wzory. Wówczas wszystkie własności przemienności, łączności, rozdzielność, możliwość zdefiniowania odejmowania i dzielenia są dosyć prostym następstwem tej definicji i własności liczb rzeczywistych.

Niech $z = a + bi$. Liczbą sprzężoną do z nazywamy liczbę $\bar{z} = a - bi$. Zauważmy, że $z\bar{z} = a^2 - (bi)^2 = a^2 + b^2$, więc gdy $z \neq 0$, to liczba $w = \frac{\bar{z}}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$ jest odwrotnością z (ten wniosek pozwala przy powyższej definicji uzasadnić, że niezerowe liczby zespolone mają swoje zespolone odwrotności, a stąd wynika, że można dzielić). Liczbę $|z| = \sqrt{a^2 + b^2} = \sqrt{z\bar{z}}$ nazywamy modułem lub normą z. Jest ona odpowiednikiem wartości bezwzględnej liczby rzeczywistej.

Przydatne są własności sprzężenia i modułu. Dla $z, w \in \mathbb{C}$ zachodzą następujące wzory:

$$\overline{z} + \overline{w} = \overline{z + w}$$

$$\overline{z} \cdot \overline{w} = \overline{zw}$$

$$\overline{\left(\frac{z}{w}\right)} = \frac{(\overline{z})}{(\overline{w})}$$

$$|z|\,|w| = |zw|$$

Ważna jest też tzw. nierówność trójkąta:

$$|z| + |w| \geqslant |z + w|$$

1.2 Zasadnicze twierdzenie algebry

Równość $i^2 = -1$ pokazuje, że równanie $x^2 + 1 = 0$ ma rozwiązanie zespolone, choć nie może mieć rozwiązania rzeczywistego. Okazuje się, że każde nietrywialne równanie wielomianowe jednej zmiennej ma jakieś rozwiązanie zespolone. Niech bowiem $a_0, \ldots, a_n \in \mathbb{C}$ będą współczynnikami wielomianu $P(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ i niech do tego będzie $n \geqslant 1$ oraz $a_n \neq 0$, tzn. P jest stopnia n. Wówczas istnieje liczba zespolona z taka, że $P(z) = 0$.

Tw. Bezout pozwala ten fakt, zwany zasadniczym twierdzeniem algebry, wyrazić inaczej:

Twierdzenie 1 (Zasadnicze twierdzenie algebry)**.** Jeśli P jest takie jak powyżej, to istnieją liczby zespolone $c_1, \ldots, c_n$ takie, że zachodzi równośc wielomianów $P(x) = a_n(x - c_1) \ldots (x - c_n)$.

2 Wielomiany, także wielu zmiennych

2.1 Oznaczenia i nazewnictwo

Niech k będzie jednym ze zbiorów $\{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ - z tego zbioru będą pochodziły współczynniki wielomianów. k jest nieskończone i zamknięte na działania arytmetyczne $(+, -, /, \cdot)$.

Przez $\mathbb{Z}_{\geqslant 0}$ rozumiemy zbiór liczb całkowitych nieujemnych.

Ustalmy $n \geqslant 1$. Zmiennymi będą u nas $x_1, \cdots, x_n$ (ale dla małych n będziemy pisać np. x, y, z). Jednomianem nazwiemy wyrażenie postaci $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, gdzie $(a_1, \ldots, a_n) \in (\mathbb{Z}_{\geqslant 0})^n$, czyli dowolny iloczyn zmiennych x_i. By uprościć nazewnictwo, dla $\alpha = (a_1, \ldots, a_n) \in (\mathbb{Z}_{\geqslant 0})^n$ będziemy oznaczać $x^\alpha := x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ (gdy $\alpha = (0, \ldots, 0)$, to przyjmujemy $x^\alpha = 1$), zaś α będziemy nazywać wykładnikiem.

Jeśli $\alpha = (a_1, \ldots, a_n)$ oraz $\beta = (b_1, \ldots, b_n)$, to określamy $\alpha + \beta = (a_1 + b_1, \ldots, a_n + b_n)$. Analogicznie definiujemy $\alpha - \beta$.

Wielomianem zmiennych $x_1, \ldots, x_n$ nazwiemy dowolne wyrażenie postaci

$$f = \sum_{\alpha \in A} c_\alpha x^\alpha,$$

gdzie $c_\alpha \in k$ są współczynnikami, zaś $A \subset (\mathbb{Z}_{\geqslant 0})^n$ skończonym podzbiorem wykładników. Zbiór takich wielomianów oznaczamy przez $k[x_1, \ldots, x_n]$. Wielomian f możemy traktować jako funkcję $k^n \to k$, poprzez wstawianie danych argumentów w miejsce x_i. Można udowodnić, że skoro k jest nieskończone, to różne wielomiany (mające jakiekolwiek różne współczynniki przy tym samym jednomianie), zadają koniecznie różne funkcje.

W naturalny sposób definiujemy dodawanie i mnożenie wielomianów, a działania te okazują się być łączne, przemienne i rozdzielne. Definiujemy przede wszystkim $x^\alpha \cdot x^\beta = x^{\alpha+\beta}$. Alternatywnie, dla k nieskończonego, gdy $f, g \in k[x_1, \ldots, x_n]$, to wielomiany $f + g$ i $f \cdot g$ można rozumieć jako te wielomiany, które odpowiadają jako funkcja sumie i iloczynowi funkcji zadanych przez f i g

Dla wykładnika $\alpha = (a_1, \ldots, a_n)$ określamy jego stopień jako $|\alpha| = a_1 + a_2 + \ldots + a_n$, czyli liczbę zmiennych (z powtórzeniami) w iloczynie x^α. Stopniem całkowitym wielomianu f nazwiemy największą liczbę postaci $|\alpha|$ dla takich α, które spełniają $c_\alpha \neq 0$, czyli największy stopień jednomianu w zapisie. Np. $f = 4x^2y^3 + z^7 - x^2yw^{13}$ ma stopień całkowity 16. Jeśli $f = 0$, to określamy jego stopień całkowity jako $-\infty$.

2.2 Porządki jednomianowe

Zajmiemy się teraz zagadnieniem uporządkowania jednomianów występujących w zapisie danego niezerowego wielomianu $f \in k[x_1, \ldots, x_n]$. Poza jednolitą prezentacją, otrzymamy w ten sposób

bardzo przydatne narzędzie, np. do analizy algorytmów, a także kilka ciekawych problemów do rozwiązania.

Chcemy dla każdych dwóch różnych $\alpha, \beta \in (\mathbb{Z}_{\geqslant 0})^n$ wiedzieć, które z nich uznajemy za większe jako wykładnik. Chcemy móc pisać $\alpha < \beta$ albo $\alpha > \beta$ w zależności od tego, które jest większe.

Ustalamy, że napis $\alpha < \beta$ będzie miał sens tylko dla $\alpha, \beta \in (\mathbb{Z}_{\geqslant 0})^n$ i może być zdaniem prawdziwym lub fałszywym. (Chodzi o to, że $<$ to relacja dwuargumentowa na $(\mathbb{Z}_{\geqslant 0})^n$.)

Definicja 1. $<$ nazwiemy porządkiem jednomianowym, jeśli spełnia następujące warunki:

1. Dla dowolnych $\alpha, \beta, \gamma \in (\mathbb{Z}_{\geqslant 0})^n$, jeśli $\alpha < \beta$ i $\beta < \gamma$, to $\alpha < \gamma$.
2. Dla dowolnych $\alpha, \beta \in (\mathbb{Z}_{\geqslant 0})^n$, zachodzi dokładnie jeden z trzech warunków:
   (a) $\alpha < \beta$
   (b) $\alpha > \beta$
   (c) $\alpha = \beta$
3. Dla dowolnych $\alpha, \beta, \gamma \in (\mathbb{Z}_{\geqslant 0})^n$, jeśli $\alpha < \beta$, to $\alpha + \gamma < \beta + \gamma$.
4. Każdy niepusty podzbiór $A \subset (\mathbb{Z}_{\geqslant 0})^n$ ma element najmniejszy w sensie $<$, czyli, równoważnie, nie istnieje nieskończony ciąg $a_1 > a_2 > \ldots > a_n > \ldots$ elementów A.

Kiedy mamy już porządek jednomianowy $<$, to dla niezerowego $f = \sum_{\alpha \in A} c_\alpha x^\alpha$ niech α będzie największym wykładnikiem w sensie $<$. Dla takiego f definiujemy kolejno:

1. *stopień* f jako $\deg(f) = \alpha$,
2. *jednomian wiodący* f jako $\mathrm{LM}(f) = x^\alpha$,
3. *wyraz wiodący* f jako $\mathrm{LT}(f) = c_\alpha x^\alpha$,
4. *współczynnik wiodący* f jako $\mathrm{LC}(f) = c_\alpha$.

Być może najprotszym przykładem porządku jednomianowego jest porządek leksykograficzny $<_{lex}$, który definiujemy następująco: $\alpha >_{lex} \beta$ wtedy i tylko wtedy, gdy ciąg $\alpha - \beta$ ma jakiekolwiek niezerowe wyrazy (tzn. $\alpha \neq \beta$) i pierwszy jego niezerowy element od lewej jest dodatni. Jest to tak naprawdę zwykły porządek leksykograficzny, przy założeniu, że $x_1 >_{lex} x_2 >_{lex} \ldots >_{lex} x_n$.

Jeśli rozważymy porządek $<_{lex}$ (x_1, x_2, x_3 nazywamy odpowiednio x, y, z) i wielomian $f = 2x^3y^6z^5 + 4x^2y^5 + 5x^3y^7$, to wykładnikami jednomianów są $(3,6,5)$, $(2,5,0)$, $(3,7,0)$, a największy spośród nich to $(3,7,0)$, bo $(3,7,0) - (2,5,0) = (1,2,0)$ oraz $(3,7,0) - (3,6,5) = (0,1,-5)$.

Mamy zatem kolejno $\deg(f) = (3,7,0)$, $\mathrm{LM}(f) = x^3y^7$, $\mathrm{LT}(f) = 5x^3y^7$, $\mathrm{LC}(f) = 5$.

2.3 Ideały w $k[x_1, \ldots, x_n]$ i zbiory algebraiczne

Niepusty podzbiór $I \subset k[x_1, \ldots, x_n]$ nazwiemy ideałem, jeśli spełnione są warunki:

- Jeśli $f, g \in I$, to $f + g \in I$.
- Jeśli $f \in I$, $g \in k[x_1, \ldots, x_n]$, to $fg \in I$.

Jeśli ustalimy $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$, to przykładem ideału jest tzw. ideał generowany przez $f_1, \ldots, f_m$, oznaczany jako $(f_1, \ldots, f_m) = \{g_1f_1 + g_2f_2 + \ldots + g_mf_m \mid g_1, g_2, \ldots, g_m \in k[x_1, \ldots, x_n]\}$. Okazuje się, że wszystkie ideały w $k[x_1, \ldots, x_n]$ dają się tak zapisać.

Dla ustalonych $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ oznaczamy zbiór ich wspólnych zer przez $\mathrm{V}(f_1, \ldots, f_m) = \{a \in k^n \mid f_1(a) = f_2(a) = \ldots = f_m(a) = 0\}$. Zbiory postaci $\mathrm{V}(f_1, \ldots, f_m)$

nazywamy zbiorami algebraicznymi w k^n. Np. dla $n = 2$, $\mathrm{V}(x^2 - y)$ to parabola, podobnie wiele innych krzywych jest zbiorami algebraicznymi.

Odwrotnie, dla dowolnego zbioru $A \subset k^n$, definiujemy
$I(A) = \{f \in k[x_1, \ldots, x_n] \,|\, \forall_{a \in A}\, f(a) = 0\}$.