2 Liczby zespolone, ciała

Nasza dyskusja równań liniowych opierała się na jedynie na regułach arytmetyki liczb rzeczywistych i zbiór liczb rzeczywistych można tu zastąpić innymi obiektami algebraicznymi – ciałami, których elementy można dodawać i mnożyć zgodnie z analogicznymi regułami.

Z punktu widzenia tego wykładu najważniejszym, obok $\mathbb{R}$, ciałem jest ciało liczb zespolonych, które otrzymuje się dołączając do $\mathbb{R}$, w możliwie oszczędny sposób, rozwiązanie równania $x^2 = -1$ (którego nie ma w ciele $\mathbb{R}$).

Wspomnimy też jednak o ciałach zupełnie innego typu – ciałach skończonych $\mathbb{Z}_p$.

2.1 Liczby zespolone.

Liczby rzeczywiste $\mathbb{R}$ rozszerzymy dołączając "liczbę urojoną" $\sqrt{-1}$ oznaczaną symbolem i, tak aby na otrzymanych "liczbach zespolonych" można było wykonywać algebraiczne operacje dodawania i mnożenia zgodnie ze standardowymi regułami arytmetyki liczb rzeczywistych.

W części **??** pokażemy, że dołączenie $\sqrt{-1}$ prowadzi do systemu liczbowego, w którym każdy wielomian stopnia dodatniego $a_0 + a_1x^1 + \ldots + a_nx^n$ ma pierwiastek (zasadnicze twierdzenie algebry).

Definicja 2.1.1 *Liczbami zespolonymi będziemy nazywać wyrażenia postaci $a + ib$ (gdzie $i = \sqrt{-1}$ oraz $a + ib = c + id \Leftrightarrow a = c,\ b = d$) z następującymi operacjami dodawania $\oplus$ i mnożenia $\odot$:*

$$(a + ib) \oplus (c + id) = (a + c) + i(b + d)\ ; \qquad (a + ib) \odot (c + id) = (ac - bd) + i(ad + bc)$$

Zbiór liczb zespolonych z tak określonymi działaniami oznaczamy symbolem $\mathbb{C}$.

Uwaga 2.1.2 (a) Wyrażenie $a + i0$ zapisujemy jako a i utożsamiamy je z liczbą rzeczywistą a. W ten sposób $\mathbb{R} \subset \mathbb{C}$, przy czym działania $\oplus$ i $\odot$ pokrywają się na $\mathbb{R}$ ze zwykłym dodawaniem i mnożeniem.

(b) Zamiast $0 + ib$, $b \neq 0$ piszemy ib (lub i jeśli $b = 1$); w szczególności $i \odot i = -1$, tzn. $i^2 = -1$ w $\mathbb{C}$.

(c) Liczbę zespoloną $z = a + ib$ można interpretować jako punkt (a, b) płaszczyzny kartezjańskiej. Współrzędne a, b tego punktu będziemy nazywać odpowiednio *częścią rzeczywistą* Rez i *częścią urojoną* Imz liczby z □

Uwaga 2.1.3 Dodawanie i mnożenie liczb zespolonych spełniają standardowe reguły arytmetyki liczb rzeczywistych, mają elementy neutralne ze względu na dodawanie i mnożenie (zero i jedynkę); w $\mathbb{C}$ wykonlne są operacje odejmowania i dzielenia przez liczby różne od zera:

(1)	przemienność	$z_1 \oplus z_2 = z_2 \oplus z_1$,	$z_1 \odot z_2 = z_2 \odot z_1$;
(2)	łączność	$(z_1 \oplus z_2) \oplus z_3 = z_1 \oplus (z_2 \oplus z_3)$,	$(z_1 \odot z_2) \odot z_3 = z_1 \odot (z_2 \odot z_3)$;
(3)	elementy neutralne	0 dla dodawania: $z \oplus 0 = z$,	1 dla mnożenia: $1 \odot z = z$;
(4)	istnienie elementu	przeciwnego $-z$: $z \oplus -z = 0$	odwrotnego z^{-1}, dla $z \neq 0$: $z \odot z^{-1} = 1$
		$-(a + ib) = (-a) + i(-b)$,	$a + ib \neq 0$, to $(a + ib)^{-1} = (\frac{a}{a^2+b^2}) + i(\frac{-b}{a^2+b^2})$;
(5)	rozdzielność mnożenia względem dodawania	$z_1 \odot (z_2 \oplus z_3) = z_1 \odot z_2 \oplus z_1 \odot z_3$.	

□

W dalszym ciągu zamiast $\oplus$ i $\odot$ będziemy używali zwykłych symboli dodawania i mnożenia w $\mathbb{R}$. Odejmowanie definiujemy jako dodanie liczby przeciwnej $z_1 - z_2 = z_1 + (-z_2)$, dzielenie jako mnożenie przez liczbę odwrotną $z_1 : z_2 = \frac{z_1}{z_2} = z_1(z_2^{-1})$, n-tą potęgę z^n jako iloczyn n egzemplarzy liczby z, dla $n > 0$, $z^0 = 1$ i $z^{-n} = (z^{-1})^n$, tzn. rozszerzamy na $\mathbb{C}$ konwencje związane z działaniami w $\mathbb{R}$.

2.2 Postać trygonometryczna.

Modułem liczby zespolonej $z = a + ib$ nazywamy liczbę $|z| = \sqrt{a^2 + b^2} \in \mathbb{R}$. Interpretując liczbę $z \neq 0$ jako punkt (a, b) płaszczyzny kartezjańskiej widzimy, że $|z|$ jest odległością z od 0, a liczba $\frac{z}{|z|}$ odpowiadająca punktowi okręgu jednostkowego na płaszczyźnie ma postać $\frac{z}{|z|} = \cos\theta + i\sin\theta$, gdzie kąt θ zwany *argumentem* z i oznaczany przez $\arg z$ jest wyznaczony z dokładnością do całkowitych wielokrotności 2π.

Otrzymujemy stąd *zapis liczby zespolonej $z \neq 0$ w postaci trygonometrycznej*

$$\boxed{z = |z|(\cos\theta + i\sin\theta),}$$

gdzie $|z|$ jest modułem z, a θ argumentem z.

Twierdzenie 2.2.1 *Niech $z_1 = |z_1|(\cos\theta_1 + i\sin\theta_1)$, $z_2 = |z_2|(\cos\theta_2 + i\sin\theta_2)$. Wtedy*

$$z_1 z_2 = |z_1||z_2|(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2)),$$

tzn. moduł iloczynu jest iloczynem modułów, a argument iloczynu jest sumą argumentów czynników.

Dowód. $z_1 z_2 = |z_1|(\cos\theta_1 + i\sin\theta_1)|z_2|(\cos\theta_2 + i\sin\theta_2) = |z_1||z_2|(\cos\theta_1 + i\sin\theta_1)(\cos\theta_2 + i\sin\theta_2) = |z_1||z_2|(\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2 + i(\sin\theta_1\cos\theta_2 + \cos\theta_1\sin\theta_2)) = |z_1||z_2|(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2))$. ■

Wniosek 2.2.2 (Formuła de Moivre'a). $(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$.

Sprzężeniem liczby $z = a + ib$ nazywamy liczbę $\overline{z} = a - ib$. Dla $z \neq 0$ mamy $z\overline{z} = |z|^2$ i $\frac{1}{z} = \frac{\overline{z}}{|z|^2}$.

2.3 Pierwiastki z jedności.

Ustalmy liczbę naturalną $n > 1$. *Pierwiastkiem stopnia n z jedności* będziemy nazywać każdą liczbę zespoloną z taką, że $z^n = 1$.

Niech $\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Z formuły de Moivre'a wynika natychmiast, że liczby $\omega^k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$, $k = 0, 1, \ldots, n-1$, są wszystkimi pierwiastkami stopnia n z jedności.

Punkty płaszczyzny kartezjańskiej odpowiadające pierwiastkom stopnia n z jedności są wierzchołkami n-kąta foremnego wpisanego w okrąg jednostkowy, mającego wierzchołek w $\omega^0 = 1$.

Pierwiastek stopnia n z jedności nazywamy *pierwotnym* jeśli nie jest nie jest pierwiastkiem z jedności stopnia $< n$. Do scharakteryzowania pierwiastków pierwotnych skorzystamy z następującego faktu związanego z dzieleniem z resztą liczb naturalnych.

Lemat 2.3.1 *Dla względnie pierwszych liczb naturalnych $0 < k < n$ istnieją liczby całkowite l, t takie, że $lk + tn = 1$. Co więcej, można zakładać, że $0 < l < n$.*

Dowód. Niech d będzie najmniejszą liczbą dodatnią postaci $d = sk + tn$, gdzie s, t są całkowite. Wystarczy pokazać, że d jest dzielnikiem k i n. Dla reszty $r = k - qd$ z dzielenia k przez d mamy $r = k - q(sk + tn) = (1 - qs)k + (-t)n$, więc $r = 0$ z minimalności d. Analogicznie pokazuje się, że d dzieli n. Drugą część tezy otrzymujemy przyjmując za l resztę z dzielenia s przez n. Wtedy $s = qn + l$, więc $1 = sk + tn = (qn + l)k + tn = lk + (qk + t)n$ i w szczególności $l > 0$. ■

Twierdzenie 2.3.2 *Pierwiastek $\omega^k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$, $1 < k < n$ stopnia n z jedności jest pierwotny wtedy i tylko wtedy, gdy k i n są względnie pierwsze.*

Dowód. Niech k i n będą względnie pierwsze. Z lematu istnieją l, t takie, że $1 = lk + tn$, a stąd $\omega = \omega^{lk+tn} = \omega^{lk}(\omega^n)^t = \omega^{lk}$. Jeśli $m > 0$ spełnia $(\omega^k)^m = 1$, to $\omega^m = (\omega^{lk})^m = (\omega^{km})^l = 1$, więc $m \geqslant n$, czyli ω^k jest pierwotny.

Załóżmy teraz, że $d > 1$ jest wspólnym dzielnikiem k i n, a q oraz m są takie, że $k = qd$ oraz $n = md$. Wtedy $(\omega^k)^m = (\omega^{qd})^m = (\omega^{md})^q = 1$, więc pierwiastek ω^k nie jest pierwotny ■

2.4 Ciała.

Własności dodawania i mnożenia w $\mathbb{R}$ i w $\mathbb{C}$ zebrane w Uwadze 2.1.3, stanowią punkt wyjścia definicji ciała.

Definicja 2.4.1 *Zbiór K z dwoma ustalonymi elementami: $0, 1$ ($0 \neq 1$) oraz dwoma działaniami: dodawania "$+$" i mnożenia "$\cdot$" nazywamy ciałem jeśli dla dowolnych $a, b, c \in K$ spełnione są warunki (dziewięć aksjomatów ciała)*

(1)	*przemienność*	$a + b = b + a,$	$a \cdot b = b \cdot a;$
(2)	*łączność*	$(a + b) + c = a + (b + c),$	$(a \cdot b) \cdot c = a \cdot (b \cdot c);$
(3)	*elementy neutralne*	0 *dla dodawania:* $a + 0 = a,$	1 *dla mnożenia:* $1 \cdot a = a;$
(4)	*istnienie elementu*	*przeciwnego* a'*:* $a + a' = 0,$	*odwrotnego* a^**, dla* $a \neq 0$*:* $a \cdot a^* = 1;$
(5)	*rozdzielność mnożenia względem dodawania*	$a \cdot (b + c) = a \cdot b + a \cdot c.$	

Dla podkreślenia, że ciało to zbiór z wyróżnionymi zerem i jedynką oraz z ustalonymi działaniami, będziemy pisać $\mathbb{K}$ zamiast K.

Równanie $x + a = b$ ma w ciele $\mathbb{K}$ dokładnie jedno rozwiązanie, bo dodając do obu stron tego równania a' – ustalony element przeciwny do a otrzymujemy, po uporządkowaniu równoważne równanie $x = b + a'$.

W szczególności wynika stąd, że 0 i element przeciwny do a (oznaczany przez $-a$) są wyznaczone jednoznacznie. Analogiczne rozumowanie dla równania $x \cdot a = b$, gdzie $a \neq 0$, pokazuje że 1 i element odwrotny do a (oznaczany przez a^{-1}) są wyznaczone jednoznacznie. Ułamek $\frac{b}{a}$ oznacza iloczyn $b \cdot a^{-1}$.

Wszystko, co powiedzieliśmy w pierwszym rozdziale o układach równań liniowych o współczynnikach z ciała liczb rzeczywistych przenosi się bez zmian na układy o współczynnikach z dowolnego ciała, tzn. na układy postaci $AX = B$, gdzie $A \in \mathbb{K}^m_n, B \in \mathbb{K}^m$.

W dowolnym ciele prawdziwe są dobrze znane własności działań w $\mathbb{R}$ (będziemy pisać ab zamiast $a \cdot b$).

Uwaga 2.4.2 Dla dowolnych $a, b \in \mathbb{K}$:

a) $a0 = 0$ (bo do obu stron $a0 + a0 = a(0 + 0) = a0$ można dodać $-(a0)$).

b) $ab = 0$, to $a = 0$ lub $b = 0$ (bo $a \neq 0$, to obie strony można pomnożyć przez a^{-1}).

c) $(-1)a = -a$ (bo $a + (-1)a = (1 + (-1))a = 0a = 0$). □

2.5 Ciała $\mathbb{Z}_p$.

Ważne przykłady ciał, które określimy w tej części są, w odróżnieniu od ciała liczb rzeczywistych $\mathbb{R}$, ciała liczb wymiernych $\mathbb{Q}$ i ciała liczb zespolonych $\mathbb{C}$ – ciałami skończonymi.

Niech p będzie liczbą pierwszą i niech $\omega = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$ będzie pierwiastkiem stopnia p z jedności. Wszystkie potęgi ω^n są również pierwiastkami stopnia p z jedności. Zbiór $\mathbb{Z}_p = \{\omega^0, \omega^1, \ldots, \omega^{p-1}\}$ wszystkich pierwiastków stopnia p z jedności jest więc zamknięty ze względu na działania

$$\omega^k \oplus \omega^l = \omega^{k+l}; \qquad \omega^k \odot \omega^l = \omega^{kl}.$$

Twierdzenie 2.5.1 *$\mathbb{Z}_p$ z ustalonym elementem zerowym $\mathbf{0} = \omega^0$, jedynką $\mathbf{1} = \omega^1$ oraz działaniami dodawania $\oplus$ i mnożenia $\odot$ jest ciałem.*

Dowód. Elementem przeciwnym do $\omega^k \in \mathbb{Z}_p$ jest ω^{p-k}, bo $\omega^k + \omega^{p-k} = \omega^p = \mathbf{0}$. Jeśli $\omega^k \in \mathbb{Z}_p \setminus \{\mathbf{0}\}$, to z Lematu 2.3.1 dla $n = p$ istnieją l, t takie, że $1 = lk + tp$. Elementem odwrotnym do $\omega^k \neq \mathbf{0}$ jest wtedy ω^l, bo $\mathbf{1} = \omega^1 = \omega^{lk}\omega^{tp} = \omega^{lk} = \omega^k \odot \omega^l$. Pozostałe aksjomaty wynikają z odpowiednich własności dodawania i mnożenia liczb naturalnych. ■