# Algebra

Michał Dobranowski

semestr zimowy 2022
v0.3

Poniższy skrypt zawiera materiał obejmujący wykłady z Algebry prowadzone przez dr hab. Jakuba Przybyło na I semestrze Informatyki na AGH oraz tematy, które uznałem za warte uwagi podczas własnych studiów nad tematem.

## Spis treści

# §1 Liczy zespolone

**Definicja 1.1.** Liczba zespolona $z$ to uporządkowana para liczb rzeczywistych. Pierwszy element tej pary to **część rzeczywista**, ozaczana symbolem $\mathrm{Re}(z)$, a drugi to **część urojona**, oznaczana symbolem $\mathrm{Im}(z)$. Zbiór liczb zespolonych oznaczamy przez $\mathbb{C}$.

Liczby zespolone można reprezentować w kilku postaciach, jedna z nich to **postać algebraiczna**. Używając jej, liczba $z = (x, y)$ jest zapisywana jako

$$z = x + iy,$$

gdzie $i$ nazywamy **jednostką urojoną**, która spełnia

$$i^2 = -1.$$

## §1.1 Działania na liczbach zespolonych

Niech $z_1 = x_1 + iy_1$ oraz $z_2 = x_2 + iy_2$. Określamy:

- dodawanie $z_1 + z_2 = x_1 + x_2 + i(y_1 + y_2)$
- mnożenie $z_1 z_2 = x_1 x_2 + i x_1 y_2 + i x_2 y_1 + i^2 y_1 y_2$
  $= x_1 x_2 - y_1 y_2 + i(x_1 y_2 + x_2 y_1)$

**Wniosek 1.2**

Dodawanie i mnożenie liczb zespolonych jest przemienne i łączne. Mnożenie jest rozdzielne względem dodawania.

**Definicja 1.3.** Sprzężenie liczby zespolonej $z = x + iy$ to liczba $\overline{z} = x - iy$.

**Definicja 1.4.** Moduł liczby zespolonej $z = x + iy$ to liczba $|z| = \sqrt{x^2 + y^2}$.

Zachodzi pewna własność, wynikająca ze wzoru skróconego mnożenia:

$$z\overline{z} = (x + iy)(x - iy) = x^2 - i^2 y^2 = x^2 + y^2$$

$$z\overline{z} = |z|^2 \tag{1}$$

Powyższa liczba jest liczbą rzeczywistą, więc znaleźliśmy prosty sposób na dzielenie liczb zespolonych przez siebie, mnożąc licznik i mnianownik przez sprzężenie mianownika. Na przykład:

$$\frac{1 + 2i}{-1 - i} = \frac{(1 + 2i)(-1 + i)}{(-1 - i)(-1 + i)} = \frac{-3 - i}{2} = \frac{-3}{2} - \frac{i}{2}.$$

**Lemat 1.5**

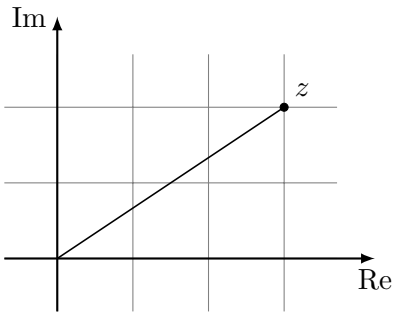
Oprócz $z\overline{z} = |z|^2$, zachodzą również równości:

- $|\overline{z}| = |z|$
- $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
- $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$
- $|z_1 z_2| = |z_1||z_2|$

Ich dowody można w łatwy sposób przeprowadzić z definicji poszczególnych działań.

## §1.2 Interpretacja geometryczna liczb zespolonych

Liczby zespolone można interpretować jako punkty na **płaszczyźnie zespolonej**. Dla przykładu liczba $z = 3 + 2i$.




**Fakt 1.6.** Moduł liczby zespolonej $z$ to długość wektora wodzącego tej liczby na płaszczyźnie zespolonej.

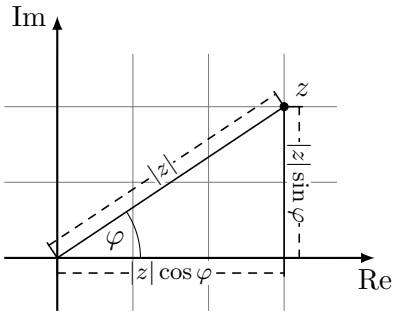
*Dowód.* Wynika to z twierdzenia Pitagorasa oraz definicji modułu (1.4). □

Możemy wyprowadzić **postać trygonometryczną** liczby zespolonej, która, zamiast dwóch współrzędnych, będzie operować na długości wektora wodzącego oraz kącie skierowanym. Mamy więc

$$z = |z|(\cos\varphi + i\sin\varphi)$$

gdzie $\varphi$ to miara kąta skierowanego między wektorem wodzącym liczby zespolonej $z$ a osią liczb rzeczywistych. Ten kąt nazywany jest **argumentem** i oznaczany przez $\mathrm{Arg}(z)$. Argument nie jest określony jednoznacznie – dowolne dwa argumenty jednej liczby różnią się o wielokrotność $2\pi$. Jeśli argument jest w przedziale $[0, 2\pi)$, to mówimy, że jest to **argument główny** liczby $z$ i oznaczamy $\arg(z)$.

Za pomocą podstawowej trygonometrii możemy łatwo zamieniać postać algebraiczną i trygonometryczną między sobą.




$$\mathrm{Re}\, z = |z|\cos\varphi, \qquad \mathrm{Im}\, z = |z|\sin\varphi \tag{2}$$

Na potrzeby dalszych rozważań przyjmujemy, że $\arg(0) = 0$.

**Fakt 1.7.** Odległość między liczbami $z_1$ i $z_2$ na płaszczyźnie zespolonej wynosi $|z_1 - z_2|$.

**Lemat 1.8**

Zachodzą następujące nierówności:

- $|z_1 + z_2| \leq |z_1| + |z_2|$
- $||z_1| - |z_2|| \leq |z_1 - z_2|$

Możemy łatwo mnożyć dwie liczby zespolone w postaci trygonometrycznej przez siebie za pomocą poniższego wzoru.

$$\begin{aligned} z_1 \cdot z_2 &= |z_1|(\cos\varphi_1 + i\sin\varphi_1)|z_2|(\cos\varphi_2 + i\sin\varphi_2) \\ &= |z_1||z_2|(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2 + i(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2)) \\ &= |z_1||z_2|(\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)) \end{aligned} \tag{3}$$

Stosując wzór 3 $n$ razy otrzymujemy dowód następującego twierdzenia.

**Twierdzenie 1.9** (Wzór de Moivre'a)

Dla $z = |z|(\cos\varphi + i\sin\varphi)$ oraz $n \in \mathbb{Z}$ zachodzi równość

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

Wzór de Moivre'a zapewnia prosty sposób na potęgowanie liczb zespolonych. Dlatego, mając za zadanie obliczyć

$$(-2\sqrt{3} - 2i)^{16}$$

najłatwiej będzie zmienić postać liczby do postaci trygonometrycznej, a następnie skorzystać z twierdzenia 1.9.

## §1.3 Pierwiastkowanie liczb zespolonych

**Definicja 1.10** (Pierwiastek liczby zespolonej)**.** Jeśli $z$ jest liczbą zespoloną, to $\sqrt[n]{z}$ jest zbiorem wszystkich takich $w \in \mathbb{C}$, że $w^n = z$.

Korzystając ze wzoru de Moivre'a (twierdzenie 1.9) łatwo wyprowadzić wzór

$$\sqrt[n]{z} = \sqrt[n]{|z|}\left(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}\right), k \in \mathbb{Z} \tag{4}$$

**Fakt 1.11.** Pierwiastków $n$-tego stopnia z $z \neq 0$ jest dokładnie $n$ i leżą one w równych odstępach na okręgu o środku w 0 i promieniu $\sqrt[n]{|z|}$.

*Dowód.* Dla $k \in \{0, 1, \ldots, n-1\}$ liczba z równości 4 będzie przyjmować różne wartości (wynika to z okresowości funkcji trygonometrycznych). Liczby te będą na wspomnianym okręgu (to wynika wprost z postaci trygonometrycznej), a ich argumenty główne różnić będzie wielokrotność $\frac{2\pi}{n}$. □

## §1.4 Postać wykładnicza

Postać $z = |z|e^{i\varphi}$ liczby zespolonej bedziemy nazywać **postacią wykładniczą** tej liczby.

**Twierdzenie 1.12** (Wzór Eulera)
Dla każdego $\varphi \in \mathbb{R}$ zachodzi

$$e^{i\varphi} = \cos\varphi + i\sin\varphi.$$

*Dowód.* Weźmy $z = \cos\varphi + i\sin\varphi$. Różniczkując po zmiennej $\varphi$ otrzymujemy

$$\frac{dz}{d\varphi} = -\sin\varphi + i\cos\varphi = iz$$

$$\therefore \frac{dz}{z} = id\varphi.$$

Po obustronnym całkowaniu mamy

$$\int \frac{dz}{z} = \int id\varphi$$

$$\ln z = i\varphi + c$$

$$e^{\ln z} = e^{i\varphi + c}$$

$$z = e^{i\varphi + c}.$$

Podstawiając $\varphi = 0$ otrzymujemy $1 = e^c$, skąd mamy $c = 0$, co kończy dowód. □

## §2 Relacje

**Definicja 2.1.** Relacja to trójka $\mathcal{R} = (X, \operatorname{gr}\mathcal{R}, Y)$, gdzie $X$ i $Y$ są zbiorami, a $\operatorname{gr}\mathcal{R} \subset X \times Y$.

Zbiór $X$ nazywamy **naddziedziną**, $Y$ **zapasem**, $\operatorname{gr}\mathcal{R}$ to **wykres** relacji. Piszemy, że $x\mathcal{R}y$, jesli $(x, y) \in \operatorname{gr}\mathcal{R}$. **Dziedzina** relacji $\mathcal{R}$ to zbiór

$$D_{\mathcal{R}} = \{x \in X : \exists y \in Y : x\mathcal{R}y\},$$

a jej **przeciwdziedzina** to zbiór

$$\mathcal{C}_{\mathcal{R}} = \{y \in Y : \exists x \in X : x\mathcal{R}y\}.$$

**Definicja 2.2.** Relacja odwrotna do relacji $\mathcal{R} = (X, \operatorname{gr}\mathcal{R}, Y)$ to taka relacja $\mathcal{R}^{-1} = (Y, \operatorname{gr}\mathcal{R}^{-1}, X)$, że

$$\operatorname{gr}\mathcal{R}^{-1} = \{(y, x) \in Y \times X : (x, y) \in \operatorname{gr}\mathcal{R}\}.$$

**Definicja 2.3.** Złożeniem relacji $\mathcal{R} = (X, \operatorname{gr}\mathcal{R}, Y)$ z relacją $\mathcal{S} = (Y, \operatorname{gr}\mathcal{S}, Z)$ nazywamy relację

$$\mathcal{R} \circ \mathcal{S} = (X, \operatorname{gr}(\mathcal{R} \circ \mathcal{S}), Z),$$

gdzie

$$\operatorname{gr}(\mathcal{R} \circ \mathcal{S}) = \{(x, z) \in X \times Z : \exists y \in Y : x\mathcal{R}y \wedge y\mathcal{S}z\}.$$

**Definicja 2.4** (rodzaje relacji)**.** Relacja $\mathcal{R} = (X, \operatorname{gr}\mathcal{R}, X)$ jest:

- **zwrotna** $\Leftrightarrow \forall x \in X : x\mathcal{R}x$,
- **symetryczna** $\Leftrightarrow \forall x, y \in X : x\mathcal{R}y \Rightarrow y\mathcal{R}x$,

- **antysymetryczna** $\Leftrightarrow \forall x, y \in X : x\mathcal{R}y \wedge y\mathcal{R}x \Rightarrow x = y$,
- **asymetryczna** $\Leftrightarrow \forall x, y \in X : x\mathcal{R}y \Rightarrow \neg y\mathcal{R}x$,
- **przechodnia** $\Leftrightarrow \forall x, y, z \in X : x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z$,
- **spójna** $\Leftrightarrow \forall x, y \in X : x\mathcal{R}y \vee y\mathcal{R}x \vee x = y$.

**Definicja 2.5.** Relacja równoważności to relacja $\mathcal{R} = (X, \operatorname{gr}\mathcal{R}, X)$, która jest zwrotna, przechodnia i symetryczna.

**Definicja 2.6.** Jeżeli $(X, \mathcal{R})$ zbiorem z relacją równoważności, to dla każdego $x \in X$ klasą abstrakcji (klasą równoważności) tego elementu nazywamy zbiór

$$[x] = \{y \in X : x\mathcal{R}y\}.$$

**Definicja 2.7.** Zbiór ilorazowy relacji $\mathcal{R}$ to zbiór klas abstrakcji tej relacji; przyjmujemy oznaczenie

$$X/\mathcal{R} = \{[x] : x \in X\}.$$

**Twierdzenie 2.8**

Niech $(X, \mathcal{R})$ będzie zbiorem z relacją równoważności. Wtedy

$$\forall x, y \in X : [x] \neq [y] \Leftrightarrow [x] \cap [y] = \emptyset.$$

*Dowód wystarczalności.* Załóżmy przez sprzeczność, że $[x] \cap [y] \neq \emptyset$, a więc $\exists z \in X : x\mathcal{R}z \wedge y\mathcal{R}z$. Teraz weźmy dowolny element $a \in [x]$. Mamy więc $x\mathcal{R}a$. Korzystając z symetryczności i przechodniości relacji $\mathcal{R}$ mamy

$$a\mathcal{R}x \wedge x\mathcal{R}z \wedge z\mathcal{R}y,$$

$$\therefore y\mathcal{R}a.$$

Z tego wynika, że $[x] \subset [y]$. Analogicznie (przyjmując na początku $a \in [y]$) dostaniemy, że $[y] \subset [x]$, wiec $[x] = [y]$, co jest sprzeczne z założeniem.

*Dowód konieczności.* Załóżmy przez sprzeczność, że $[x] = [y]$. Wtedy $[x] \cap [y] = [x] \cap [x] = [x]$ nie może być zbiorem pustym, ponieważ ze zwrotności relacji $\mathcal{R}$ wynika, że $x\mathcal{R}x$, więc $[x]$ to zbiór przynajmniej jednoelementowy. □

Z powyższego twierdzenie wynika, że relacja równoważności w danym zbiorze $X$ dzieli ten zbiór na niepuste i rozłączne podzbiory, których suma daje cały zbiór $X$.

## §2.1 Porządki

**Definicja 2.9.** Porządek (częściowy) to relacja $\mathcal{R} = (X, \operatorname{gr}\mathcal{R}, X)$, która jest zwrotna, przechodnia i antysymetryczna. Zbiór $X$ nazywamy zbiorem (częściowo) uporządkowanym.

**Definicja 2.10.** Porządek liniowy (totalny) to porządek, który jest spójny.

Niech $(X, \preceq)$ będzie zbiorem z porządkiem częściowym. Wtedy **element największy** $\overline{M} \in X$ zbioru $X$ to taki element, że

$$\forall x \in X : x \preceq \overline{M},$$

a **element maksymalny** $M_{\max} \in X$ to taki element, że

$$\forall x \in X : (M_{\max} \preceq x) \Rightarrow (M_{\max} = x).$$

**Uwaga 2.11.** Analogicznie można zdefiniować **element najmniejszy** $\overline{m}$:

$$\forall x \in X : \overline{m} \preceq x$$

oraz **element minimalny** $m_{\min}$:

$$\forall x \in X : x \preceq m_{\min} \Rightarrow (x = m_{\min})$$

**Twierdzenie 2.12**

Niech $(X, \preceq)$ będzie zbiorem z porządkiem częściowym. Jeśli w zbiorze $X$ istnieje element największy, to jest on jedyny.

*Dowód.* Załóżmy przeciwnie, że istnieją dwa elementy największe $M_1, M_2$. Z definicji zachodzi

$$M_1 \preceq M_2$$

oraz

$$M_2 \preceq M_1,$$

co jest sprzeczne z antysymetrycznością porządków. □

**Twierdzenie 2.13**

Niech $(X, \preceq)$ będzie zbiorem z porządkiem częściowym. Jeśli $M \in X$ jest elementem największym zbioru $X$, to jest on jedynym elementem maksymalnym tego zbioru.

*Dowód.* Skoro $M$ jest elementem największym, to poprzednik implikacji[1] w definicji elementu maksymalnego będzie prawdziwy tylko dla $x = M$, więc sama implikacja zawsze będzie prawdziwa. □

**Fakt 2.14.** W zbiorach z porządkiem totalnym pojęcia elementu największego i maksymalnego oraz najmniejszego i minimalnego są tożsame ze sobą. Wynika to ze spójności porządków totalnych.

Niech $(X, \preceq)$ będzie zbiorem uporządkowanym, a zbiór $A \subset X$ jego podzbiorem. Element $M \in X$ jest **majorantą** (ograniczeniem górnym) zbioru $A$ jeśli

$$\forall x \in A : x \preceq M.$$

**Kresem górnym** (supremum) zbioru $A$ (w zbiorze $X$) jest element najmniejszy zbioru majorant. Oznaczamy go symbolem

$$\sup A.$$

**Uwaga 2.15.** Analogicznie można zdefiniować **minorantę** (ograniczenie dolne) $m \in X$ zbioru $A \subset X$:

$$\forall x \in A : m \preceq x$$

oraz **kres dolny** (infimum) tego zbioru (jest nim element największy zbioru minorant), który oznaczamy symbolem

$$\inf A.$$

[1] to znaczy jej lewa strona.

**Twierdzenie 2.16**

Niech $(X, \preceq)$ będzie zbiorem z porządkiem częściowym oraz $A \subset X$. Jeśli $A$ ma element największy, to jest on również supremum tego zbioru.

*Dowód.* Z definicji majoranty wynika, że element największy zbioru $A$ jest również jego majorantą. Każda majoranta $M \in X$ zbioru $A$ oczywiście jest „większa" niż dowolny element zbioru $A$ (w tym również jego element największy $\overline{M}$), to znaczy

$$\forall M : \overline{M} \preceq M,$$

z czego wynika, że $\overline{M}$ jest elementem najmniejszym zbioru majorant zbioru $A$, a więc supremum tego zbioru. □

**Wniosek 2.17**

Jeśli zbiór częściowo uporządkowany $X$ ma supremum, które nie należy do tego zbioru, to zbiór $X$ nie ma elementu największego.

*Dowód.* Ponieważ dowolny zbiór (na mocy twierdzenia 2.12) ma co najwyżej jedno supremum, to gdyby zbiór $X$ miał element najwiekszy, to na mocy twierdzenia 2.16 byłoby ono również supremum, które należy do zbioru $X$. □

**Przykład 2.18**

Weźmy zbiór liniowo uporządkowany $(\mathbb{R}, \leq)$ oraz jego podzbiór $A = [0, 1) \subset \mathbb{R}$. Zbiór majorant zbioru $A$ to przedział $[1, \infty)$, a jego najmniejszy element (a zarazem supremum zbioru $A$) to liczba 1. Mamy więc

$$\sup A = 1.$$

Liczba 1 nie należy jednak do zbioru $A$, więc, na mocy wniosku 2.17, element największy (a z faktu 2.14 również maksymalny) nie istnieje.

**Przykład 2.19**

Weźmy zbiór częściowo uporządkowany $(\mathbb{C}, \preceq)$, gdzie zdefiniujemy

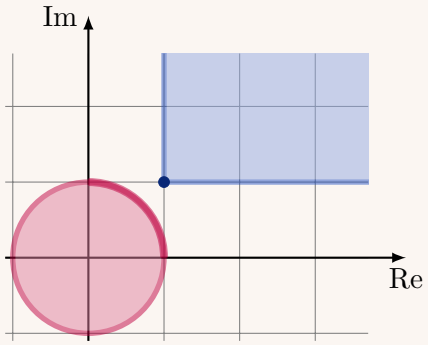
$$x \preceq y \Leftrightarrow \operatorname{Re} x \leq \operatorname{Re} y \wedge \operatorname{Im} x \leq \operatorname{Im} y.$$

Oczywiście niektóre elementy nie będą w tym porządku porównywalne, na przykład 1 oraz $i$.

Weźmy również podzbiór $A \subset \mathbb{C}$ taki, że

$$A = \{z : |z| \leq 1\}.$$

Na rysunku zaznaczono zbiór $A$, zbiór majorant $M$ zbioru $A$, supremum zbioru $A$ oraz zbiór elementów maksymalnych (jako ćwierćokrąg). Na mocy wniosku 2.17 element największy nie istnieje.




**Definicja 2.20.** Łańcuch to taki podzior $C \subset X$, że $(X, \preceq)$ jest zbiorem z porządkiem częściowym, a $(C, \preceq)$ jest zbiorem z porządkiem liniowym.

**Definicja 2.21.** Silny porządek to relacja, która jest przechodnia i asymetryczna. Silnie uporządkowany zbiór $X$ oznaczamy przez $(X, \prec)$.

## §3 Struktury algebraiczne

**Działaniem** (wewnętrznym) w zbiorze $A$ nazwiemy każde odwzorowanie $h$ takie, że

$$h : A \times A \to A.$$

**Działaniem zewnętrznym** w zbiorze $A$ jest odwzorowanie

$$h : F \times A \to A.$$

Jeśli zamiast $h$ weźmiemy jakiś symbol, na przykład $\circ$, to zamiast $h(a, b)$ będziemy pisać $a \circ b$.

**Definicja 3.1** (rodzaje działań)**.** W zbiorze z działaniem $(A, \circ)$ działanie $\circ$ jest:

- **łączne** $\Leftrightarrow \forall x, y, z \in A : (x \circ y) \circ z = x \circ (y \circ z)$,
- **przemienne** $\Leftrightarrow \forall x, y, \in A : x \circ y = y \circ x$.

Jeśli dla pewnego elementu $e \in A$ zachodzi

$$\forall x \in A : x \circ e = e \circ x = x,$$

to $e$ jest **elementem neutralnym**.

**Fakt 3.2.** Jeżeli w zbiorze $A$ z działaniem $\circ$ istnieje element neutralny, to jest on jedyny.

*Dowód.* Jeśli mielibyśmy dwa elementy neutralne $e_1, e_2$ to mamy

$$e_1 \circ e_2 = e_1 = e_2.$$

□

Jeżeli istnieje element neutralny $e \in A$ działania $\circ$, to **elementem symetrycznym** do $x \in A$ jest taki element $x' \in A$, że

$$x \circ x' = e = x' \circ x.$$

**Lemat 3.3**

Jeśli działanie $\circ$ jest łączne w zbiorze $A$ i istnieje element neutralny $e \in A$, to jeśli dany element $x \in A$ ma element symetryczny, to jest on jedyny oraz zachodzi $(x')' = x$.

*Dowód.* Jeśli mielibyśmy dwa elementy symetryczne $x_1', x_2'$, to mamy

$$x_1' = x_1' \circ e = x_1' \circ (x \circ x_2') = (x_1' \circ x) \circ x_2' = e \circ x_2' = x_2'.$$

Ponadto z definicji elementu symetrycznego mamy

$$x' \circ x = e$$

oraz

$$x' \circ (x')' = e,$$

a więc $x$ jest elementem symetrycznym $x'$, ergo $(x')' = x$. □

## §3.1 Grupy

**Definicja 3.4.** Grupa to para $(A, \circ)$, gdzie $A$ jest zbiorem, a działanie $\circ$ jest:
1. wewnętrzne,
2. łączne,
3. ma element neutralny,
4. a każdy element $x \in A$ ma element symetryczny.

**Definicja 3.5.** Grupa abelowa (przemienna) to grupa, w której działanie $\circ$ jest przemienne.

**Przykład 3.6**

Przykłady grup:

1. $(\mathbb{Z}, +)$ – grupa abelowa,
2. $(\mathbb{Z}_n, +_n)$ – grupa abelowa[a],
3. $(\mathbb{Q}_+, \cdot)$ – grupa abelowa,
4. grupą nieabelową jest grupa obrotów danego obiektu o $90°$ względem dowolnej z trzech osi.

[a] gdzie $\mathbb{Z}_n$ oznacza zbiór $\{0, 1, \ldots, n-1\}$, a $+_n$ operację dodawania modulo $n$

**Twierdzenie 3.7**

$(\mathbb{Z}_n \setminus \{0\}, \cdot_n)$ jest grupą wtedy i tylko wtedy, gdy $n \geq 2$ jest liczbą pierwszą.

Łatwo sprawdzić, że mnożenie modulo $n$ w zbiorze $\mathbb{Z}_n \setminus \{0\}$ jest wewnętrze i łączne. Ma również element neutralny 1. Będziemy więc dowodzić jedynie istnienia elementu symetrycznego dla każdego elementu.

*Dowód wystarczalności.* Załóżmy przeciwnie, że istnieje $k \in \mathbb{Z}_n \setminus \{0, 1\}$ takie, że $k \mid n$. Skoro $(\mathbb{Z}_n \setminus \{0\}, \cdot_n)$ jest grupą, to $k$ ma element symetryczny $k^{-1}$. Zachodzi więc

$$kk^{-1} \equiv 1 \pmod{n},$$

czyli inaczej

$$\exists m \in \mathbb{Z} : kk^{-1} - 1 = mn.$$

Co jednak prowadzi do sprzeczności, ponieważ

$$kk^{-1} - 1 \not\equiv mn \pmod{k}$$

$$-1 \not\equiv 0 \pmod{k}.$$

*Dowód dostateczności.* Skoro $n$ jest liczbą pierwszą, to z małego twierdzenia Fermata mamy

$$a^{n-1} \equiv 1 \pmod{n}$$

dla każdego $a \in \mathbb{Z}_n \setminus \{0\}$. Z tego wynika, że dla dowolnego elementu $a$ jego elementem symetrycznym będzie $a^{n-2}$. □

## §3.2 Pierścienie i ciała

**Definicja 3.8.** Pierścień to trójka $(P, \circ, *)$, gdzie $P$ jest zbiorem, $\circ, *$ to działania wewnętrzne oraz

1. $(P, \circ)$ jest grupą abelową
2. działanie $*$ jest łączne
3. działanie $*$ jest rozdzielne względem $\circ$, czyli

$$\forall x, y, z \in P : \begin{array}{l} (x \circ y) * z = (x * z) \circ (y * z), \\ x * (y \circ z) = (x * y) \circ (x * z). \end{array}$$

**Definicja 3.9.** Pierścień przemienny to pierścień $(P, \circ, *)$, w którym $*$ jest działaniem przemiennym[2].

Pierwsze działanie w pierścieniu nazywamy **działaniem addytywnym** i oznaczamy przez $+$. Element neutralny tego działania nazywamy zerem ($\mathbf{0}$), a element symetryczny do elementu $x$ nazywamy elementem przeciwnym i oznaczamy $-x$.

Drugie działanie nazywamy **działaniem multiplikatywnym** i oznaczamy przez $\cdot$. Jeśli w $P$ dodatkowo istnieje element neutralny tego działania, to ten element nazywamy jedynką ($\mathbf{1}$), a pierścień nazywamy **pierścieniem z jedynką**. Element symetryczny do elementu $x$ nazywamy elementem odwrotnym i oznaczamy $x^{-1}$.

[2] wtedy też rozdzielność prawo- i lewostronna stają się tożsame

**Definicja 3.10.** Dzielnikiem zera jest taki element pierścienia $a \neq \mathbf{0}$, że istnieje niezerowy element $b$, dla którego zachodzi $a \cdot b = \mathbf{0}$.

**Definicja 3.11.** Pierścień całkowity to pierścień z jedynką, w którym nie ma dzielników zera.

**Lemat 3.12**

W pierścieniach całkowitych zachodzi **własność skracania**, to znaczy, że dla elementów pierścienia $a, b, c$ przy $c \neq \mathbf{0}$ zachodzi

$$ac = bc \Rightarrow a = b.$$

*Dowód.* Jeśli $ac = bc$, to $ac - bc = \mathbf{0}$. Z rozdzielności dostajemy

$$(a - b)c = \mathbf{0}.$$

W pierścieniu całkowitym nie ma jednak dzielników zera, więc $a - b = \mathbf{0}$, co dowodzi tezy. □

**Definicja 3.13.** Ciało to pierścień z jedynką, w którym dla każdego elementu $x \neq \mathbf{0}$ istnieje element odwrotny $x^{-1}$.

Ciałem przemiennym będzie ciało, w którym działanie $\cdot$ jest przemienne. Niektórzy autorzy utożsamiają pojęcie ciała z ciałem przemiennym.

Można zauważyć, że struktura $(K, +, \cdot)$ jest ciałem (przemiennym) jeżeli:

1. $(K, +)$ jest grupą abelową,
2. $(K \setminus \{\mathbf{0}\}, \cdot)$ jest grupą (przemienną),
3. zachodzi warunek rozdzielności $\cdot$ względem $+$.

**Lemat 3.14**

Dla każdego elementu ciała $a$ zachodzi $a \cdot \mathbf{0} = \mathbf{0}$.

*Dowód.*

$$\begin{aligned} a \cdot \mathbf{0} &= a \cdot (\mathbf{0} + \mathbf{0}) \\ a \cdot \mathbf{0} &= a \cdot \mathbf{0} + a \cdot \mathbf{0} \\ a \cdot \mathbf{0} + -a \cdot \mathbf{0} &= a \cdot \mathbf{0} + a \cdot \mathbf{0} + -a \cdot \mathbf{0} \\ \mathbf{0} &= a \cdot \mathbf{0} + \mathbf{0} \\ \mathbf{0} &= a \cdot \mathbf{0} \end{aligned}$$

□

**Twierdzenie 3.15**

Każde ciało jest pierścieniem całkowitym.

*Dowód.* Załóżmy przeciwnie, że istnieją dzielniki zera, czyli takie dwa elementy ciała $x, y$, że $x, y \neq \mathbf{0}$ oraz $x \cdot y = \mathbf{0}$. Mamy

$$\begin{aligned} x \cdot y &= \mathbf{0} \\ x^{-1} \cdot x \cdot y &= x^{-1} \cdot \mathbf{0} \\ y &= x^{-1} \cdot \mathbf{0}, \end{aligned}$$

co, na mocy lematu 3.14, jest sprzecznością z założeniem. □

**Twierdzenie 3.16**

Każdy skończony pierścień całkowity jest ciałem.

*Dowód.* Załóżmy przeciwnie, że istnieje element pierścienia $a \neq \mathbf{0}$, który nie ma elementu odwrotnego. Rozważmy iloczyny $aa_1, aa_2, aa_3, \ldots$ elementu $a$ ze wszystkimi innymi elementami pierścienia (w tym z $\mathbf{1}$). Z założenia nie ma wsród nich jedynki, więc, skoro $\cdot$ jest działaniem wewnętrznym, to z zasady szufladkowej istnieją takie $a_k \neq a_l$, że $aa_k = aa_l$. To stwierdzenie jest jednak sprzecznością na mocy lematu 3.12, ponieważ rozważamy pierścienie całkowite, w których nie ma dzielników zera. □

**Przykład 3.17**

Przykłady pierścieni i ciał:

- $(\mathbb{Z}, +, \cdot)$ – pierścień całkowity, który nie jest ciałem (nie ma dzielników zera, ale często elementy odwrotne nie zawierają się z zbiorze $\mathbb{Z}$),
- $(\mathbb{Q}, +, \cdot)$ – ciało liczb wymiernych,
- $(\mathbb{R}, +, \cdot)$ – ciało liczb rzeczywistych,
- $(\mathbb{C}, +, \cdot)$ – ciało liczb zespolonych,
- $(\mathbb{Z}_n, +_n, \cdot_n)$ – pierścień przemienny z jedynką.

**Wniosek 3.18** (z twierdzenia 3.7)

Pierścień $(\mathbb{Z}_n, +_n, \cdot_n)$ jest ciałem wtedy i tylko wtedy, gdy $n$ jest liczbą pierwszą.

## §3.3 Morfizmy

**Definicja 3.19.** Homomorfizmem grupy $(A_1, +)$ w grupę $(A_2, \oplus)$ jest takie odwzorowanie $h : A_1 \to A_2$, że

$$\forall x, y \in A_1 : h(x + y) = h(x) \oplus h(y).$$

**Fakt 3.20.** Jeśli $h : A_1 \to A_2$ jest homomorfizmem grupy $(A_1, +)$ w $(A_2, \oplus)$, to

1. $e \in A_1$ jest elementem neutralnym w $(A_1, +) \implies h(e) \in A_2$ jest elementem neutralnym w $(A_2, \oplus)$,
2. $\forall x \in A_1 : h(x') = h(x)'$.

**Definicja 3.21.** Izomorfizm między grupami $(A_1, +), (A_2, \oplus)$ jest homomorfizmem bijektywnym. Jeśli taki izomorfizm istnieje, to dwie grupy nazywamy izomorficznymi.

**Definicja 3.22.** Automorfizm to izomorfizm struktury na samą siebie.

Analogicznie definiujemy morfizmy między pierścieniami i ciałami (wtedy równość z definicji 3.19 musi zachodzić dla obydwu działań).

**Przykład 3.23**

Przykłady morfizmów:

- $h(x) = x^2$ jest homomorfizmem grupy $(\mathbb{R} \setminus \{0\}, \cdot)$ w $(\mathbb{R}_+, \cdot)$,
- $h(x) = e^x$ jest izomorfizmem grupy $(\mathbb{R}, +)$ w $(\mathbb{R}_+, \cdot)$, ponieważ
$$h(x + y) = e^{x+y} = e^x \cdot e^y = h(x) \cdot g(y),$$
- $h(z) = \overline{z}$ jest automorfizmem grupy $(\mathbb{C}, +)$.

Na podobnej zasadzie jak w przykładzie drugim, można pokazać izomorfizm grupy $(\mathbb{Z}_n, +_n)$ z grupą pierwiastów $n$-tego stopnia z jedności względem mnożenia $(\mu_n(\mathbb{C}), \cdot)$. Biorąc funkcję $h(x) = \cos(\frac{2\pi}{n}x) + i\sin(\frac{2\pi}{n}x)$, mamy

$$\begin{aligned} h(x+y) &= \cos(\tfrac{2\pi}{n}(x+y)) + i\sin(\tfrac{2\pi}{n}(x+y)) \\ &= \big(\cos(\tfrac{2\pi}{n}x) + i\sin(\tfrac{2\pi}{n}x)\big) \cdot \big(\cos(\tfrac{2\pi}{n}y) + i\sin(\tfrac{2\pi}{n}y)\big) = h(x) \cdot h(y) \end{aligned}$$