Matematyka 2
Algebra

Definicje, twierdzenia, przykłady

Informatyka Stosowana, I rok

1 Grupy, pierścienie i ciała

1.1 Definicja (Działanie)**. Działaniem dwuargumentowym w zbiorze** A nazywamy dowolną funkcję typu $f : A \times A \to A$.

1. Działanie $\circ$ jest łączne, gdy
$$\forall a, b, c \,.\, (a \circ b) \circ c = a \circ (b \circ c).$$
2. Działanie $\circ$ jest przemienne, gdy
$$\forall a, b \,.\, a \circ b = b \circ a.$$
3. Element e jest elementem neutralnym działania $\circ$, gdy
$$\forall a \,.\, a \circ e = e \circ a = a.$$

1.2 Definicja. Niech G będzie niepustym zbiorem oraz niech $+$ będzie działaniem na G i elementem wyróżnionym $0 \in G$. Strukturę $\mathbf{G} = (G, +)$ nazywamy **grupę**, gdy spełnione są następujące warunki:

1. $+$ jest działaniem łącznym,
2. 0 jest elementem neutralnym działania $+$,
3. elementy odwrotne/przeciwne $\forall x \exists d \,.\, x + d = 0$,
4. ponadto, gdy działanie $+$ jest przemienne, to G nazywamy **grupą abelową** lub **grupą przemienną**.

1.3 Definicja. Niech R będzie zbiorem co najmniej o 2 elementach oraz niech $+$ i $\cdot$ będą działaniami w R oraz niech 0 i 1 będą elementami wyróżnionymi. Strukturę $\mathbf{R} = (R, +, \cdot)$ nazywamy **pierścieniem** (**przemiennym z jedynką**), gdy:

1. $(R, +)$ jest grupą abelową z elementem neutralnym 0,

2. działanie $\cdot$ jest łączne,
3. 1 jest elementem nutralnym działania $\cdot$,
4. działanie $\cdot$ jest rozdzielne względem $+$, czyli

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c),$$

5. działanie $\cdot$ jest przemienne.

1.4 Przykład. Niech F będzie zbiorem z działaniami $+$ i $\cdot$ oraz wyróżnione elementy 0 i 1. Strukturę $\mathbf{F} = (F, +, \cdot)$ nazywamy ciałem, gdy

1. $(F, +, \cdot)$ jest **pierścieniem**
2. $(\mathbb{Z}, +, \cdot)$: pierścień przemienny z jedynką,
3. $(2\mathbb{Z}, +, \cdot)$: pierścień przemienny bez jedynki,
4. $(\mathbb{R}, +, \cdot)$: ciało,
5. $(P(X), \div, \cap)$: pierścień przemienny z jedynką,
6. M_n^n zbiór macierzy $n \times n$ o wyrazach rzeczywistych z dodawaniem i mnożeniem macierzy jest pierścieniem nieprzemiennym z 1.
7. i istnieją elementy odwrotne $\forall a \neq 0 \exists x \;\; a \cdot x = x \cdot a = 1$.

1.5 Przykład.

1. $(\mathbb{Z}, +, \cdot)$: pierścień przemienny z jedynką,
2. $(2\mathbb{Z}, +, \cdot)$: pierścień przemienny bez jedynki,
3. $(\mathbb{R}, +, \cdot)$: ciało,
4. $(P(X), \div, \cap)$: pierścień przemienny z jedynką,
5. M_n^n zbiór macierzy $n \times n$ o wyrazach rzeczywistych z dodawaniem i mnożeniem macierzy jest pierścieniem nieprzemiennym z 1.
6. Pierścień funkcji określonych na zbiorze A o wartościach w pierścieniu P, oznaczenie P^A:
   - działania w P^A, dla wszystkich $f, g \in P^A$, oraz $a \in A$:
     $(f \mathbf{+} g)(a) = f(a) + g(a)$ oraz $(f \mathbf{\cdot} g)(a) = f(a) \cdot g(a)$
   - elementy wyróżnione:
     $\mathbf{0}$ = funkcja stała równa 0 oraz $\mathbf{1}$ = funkcja stała równa 1.
7. Pierścień wielomianów $\mathbb{Q}[X]$
   - działania w $\mathbb{Q}[X]$, dla wszystkich $u, w \in \mathbb{Q}[X]$:
     $u \mathbf{+} w$ = suma wielomianów oraz
     $u \mathbf{\cdot} w$ = iloczyn wielomianów,
   - elementy wyróżnione:
     $\mathbf{0}$ = wielomian zerowy oraz $\mathbf{1}$ = wielomian równy 1, gdzie $0, 1 \in P$.

1.6 Uwaga. Czasem mówi się skrótowo $\mathbf{F} = (F, +, \cdot)$, zamiast $\mathbf{F} = (F, +, \cdot, 0, 1, (\cdot)^{-1})$.

2 Podzielność

2.1 Twierdzenie. Dla dowolnych liczb całkowitych a i b różnych od 0 istnieje $q \in \mathbb{Z}$ i $r \in \mathbb{N}$ takie, że

$$a = bq + r \text{ oraz } r < |b|.$$

Idea dowodu. Jako r bierzemy minimum zbioru $\{a - bs : s \in \mathbb{Z} \wedge a - bs > 0\}$ i kontynuujemy tę procedurę aż do momentu kiedy procedura stabilizuje się. $\dashv$

Algorytm Euklidesa. Dla dowolnych liczb całkowitych a i b różnych od zera:

$$a = bq_0 + r_1 \quad \text{oraz} \quad r_1 < |b| \tag{1}$$
$$b = r_1 q_1 + r_2 \quad \text{oraz} \quad r_2 < r_1 \tag{2}$$
$$r_1 = r_2 q_2 + r_3 \quad \text{oraz} \quad r_3 < r_2 \tag{3}$$
$$r_{n_2} = r_{n-1} q_{n-1} + r_n \quad \text{oraz} \quad r_n < r_{n-1} \tag{4}$$

Wówczas ostatnia niezerowa reszta r_n jest $NWD(a, b)$.

Równania diofantyczne

2.2 Twierdzenie. Dla dowolnych $a, b, c \in \mathbb{Z}$ równanie

$$aX + bY = c$$

ma rozwiązanie w liczbach całkowitych wtedy i tylko wtedy gdy $\text{NWD}(a, b) \mid c$. Jeśli para (x_0, y_0) jest jednym z rozwiązań równania, to wszystkie pozostałe otrzymujemy ze wzorów:

$$X = x_0 + \frac{b}{\text{NWD}(a, b)} k$$

$$Y = y_0 - \frac{a}{\text{NWD}(a, b)} k,$$

gdzie $k \in \mathbb{Z}$.

3 Pierścienie reszt

Ustalmy $n \in \mathbb{N}$, $n > 1$. Oznaczmy przez $\mathbb{Z}_n$ zbiór wszystkich reszt z dzielenia liczb całkowitych przez n, to znaczy

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

Symbolem $(a \mod n)$ oznaczmy resztę z dzielenia a przez n.
W zbiorze $\mathbb{Z}_n$ definiujemy działania:

$$a \oplus b := (a + b \mod n)$$

$$a \odot b := (a \cdot b \mod n).$$

3.1 Twierdzenie. Dla dowolnego $n \in \mathbb{N}$, $(\mathbb{Z}_n, \oplus, \odot)$ jest pierścieniem przemiennym z jedynką.

3.2 Przykład. $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_5$.

Ciała skończone

3.3 Twierdzenie. $\mathbb{Z}_p$ jest ciałem wtedy i tylko wtedy, gdy p jest liczbą pierwszą.

Dowód. Załóżmy, że $a \in \mathbb{Z}_n$ jest elementem odwracalnym. Wtedy $a \odot b = 1$ dla pewnego $b \in \mathbb{Z}_n$ to $(a \cdot b \mod n) = 1$, czyli dla pewnego $y \in \mathbb{Z}$ mamy $ab + yn = 1$. Stąd wynika, że $\mathrm{NWD}(a, n)|1$, zatem $\mathrm{NWD}(a, n) = 1$.

Z drugiej strony, jeśli $\mathrm{NWD}(a, n) = 1$, to dla pewnych $x, y \in \mathbb{Z}$ mamy $xa + yn = 1$. Zatem

$$1 = (xa + yn \mod n) = (x \mod n) \odot a,$$

co oznacza, że a ma element odwrotny. ⊣

3.4 Twierdzenie. Dla każdej liczby pierwszej p i dowolnego n naturalnego istnieje ciało które ma p^n elementów.