Wykład 1
Podstawowe struktury algebraiczne

1 Działanie w zbiorze

Mając dane dowolne dwa przedmioty a, b możemy z nich utworzyć **parę uporządkowaną** (a, b) o poprzedniku a i następniku b.

Warunek na równość par uporządkowanych:

$$(a, b) = (c, d) \iff (a = c \text{ i } b = d).$$

Iloczynem kartezjańskim zbiorów A i B nazywamy zbiór $A \times B$ wszystkich par uporządkowanych (a, b) takich, że $a \in A$ i $b \in B$.

Definicja 1.1. Działaniem w niepustym zbiorze A nazywamy każde odwzorowanie zbioru $A \times A$ w zbiór A. Jeżeli $\circ$ jest działaniem w zbiorze A i $a, b \in A$, to $\circ((a, b))$ oznaczamy przez $a \circ b$ i nazywamy **wynikiem działania** $\circ$ na parze (a, b).

Działania będziemy oznaczali symbolami: $\circ$, $\cdot$, $+$, $\oplus$, itd.

Działaniu w zbiorze skończonym A można przyporządkować tabelkę wpisując w lewym górnym rogu oznaczenie działania i wypisując dwukrotnie elementy zbioru A: raz w pierwszym rzędzie poziomym i raz w pierwszym rzędzie pionowym, a następnie wpisując na przecięciu rzędu poziomego odpowiadającego elementowi a i rzędu pionowego odpowiadającego elementowi b wynik omawianego działania na parze (a, b). Odwrotnie, każda tabelka, która w pierwszym rzędzie poziomym i pierwszym rzędzie pionowym zawiera wszystkie elementy danego skończonego zbioru A napisane tylko jeden raz, a na pozostałych miejscach ma wpisane w dowolny sposób pewne elementy zbioru A, określa w A działanie. Wynikiem tego działania na parze (a, b) jest element stojący w rzędzie poziomym odpowiadającym a i rzędzie pionowym odpowiadającym b. Wynika stąd w szczególności, że w zbiorze n-elementowym można określić dokładnie n^{n^2} różnych działań.

Przykład 1.2. Niżej podajemy tabelki wszystkich możliwych działań w zbiorze 2-elementowym $A = \{0, 1\}$:

$\circ_1$	0	1
0	0	0
1	0	0

$\circ_2$	0	1
0	1	0
1	0	0

$\circ_3$	0	1
0	0	1
1	0	0

$\circ_4$	0	1
0	0	0
1	1	0

$\circ_5$	0	1
0	0	0
1	0	1

$\circ_6$	0	1
0	0	0
1	1	1

$\circ_7$	0	1
0	1	1
1	0	0

$\circ_8$	0	1
0	0	1
1	1	0

$\circ_9$	0	1
0	0	1
1	0	1

$\circ_{10}$	0	1
0	1	0
1	1	0

$\circ_{11}$	0	1
0	1	0
1	0	1

$\circ_{12}$	0	1
0	0	1
1	1	1

$\circ_{13}$	0	1
0	1	0
1	1	1

$\circ_{14}$	0	1
0	1	1
1	0	1

$\circ_{15}$	0	1
0	1	1
1	1	0

$\circ_{16}$	0	1
0	1	1
1	1	1

Niech $\circ$ będzie działaniem w zbiorze A. Powiemy, że
(1) działanie $\circ$ jest **łączne**, jeżeli $(a \circ b) \circ c = a \circ (b \circ c)$, dla dowolnych $a, b, c \in A$,
(2) działanie $\circ$ jest **przemienne**, jeżeli $a \circ b = b \circ a$, dla dowolnych $a, b \in A$,
(3) $e \in A$ jest **elementem neutralnym** działania $\circ$, jeżeli $e \circ a = a \circ e = a$, dla każdego $a \in A$.

Można wykazać, że jeśli działanie $\circ$ w zbiorze A jest łączne, to wynik tego działania na układzie elementów $a_1, \ldots, a_n \in A$ nie zależy od sposobu rozmieszczenia nawiasów. Na przykład

$$(a_1 \circ (a_2 \circ a_3)) \circ a_4 = (a_1 \circ a_2) \circ (a_3 \circ a_4) = a_1 \circ (a_2 \circ (a_3 \circ a_4)) = \\ = a_1 \circ ((a_2 \circ a_3) \circ a_4) = ((a_1 \circ a_2) \circ a_3) \circ a_4.$$

Pozwala to na pomijanie nawiasów i używanie zapisu $a_1 \circ a_2 \circ \ldots \circ a_n$ dla dowolnej liczby naturalnej n.

Uwaga 1.3. Łatwo zauważyć, że działanie w zbiorze skończonym jest przemienne wtedy i tylko wtedy, gdy jego tabelka jest symetryczna względem głównej przekątnej. W szczególności w zbiorze n-elementowym istnieje dokładnie $n^{\frac{n(n+1)}{2}}$ różnych działań przemiennych. Spośród działań z przykładu 1.2 przemiennymi są zatem jedynie $\circ_1, \circ_2, \circ_5, \circ_8, \circ_{11}, \circ_{12}, \circ_{15}, \circ_{16}$.

Uwaga 1.4. Każde działanie w zbiorze A może posiadać co najwyżej jeden element neutralny. Rzeczywiście, niech e i f będą elementami neutralnymi działania $\circ$ w zbiorze A. Wtedy w szczególności $e \circ a = a$ oraz $b \circ f = b$ dla dowolnych $a, b \in A$. Podstawiając $a = f$ i $b = e$ uzyskamy stąd, że $e \circ f = f$ i $e \circ f = e$, skąd $e = f$. Spośród działań z przykładu 1.2 element neutralny posiadają jedynie $\circ_5, \circ_8, \circ_{11}, \circ_{15}, \circ_{12}$.

Uwaga 1.5. Po dość uciążliwych rachunkach można sprawdzić, że spośród wszystkich działań z przykładu 1.2 łącznymi są jedynie $\circ_1, \circ_5, \circ_6, \circ_8, \circ_9, \circ_{11}, \circ_{12}, \circ_{16}$. Przy sprawdzaniu prawdziwości formuły $(a \circ (b \circ c) = a \circ (b \circ c)$ mamy aż 8 przypadków!

Przykład 1.6. Ważnymi w informatyce działaniami są tzw. **dodawanie i mnożenie modulo** n. Mianowicie, niech $n > 1$ będzie ustaloną liczbą naturalną i niech $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ będzie zbiorem wszystkich reszt z dzielenia liczb całkowitych przez n. Wtedy zbiór $\mathbb{Z}_n$ ma dokładnie n elementów. **Dodawanie modulo** n definiujemy dla $a, b \in \mathbb{Z}_n$ przy pomocy wzoru:

$$a +_n b = \text{reszta z dzielenia } a + b \text{ przez } n. \tag{1}$$

Natomiast **mnożenie modulo** n definiujemy dla $a, b \in \mathbb{Z}_n$ następująco:

$$a \cdot_n b = \text{reszta z dzielenia } a \cdot b \text{ przez } n. \tag{2}$$

Nietrudno jest pokazać, że oba te działania są przemienne i łączne oraz posiadają element neutralny 0 i 1 odpowiednio. Niżej podajemy tabelki działań $+_5$ i $\cdot_5$:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

2 Grupy

Definicja 1.7. Układ $(A, \circ_1, \ldots, \circ_n, e_1, \ldots, e_k)$, w którym A jest niepustym zbiorem, $\circ_1, \ldots, \circ_n$ są działaniami w zbiorze A, zaś $e_1, \ldots, e_k \in A$ są wyróżnionymi elementami zbioru A nazywamy **strukturą algebraiczną**.

Definicja 1.8. Strukturę algebraiczną $(G, \circ, e)$ nazywamy **grupą**, jeżeli spełnia następujące warunki (aksjomaty grupy):

G1. $a \circ (b \circ c) = (a \circ b) \circ c$, dla dowolnych $a, b, c \in G$ (tzn. działanie $\circ$ jest łączne) .

G2. $a \circ e = e \circ a = a$, dla każdego $a \in G$ (tzn. e jest elementem neutralnym działania $\circ$).

G3. dla każdego $a \in G$ istnieje $x \in G$ taki, że $a \circ x = x \circ a = e$.

Definicja 1.9. Mówimy, że grupa $(G, \circ, e)$ jest **abelowa**, jeżeli działanie $\circ$ jest przemienne.

Uwaga 1.10. W dowolnej grupie $(G, \circ, e)$ zachodzą **prawa skracania równości**:
(I) $\forall_{a,b,c \in G}\ [a \circ b = a \circ c \Rightarrow b = c]$ oraz (II) $\forall_{a,b,c \in G}\ [b \circ a = c \circ a \Rightarrow b = c]$.

Rzeczywiście, na mocy **(G3)** istnieje $x \in G$ taki, że $x \circ a = a \circ x = e$, więc jeżeli $a \circ b = a \circ c$, to $x \circ (a \circ b) = x \circ (a \circ c)$, skąd z **(G1)** $(x \circ a) \circ b = (x \circ a) \circ c$, czyli $e \circ b = e \circ c$. Zatem z **(G2)** $b = c$, co dowodzi (I). Dowód (II) jest analogiczny.

Uwaga 1.11. Element x w aksjomacie **(G3)** jest wyznaczony jednoznacznie przez element a, gdyż jeżeli dodatkowo $y \in G$ spełnia warunek $a \circ y = y \circ a = e$, to $a \circ x = a \circ y$, więc z uwagi 1.10, $x = y$. Ten dokładnie jeden element x nazywamy **elementem odwrotnym (przeciwnym)** do a i oznaczamy przez a^{-1} (przez $-a$, gdy $\circ = +$). Z uwagi 1.10 wynika od razu, że x jest elementem odwrotnym do a wtedy i tylko wtedy, gdy $a \circ x = e$. Ponieważ $a^{-1} \circ a = e$, więc a jest elementem odwrotnym do a^{-1}, skąd mamy wzór

$$(a^{-1})^{-1} = a \text{ dla każdego } a \in G.$$

Ponadto dla dowolnych $a, b \in G$ zachodzi wzór:

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1}.$$

Rzeczywiście, wystarczy zauważyć, że $(a \circ b) \circ (b^{-1} \circ a^{-1}) = e$. Z łączności działania $\circ$ mamy $(a \circ b) \circ (b^{-1} \circ a^{-1}) = ((a \circ b) \circ b^{-1}) \circ a^{-1} = (a \circ (b \circ b^{-1})) \circ a^{-1} = (a \circ e) \circ a^{-1} = a \circ a^{-1} = e$.

I. Niech $(G, \cdot, e)$ będzie grupą. Wówczas dla $a \in G$, a^{-1} jest elementem odwrotnym do a. Całkowitą potęgę elementu a określamy następująco:

1. $a^0 = e$,
2. $a^1 = a$,
3. $a^{n+1} = a^n \cdot a$ dla $n = 1, 2, \ldots$
4. $a^{-n} = (a^{-1})^n$ dla $n = 1, 2, \ldots$

Zatem dla $n = 1, 2, \ldots$

$$a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n}.$$

Można udowodnić, że dla dowolnych liczb całkowitych m, n i dla każdego $a \in G$ zachodzą wzory:

$$(1)\ a^n \cdot a^m = a^{n+m} \text{ oraz } (2)\ (a^n)^m = a^{nm}.$$

Ponadto jeżeli $a, b \in G$ są takie, że $a \cdot b = b \cdot a$, to dla dowolnego całkowitego n zachodzi wzór:

$$(a \cdot b)^n = a^n \cdot b^n.$$

Zapis użyty w **I** nazywamy **multiplikatywnym** (od łacińskiego *mutiplicare* — mnożyć). W tym zapisie często element neutralny e oznacza się przez 1, chociaż nie musi to być liczba naturalna 1.

II. Niech $(G, +, 0)$ będzie grupą abelową. Wówczas dla $a \in G$, $-a$ jest elementem przeciwnym do a. Całkowitą wielokrotność elementu a określamy następująco:
1'. $0 \cdot a = 0$,
2'. $1 \cdot a = a$,
3'. $(n+1) \cdot a = n \cdot a + a$ dla $n = 1, 2, \ldots$
4'. $(-n) \cdot a = n \cdot (-a)$ dla $n = 1, 2, \ldots$

Taki zapis nazywamy **addytywnym** (od łacińskiego *addere* — dodawać) i z reguły jest on stosowany jedynie w przypadku grup abelowych. W tym zapisie element neutralny grupy jest oznaczany przez 0, chociaż nie musi to być liczba całkowita 0.

Z **I** wynika, że dla dowolnych liczb całkowitych m, n i dla każdego $a \in G$ zachodzą wzory:

$$(1)'\ n \cdot a + m \cdot a = (n+m) \cdot a \text{ oraz } (2)'\ n \cdot (m \cdot a) = (nm) \cdot a.$$

Jeżeli napiszemy *niech G będzie grupą*, to będziemy mieli na myśli grupę multiplikatywną z działaniem oznaczonym kropką, którą — tak jak w przypadku wyrażeń algebraicznych — często będziemy pomijać.

Przykład 1.12. Niech $n \in \mathbb{N}$ oraz $X = \{1, 2, \ldots, n\}$. Przypomnijmy, że każdą bijekcję $f\colon X \to X$ nazywamy permutacją zbioru X. Niech S_n oznacza zbiór wszystkich permutacji zbioru X. Wówczas S_n ze zwykłym składaniem przekształceń i przekształceniem tożsamościowym id_X tworzy grupę. Nazywamy ją **grupą permutacji** zbioru n-elementowego. □

Przykład 1.13. Niech $n > 1$ będzie dowolną liczbą naturalną. Wówczas $(\mathbb{Z}_n, +_n, 0)$ jest grupą abelową, którą będziemy oznaczali przez $\mathbb{Z}_n^+$. Zauważmy, że $-0 = 0$, zaś dla $0 \neq a \in \mathbb{Z}_n$ mamy, że $-a = n - a$, czyli $n - a$ jest elementem przeciwnym do a.

Definicja 1.14. Podgrupą grupy $(G, \cdot, e)$ nazywamy taki podzbiór $H \subseteq G$, że $e \in H$, $h^{-1} \in H$ dla każdego $h \in H$ oraz $h_1 \cdot h_2 \in H$ dla dowolnych $h_1, h_2 \in H$.

Stwierdzenie 1.15. *Niech $(G, \cdot, e)$ będzie grupą. Podzbiór $H \subseteq G$ jest podgrupą grupy G wtedy i tylko wtedy, gdy H tworzy grupę ze względu na ograniczenie do H działania $\cdot$.*

Definicja 1.16. Niech a będzie elementem grupy $(G, \cdot, e)$. Jeżeli istnieje liczba naturalna k taka, że $a^k = e$, to najmniejszą taką liczbę naturalną k nazywamy **rzędem elementu** a. W przeciwnym przypadku (tzn. gdy $a^n \neq e$ dla każdego $n \in \mathbb{N}$) mówimy, że rząd elementu a jest równy ∞ (nieskończoność). Rząd elementu a oznaczamy przez $o(a)$.

3 Pierścienie i ciała

Definicja 1.17. Pierścieniem nazywamy system algebraiczny $(P, +, \cdot, 0, 1)$ taki, że

P1. $(P, +, 0)$ jest grupą abelową;

P2. $a \cdot (b + c) = a \cdot b + a \cdot c$ dla dowolnych $a, b, c \in P$;

P3. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ dla dowolnych $a, b, c \in P$;

P4. $a \cdot 1 = a$ dla każdego $a \in P$;

P5. $a \cdot b = b \cdot a$ dla dowolnych $a, b \in P$.

Działanie oznaczane przez $+$ nazywamy **dodawaniem**, zaś działanie oznaczane przez $\cdot$ nazywamy **mnożeniem**, natomiast element oznaczony symbolem 1 nazywamy **jedynką pierścienia** P. Grupę abelową $(P, +, 0)$ nazywamy **grupą addytywną pierścienia** P i oznaczamy przez P^+.

Niech $(P, +, \cdot, 0, 1)$ będzie pierścieniem. Wówczas możemy w P określić odejmowanie przyjmując dla dowolnych $a, b \in P$:

$$a - b = a + (-b). \tag{3}$$

Zachodzą też następujące własności:

1. $\forall_{a \in P}\ a \cdot 0 = 0 \cdot a = 0$.

Dowód. Ponieważ $0 = 0 + 0$, więc na mocy **P2**: $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, czyli $a \cdot 0 + 0 = a \cdot 0 + a \cdot 0$, skąd z prawa skracania w grupach abelowych mamy, że $a \cdot 0 = 0$. Zatem na mocy **P5** także $0 \cdot a = 0$. □

2. $\forall_{a,b \in P}\ -(a \cdot b) = (-a) \cdot b = a \cdot (-b)$.

Dowód. Na mocy **P2** i **1** mamy, że $a \cdot b + a \cdot (-b) = a \cdot [b + (-b)] = a \cdot 0 = 0$, skąd $a \cdot (-b) = -(a \cdot b)$. Stąd na mocy **P5**: $-(a \cdot b) = -(b \cdot a) = b \cdot (-a) = (-a) \cdot b$. □

3. $\forall_{a,b,c \in P}\ (a + b) \cdot c = a \cdot c + b \cdot c$.

Dowód. Na mocy **P5**, **P2** i znowu **P5** mamy, że $(a+b) \cdot c = c \cdot (a+b) c \cdot a + c \cdot b = a \cdot c + b \cdot c$. □

4. $\forall_{a \in P}\ (-1) \cdot a = a \cdot (-1) = -a$.

Dowód. Na mocy **P4** i **P5** mamy, że $a = a \cdot 1 = 1 \cdot a$, wic z **2** i **P5**, $-a = -(a \cdot 1) = a \cdot (-1) = (-1) \cdot a$. □

5. $\forall_{a,a_1,\ldots,a_n \in P}\ a \cdot (a_1 + \ldots + a_n) = a \cdot a_1 + \ldots + a \cdot a_n$.

Dowód. Indukcja względem n. Dla $n = 2$ teza wynika z **P2**. Załóżmy, że teza zachodzi dla pewnej liczby naturalnej $n \geq 2$ i niech $a_1, \ldots, a_n, a_{n+1} \in P$. Wtedy na mocy **P2** i założenia indukcyjnego: $a \cdot (a_1 + \ldots + a_n + a_{n+1}) = a \cdot [(a_1 + \ldots + a_n) + a_{n+1}] = a \cdot (a_1 + \ldots + a_n) + a \cdot a_{n+1} = a \cdot a_1 + \ldots + a \cdot a_n + a \cdot a_{n+1}$, czyli teza zachodzi dla liczby $n + 1$. □

6. $\forall_{a,b,c \in P}\ a \cdot (b - c) = a \cdot b - a \cdot c$.

Dowód. Z określenia odejmowania, z **P2**, z **2** i znowu z określenia odejmowania mamy, że $a \cdot (b - c) = a \cdot (b + (-c)) = a \cdot b + a \cdot (-c) = a \cdot b + (-(a \cdot c)) = a \cdot b - a \cdot c$. □

Ponieważ $(P, +, 0)$ jest grupą abelową, więc ma sens całkowita wielokrotność $k \cdot a$ elementu $a \in P$ przez liczbę całkowitą k. Z teorii grup mamy zatem następujące własności:

7. $\forall_{a \in P} \forall_{n,m \in \mathbb{Z}}\ n \cdot (m \cdot a) = (nm) \cdot a$.

8. $\forall_{a\in P}\forall_{n,m\in\mathbb{Z}}\ (n+m)\cdot a = n\cdot a + m\cdot a$.

9. $\forall_{a,b\in P}\forall_{n\in\mathbb{Z}}\ n\cdot(a+b) = n\cdot a + n\cdot b$.

Można także udowodnić następującą własność:

10. $\forall_{a,b\in P}\forall_{n\in\mathbb{Z}}\ n\cdot(a\cdot b) = (n\cdot a)\cdot b = a\cdot(n\cdot b)$.

W pierścieniu P możemy też określić nieujemną całkowitą potęgę dowolnego elementu $a \in P$ przyjmując, że:

$a^0 = 1$, $a^1 = a$ oraz dla $n \in \mathbb{N}$: $a^{n+1} = a^n \cdot a$ (czyli $a^n = \underbrace{a\cdot\ldots\cdot a}_{n}$).

Przez prostą indukcję możemy wówczas udowodnić następujące własności:

11. $\forall_{a\in P}\forall_{n,m\in\mathbb{N}}\ a^n\cdot a^m = a^{n+m}$.

12. $\forall_{a\in P}\forall_{n,m\in\mathbb{N}}\ (a^n)^m = a^{nm}$.

13. $\forall_{a,b\in P}\forall_{n\in\mathbb{N}}\ (a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$.

Przykład 1.18. Podstawowym i wzorcowym przykładem pierścienia jest pierścień liczb całkowitych $\mathbb{Z}$. Bardzo ważną rolę w informatyce odgrywają pierścienie reszt modulo liczba naturalna $n > 1$. Mianowicie są to pierścienie $(\mathbb{Z}_n, +_n, \cdot_n, 0, 1)$, które będziemy oznaczali przez $\mathbb{Z}_n$.

Definicja 1.19. Mówimy, że element a pierścienia P jest **odwracalny**, jeżeli istnieje $b \in P$ takie, że $a\cdot b = 1$. Element b nazywamy w tej sytuacji **elementam odwrotnym** do elementu a i oznaczamy przez a^{-1}. Zbiór wszystkich elementów odwracalnych pierścienia P oznaczamy przez P^*.

Twierdzenie 1.20. Dla dowolnego pierścienia $(P, +, \cdot, 0, 1)$ system algebraiczny $(P^*, \cdot, 1)$ jest grupą abelową.

Przykład 1.21. Dla dowolnej liczby naturalnej $n > 1$ wykazuje się, że

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : NWD(a, n) = 1\}.$$

W szczególności $\mathbb{Z}_6 = \{1, 5\}$, $\mathbb{Z}_9 = \{1, 2, 4, 5, 7, 8\}$. W pierścieniu $\mathbb{Z}_5$ mamy, że $2^{-1} = 3$, bo $2 \cdot_5 3 = 1$. Natomiast w pierścieniu $\mathbb{Z}_9$ mamy, że $2^{-1} = 5$, gdyż $2 \cdot_9 5 = 1$. W celu wyznaczenia elementu odwrotnego do 5 w pierścieniu $\mathbb{Z}_{13}$ można posłużyć się tabelką:

x	1	2	3	4	5	6	7	8	9	10	11	12
$5 \cdot_{13} x$	5	10	2	7	12	4	9	1				

z której odczytujemy, że $5^{-1} = 8$. Tak więc obliczamy po kolei $5 \cdot_{13} 1, 5 \cdot_{13} 2$, itd, aż dochodzimy do $5 \cdot_{13} 8 = 1$ i kończymy nasz algorytm wypisując $5^{-1} = 8$.

Definicja 1.22. Ciałem nazywamy taki pierścień $(K, +, \cdot, 0, 1)$, że zbiór K ma co najmniej dwa elementy oraz każdy niezerowy element należący do K jest odwracalny.

Przykład 1.23. Można wykazać, że dla dowolnej liczby pierwszej p pierścień $\mathbb{Z}_p$ jest ciałem. Natomiast dla liczb naturalnych złożonych n pierścień $\mathbb{Z}_n$ nie jest ciałem.

Przykład 1.24. Zbiory: liczb wymiernych i liczb rzeczywistych, ze zwykłym mnożeniem i dodawaniem liczb tworzą ciała. Nazywamy je odpowiednio **ciałem liczb wymiernych** i **ciałem liczb rzeczywistych** oraz oznaczamy przez $\mathbb{Q}$ i $\mathbb{R}$ odpowiednio.

Dzielenie przez niezerowe elementy w ciele K określamy wzorem:

$$\tfrac{a}{b} = a \cdot b^{-1}$$

dla dowolnych $a, b \in K$, $b \neq 0$.

Własności działań w dowolnym ciele K są analogiczne jak w ciele $\mathbb{R}$. W szczególności dla $a, b \in K \setminus \{0\}$ mamy, że $a \cdot b \neq 0$.

Przykład 1.25 (Ciało liczb zespolonych). Podamy konstrukcję bardzo ważnego w algebrze ciała $\mathbb{C}$ zwanego **ciałem liczb zespolonych**. W zbiorze $\mathbb{R} \times \mathbb{R}$ wprowadzamy działania $+$ i $\cdot$ przy pomocy wzorów:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2), \tag{4}$$

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2 - b_1 \cdot b_2, a_1 \cdot b_2 + a_2 \cdot b_1), \tag{5}$$

dla dowolnych $a_1, a_2, b_1, b_2 \in \mathbb{R}$. Bez większego problemu można sprawdzić, że system algebraiczny $(\mathbb{R} \times \mathbb{R}, +, \cdot, (0,0), (1,0))$ jest pierścieniem, przy czym zerem jest $(0,0)$, zaś jedynką $(1,0)$ oraz dla $a, b \in \mathbb{R}$ zachodzi wzór:

$$-(a, b) = (-a, -b).$$

Jeżeli $(0,0) \neq (a,b) \in \mathbb{R} \times \mathbb{R}$, to $a^2 + b^2 > 0$ oraz $(a,b) \cdot \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = (1,0)$. Zatem mamy wzór

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

Wobec tego system algebraiczny $(\mathbb{R} \times \mathbb{R}, +, \cdot, (0,0), (1,0))$ jest ciałem. Nazywamy je **ciałem liczb zespolonych** i oznaczamy przez $\mathbb{C}$. Elementy ciała $\mathbb{C}$ nazywamy **liczbami zespolonymi** i oznaczamy literami: z, w, z_1, z_2. Geometrycznie liczby zespolone można więc traktować jako punkty na płaszczyźnie. Ze wzoru (4) wynika, że liczby zespolone dodajemy analogicznie jak wektory na płaszczyźnie zaczepione w początku układu współrzędnych. Z tego powodu liczbę zespoloną (a, b) możemy utożsamić z wektorem o początku w punkcie $(0,0)$ i końcu w punkcie (a, b).

Łatwo zauważyć, że dla dowolnych liczb rzeczywistych a, b

$$(a, 0) + (b, 0) = (a + b, 0),$$
$$(a, 0) \cdot (b, 0) = (a \cdot b, 0).$$

Z tego powodu dla liczb rzeczywistych a można dokonać utożsamienia:

$$(a, 0) \equiv a. \tag{6}$$

Przy takim utożsamieniu $\mathbb{R} \subseteq \mathbb{C}$. Liczbę zespoloną

$$i = (0, 1) \tag{7}$$

nazywamy **jednostką urojoną**. Zachodzi dla niej bardzo ważny wzór:

$$i^2 = -1. \tag{8}$$

Rzeczywiście, ze wzoru (5), $i^2 = (0,1)\cdot(0,1) = (0\cdot 0 - 1\cdot 1, 0\cdot 1 + 1\cdot 0) = (-1,0) \equiv -1$.
Stosując wzory (4)-(7) łatwo zauważyć, że dla liczb rzeczywistych a, b można dokonać utożsamienia:

$$(a,b) \equiv a + bi. \tag{9}$$

Otrzymujemy w ten sposób **postać algebraiczną** $a + bi$ liczby zespolonej (a,b).

Dodawanie, odejmowanie i mnożenie liczb zespolonych zapisanych w postaci algebraicznej wykonuje się zatem tak samo jak dodawanie, odejmowanie i mnożenie wielomianów zmiennej i, przy czym należy pamiętać o tym, że w miejsce i^2 należy zawsze podstawić (-1). Np. $(1+2i)\cdot(3-i) = 3 - i + 6i - 2i^2 = 3 + 5i + 2 = 5 + 5i$, $(1+2i) + (3-i) = 4 + i$, $(1+2i) - (3-i) = -2 + 3i$.

Natomiast przy dzieleniu liczb zepolonych wygodnie jest wykorzystywać tzw. liczby sprzężone. Jeżeli a i b są liczbami rzeczywistymi, to **liczbą sprzężoną** do liczby $z = a + bi$ nazywamy liczbę $\overline{z} = a - bi$. Łatwo zauważyć, że wówczas $z\cdot\overline{z} = a^2 + b^2$. Zatem **aby podzielić liczbę zespoloną w przez liczbę zespoloną $z \neq 0$ należy licznik i mianownik ułamka $\frac{w}{z}$ pomnożyć przez liczbę sprzężoną z mianownikiem tego ułamka**, czyli $\frac{w}{z} = \frac{w\cdot\overline{z}}{z\cdot\overline{z}} = \frac{w\cdot\overline{z}}{a^2+b^2}$. Np. $\frac{2+3i}{1+i} = \frac{(2+3i)\cdot(1-i)}{(1+i)\cdot(1-i)} = \frac{2-2i+3i-3i^2}{1^2+1^2} = \frac{2+i+3}{2} = \frac{5}{2} + \frac{1}{2}i$.

4 Zadania do samodzielnego rozwiązania

Zadanie 1.26. Wypisz tabliczki działań $+_m$ i $\cdot_m$ dla $m = 2,3,4,5,6$.

Zadanie 1.27. Oblicz:
(a) $3+4$, $3-4$, $3\cdot 4$, $3\cdot 2^{-2}$ w ciele $\mathbb{Z}_5$,
(b) 3^{-1} kolejno w $\mathbb{Z}_5$, $\mathbb{Z}_7$, $\mathbb{Z}_{11}$, $\mathbb{Z}_{13}$,
(c) $4^{12}\cdot(5^2-6)\cdot(2\cdot(-3))^{-1}$ w ciele $\mathbb{Z}_{11}$.

Zadanie 1.28. Udowodnij, że dla dowolnego naturalnego $m \geq 2$, $(\mathbb{Z}_m, +_m, 0)$ jest grupą abelową.

Zadanie 1.29. Udowodnij, że dla dowolnego naturalnego $m \geq 2$, $(\mathbb{Z}_m, +_m, \cdot_m, 0, 1)$ jest pierścieniem.

Zadanie 1.30. Udowodnij, że dla dowolnych niezerowych elementów a i b ciała K mamy, że $a\cdot b \neq 0$.

Zadanie 1.31. Udowodnij, że jeśli m jest liczbą złożoną, to pierścień $\mathbb{Z}_m$ nie jest ciałem.

Zadanie 1.32. Znajdź takie liczby rzeczywiste a i b, aby zachodziły równości:
a) $a(2+3i) + b(4-5i) = 6 - 2i$, b) $a(-\sqrt{2}+i) + b(3\sqrt{2}+5i) = 8i$,
c) $a(4-3i)^2 + b(1+i)^2 = 7 - 12i$, d) $\frac{a}{2-3i} + \frac{b}{3+2i} = 1$, e) $a\frac{2+i}{3-i} + b\left(\frac{4-i}{1-3i}\right)^2 = 1 + i$,
f) $\frac{2a-3i}{5-3i} + \frac{3b+2i}{3-5i} = 0$.

Odp. a) $a = b = 1$. b) $a = 3$, $b = 1$. c) $a = 1$, $b = 6$. d) $a = 2$, $b = 3$. e) $a = 2$, $b = 0$. f) $a = -\frac{11}{16}$, $b = \frac{7}{8}$.

Zadanie 1.33. Przedstaw w postaci algebraicznej następujące liczby zespolone:
a) $(2 + i) \cdot (4 - i) + (1 + 2i) \cdot (3 + 4i)$, b) $\frac{(3+i)\cdot(7-6i)}{3+i}$, c) $(1 + 2i) \cdot i + \frac{2+3i}{1-4i}$, d) $\frac{(1+3i)(8-i)}{(2+i)^2}$.

Odp. a) $4 + 12i$. b) $7 - 6i$. c) $-\frac{44}{17} + \frac{28}{17}i$. d) $5 + i$.

Zadanie 1.34. Przedstaw w postaci algebraicznej rozwiązania następujących równań liniowych z jedną niewiadomą $z \in \mathbb{C}$:
a) $(a-bi)z = a+bi$, b) $(a+bi)^2(1-z)+(a-bi)^2(1+z) = 0$, c) $(a+bi)z = (2a+3b)+(2b-3a)i$, d) $(1 - i)z = (2a - b) - (2a + b)i$.

Odp. a) $z = \frac{a^2-b^2}{a^2+b^2} + \frac{2ab}{a^2+b^2}i$. b) $z = \frac{b^2-a^2}{4ab}i$. c) $z = 2 - 3i$. d) $z = 2a - bi$.