

Część 1. Prolegomena: Struktury algebraiczne

Jedną z najbardziej fundamentalnych składowych formalnego opisu rzeczywistości poznawalnej, motywowanego potrzebą komunikacji wyników jej obserwacji dla zobiektywizowania wyciąganych na ich podstawie wniosków poznawczych, jest pojęcie **zbioru**, określanego choćby poprzez wskazanie cechy uwspólnianej przez wszystkie jego elementy. Kategorifikacja bytów i zjawisk fizycznych prowadzi dalej do określenia klas obiektów fizycznych ze strukturą i wskazania relacji pomiędzy nimi zachowujących ową strukturę (np. klasy obserwatorów inercjalnych i transformacji Lorentza jako relacji pomiędzy nimi). Ta prosta konstatacja stanowi elementarne uzasadnienie konieczności wnikliwej i abstrakcyjnej dyskusji **zbiorów ze strukturą**. Część tej dyskusji ma charakter analityczny i jest przedmiotem wykładu z analizy matematycznej, część zaś, o charakterze algebraicznym i geometrycznym, stanowi treść niniejszego wykładu z algebry. Naturalnie istnieje silne sprzężenie strukturalne obu kursów. Dla sprecyzowania przedmiotu dociekań zaczniemy od kilku podstawowych definicji.

Definicja 1. Niechaj S będzie zbiorem i wprowadźmy oznaczenie

$$S^{\times n} := \bigtimes_{i=1}^n S.$$

Dla dowolnej liczby $n \in \mathbb{N} \setminus \{0\}$ **operacja n -argumentowa** na S to odwzorowanie

$$\phi_n : S^{\times n} \longrightarrow S.$$

Pojęcie to rozszerzamy na przypadek $n = 0$ przyjmując konwencję $S^{\times 0} := \{\bullet\}$ (zbiór jednoelementowy, czyli singleton) i określając **operację 0-argumentową**

$$\phi_0 : S^{\times 0} \longrightarrow S,$$

którą w dalszej części wykładu będziemy najczęściej utożsamiać z obrazem elementu $\bullet$ w S względem ϕ_0 ,

$$\phi_0(\bullet) \equiv e_0 \in S,$$

zwanym **stałą**.

Powyższa definicja pozwala wprowadzić pojęcie centralne dla całej naszej dalszej dyskusji.

Definicja 2. W notacji Def. 1 **struktura algebraiczna o nośniku S** to kolekcja

$$\mathcal{S} := (S, \phi_{k_1}, \phi_{k_2}, \dots, \phi_{k_N})$$

złożona ze zbioru S oraz – dla pewnych ustalonych liczb naturalnych $k_1 \geq k_2 \geq \dots \geq k_N \geq 0$, $N \in \mathbb{N} \setminus \{0\}$ – z operacji k_i -argumentowych ϕ_{k_i} , $i \in \overline{1, N}$.

Podstruktura algebraiczna na podzbiórze $P \subset S$ to analogiczna do poprzedniej kolekcja

$$(P, \phi_{k_1}, \phi_{k_2}, \dots, \phi_{k_N})$$

spełniająca **warunki domkniętości**

$$\forall_{i \in \overline{1, N}} : \phi_{k_i}(P^{\times k_i}) \subset P.$$

W dalszej części wykładu dokonamy abstrakcji prostych struktur algebraicznych ze znanych konstrukcji arytmetycznych.

Przykład(y) 1.

(1) Liczby naturalne:

- zbiór $\mathbb{N} = \{0, 1, 2, \dots\}$;

- operacja 2-argumentowa

$$+ : \mathbb{N}^{\times 2} \longrightarrow \mathbb{N} : (m, n) \longmapsto m + n$$

o własnościach:

$$\forall_{m,n \in \mathbb{N}} : m + n = n + m \quad (\text{przemienność});$$

$$\forall_{k,l,m \in \mathbb{N}} : (k + l) + m = k + (l + m) \quad (\text{łączność});$$

- element 0 neutralny względem +, który spełnia

$$\forall_{n \in \mathbb{N}} : n + 0 = n = 0 + n.$$

(2) Liczby całkowite:

- zbiór $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$;
- operacja 2-argumentowa

$$+ : \mathbb{Z}^{\times 2} \longrightarrow \mathbb{Z} : (m, n) \longmapsto m + n$$

o własnościach j/w;

- element 0 neutralny względem + j/w;
- operacja 1-argumentowa

$$P : \mathbb{Z} \longrightarrow \mathbb{Z} : n \longmapsto -n$$

o własności

$$\forall_{n \in \mathbb{Z}} : n + P(n) = 0.$$

Stosujemy tu skrócony zapis: $m + (-n) \equiv m - n$.

(3) Liczby wymierne:

- zbiór $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \times \{0\})) / \sim$, przy czym $(p, q) \sim (r, s) \iff p \cdot s = q \cdot r$ – łatwo pokazać, że jest to relacja równoważności¹ na $\mathbb{Z} \times (\mathbb{Z} \times \{0\})$, zadająca rozkład zbioru na klasy abstrakcji $[(p, q)] \equiv \frac{p}{q}$;
- operacje 2-argumentowe

$$+_Q : \mathbb{Q}^{\times 2} \longrightarrow \mathbb{Q} : ([p, q], [r, s]) \longmapsto [(p \cdot s + q \cdot r, q \cdot s)],$$

$$\cdot_Q : \mathbb{Q}^{\times 2} \longrightarrow \mathbb{Q} : ([p, q], [r, s]) \longmapsto [(p \cdot r, q \cdot s)]$$

o własnościach:

- $+_Q$ i $\cdot_Q$ przemienne i łączne j/w;
- $\forall_{a,b,c \in \mathbb{Q}} : a \cdot_Q (b +_Q c) = (a \cdot_Q b) +_Q (a \cdot_Q c)$ (rozdzielność $\cdot_Q$ względem $+_Q$);
- elementy neutralne: $[(0, 1)]$ względem $+_Q$ o własności j/w oraz $[(1, 1)]$ względem $\cdot_Q$ o własności

$$\forall_{q \in \mathbb{Q}} : [(1, 1)] \cdot_Q q = q;$$

- operacja 1-argumentowa $P : \mathbb{Q} \longrightarrow \mathbb{Q} : [(p, q)] \longmapsto [(-p, q)]$ o własności j/w;
- operacja 1-argumentowa (o ograniczonym nośniku) $\text{Inv} : \mathbb{Q} \setminus \{[(0, 1)]\} \longrightarrow \mathbb{Q} : [(p, q)] \longmapsto [(q, p)]$ o własności

$$\forall_{q \in \mathbb{Q} \setminus \{[(0, 1)]\}} : q \cdot_Q \text{Inv}(q) = [(1, 1)].$$

Wymienione przykłady prowadzą do następujących definicji.

I Struktury grupopodobne.

Definicja 3. **Magma** to para (S, ϕ_2) złożona ze zbioru S oraz operacji 2-argumentowej $\phi_2 : S^{\times 2} \longrightarrow S$.

Przykład(y) 2. Para $(\mathbb{N} \setminus \{0\} =: \mathbb{N}_{>0}, \wedge)$ złożona ze zbioru $\mathbb{N}_{>0}$ dodatnich liczb całkowitych i operacji 2-argumentowej (nieprzemiennej i niełącznej)

$$\wedge : \mathbb{N}_{>0}^{\times 2} \longrightarrow \mathbb{N}_{>0} : (m, n) \longmapsto m^n.$$

¹O relacjach równoważności traktuje kurs analizy matematycznej, por., np., [Mau91, Rozdz. I § 4] i [Die65, Rozdz. I.8].

Definicja 4. Półgrupa to magma (S, ϕ_2) , w której operacja ϕ_2 jest łączna, co wyraża diagram przemienny

$$\begin{array}{ccc} S \times S \times S & \xrightarrow{\phi_2 \times \text{id}_S} & S \times S \\ \text{id}_S \times \phi_2 \downarrow & & \downarrow \phi_2 \\ S \times S & \xrightarrow{\phi_2} & S \end{array} .$$

Przykład(y) 3. Para $(\mathfrak{T}, \Gamma)$ złożona z następujących elementów:

- $\mathfrak{T}$ jest zbiorem **osadzonych drzew binarnych**, tj. niezorientowanych grafów acyklicznych i spójnych (czyli takich, których krawędzie są odcinkami bez wyróżnionej orientacji, tj. bez wyróżnionego porządku na zbiorze końców, i w których od każdego wierzchołka do każdego innego wierzchołka można dotrzeć wzdłuż grafu dokładnie jedną ścieżką), o wierzchołkach, z których każdy leży na końcu nie więcej niż trzech krawędzi (czyli ma **walencję** $w \leq 3$), i z wyróżnionym wierzchołkiem – zwanym **korzeniem** – o walencji 1, a także z wyróżnionym uporządkowaniem (tj. przypisaniem cech „prawy/lewy”) dwójki krawędzi wychodzących z każdego z wierzchołków o walencji 3 przy przemierzaniu grafu w kierunku od korzenia do tegoż wierzchołka;
- Γ jest łączną (i nieprzemienną) operacją 2-argumentową, zwaną **szczepieniem**, która polega na przyłączeniu korzenia drugiego argumentu do wyróżnionego wierzchołka pierwszego argumentu, który leży na końcu ścieżki prowadzącej od korzenia i skręcającej w prawo w każdym wierzchołku łączącym ze sobą trzy krawędzie.

Definicja 5. Monoid to trójka (S, ϕ_2, ϕ_0) , w której para (S, ϕ_2) jest półgrupą, natomiast ϕ_0 jest operacją 0-argumentową zadającą stałą $\phi_0(\bullet) = e \in S$, która jest elementem neutralnym względem operacji ϕ_2 , przy czym tę ostatnią własność wyrażają diagramy przemienne

$$\begin{array}{ccc} S \times \{\bullet\} & \xrightarrow{\text{id}_S \times \phi_0} & S \times S \\ & \searrow \text{pr}_1 & \downarrow \phi_2 \\ & & S \end{array} , \quad \begin{array}{ccc} \{\bullet\} \times S & \xrightarrow{\phi_0 \times \text{id}_S} & S \times S \\ & \searrow \text{pr}_2 & \downarrow \phi_2 \\ & & S \end{array} .$$

Przykład(y) 4.

- (1) Trójka $(\mathbb{N}, +, \mathbf{0})$ złożona ze zbioru $\mathbb{N}$ liczb naturalnych, dodawania $+$ oraz operacji 0-argumentowej $\mathbf{0}$, której obrazem jest stała $0 \in \mathbb{N}$.
- (2) Trójka $(\mathcal{A}_X, \mathbf{c}, \emptyset)$ złożona ze **słownika** $\mathcal{A}_X$ będącego zbiorem skończonych ciągów elementów zbioru skończonego $X = \{x_1, x_2, \dots, x_n\}$, $n \in \mathbb{N}$, zwanego **alfabetem**, z operacji 2-argumentowej $\mathbf{c}$ zwanej **konkatenacją** i polegającej na dostawianiu wyrazów drugiego argumentu do wyrazów pierwszego argumentu na jego końcu, tj., np.

$$\mathbf{c}((x_{i_1}, x_{i_2}, \dots, x_{i_M}), (x_{j_1}, x_{j_2}, \dots, x_{j_N})) = (x_{i_1}, x_{i_2}, \dots, x_{i_M}, x_{j_1}, x_{j_2}, \dots, x_{j_N}),$$

oraz z operacji 0-argumentowej $\emptyset$, której obrazem jest ciąg pusty. Elementy słownika (tj. **wyrazy**) są zwykle zapisywane z opuszczeniem nawiasów i przecinków, np.

$$(x_{i_1}, x_{i_2}, \dots, x_{i_M}) \equiv x_{i_1} x_{i_2} \dots x_{i_M} .$$

Opisany monoid nosi miano **monoidu swobodnego nad X** .

Definicja 6. Grupa to czwórka $(S, \phi_2, \phi_1, \phi_0)$, w której trójka (S, ϕ_2, ϕ_0) jest monoidem, natomiast $\phi_1 : S \curvearrowright$ jest operacją 1-argumentową o własności wyrażonej przez diagramy przemienne

$$\begin{array}{ccc} S \times \{\bullet\} & \xrightarrow{(\text{id}_S, \phi_1) \circ \text{pr}_1} & S \times S \\ & \searrow \phi_0 \circ \text{pr}_2 & \downarrow \phi_2 \\ & & S \end{array} , \quad \begin{array}{ccc} S \times \{\bullet\} & \xrightarrow{(\phi_1, \text{id}_S) \circ \text{pr}_1} & S \times S \\ & \searrow \phi_0 \circ \text{pr}_2 & \downarrow \phi_2 \\ & & S \end{array} .$$

W szczególności **grupa przemienna** (zwana także **abelową**) to taka, w której operacja ϕ_2 jest przemienna, co wyraża diagram przemienny

$$\begin{array}{ccc} S \times S & \xrightarrow{\tau_S} & S \times S \\ & \searrow \phi_2 & \downarrow \phi_2 \\ & & S \end{array} .$$

Przykład(y) 5.

- (1) Czwórka $(\mathfrak{S}_X, \circ, (\cdot)^{-1}, \bullet \mapsto \text{id}_X)$ złożona ze zbioru $\mathfrak{S}_X$ permutacji elementów pewnego zbioru X (tj. bijektywnych odwzorowań $\sigma : X \rightarrow X$), (nieprzemiennej) operacji 2-argumentowej $\circ$ będącej złożeniem (czyli superpozycją) odwzorowań, operacji 1-argumentowej $\sigma \mapsto \sigma^{-1}$ brania odwrotności odwzorowania i operacji 0-argumentowej $\bullet \mapsto \text{id}_X$, której obrazem jest odwzorowanie identycznościowe. Opisana grupa nosi miano **grupy symetrycznej na X** . W przypadku zbioru X o mocy $|X| = n$ stosuje się zwykle oznaczenie $\mathfrak{S}_X \equiv \mathfrak{S}_n$.
- (2) Czwórka $(\mathcal{Z}(G), \phi_2, \phi_1, \phi_0)$ będąca podgrupą (dowolnej) grupy $(G, \phi_2, \phi_1, \phi_0)$ o nośniku

$$\mathcal{Z}(G) := \{ z \in G \mid \forall_{g \in G} : \phi_2(z, g) = \phi_2(g, z) \}$$

zwanym **centrum grupy G** .

II Struktury pierścieniopodobne.

Definicja 7. Półpierścień to piątka $(S, \phi_2^{(1)}, \phi_2^{(2)}, \phi_0^{(1)}, \phi_0^{(2)})$, w której obie trójki $(S, \phi_2^{(\alpha)}, \phi_0^{(\alpha)})$, $\alpha \in \{1, 2\}$ są monoidami, a przy tym

(PP1) operacja $\phi_2^{(1)}$ jest przemienna;

(PP2) operacja $\phi_2^{(2)}$ jest rozdzielna względem operacji $\phi_2^{(1)}$, co wyrażają diagramy przemienne

$$\begin{array}{ccc} S \times S \times S & \xrightarrow{\text{id}_S \times \phi_2^{(1)}} & S \times S \\ \downarrow (\phi_2^{(2)} \circ \text{pr}_{1,2}, \phi_2^{(2)} \circ \text{pr}_{1,3}) & & \downarrow \phi_2^{(2)} \\ S \times S & \xrightarrow{\phi_2^{(1)}} & S \end{array} , \quad \begin{array}{ccc} S \times S \times S & \xrightarrow{\phi_2^{(1)} \times \text{id}_S} & S \times S \\ \downarrow (\phi_2^{(2)} \circ \text{pr}_{1,3}, \phi_2^{(2)} \circ \text{pr}_{2,3}) & & \downarrow \phi_2^{(2)} \\ S \times S & \xrightarrow{\phi_2^{(1)}} & S \end{array} ;$$

(PP3) operacja 0-argumentowa $\phi_0^{(1)}$ spełnia tożsamości wyrażone przez diagramy przemienne

$$\begin{array}{ccc} \{\bullet\} \times S & \xrightarrow{\phi_0^{(1)} \times \text{id}_S} & S \times S \\ & \searrow \phi_0^{(1)} \circ \text{pr}_1 & \downarrow \phi_2^{(2)} \\ & & S \end{array} , \quad \begin{array}{ccc} S \times \{\bullet\} & \xrightarrow{\text{id}_S \times \phi_0^{(1)}} & S \times S \\ & \searrow \phi_0^{(1)} \circ \text{pr}_2 & \downarrow \phi_2^{(2)} \\ & & S \end{array} .$$

Przykład(y) 6. Piątka $(\mathbb{R} \cup \{\infty\}, (x, y) \mapsto \min(x, y), (x, y) \mapsto x + y, \bullet \mapsto \infty, \bullet \mapsto 0)$. Z racji związku z tzw. geometrią tropikalną, opisana struktura nosi miano **półpierścienia tropikalnego**.

Definicja 8. Pierścień to szóstka $(S, \phi_2^{(1)}, \phi_2^{(2)}, \phi_1, \phi_0^{(1)}, \phi_0^{(2)})$, w której piątka $(S, \phi_2^{(1)}, \phi_2^{(2)}, \phi_0^{(1)}, \phi_0^{(2)})$ jest półpierścieniem (przy czym aksjomat (PP3) jest tu konsekwencją pozostałych aksjomatów), a ponadto czwórka $(S, \phi_2^{(1)}, \phi_1, \phi_0^{(1)})$ jest grupą przemienną. W szczególności **pierścień przemienny** to taki, w którym operacja $\phi_2^{(2)}$ jest przemienna.

Przykład(y) 7. Szóstka $(\mathbb{Z}, +, \cdot, n \mapsto -n, \bullet \mapsto 0, \bullet \mapsto 1)$. Jest to pierścień przemienny.

Definicja 9. Ciało to siódemka $(S, \phi_2^{(1)}, \phi_2^{(2)}, \phi_1^{(1)}, \phi_1^{(2)}, \phi_0^{(1)}, \phi_0^{(2)})$, w której szóstka $(S, \phi_2^{(1)}, \phi_2^{(2)}, \phi_1^{(1)}, \phi_0^{(1)}, \phi_0^{(2)})$ jest pierścieniem przemiennym, natomiast $\phi_1^{(2)} : S \setminus \{\phi_0^{(1)}(\bullet)\} \rightarrow S^\times$

jest operacją 1-argumentową (o ograniczonym nośniku) o własności wyrażonej przez diagram przemienności

$$\begin{array}{ccc}
 S^\times \times \{\bullet\} & \xrightarrow{(\text{id}_S, \phi_1^{(2)}) \circ \text{pr}_1} & S^\times \times S^\times \\
 & \searrow \phi_0^{(2)} \circ \text{pr}_2 & \downarrow \phi_2^{(2)} \\
 & & S^\times
 \end{array} \quad (F)$$

Przykład(y) 8. Siódemka $(\mathbb{Z}/p\mathbb{Z}, ([k]_p, [l]_p) \mapsto [k+l]_p, ([k]_p, [l]_p) \mapsto [k \cdot l]_p, [k]_p \mapsto [p-k]_p, \bullet \mapsto [0]_p, \bullet \mapsto [1]_p)$, określona dla dowolnej liczby pierwszej p , o nośniku

$$\mathbb{Z}/p\mathbb{Z} = \{[0]_p, [1]_p, [2]_p, \dots, [p-1]_p\}$$

będącym zbiorem reszt *modulo* p ($[x]_p$ jest resztą z dzielenia liczby x przez p). Struktura ta nosi miano **ciała reszt modulo** p .

Oprócz powyższych rozpatruje się struktury bardziej złożone, jak choćby struktury modulo- i algebropodobne, w których skład wchodzi dwa zbiory i kilka operacji 2-argumentowych, także mieszanych. W dalszej części kursu zajmiemy się tymi spośród nich, które pełnią szczególnie istotną rolę w matematycznym modelowaniu przyrody, a mianowicie przestrzeniami liniowymi nad ciałem danym i – jeśli czas na to pozwoli – algebrami Liego. Ponadto wspomnimy o strukturach noszących miano algebr Clifforda, wyposażonych w co najmniej 4 działania 2-argumentowe (zwane iloczynem zewnętrznym i iloczynami wewnętrznymi). Pojawią się też przestrzenie Hilberta o dodatkowej strukturze (analitycznej) przestrzeni Banacha.

Zanim przejdziemy do dyskusji ważnych – z matematycznego i przede wszystkim fizycznego punktu widzenia – przykładów struktur wymienionych wyżej, wprowadzimy ważne pojęcie odwzorowania transportującego strukturę algebraiczną z dziedziny na przeciwdziedzinę.

Definicja 10. Przyjmijmy notację Def.1 i 2. **Homomorfizm² struktury algebraicznej** $(S^{(1)}, \phi_{k_1}^{(1)}, \phi_{k_2}^{(1)}, \dots, \phi_{k_N}^{(1)})$ **w strukturę algebraiczną** (tego samego typu) $(S^{(2)}, \phi_{k_1}^{(2)}, \phi_{k_2}^{(2)}, \dots, \phi_{k_N}^{(2)})$ to odwzorowanie pomiędzy ich nośnikami,

$$\chi : S^{(1)} \longrightarrow S^{(2)},$$

zgodne z obecną na nich strukturą algebraiczną w sensie wyrażanym przez rodzinę diagramów przemienności:

$$\forall_{i \in \overline{1, N}} : \quad \begin{array}{ccc}
 (S^{(1)})^{\times k_i} & \xrightarrow{\phi_{k_i}^{(1)}} & S^{(1)} \\
 \downarrow \times_{i=1}^{k_i} \chi & & \downarrow \chi \\
 (S^{(2)})^{\times k_i} & \xrightarrow{\phi_{k_i}^{(2)}} & S^{(2)}
 \end{array}$$

Wyróżniamy następujące typy homomorfizmów:

- **monomorfizmy**, czyli homomorfizmy injektywne $S^{(1)} \hookrightarrow S^{(2)}$;
- **epimorfizmy**, czyli homomorfizmy surjektywne $S^{(1)} \twoheadrightarrow S^{(2)}$;
- **izomorfizmy**, czyli homomorfizmy bijektywne, $S^{(1)} \xrightarrow{\cong} S^{(2)}$;
- **endomorfizmy**, czyli homomorfizmy wewnętrzne $S^{(2)} \equiv S^{(1)} \circlearrowright$;
- **automorfizmy**, czyli bijektywne homomorfizmy wewnętrzne.

Należy w tym momencie przypomnieć, że odwzorowanie $f : X \longrightarrow Y$ ze zbioru X w zbiór Y jest

- **iniektywne**, gdy dla dowolnych $x, y \in X$ zachodzi implikacja

$$f(x) = f(y) \implies x = y;$$

²Homomorfizm to algebraiczna specjalizacja fundamentalnego w teorii kategorii [ML71] pojęcia morfizmu. Oto więc w naszych rozważaniach miejsce ogólnej klasy obiektów zajmuje klasa zbiorów z ustaloną strukturą algebraiczną, w roli zaś morfizmów, tj. odwzorowań pomiędzy obiektami zachowujących definiujące własności kategorii, występują homomorfizmy.

- surjektywne, gdy prawdziwe jest zdanie

$$\forall y \in Y \exists x \in X : y = f(x);$$

- bijektywne, gdy jest iniektywne i surjektywne zarazem.

Przykład(y) 9.

- (1) Monomorfizmem ciała $(\mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}}, P_{\mathbb{Q}}, \text{Inv}_{\mathbb{Q}}, \frac{0}{1}, \frac{1}{1})$ liczb wymiernych (opisanego wcześniej) w ciało $(\mathbb{R}, +_{\mathbb{R}}, \cdot_{\mathbb{R}}, P_{\mathbb{R}}, \text{Inv}_{\mathbb{R}}, [(\frac{0}{1})_{n \in \mathbb{N}}]_{\sim}, [(\frac{1}{1})_{n \in \mathbb{N}}]_{\sim})$ liczb rzeczywistych (o nośniku rozumianym – w duchu konstrukcji Cantora–Méraya – jako zbiór klas abstrakcji ciągów Cauchy’ego liczb wymiernych względem relacji „dowolnej bliskości wyrazów o dostatecznie dużych indeksach”, co opisuje, np., K. Maurin w [Mau91, §6 i §7]) jest odwzorowanie

$$\mathbb{Q} \rightarrow \mathbb{R} : \frac{p}{q} \mapsto [(\frac{p}{q})_{n \in \mathbb{N}}]_{\sim},$$

przypisujące liczbie $\frac{p}{q}$ klasę ciągu stałego $(\frac{p}{q})_{n \in \mathbb{N}}$.

- (2) Epimorfizmem grupy

$$\left(\text{GL}(2, \mathbb{R}), \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right) \mapsto \begin{pmatrix} a \cdot e + b \cdot g & a \cdot f + b \cdot h \\ c \cdot e + d \cdot g & c \cdot f + d \cdot h \end{pmatrix}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{1}{a \cdot d - b \cdot c} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right)$$

odwracalnych macierzy wymiaru 2×2 o wyrazach rzeczywistych (zwanej **pełną grupą liniową stopnia 2 nad $\mathbb{R}$**) na grupę $(\mathfrak{H}_{\overline{\mathbb{R}}}, \circ, h \mapsto h^{-1}, \text{id}_{\overline{\mathbb{R}}})$ homografii uzwarconej osi rzeczywistej $\overline{\mathbb{R}} := \mathbb{R} \cup \{\infty\}$, tj. odwzorowań postaci

$$h : \overline{\mathbb{R}} \circ : x \mapsto \frac{a \cdot x + b}{c \cdot x + d}, \quad a, b, c, d \in \mathbb{R}, \quad a \cdot d - b \cdot c \neq 0,$$

jest odwzorowanie

$$\text{GL}(2, \mathbb{R}) \rightarrow \mathfrak{H}_{\overline{\mathbb{R}}} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \left(x \mapsto \frac{a \cdot x + b}{c \cdot x + d} \right).$$

- (3) Izomorfizmem monoidu $(\mathbb{N}, +, \mathbf{0})$ liczb naturalnych w monoid $(2\mathbb{N}, +, \mathbf{0})$ parzystych liczb naturalnych jest odwzorowanie

$$\mathbb{N} \xrightarrow{\cong} 2\mathbb{N} : n \mapsto 2n.$$

- (4) Endomorfizmem dowolnego półpierścienia $(S, \phi_2^{(1)}, \phi_2^{(2)} \equiv \cdot, \phi_0^{(1)}, \phi_0^{(2)})$ jest odwzorowanie

$$S \circ : s \mapsto x \cdot s \cdot x,$$

określone dla dowolnego jego elementu **unipotentnego** $s \in S$, tj. takiego, który spełnia tożsamość

$$x \cdot x = \phi_0^{(2)}(\bullet).$$

- (5) Automorfizmem dowolnej grupy $(G, \phi_2 \equiv \cdot, \phi_1 \equiv \text{Inv}, \phi_0)$ jest odwzorowanie, określone dla dowolnego jej elementu $h \in G$,

$$\text{Ad}_h : G \circ : g \mapsto h \cdot g \cdot h^{-1}.$$

Nierzadko narzucenie warunku zachowania niektórych elementów rozważanej struktury algebraicznej pociąga za sobą zachowanie teŝe w całości. Przykładu dostarcza tutaj teoria homomorfizmów grup, którą omówimy w dziale 3.

Zanim przejdziemy do bardziej szczegółowej dyskusji konkretnych struktur algebraicznych, wysłowimy oczywistą acz przydatną obserwację.

Stwierdzenie 1. *Każdy monomorfizm jest izomorfizmem dziedziny na jej obraz względem tego monomorfizmu.*

*

*

*

Literatura uzupełniająca: Szczegółowe omówienie wprowadzonych tu (i wielu innych) struktur algebraicznych można znaleźć w opracowaniu Bourbakiego [Bou07] oraz w klasycznym kursie Langa [Lan02] i doskonałej trytomowej monografii Cohna [Coh74, Coh77, Coh90].

Część 2. Struktury proste

Celem pierwszej części niniejszego kursu, a zarazem oczywistym punktem wyjścia do dyskusji zastosowań algebry w fizyce i geometrii, jest dokładne zbadanie wybranych elementarnych struktur algebraicznych, których związek z nowoczesnym opisem zjawisk – ledwie wzmiankowany w poświęconych im rozdziałach – dowodnie wykażą przyszłe kursy specjalistyczne z różnych dziedzin fizyki teoretycznej i matematycznej. Konsekwentnie realizowany schemat opisu, wedle którego po aksjomatyzacji struktury podstawowej następuje szczegółowa analiza morfizmów tejże struktury oraz relacji indukowanych w jej nośniku, ma w zamyśle posłużyć wykształceniu narzędzi precyzyjnego, efektywnego i (choćby już z tych tylko względów) naturalnego opisu obiektów o charakterze algebraicznym, także tych bardziej złożonych, jak również strukturalnych relacji pomiędzy nimi. W opisanym schemacie dociekliwy Czytelnik dostrzeże bez trudu odzwierciedlenie logicznego porządku, jaki w opisie struktur algebraicznych (i nie tylko) wprowadza teoria kategorii [ML71].

1. CIAŁO LICZB ZESPOŁONYCH

Dyskusję konkretnych struktur algebraicznych o znaczeniu fizycznym zaczniemy od szczegółowego omówienia rozszerzenia algebraicznego dobrze znanego (choćby z wykładu analizy matematycznej) ciała liczb rzeczywistych. Rozszerzenie to stanowi ważny przykład ciała algebraicznie domkniętego, a w przyszłości znajdzie szereg zastosowań – zarówno technicznych jak i strukturalnych – w mechanice fal, klasycznej teorii elektromagnetyzmu, mechanice kwantowej, kwantowej teorii pola i teorii strun. Zaczniemy od wypisania w jawnej postaci aksjomatów ciała.

Definicja 9’. Ciałem to siódemka $(\mathbf{k}, A, M, P, \text{Inv}, \mathbf{0}, \mathbf{1})$, w której

- $\mathbf{k}$ jest zbiorem;
- $A : \mathbf{k}^{\times 2} \rightarrow \mathbf{k} : (x, y) \mapsto A(x, y) \equiv x +_{\mathbf{k}} y$ jest operacją 2-argumentową zwaną **dodawaniem**;
- $M : \mathbf{k}^{\times 2} \rightarrow \mathbf{k} : (x, y) \mapsto M(x, y) \equiv x \cdot_{\mathbf{k}} y$ jest operacją 2-argumentową zwaną **mnożeniem**;
- $P : \mathbf{k} \rightarrow \mathbf{k} : x \mapsto P(x) \equiv -x$ jest operacją 1-argumentową zwaną **braniem przeciwności**;
- $\text{Inv} : \mathbf{k} \setminus \{\mathbf{0}(\bullet)\} \rightarrow \mathbf{k}^{\times} : x \mapsto \text{Inv}(x) \equiv x^{-1}$ jest operacją 1-argumentową (o ograniczonym nośniku) zwaną **braniem odwrotności**;
- $\mathbf{0} : \{\bullet\} \rightarrow \mathbf{k} : \bullet \mapsto 0$ jest operacją 0-argumentową zwaną **zerem**;
- $\mathbf{1} : \{\bullet\} \rightarrow \mathbf{k} : \bullet \mapsto 1$ jest operacją 0-argumentową zwaną **jedynką**,

przy czym składowe struktury spełniają następujące aksjomaty (wyrażone przez diagramy przemienne i równoważne zdania logiczne):

(F1) (łączność działań)

$$\begin{array}{ccc}
 \mathbf{k} \times \mathbf{k} \times \mathbf{k} & \xrightarrow{A \times \text{id}_{\mathbf{k}}} & \mathbf{k} \times \mathbf{k} \\
 \text{id}_{\mathbf{k}} \times A \downarrow & & \downarrow A \\
 \mathbf{k} \times \mathbf{k} & \xrightarrow{A} & \mathbf{k}
 \end{array} \quad \equiv \quad \forall_{x,y,z \in \mathbf{k}} : (x +_{\mathbf{k}} y) +_{\mathbf{k}} z = x +_{\mathbf{k}} (y +_{\mathbf{k}} z);$$

$$\begin{array}{ccc}
 \mathbf{k} \times \mathbf{k} \times \mathbf{k} & \xrightarrow{M \times \text{id}_{\mathbf{k}}} & \mathbf{k} \times \mathbf{k} \\
 \text{id}_{\mathbf{k}} \times M \downarrow & & \downarrow M \\
 \mathbf{k} \times \mathbf{k} & \xrightarrow{M} & \mathbf{k}
 \end{array} \quad \equiv \quad \forall_{x,y,z \in \mathbf{k}} : (x \cdot_{\mathbf{k}} y) \cdot_{\mathbf{k}} z = x \cdot_{\mathbf{k}} (y \cdot_{\mathbf{k}} z);$$

(F2) (przemienność działań)

$$\begin{array}{ccc}
 \mathbf{k} \times \mathbf{k} & \xrightarrow{\tau_{\mathbf{k}}} & \mathbf{k} \times \mathbf{k} \\
 & \searrow A & \downarrow A \\
 & & \mathbf{k}
 \end{array} \quad \equiv \quad \forall_{x,y \in \mathbf{k}} : x +_{\mathbf{k}} y = y +_{\mathbf{k}} x;$$

$$\begin{array}{ccc}
\mathbf{k} \times \mathbf{k} & \xrightarrow{\tau_{\mathbf{k}}} & \mathbf{k} \times \mathbf{k} \\
& \searrow M & \downarrow M \\
& & \mathbf{k}
\end{array} \quad \equiv \quad \forall_{x,y \in \mathbf{k}} : x \cdot_{\mathbf{k}} y = y \cdot_{\mathbf{k}} x ;$$

(F3) (rozdzielność mnożenia względem dodawania)

$$\begin{array}{ccc}
\mathbf{k} \times \mathbf{k} \times \mathbf{k} & \xrightarrow{\text{id}_{\mathbf{k}} \times A} & \mathbf{k} \times \mathbf{k} \\
(M \circ \text{pr}_{1,2}, M \circ \text{pr}_{1,3}) \downarrow & & \downarrow M \\
\mathbf{k} \times \mathbf{k} & \xrightarrow{A} & \mathbf{k}
\end{array} \quad \equiv \quad \forall_{x,y,z \in \mathbf{k}} : x \cdot_{\mathbf{k}} (y +_{\mathbf{k}} z) = (x \cdot_{\mathbf{k}} y) +_{\mathbf{k}} (x \cdot_{\mathbf{k}} z) ;$$

(F4) (istnienie elementów neutralnych względem działań)

$$\begin{array}{ccc}
\mathbf{k} \times \{\bullet\} & \xrightarrow{\text{id}_{\mathbf{k}} \times 0} & \mathbf{k} \times \mathbf{k} \\
& \searrow \text{pr}_1 & \downarrow A \\
& & \mathbf{k}
\end{array} \quad \equiv \quad \forall_{x \in \mathbf{k}} : x +_{\mathbf{k}} 0 = x ;$$

$$\begin{array}{ccc}
\mathbf{k} \times \{\bullet\} & \xrightarrow{\text{id}_{\mathbf{k}} \times 1} & \mathbf{k} \times \mathbf{k} \\
& \searrow \text{pr}_1 & \downarrow M \\
& & \mathbf{k}
\end{array} \quad \equiv \quad \forall_{x \in \mathbf{k}} : x \cdot_{\mathbf{k}} 1 = x ;$$

(F5) (istnienie elementów przeciwnych i odwrotnych do niezerowych)

$$\begin{array}{ccc}
\mathbf{k} \times \{\bullet\} & \xrightarrow{(\text{id}_{\mathbf{k}}, P) \circ \text{pr}_1} & \mathbf{k} \times \mathbf{k} \\
& \searrow 0 \circ \text{pr}_2 & \downarrow A \\
& & \mathbf{k}
\end{array} \quad \equiv \quad \forall_{x \in \mathbf{k}} : x +_{\mathbf{k}} (-x) = 0 ;$$

$$\begin{array}{ccc}
\mathbf{k}^{\times} \times \{\bullet\} & \xrightarrow{(\text{id}_{\mathbf{k}}, \text{Inv}) \circ \text{pr}_1} & \mathbf{k}^{\times} \times \mathbf{k}^{\times} \\
& \searrow 1 \circ \text{pr}_2 & \downarrow M \\
& & \mathbf{k}^{\times}
\end{array} \quad \equiv \quad \forall_{x \in \mathbf{k}^{\times}} : x \cdot_{\mathbf{k}} x^{-1} = 1 ;$$

(F6) (nietrywialność) $0 \neq 1$.

Przykład(y) 10.

- (1) Liczby wymierne z podaną wcześniej strukturą.
- (2) Liczby rzeczywiste ze strukturą indukowaną przez powyższą w konstrukcji Cantora–Méraya.
- (3) Ciało Galois rzędu 2 (najmniejsze ciało nietrywialne) o nośniku $\text{GF}_2 = \{0, 1\}$ i tabelkach

$$\text{działań: } \begin{array}{c|cc} +_{\text{GF}_2} & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \text{ oraz } \begin{array}{c|cc} \cdot_{\text{GF}_2} & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array} .$$

- (4) Ciało rzeczywistych funkcji wymiernych o nośniku $\mathbb{R}(\cdot) := \left\{ \frac{f(\cdot)}{g(\cdot)} \mid f, g \in \mathbb{R}[\cdot] \wedge g \neq 0 \right\}$ ($\mathbb{R}[\cdot]$ to zbiór wielomianów o współczynnikach rzeczywistych) z dodawaniem i mnożeniem punktowym funkcji.
- (5) Ciało liczb zespolonych, które skonstruujemy i zbadamy dokładnie poniżej.

Przykroiwszy treść ogólnej Definicji 10 do zdefiniowanej powyżej struktury algebraicznej, otrzymujemy

Definicja 11. W notacji Def. 9' **homomorfizm ciała** $(\mathbf{k}^{(1)}, A^{(1)}, M^{(1)}, P^{(1)}, \text{Inv}^{(1)}, \mathbf{0}^{(1)}, \mathbf{1}^{(1)})$ w ciało $(\mathbf{k}^{(2)}, A^{(2)}, M^{(2)}, P^{(2)}, \text{Inv}^{(2)}, \mathbf{0}^{(2)}, \mathbf{1}^{(2)})$ to odwzorowanie

$$\chi : \mathbf{k}^{(1)} \longrightarrow \mathbf{k}^{(2)}$$

o własnościach

$$\forall_{x,y \in \mathbf{k}} : (\chi(x +_{\mathbf{k}^{(1)}} y) = \chi(x) +_{\mathbf{k}^{(2)}} \chi(y) \quad \wedge \quad \chi(x \cdot_{\mathbf{k}^{(1)}} y) = \chi(x) \cdot_{\mathbf{k}^{(2)}} \chi(y)) .$$

Jądro homomorfizmu to zbiór

$$\text{Ker } \chi := \{ x \in \mathbf{k}^{(1)} \mid \chi(x) = \mathbf{0}^{(2)} \} ,$$

natomiast **obraz homomorfizmu** to zbiór

$$\text{Im } \chi := \{ x \in \mathbf{k}^{(2)} \mid \exists_{y \in \mathbf{k}^{(1)}} : x = \chi(y) \} .$$

Przykład(y) 11. Niechaj $(\mathbf{k}, A, M, P, \text{Inv}, \bullet \mapsto 0, \bullet \mapsto 1)$ będzie ciałem o **charakterystyce** $\text{char}(\mathbf{k}) = p$ danej przez liczbę pierwszą p , przy czym przez charakterystykę ciała rozumiemy najmniejszą z liczb $n \in \mathbb{N} \setminus \{0\}$, dla których jest spełniona równość

$$\underbrace{1 + 1 + \dots + 1}_{n \text{ razy}} = 0 ,$$

np. $\text{char}(\mathbb{Z}/p\mathbb{Z}) = p$. Odwzorowanie

$$\mathbf{k} \ni x \longmapsto x^p$$

jest iniektywnym endomorfizmem ciała $\mathbf{k}$. Prawdziwość tego stwierdzenia jest prostą konsekwencją twierdzenia o współczynniku dwumianowym dla liczby pierwszej p , które stwierdza, co następuje:

$$\forall_{k \in \overline{1, p-1}} : \left[\binom{p}{k} \right]_p = 0$$

(dowód stanowi proste zastosowanie Lematu Euklidesa, patrz: dział 2).

Definicja 12. **Ciało liczb zespolonych** to siódemka $(\mathbb{C}, A, M, P, \text{Inv}, \mathbf{0}, \mathbf{1})$, w której

- $\mathbb{C} := \mathbb{R}^{\times 2}$;
- $A : \mathbb{C}^{\times 2} \longrightarrow \mathbb{C} : ((x_1, y_1), (x_2, y_2)) \longmapsto (x_1 + y_1, x_2 + y_2)$;
- $M : \mathbb{C}^{\times 2} \longrightarrow \mathbb{C} : ((x_1, y_1), (x_2, y_2)) \longmapsto (x_1 \cdot x_2 - y_1 \cdot y_2, x_1 \cdot y_2 + x_2 \cdot y_1)$;
- $P : \mathbb{C} \longrightarrow \mathbb{C} : (x, y) \longmapsto (-x, -y)$;
- $\text{Inv} : \mathbb{C} \setminus \{(0, 0)\} =: \mathbb{C}^\times \longrightarrow \mathbb{C} : (x, y) \longmapsto \left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2} \right)$;
- $\mathbf{0} := (0, 0)$;
- $\mathbf{1} := (1, 0)$.

Twierdzenie 1. *Ciało liczb zespolonych jest ciałem nietrywialnym.*

Relację pomiędzy opisaną powyżej strukturą ciała na zbiorze par liczb rzeczywistych a taką strukturą na zbiorze liczb rzeczywistych ustala

Stwierdzenie 2. *W notacji Def. 12 odwzorowanie*

$$\iota : \mathbb{R} \longrightarrow \mathbb{C} : x \longmapsto (x, 0) \tag{1.1}$$

jest monomorfizmem ciała.

Ostatnia obserwacja pozwala – w świetle Stw. 1, które implikuje $\iota(\mathbb{R}) \cong \mathbb{R}$ – utożsamić $\mathbb{R}$ z obrazem tegoż ciała względem włożenia ι i tym samym traktować $\mathbb{R}$ jako podciało $\mathbb{C}$. Możemy też zdefiniować strukturę $\mathbb{R}$ -modułu³ (czyli działanie $\mathbb{R}$) na $\mathbb{C}$.

Definicja 13. W notacji Def. 12 i Stw. 2 **struktura modułu nad ciałem $\mathbb{R}$ na ciele $\mathbb{C}$** to odwzorowanie

$$\mathbb{R} \times \mathbb{C} \longrightarrow \mathbb{C} : (x, (y, z)) \longmapsto \iota(x) \cdot_{\mathbb{C}} (y, z) =: x \cdot (y, z) \tag{1.2}$$

o własności

$$\forall_{x,y,u,v \in \mathbb{R}} : x \cdot (y \cdot (u, v)) = (x \cdot y) \cdot (u, v) .$$

³Nasza uwaga ma na obecnym etapie charakter wyłącznie pomocniczy. Istotne elementy teorii modułów nad pierścieniem zostaną omówione w dziale 6.

Dotychczasowa dyskusja prowadzi wprost do wygodnej realizacji struktury algebraicznej na $\mathbb{C}$ w terminach dobrze znanego jej odpowiednika na $\mathbb{R}$, przy czym ostatnim brakującym elementem jest tutaj analiza własności wyróżnionej liczby zespolonej $(0, 1)$.

Stwierdzenie 3. W notacji Def. 12 i 1.2 oraz Stw. 2 i dla **jednostki urojonej**

$$i := (0, 1) \in \mathbb{C}$$

zachodzi

$$i \cdot_{\mathbb{C}} i = \iota(-1),$$

a ponadto

$$\forall_{(x,y) \in \mathbb{C}} : (x, y) = x \cdot \iota(1) +_{\mathbb{C}} y \cdot i.$$

Powyższy zapis uzasadnia

Definicja 14. W notacji Def. 12 **część rzeczywista** liczby zespolonej $(x, y) \in \mathbb{C}$ to

$$\Re(x, y) := x,$$

natomiast jej **część urojona** to

$$\Im(x, y) := y.$$

Notacja 1. W dalszej części wykładu przyjmiemy wygodną (i powszechnie stosowaną) umowę dotyczącą zapisu liczb zespolonych zwanego **zapisem kartezjańskim**. Jej podstawą jest opuszczenie oznaczenia monomorfizmu (1.1), pozwalające zapisać

$$\forall_{x \in \mathbb{R}} : \iota(x) \equiv x,$$

jak również indeksów $\mathbb{C}$ na symbolach działań w $\mathbb{C}$ oraz znaku działania $\mathbb{R}$ na $\mathbb{C}$. Zapiszemy zatem dowolną liczbę zespoloną $z \in \mathbb{C}$ w postaci

$$z = \Re(z) + i \Im(z).$$

Oczywista korzyść ze stosowania takiego zapisu to możliwość wykonywania wszelkich operacji algebraicznych na liczbach zespolonych według reguł obowiązujących w ciele $\mathbb{R}$, wzbogaconych o jedną dodatkową regułę:

$$i^2 = -1.$$

✓

Prostej ilustracji przydatności przyjętej konwencji zapisu liczb zespolonych dostarczają poniższe proste rachunki (prowadzone dla dowolnych $(x, y), (x_1, y_1), (x_2, y_2) \in \mathbb{C}$):

$$(x_1 + i y_1) + (x_2 + i y_2) = (x_1 + x_2) + i(y_1 + y_2),$$

$$(x_1 + i y_1) \cdot (x_2 + i y_2) = x_1 \cdot x_2 + i(x_1 \cdot y_2 + y_1 \cdot x_2) + i^2 y_1 \cdot y_2 = (x_1 \cdot x_2 - y_1 \cdot y_2) + i(x_1 \cdot y_2 + y_1 \cdot x_2),$$

$$\begin{aligned} (x + i y)^{-1} &= \frac{1}{x + i y} \cdot \frac{1}{x - i y} \cdot (x - i y) = \frac{1}{(x + i y) \cdot (x - i y)} \cdot (x - i y) = \frac{1}{x^2 + y^2} \cdot (x - i y) \\ &\equiv \frac{x}{x^2 + y^2} + i \frac{(-y)}{x^2 + y^2}. \end{aligned}$$

Możemy już teraz przejść do opisu dodatkowej struktury obecnej w ciele liczb zespolonych.

Definicja 15. W notacji Def. 12 **moduł (liczby zespolonej)** to odwzorowanie

$$|\cdot| : \mathbb{C} \longrightarrow \mathbb{R} : z \longmapsto \sqrt{\Re(z)^2 + \Im(z)^2}.$$

Definicja 16. W notacji Def. 12 **sprzężenie (zespolone)** to odwzorowanie

$$\bar{\cdot} : \mathbb{C} \longrightarrow \mathbb{C} : z \longmapsto \Re(z) - i \Im(z) =: \bar{z},$$

spełniające oczywiste tożsamości:

$$\Re(z) = \frac{z + \bar{z}}{2}, \quad \Im(z) = \frac{z - \bar{z}}{2i}.$$

Proste własności modułu są zebrane poniżej.

Stwierdzenie 4. W notacji Def. 12 oraz 15 i dla dowolnych $z, z_1, z_2 \in \mathbb{C}$ zachodzą następujące relacje:

- (i) $|z| = 0 \iff z = 0$;
- (ii) $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$;
- (iii) $|z|^2 = z \cdot \bar{z}$;
- (iv) $|z_1 + z_2| = \sqrt{|z_1|^2 + |z_2|^2 + 2\Re(z_1 \cdot \bar{z}_2)} \leq |z_1| + |z_2|$ (nierówność trójkąta);
- (v) $|z_1 - z_2| \geq ||z_1| - |z_2||$.

Dowód: (Na ćwiczeniach lub w domu.) □

Własności sprzężenia zespolonego opisuje

Stwierdzenie 5. Sprzężenie zespolone jest inwolutywnym automorfizmem ciała liczb zespolonych, tj. w notacji Def. 12 oraz 16 i dla dowolnych $z, z_1, z_2 \in \mathbb{C}$ zachodzi, co następuje:

- (i) $\bar{\cdot} : \mathbb{C} \rightarrow \mathbb{C}$;
- (ii) $\text{Ker } \bar{\cdot} = \{0\} \quad \wedge \quad \text{Im } \bar{\cdot} = \mathbb{C}$;
- (iii) $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$;
- (iv) $\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$;
- (v) $\bar{\bar{z}} = z$.

Ponadto, w notacji Stw. 2,

$$\bar{z} = z \iff z \in \iota(\mathbb{R}) \equiv \mathbb{R},$$

$$\bar{z} = -z \iff z \in i \cdot \iota(\mathbb{R}) \equiv i\mathbb{R}.$$

Zgromadzona dotąd wiedza na temat ciała liczb zespolonych daje podstawy do naturalnej interpretacji geometrycznej części struktury algebraicznej na $\mathbb{C}$, a mianowicie $(\mathbb{C}, +_{\mathbb{C}}, \mathbf{P})$, w terminach elementarnego rachunku wektorowego na $\mathbb{R}^2$, znanego ze szkoły średniej⁴. W rachunku tym przedmiotem zainteresowania jest zbiór wektorów zaczepionych w wyróżnionym punkcie o współrzędnych $(0,0)$ na płaszczyźnie $\mathbb{R}^2$,

$$\text{Vect}(\mathbb{R}^2) := \{ \overrightarrow{[(0,0); (x,y)]} \mid (x,y) \in \mathbb{R}^2 \}.$$

Jego elementy możemy dodawać według dobrze znanej „reguły równoległoboku”, a ponadto każdemu z nich przypisujemy liczbę nieujemną zwaną długością wektora i równą – z definicji – długości wyznaczanego przezeń odcinka, obliczanej na podstawie twierdzenia Pitagorasa. Sumę wektorową wektorów $\vec{v}_1$ i $\vec{v}_2$ oznaczmy symbolem $\vec{v}_1 + \vec{v}_2$, długość zaś wektora $\vec{v}$ zapiszemy jako $\|\vec{v}\|$. Punktem wyjścia dla zapowiedzianej interpretacji geometrycznej jest określenie bijekcji

$$\vec{\cdot} : \mathbb{C} \longrightarrow \text{Vect}(\mathbb{R}^2) : z \longmapsto \overrightarrow{[(0,0); (\Re(z), \Im(z))]} =: \vec{z}.$$

Łatwo stwierdzamy prawdziwość tożsamości (zapisanej dla dowolnych $z_1, z_2 \in \mathbb{C}$)

$$\overrightarrow{z_1 +_{\mathbb{C}} z_2} = \vec{z}_1 + \vec{z}_2,$$

a ponadto dowodzimy, dla dowolnej liczby $z \in \mathbb{C}$, równości

$$|z| = \|\vec{z}\|.$$

Na koniec wreszcie możemy w prosty sposób zrealizować sprzężenie zespolone

$$\bar{z} = \text{P}_{OX}(\vec{z})$$

jako odbicie wektora przyporządkowanego liczbie zespolonej z w prostej w $\mathbb{R}^2$ o wektorze kierunkowym $\overrightarrow{[(0,0); (1,0)]}$.

W celu rozszerzenia interpretacji geometrycznej na pozostałą część struktury algebraicznej na $\mathbb{C}$ wygodnie jest przejść do odmiennej (od kartezjańskiej) prezentacji liczb zespolonych, przy czym przejście to w języku geometrii płaszczyzny kartezjańskiej odpowiada zmianie układu współrzędnych używanego w opisie punktów i wektorów z kartezjańskiego na biegunowy. Tym razem zaczynamy od konstatacji, słusznej dla dowolnej pary $(x,y) \in \mathbb{R}^2 \setminus \{(0,0)\}$ wobec przebiegu funkcji $\sin$, że oto oczywista równość

$$\left(\frac{x}{\sqrt{x^2 + y^2}} \right)^2 + \left(\frac{y}{\sqrt{x^2 + y^2}} \right)^2 = 1$$

⁴W istocie pełną strukturę ciała na $\mathbb{C}$ wraz ze strukturą modułu nad ciałem $\mathbb{R}$ można bez trudu zinterpretować w terminach standardowej struktury przestrzeni $\mathbb{R}$ -liniowej z normą (euklidesową) na $\mathbb{R}^2$, wzbogaconej o strukturę modułu nad grupą dylatacji (przeskalowań) i translacji. Taka interpretacja wyprzedza jednak bieg niniejszego kursu i dlatego zostanie (chwilowo) przemilczana.

w połączeniu z układem nierówności

$$-1 \leq \frac{x}{\sqrt{x^2 + y^2}} \leq 1$$

proceedzi do wniosku

$$\exists_{\varphi(x,y) \in \mathbb{R}} : \frac{x}{\sqrt{x^2 + y^2}} = \cos \varphi(x, y), \quad (1.3)$$

przy czym liczba $\varphi(x, y)$ jest określona wysoce niejednoznacznie. Istotnie, jeśli ustalić liczbę $\varphi_0(x, y) \in [0, 2\pi[$ spełniającą warunek definiujący (1.3) (co zawsze jest możliwe), to wówczas wszystkie liczby postaci

$$\epsilon \varphi_0(x, y) + 2k\pi, \quad (\epsilon, k) \in \{+1, -1\} \times \mathbb{Z}$$

także będą go spełniać. Otrzymujemy zatem dwie rodziny rozwiązań warunku definiującego, z których każdą tworzą liczby różniące się o całkowitą wielokrotność liczby 2π . Ustalenie rodziny, do której należy $\varphi(x, y)$, odpowiada wyborowi znaku $\epsilon' \in \{+1, -1\}$ w równości

$$\frac{y}{\sqrt{x^2 + y^2}} = \epsilon' \cdot \sin \varphi(x, y)$$

będącej konsekwencją warunku definiującego i „jedynki trygonometrycznej”. Dalsze sprecyzowanie wartości $\varphi(x, y)$ nie jest możliwe. Poniżej sformalizujemy nasze wnioski, najpierw jednak wprowadzimy pomocne oznaczenia.

Notacja 2. Definiujemy **symbol Eulera**⁵ dla dowolnej liczby $\varphi \in \mathbb{R}$

$$e^{i\varphi} := \cos \varphi + i \sin \varphi \in \mathbb{C}, .$$

Ponadto **zbiór liczb zespolonych o module jednostkowym** będziemy oznaczać symbolem

$$U(1) := \{ u \in \mathbb{C} \mid |u| = 1 \} .$$

✓

Istotne własności symbolu Eulera są opisane w

Stwierdzenie 6. Dla dowolnych $\varphi, \varphi_1, \varphi_2 \in \mathbb{R}$ prawdziwe są zdania:

- (i) $e^{i\varphi} \in U(1)$;
- (ii) $(e^{i\varphi})^{-1} = \overline{e^{i\varphi}} = e^{-i\varphi}$;
- (iii) $e^{i\varphi_1} \cdot e^{i\varphi_2} = e^{i(\varphi_1 + \varphi_2)}$ (wzór de Moivre’a);
- (iv) $e^{i\varphi_1} = e^{i\varphi_2} \iff \varphi_2 - \varphi_1 \in 2\pi\mathbb{Z}$.

Zauważmy też, że

Stwierdzenie 7. Przyjmijmy notację Def. 12 oraz 16. Zbiór $U(1)$ jest nośnikiem naturalnej struktury grupy przemiennej względem operacji 2-argumentowej (indukowanej z $\mathbb{C}$)

$$U(1) \times U(1) \longrightarrow U(1) : (u_1, u_2) \longmapsto u_1 \cdot u_2$$

oraz operacji 1-argumentowej

$$\text{Inv} : U(1) \curvearrowright : u \longmapsto \bar{u},$$

z których pierwsza ma jako element neutralny $e = 1 \in U(1)$.

W interpretacji geometrycznej zbiór $U(1)$ jest okręgiem jednostkowym na płaszczyźnie kartezjańskiej o środku w punkcie o współrzędnych $(0, 0)$, co pokazuje parametryzacja

$$U(1) = \{ e^{i\varphi} \mid \varphi \in \mathbb{R} \} .$$

Możemy teraz sformułować przydatne

⁵Drugoroczny kurs analizy matematycznej pozwoli zrozumieć symbol Eulera jako wartość przyjmowaną przez funkcję wykładniczą zmiennej zespolonej w wyróżnionym punkcie $i\varphi$ jej dziedziny, przez co podana tu definicja zyska status twierdzenia.

Twierdzenie 2. (O rozkładzie biegunowym i prezentacji trygonometrycznej liczby zespolonej) W notacji Def. 12

$$\forall z \in \mathbb{C}^\times \quad \exists!_{(r,u) \in \mathbb{R}_{>0} \times U(1)} : z = r \cdot u ,$$

przy czym

$$\forall u \in U(1) \quad \exists \varphi \in \mathbb{R} : u = e^{i\varphi} .$$

Dowód: Rzeczony rozkład istnieje, bo dowolne $z \in \mathbb{C}^\times$ możemy zapisać w postaci $z = |z| \cdot \frac{z}{|z|}$, przy czym $r = |z| \in \mathbb{R}_{>0}$ i $u = \frac{z}{|z|} \in U(1)$. Zarazem rozkład ten jest jedyny, gdyż dla dowolnego takiego rozkładu $z = r \cdot u$ zachodzi – na mocy Stw. 4 (ii) – $|z| \equiv |r \cdot u| = |r| \cdot |u| = r \cdot 1 = r$, czyli też $z = |z| \cdot u$, a stąd $u = \frac{z}{|z|}$. $\square$

Zaobserwowaną wcześniej nieusuwalną niejednoznaczność określenia liczby $\varphi(\Re(z), \Im(z))$ przypisanej danej liczbie zespolonej $z \in \mathbb{C}^\times$ zgrabnie kwantyfikuje

Definicja 17. W notacji Def. 12 **argument liczby zespolonej** (niezerowej) to odwzorowanie

$$\text{Arg} : \mathbb{C}^\times \longrightarrow \mathbb{R}/2\pi\mathbb{Z} : z \longmapsto \{ \varphi \in \mathbb{R} \mid z = |z| \cdot e^{i\varphi} \} ,$$

przy czym $\mathbb{R}/2\pi\mathbb{Z}$ oznacza tu zbiór klas abstrakcji w $\mathbb{R}$ względem relacji równoważności – zapisanej dla dowolnych $x, y \in \mathbb{R}$ –

$$x \sim y \iff x - y \in 2\pi\mathbb{Z} .$$

Argument główny liczby $z \in \mathbb{C}^\times$ to reprezentant

$$\arg(z) \in \text{Arg}(z) \cap [0, 2\pi[.$$

Elementarne własności argumentu zbiera

Stwierdzenie 8. W notacji Def. 12 oraz 17 i dla dowolnych $z, z_1, z_2 \in \mathbb{C}^\times$ zachodzi, co następuje:

- (i) $\text{Arg}(z_1 \cdot z_2) = \text{Arg}(z_1) + \text{Arg}(z_2)$, przy czym prawa strona wypisanej równości jest sumą algebraiczną podzbiorów grupy przemiennej $(\mathbb{R}, +, x \mapsto -x, \bullet \mapsto 0)$ (rozumianą w sensie Konw. 4).
- (ii) $\text{Arg}(z^{-1}) = \text{Arg}(\bar{z}) = -\text{Arg}(z)$, przy czym prawa strona wypisanego ciągu równości jest przeciwnością algebraiczną podzbioru wspomnianej grupy przemiennej.
- (iii) $z_1 = z_2 \iff (|z_1| = |z_2| \wedge \text{Arg}(z_1) = \text{Arg}(z_2))$.

Dowód: Jedynym nietrywialnym punktem powyższego stwierdzenia jest punkt (i), którego prawdziwości dowiedzimy.

Niech $\varphi \in \text{Arg}(z_1 \cdot z_2)$ i wybierzmy dowolne $\varphi_1 \in \text{Arg}(z_1)$, a wtedy na mocy Stw. 4 (ii) i 6 (iii) zachodzi $|z_2| \cdot e^{i(\varphi - \varphi_1)} = \frac{|z_1 \cdot z_2| \cdot e^{i\varphi}}{|z_1| \cdot e^{i\varphi_1}} = \frac{z_1 \cdot z_2}{z_1} = z_2$, zatem wprost z definicji $\varphi - \varphi_1 \in \text{Arg}(z_2)$, co oznacza, że $\text{Arg}(z_1 \cdot z_2) \subset \text{Arg}(z_1) + \text{Arg}(z_2)$.

I odwrotnie,

$$\begin{aligned} \varphi_\alpha \in \text{Arg}(z_\alpha), \alpha \in \{1, 2\} &\implies |z_1 \cdot z_2| \cdot e^{i(\varphi_1 + \varphi_2)} = |z_1| \cdot e^{i\varphi_1} \cdot |z_2| \cdot e^{i\varphi_2} = z_1 \cdot z_2 \implies \varphi_1 + \varphi_2 \in \text{Arg}(z_1 \cdot z_2) \\ &\implies \text{Arg}(z_1) + \text{Arg}(z_2) \subset \text{Arg}(z_1 \cdot z_2) . \end{aligned}$$

$\square$

Należy podkreślić, że własność (i) ze Stw. 8 nie jest dziedziczona przez żadnego reprezentanta klasy funkcji $\Phi : \mathbb{C}^\times \longrightarrow \mathbb{R}$ o własności $\Phi(z) \in \text{Arg}(z)$.

Stwierdzenie 9. W notacji Def. 12 i 17 nie istnieje funkcja $\Phi : \mathbb{C}^\times \longrightarrow \mathbb{R}$ o własnościach

$$\forall z, z_1, z_2 \in \mathbb{C}^\times : (\Phi(z) \in \text{Arg}(z) \wedge \Phi(z_1 \cdot z_2) = \Phi(z_1) + \Phi(z_2)) .$$

Dowód: (A.a.) Niechaj Φ będzie taką funkcją. Wówczas $\Phi(1) + \Phi(1) = \Phi(1 \cdot 1) = \Phi(1) = \Phi((-1) \cdot (-1)) = \Phi(-1) + \Phi(-1)$, zatem $\Phi(1) = 0$, skąd też $\Phi(-1) = 0$, ale w takim razie $-1 = |-1| \cdot e^{i\Phi(-1)} = e^{i0} = 1$, czyli sprzeczność. $\square$

Możemy już teraz bez trudu zinterpretować geometrycznie operację mnożenia liczb zespolonych: oto wymnożenie danej liczby z przez liczbę o rozkładzie biegunowym $\zeta = r \cdot e^{i\varphi}$ sprowadza się do przeskalowania wektora $\vec{z}$ o czynnik r , a następnie obrócenia go o kąt φ wokół punktu zaczepienia. Również operacja brania odwrotności niezerowej liczby zespolonej z nabiera prostego sensu geometrycznego złożenia odwzorowania końca wektora $\vec{z}$ w punkt doń sprzężony względem okręgu jednostkowego z odbiciem w prostej o wektorze kierunkowym $\overrightarrow{[(0,0);(1,0)]}$.

Rozkład biegunowy liczby zespolonej okazuje się szczególnie wygodny w analizie potęgowania (wzór de Moivre'a) i pierwiastkowania. Zajmiemy się teraz szczegółowo tą drugą, mniej trywialną operacją.

Definicja 18. W notacji Def. 12 i dla dowolnych $z \in \mathbb{C}$ oraz $n \in \mathbb{N} \setminus \{0\}$ **pierwiastek stopnia n z z** to zbiór

$$\sqrt[n]{z} := \{ w \in \mathbb{C} \mid w^n = z \}.$$

Łatwo się przekonać, że dla $n > 1$ zbiór ten *nie* jest singletonem.

Stwierdzenie 10. W notacji Def. 18 i dla dowolnych $(r, \varphi) \in \mathbb{R}_{\geq 0} \times \mathbb{R}$ jest

$$\sqrt[n]{r \cdot e^{i\varphi}} = \left\{ r^{\frac{1}{n}} \cdot e^{i\frac{\varphi+2\pi k}{n}} \mid k \in \overline{0, n-1} \right\}.$$

Dowód: Zauważmy, że na mocy Stw. 6 i 8 zachodzi

$$\begin{aligned} \rho \cdot e^{i\psi} \in \sqrt[n]{r \cdot e^{i\varphi}} &\iff \rho^n \cdot e^{in\psi} = r \cdot e^{i\varphi} \iff (\rho^n = r \wedge e^{in\psi} = e^{i\varphi}) \\ &\iff \left(\rho = r^{\frac{1}{n}} \wedge \exists_{k \in \mathbb{Z}} : n\psi - \varphi = 2\pi k \right) \\ &\iff \left(\rho = r^{\frac{1}{n}} \wedge \exists_{k \in \mathbb{Z}} : \psi = \frac{\varphi + 2\pi k}{n} \right), \end{aligned}$$

przy czym $\psi' = \psi + 2\pi l$, $l \in \mathbb{Z}$ spełnia równość $\rho \cdot e^{i\psi'} = \rho \cdot e^{i\psi}$, skąd teza wobec implikacji

$$k \mapsto k+n \implies \frac{\varphi+2\pi k}{n} \mapsto \frac{\varphi+2\pi k}{n} + 2\pi.$$

□

Proste intuicje dotyczące zachowania pierwiastka (rozumianego jako liczba) w dziedzinie rzeczywistej pozostają w mocy po przeniesieniu ich na poziom odnośnych zbiorów.

Stwierdzenie 11. W notacji Def. 12 i 18 jest

$$\forall_{n \in \mathbb{N} \setminus \{0\}} \forall_{z_1, z_2 \in \mathbb{C}} : \sqrt[n]{z_1 \cdot z_2} = \sqrt[n]{z_1} \cdot \sqrt[n]{z_2}.$$

Dowód: Zaczniemy od tego, że ilekroć $z_1 = 0$, teza przyjmuje trywialną postać $\{0\} = \{0\}$, możemy zatem ograniczyć się do przypadku $z_1 \neq 0$.

Niechaj $w \in \sqrt[n]{z_1 \cdot z_2}$ i wybierzmy dowolne $w_1 \in \sqrt[n]{z_1}$, a wtedy $w_2 := \frac{w}{w_1}$ spełnia $w_2^n \equiv \left(\frac{w}{w_1}\right)^n = \frac{w^n}{w_1^n} = \frac{z_1 \cdot z_2}{z_1} = z_2$, czyli $w_2 \in \sqrt[n]{z_2}$, skąd też $w = w_1 \cdot w_2 \in \sqrt[n]{z_1} \cdot \sqrt[n]{z_2}$. Jest więc

$$\sqrt[n]{z_1 \cdot z_2} \subset \sqrt[n]{z_1} \cdot \sqrt[n]{z_2}.$$

I odwrotnie, gdy $w_\alpha \in \sqrt[n]{z_\alpha}$, $\alpha \in \{1, 2\}$, to zachodzi $(w_1 \cdot w_2)^n = w_1^n \cdot w_2^n = z_1 \cdot z_2$, czyli $w_1 \cdot w_2 \in \sqrt[n]{z_1 \cdot z_2}$. Jest przeto

$$\sqrt[n]{z_1} \cdot \sqrt[n]{z_2} \subset \sqrt[n]{z_1 \cdot z_2}.$$

Ostatecznie więc

$$\sqrt[n]{z_1 \cdot z_2} = \sqrt[n]{z_1} \cdot \sqrt[n]{z_2}.$$

□

Wieloznaczności (w sensie liczbowym) odwzorowania Arg pociąga za sobą tę samą własność pierwiastka.

Stwierdzenie 12. W notacji Def. 12 i 18 nie istnieje funkcja $p_n : \mathbb{C} \rightarrow \mathbb{C}$ o własnościach

$$\forall_{z, z_1, z_2 \in \mathbb{C}} : \left(p_n(z) \in \sqrt[n]{z} \wedge p_n(z_1 \cdot z_2) = p_n(z_1) \cdot p_n(z_2) \right).$$

Dowód: (A.a.) Niechaj p_n będzie taką funkcją, wobec czego

$$\forall_{z \in \mathbb{C}} : p_n(z^n) = (p_n(z))^n = z.$$

Wówczas dla $e^{\frac{2\pi i}{n}}$, $n \in \mathbb{N} \setminus \{0, 1\}$ zachodzi $1 = p_n(1^n) = p_n(1) = p_n\left(e^{\frac{2\pi i}{n}}\right) = e^{\frac{2\pi i}{n}}$, czyli sprzeczność. $\square$

* * *

Literatura uzupełniająca: Więcej o liczbach zespolonych, w ujęciu algebraicznym i geometrycznym, można znaleźć w książce Andreescu i Andriki [AA06].

LITERATURA

- [AA06] T. Andreescu and D. Andrica, *Complex numbers from A to ... Z*, Birkhäuser, 2006.
- [Bou07] N. Bourbaki, *Éléments de mathématique, Algèbre, chapitres 1 à 3*, Springer, 2007.
- [Coh74] P.M. Cohn, *Algebra*, vol. 1, John Wiley & Sons, 1974.
- [Coh77] ———, *Algebra*, vol. 2, John Wiley & Sons, 1977.
- [Coh90] ———, *Algebra*, vol. 3, John Wiley & Sons, 1990.
- [Die65] J. Dieudonné, *Éléments d'analyse*, vol. 1, Gauthier–Villars, 1965.
- [Lan02] S. Lang, *Algebra*, Graduate Texts in Mathematics, vol. 211, Springer, 2002.
- [Mau91] K. Maurin, *Analiza. Część I. Elementy*, Biblioteka Matematyczna, vol. 69, Państwowe Wydawnictwo Naukowe, 1991.
- [ML71] S. Mac Lane, *Categories for the Working Mathematician*, Graduate Texts in Mathematics, vol. 5, Springer, 1971.

Address: KATEDRA METOD MATEMATYCZNYCH FIZYKI, WYDZIAŁ FIZYKI UNIwersYTETU WARSZAWSKIEGO, UL. HOŻA 74, PL-00-682 WARSZAWA, POLAND

E-mail address: `suszek@fuw.edu.pl`