Rozdział 1

Grupy i ciała, liczby zespolone

Dla ustalenia uwagi, będziemy używać następujących oznaczeń:

$\mathbf{N} = \{ 1, 2, 3, \dots \}$ - liczby naturalne,

$\mathbf{Z} = \{ 0, \pm 1, \pm 2, \dots \}$ - liczby całkowite,

$\mathbf{W} = \left\{ \frac{m}{n} : \ m \in \mathbf{Z}, n \in \mathbf{N} \right\}$ - liczby wymierne,

$\mathbf{R} = \overline{\mathbf{W}}$ - liczby rzeczywiste,

$\mathbf{C} = \{ (a, b) : \ a, b \in \mathbf{R} \}$ - liczby zespolone.

Dwuargumentowym *działaniem wewnętrznym* '$\circ$' w zbiorze X nazywamy dowolną funkcję z iloczynu kartezjańskiego $X \times X$ w X. Wynik takiego działania na parze (x, y) będziemy oznaczać przez $x \circ y$.

1.1 Podstawowe struktury algebraiczne

Zaczniemy od przedstawienia abstrakcyjnych definicji grupy i ciała.

1.1.1 Grupa

Definicja 1.1 *Zbiór (niepusty) G wraz z wewnętrznym działaniem dwuargumentowym '$\circ$' jest* grupą *jeśli spełnione są następujące warunki (aksjomaty grupy):*

(i) $\forall a, b, c \in G \quad (a \circ b) \circ c = a \circ (b \circ c)$
(łączność działania)

(ii) $\exists e \in G \; \forall a \in G \quad a \circ e = a = e \circ a$
(istnienie elementu neutralnego)

(iii) $\forall a \in G \; \exists a' \in G \quad a \circ a' = e = a' \circ a$
(istnienie elementów przeciwnych/odwrotnych)

Jeśli ponadto

(iv) $\forall a, b \in G \quad a \circ b = b \circ a$

to grupę nazywamy przemienną *(lub* abelową*).*

Grupę będziemy oznaczać przez $\{G, \circ\}$.

Zauważmy, że już z aksjomatów grupy wynika, iż element neutralny jest wyznaczony jednoznacznie. Rzeczywiście, załóżmy, że istnieją dwa elementy neutralne, e_1 i e_2. Wtedy, z warunku (ii) wynika, że $e_1 = e_1 \circ e_2 = e_2$. Podobnie, istnieje tylko jeden element odwrotny dla każdego $a \in G$. Jeśli bowiem istniałyby dwa odwrotne, a'_1 i a'_2, to mielibyśmy

$$a'_1 = e \circ a'_1 = (a'_2 \circ a) \circ a'_1 = a'_2 \circ (a \circ a'_1) = a'_2 \circ e = a'_2,$$

przy czym skorzystaliśmy kolejno z własności (ii), (iii), (i) i ponownie (iii) i (ii).

Łatwo też pokazać, że w grupie $\{G, \circ\}$ równania

$$a \circ x = b \qquad \text{oraz} \qquad y \circ c = d$$

dla $a, b, c, d \in G$ mają jednoznaczne rozwiązania. W uzasadnieniu, ograniczymy się tylko do pierwszego równania. Łatwo sprawdzić, że $x = a' \circ b$ jest rozwiązaniem. Z drugiej strony, jeśli x jest rozwiązaniem to $a' \circ (a \circ x) = a' \circ b$, czyli $x = a' \circ b$.

Przykładami grup są:

- $\{\mathbf{Z}, +\}$, gdzie elementem neutralnym jest $e = 0$, a elementem przeciwnym do a' do a jest $-a$.
- $\{\mathbf{W} \setminus \{0\}, *\}$, gdzie $e = 1$ a $a' = a^{-1}$ jest odwrotnością a.

- Grupa obrotów płaszczyzny wokół początku układu współrzędnych, gdzie elementem neutralnym jest obrót o kąt zerowy, a elementem odwrotnym do obrotu o kąt α jest obrót o kąt $-\alpha$.

Zwróćmy uwagę na istotność wyjęcia zera w drugim przykładzie. Ponieważ 0 nie ma elementu odwrotnego, $\{\mathbf{W}, *\}$ nie jest grupą. Nie są też grupami np. $\{\mathbf{N}, *\}$ (nie ma elementów odwrotnych) oraz $\{\mathbf{R}, -\}$ (nie ma łączności oraz elementu neutralnego).

1.1.2 Ciało

Definicja 1.2 Ciałem *(a ściślej,* ciałem przemiennym*) nazywamy (co najmniej dwuelementowy) zbiór* $\mathbf{K}$ *z dwoma dwuargumentowymi działaniami wewnętrznymi, dodawaniem '+' i mnożeniem '∗', spełniające następujące warunki (aksjomaty ciała):*

(i) $\{\mathbf{K}, +\}$ *jest grupą przemienną (w której element neutralny oznaczamy przez* 0*, a element przeciwny do* a *przez* $-a$*),*

(ii) $\{\mathbf{K} \setminus \{0\}, *\}$ *jest grupą przemienną (w której element neutralny oznaczamy przez* 1*, a odwrotny do* a *przez* a^{-1}*),*

(iii) $\forall a, b, c \in \mathbf{K} \quad a * (b + c) = a * b + a * c$
(mnożenie jest rozdzielne względem dodawania). [1]

Bezpośrednio z definicji ciała można pokazać następujące ogólne własności (uzasadnienie pozostawiamy jako proste ćwiczenie):

1. $0 \neq 1$,
2. $\forall a \in \mathbf{K} \quad 0 * a = 0 = a * 0$,
3. $\forall a \in \mathbf{K} \quad (-1) * a = -a$,
4. jeśli $a * b = 0$ to $a = 0$ lub $b = 0$,
5. jeśli $a \neq 0$ i $b \neq 0$ to $(a * b)^{-1} = b^{-1} * a^{-1}$,

[1] Przyjmujemy konwencję, że w wyrażeniach w których występują i dodawania i mnożenia najpierw wykonujemy mnożenia.

dla dowolnych $a, b \in \mathbf{K}$.

W ciele możemy formalnie zdefiniować odejmowanie i dzielenie, mianowicie

$$\begin{aligned} a - b &:= a + (-b) \qquad \forall a, b \in \mathbf{K}, \\ a/b &:= a * b^{-1} \qquad \forall a \in \mathbf{K}, b \in \mathbf{K} \setminus \{0\}. \end{aligned}$$

Przykładem ciała są liczby rzeczywiste $\mathbf{R}$ z naturalnymi działaniami dodawania i mnożenia. Ciałem jest też zbiór liczb

$$\{\, a + b\sqrt{2} : \; a, b \in \mathbf{W} \,\} \subset \mathbf{R}$$

z tymi samymi działaniami.

1.2 Ciało liczb zespolonych

Ważnym przykładem ciała jest ciało liczb zespolonych, któremu poświęcimy tą część wykładu.

1.2.1 Definicja

Definicja 1.3 *Ciało* liczb zespolonych *to zbiór par uporządkowanych*

$$\mathbf{C} := \mathbf{R} \times \mathbf{R} = \{\, (a, b) : \; a, b \in \mathbf{R} \,\}$$

z działaniami dodawania i mnożenia zdefiniowanymi jako:

$$\begin{aligned} (a, b) + (c, d) &= (a + c, b + d), \\ (a, b) * (c, d) &= (a * c - b * d, a * d + b * c), \end{aligned}$$

dla dowolnych $a, b, c, d \in \mathbf{R}$. [2]

Formalne sprawdzenie, że $\mathbf{C}$ ze zdefiniowanymi działaniami jest ciałem pozostawiamy czytelnikowi. Tu zauważymy tylko, że elementem neutralnym

[2] Zauważmy, że znaki dodawania i mnożenia występują tu w dwóch znaczeniach, jako działania na liczbach rzeczywistych oraz jako działania na liczbach zespolonych. Z kontekstu zawsze wiadomo w jakim znaczeniu te działania są użyte.

dodawania jest $(0,0)$, a mnożenia $(1,0)$. Elementem przeciwnym do (a,b) jest $-(a,b) = (-a,-b)$, a odwrotnym do $(a,b) \neq (0,0)$ jest

$$(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right).$$

Zdefiniujemy mnożenie liczby zespolonej przez rzeczywistą w następujący (naturalny) sposób. Niech $z = (a,b) \in \mathbf{C}$ i $c \in \mathbf{R}$. Wtedy

$$c * (a,b) = (a,b) * c = (c * a, c * b).$$

Przyjmując tą konwencję, mamy

$$(a,b) = a * (1,0) + b * (0,1).$$

W końcu, utożsamiając liczbę zespoloną $(a,0)$ z liczbą rzeczywistą a, oraz wprowadzając dodatkowo oznaczenie

$$\imath := (0,1)$$

otrzymujemy

$$(a,b) = a + \imath * b. \tag{1.1}$$

$a = \Re z$ nazywa się *częścią rzeczywistą*, a $b = \Im z$ *częścią urojoną* liczby zespolonej. Samą liczbę zespoloną $\imath$ nazywamy *jednostką urojoną*. Zauważmy, że

$$\imath^2 = (-1,0) = -1.$$

1.2.2 Postać trygonometryczna

Postać (1.1) jest najbardziej rozpowszechniona. Często wygodnie jest użyć również postaci trygonometrycznej, która jest konsekwencją interpretacji liczby zespolonej (a,b) jako punktu na płaszczyźnie (tzw. *płaszczyźnie zespolonej*) o współrzędnych a i b. Dokładniej, przyjmując

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

oraz kąt ϕ tak, że

$$\sin\phi = \frac{b}{|z|}, \qquad \cos\phi = \frac{a}{|z|},$$

otrzymujemy

$$z = |z|(\cos\phi + \imath \sin\phi). \tag{1.2}$$

Jest to właśnie *postać trygonometryczna*. Liczbę rzeczywistą $|z|$ nazywamy *modułem* liczby zespolonej z, a ϕ jej *argumentem*, $\phi = \arg z$.

Jeśli $z \neq 0$ i założymy, że $\phi \in [0, 2\pi)$ to postać trygonometryczna jest wyznaczona jednoznacznie. Piszemy wtedy $\phi = \mathrm{Arg} z$.

1.2.3 Wzór de Moivre'a

Niech $z = |z|(\cos\phi + \imath\sin\phi)$, $w = |w|(\cos\psi + \imath\sin\psi)$ będą dwoma liczbami zespolonymi. Wtedy

$$\begin{aligned} w * z &= |w||z|\left((\cos\phi\cos\psi - \sin\phi\sin\psi) + \imath(\sin\phi\cos\psi + \sin\psi\cos\phi)\right) \\ &= |w||z|\left(\cos(\phi+\psi) + \imath\sin(\phi+\psi)\right), \end{aligned}$$

a stąd

$$|w * z| = |w||z| \qquad \text{oraz} \qquad \arg(w * z) = \arg w + \arg z.$$

Właśnie w tych równościach przejawia się wygoda postaci trygonometrycznej. W szczególności mamy bowiem $z^2 = |z|^2(\cos 2\phi + \imath\sin 2\phi)$ i postępując dalej indukcyjnie otrzymujemy *wzór de Moivre'a*. Mianowicie, dla dowolnej liczby zespolonej z w postaci trygonometrycznej (1.2) mamy

$$z^n = |z|^n(\cos(n\phi) + \imath\sin(n\phi)), \qquad n = 0, 1, 2, \ldots \tag{1.3}$$

Łatwo zauważyć, że wzór (1.3) jest prawdziwy również dla $n = -1$, a stąd dla wszystkich całkowitych n. Przyjmując za $z^{1/n}$ szczególne rozwiązanie równania $w^n = z$, mianowicie

$$z^{1/n} = |z|^{1/n}\left(\cos(\phi/n) + \imath\sin(\phi/n)\right),$$

gdzie $\phi = \mathrm{Arg} z$, uogólniamy (1.3) dla wszystkich wykładników wymiernych. Stosując dalej argument z przejściem granicznym (każda liczba rzeczywista jest granicą ciągu liczb wymiernych) otrzymujemy w końcu następujący *uogólniony* wzór de Moivre'a:

$$\forall a \in \mathbf{R} \qquad z^a = |z|^a\left(\cos(a\phi) + \imath\sin(a\phi)\right).$$

Prostym wnioskiem z ostatniego wzoru jest równanie

$$z = |z| * \omega^{\phi},$$

gdzie $\omega = \cos 1 + \imath \sin 1 = 0,540302\ldots + \imath * 0,84147\ldots \in \mathbf{C}$. Jest to uogólnienie na przypadek liczb zespolonych wzoru $x = |x| * \mathrm{sgn}(x)$ znanego z przypadku liczb rzeczywistych.

1.2.4 Pierwiastki z jedynki

Rozpatrzmy rozwiązania równania

$$z^n = 1$$

dla dowolnej naturalej n. W dziedzinie rzeczywistej pierwiastkiem jest 1 jeśli n jest nieparzyste, albo 1 i (-1) jeśli n jest parzyste. W dziedzinie zespolonej mamy zawsze n pierwiastków. Rzeczywiście, ponieważ $1 = \cos(2k\pi) + \imath \sin(2k\pi)$, ze wzoru de Moivre'a dostajemy, że wszyskie pierwiastki wyrażają się wzorami

$$z_k := \cos\left(\frac{2k\pi}{n}\right) + \imath \sin\left(\frac{2k\pi}{n}\right), \qquad k = 0, 1, 2, \ldots, n-1.$$

Zauważmy, że z_j leżą na okręgu jednostkowym płaszczyzny zespolonej. Zbiór $G = \{z_k : k = 0, 1, \ldots, n-1\}$ ze zwykłym mnożeniem liczb zespolonych tworzy grupę z elementem neutralnym $z_0 = 1$.

1.2.5 Sprzężenie

Liczbę *sprzężoną* do $z = a + \imath b$ definiujemy jako

$$\overline{z} := a - \imath b.$$

Zauważmy, że $\overline{\overline{z}} = z$ oraz $z * \overline{z} = |z|^2$. Mamy też

$$\frac{z + \overline{z}}{2} = \Re z \quad \text{i} \quad \frac{z - \overline{z}}{2\imath} = \Im z.$$

I jeszcze jedna ważna własność sprzężenia. Jeśli $\diamond \in \{+, -, *, /\}$ to

$$\overline{w \diamond z} = \overline{w} \diamond \overline{z}.$$

Stosując indukcję, można ten wzór uogólnić w następujący sposób. Jeśli $f(u_1, u_2, \ldots, u_s)$ jest wyrażeniem arytmetycznym, gdzie u_j są stałymi lub zmiennymi zespolonymi, to

$$\overline{f(u_1, u_2, \ldots, u_s)} = f(\overline{u}_1, \overline{u}_2, \ldots, \overline{u}_s).$$

1.3 Wielomiany

Definicja 1.4 Wielomianem p *nad ciałem* $\mathbf{K}$ *nazywamy funkcję zmiennej* z *o wartościach w ciele* $\mathbf{K}$ *daną wzorem*

$$p(z) := \sum_{j=0}^{n} a_j z^j = a_0 + a_1 z + \cdots + a_n z^n,$$

gdzie $a_j \in \mathbf{K}$, $0 \leq j \leq n$, $a_n \neq 0$, *są* współczynnikami *wielomianu. Liczbę* n *nazywamy* stopniem *wielomianu i oznaczamy*

$$n = \deg p.$$

(Przyjmujemy przy tym, że $\deg 0 = -\infty$*.)*

1.3.1 Algorytm Hornera

Każdy wielomian $p(z) = \sum_{k=0}^{n} a_k z^k$ stopnia $n \geq 1$ o współczynnikach zespolonych można podzielić przez dwumian $z - \xi$ otrzymując

$$p(z) = q(z)(z - \xi) + \eta,$$

gdzie $\deg q = n - 1$, a $\eta \in \mathbf{C}$. Dodatkowo, jeśli p ma współczynniki rzeczywiste i $\xi \in \mathbf{R}$, to q ma również współczynniki rzeczywiste i $\eta \in \mathbf{R}$.

Iloraz q oraz resztę η z dzielenia można otrzymać stosując *algorytm Hornera*:

$\{\ b_n := a_n;$
for $k := n - 1$ **downto** 0 **do** $\ b_k := a_k + \xi * b_{k+1};$
$\}$

Wtedy $q(z) = \sum_{k=1}^{n} b_k z^{k-1}$ oraz reszta $\eta = b_0$.

1.3.2 Zasadnicze twierdzenie algebry

Dla wielomianów zespolonych prawdziwe jest następujące ważne twierdzenie.

Twierdzenie 1.1 (Zasadnicze Twierdzenie Algebry)
Każdy wielomian zespolony p *stopnia co najmniej pierwszego ma pierwiastek zespolony, tzn. równanie* $p(z) = 0$ *ma rozwiązanie.*

Twierdzenie 1.1 mówi, że liczby zespolone $\mathbf{C}$ są ciałem *algebraicznie domkniętym*. (Przypomnijmy, że liczby rzeczywiste $\mathbf{R}$ *nie* są algebraicznie domknięte, bo np. równanie $x^2 + 1 = 0$ nie ma rozwiązań w $\mathbf{R}$.)

Konsekwencją algebraicznej domkniętości $\mathbf{C}$ jest *faktoryzacja* (rozkład) wielomianu zespolonego na czynniki pierwszego stopnia. Dokładniej, stosując n-krotnie zasadnicze twierdzenie algebry oraz fakt, że jeśli ξ jest pierwiastkiem wielomianu p to reszta z dzielenia p przez $(\cdot - \xi)$ jest zerowa, otrzymujemy rozkład

$$p(z) = a_n(z - z_1)(z - z_2)\cdots(z - z_n), \tag{1.4}$$

gdzie z_j, $1 \leq j \leq n$, są pierwiastkami p. Zakładając, że tylko m pierwiastków jest parami różnych ($1 \leq m \leq n$), możemy równoważnie napisać, że

$$p(z) = a_n(z - u_1)^{s_1}(z - u_2)^{s_2}\cdots(z - u_m)^{s_m},$$

gdzie $u_i \neq u_j$ o ile $i \neq j$, oraz $\sum_{j=1}^{m} s_j = n$. Przy tym zapisie, s_j nazywamy *krotnością* pierwiastka u_j.

Załóżmy teraz, że współczynniki wielomianu p są rzeczywiste, $a_j \in \mathbf{R}$, $0 \leq j \leq n$. Załóżmy też, że $p(\xi) = 0$ i $\xi \notin \mathbf{R}$. Wtedy $\overline{\xi} \neq \xi$ i

$$p(\overline{\xi}) = \sum_{j=0}^{n} a_j \overline{\xi}^j = \sum_{j=0}^{n} \overline{a}_j \overline{\xi^j} = \overline{\sum_{j=0}^{n} a_j \xi^j} = \overline{0} = 0,$$

tzn. jeśli ξ jest pierwiastkiem to także liczba sprzężona $\overline{\xi}$ jest pierwiastkiem; obie występują w rozwinięciu (1.4). Ale

$$(z - \xi)(z - \overline{\xi}) = z^2 - z(\xi + \overline{\xi}) + \xi\overline{\xi} = z^2 - 2z\Re\xi + |\xi|^2$$

jest trójmianem kwadratowym o współczynnikach rzeczywistych. Stąd wniosek, że wielomian rzeczywisty daje się rozłożyć na iloczyn czynników stopnia co najwyżej drugiego.