

# Algebra - Notatki z wykładu

Rafał Włodarczyk

INA 1 Sem.

## 1 Wykład Pierwszy

### 1.1 Symbole

**Logika**  $\neg, \wedge, \vee, \implies, \iff$

**Zbiory**  $x \in A, A \cap B, A \cup B, A - B, A \setminus B, A^C, B^C, A \subseteq B, A \times B$

**Funkcje**  $f : X \rightarrow Y, f : X \times Y \rightarrow A$  funkcja dwuargumentowa

**Własność**

Dla  $\mathbb{N} \quad \forall x(n) \forall x(x|n) \implies x = 1 \vee x = n$

Jest to definicja liczb pierwszych.

### 1.2 Definicje

**Definicja 1.2.1.** Niech  $X$  - Zbiór. Działaniem na  $X$  nazywamy każdą funkcję  $f : X \cdot X \rightarrow X$

**Przykład 1.2.1.**

- $f(x, y) = x \cdot y$  Jest działaniem na  $\mathbb{R}$  - tak
- $f(x, y) = x - y$  Jest działaniem na  $\mathbb{N}$ ? - nie, ponieważ  $\exists x, y f(x, y) \notin \mathbb{N}$

**Oznaczenie**  $f(x, y) \iff x + y, x \cdot y, x \circ y$  - Działanie ogólne

**Definicja 1.2.2.** Niech  $X$  - Zbiór. Działanie  $\circ$  nazywamy łącznym, gdy:  $\forall x, y, z \in X (x \circ y) \circ z = x \circ (y \circ z)$  Działanie  $\circ$  nazywamy przemennym, gdy:  $\forall x, y \in X x \circ y = y \circ x$

**Przykład 1.2.2.**

- $+$  na  $\mathbb{R}$  jest łączne i przemienne
- $-$  na  $\mathbb{R}$  nie jest ani łączne, ani nieprzemienne

**Definicja 1.2.3.** Niech  $\circ$  - działanie na zbiorze  $X$ . Element  $e \in X$  nazywamy elementem neutralnym (dla  $\circ$ ), gdy:  $\forall x \in X e \circ x = x \circ e = x$

**Przykład 1.2.3.**

- 0 jest elementem neutralnym dla  $+$  na  $\mathbb{N}$
- 1 jest elementem neutralnym dla  $\cdot$  na  $\mathbb{R}$

**FAKT.** Niech  $\circ$  - działanie na zbiorze  $X$ . Jeżeli  $\circ$  ma element neutralny, to jest on jedyny.  
D-d. Niech  $a, b$  oznaczać elementy neutralne. Działanie  $\circ$  na  $X$ :

- $a \circ b = b$
- $a \circ b = a$

Zatem:  $a = b$   $\square$

**Definicja 1.2.4.** Niech  $\circ$  - działanie na zbiorze  $X$ . Element  $a \in X$  nazywamy elementem odwrotnym (dla  $\circ$ ), gdy:  $\forall x \in X a \circ x = x \circ a = e$

**Przykład 1.2.4.**

- $-x$  jest elementem odwrotnym dla  $+$  na  $\mathbb{R}$
- $\frac{1}{x}$  jest elementem odwrotnym dla  $\cdot$  na  $\mathbb{R}$
- $x^2$  nie ma elementu odwrotnego dla  $\cdot$  na  $\mathbb{R}$
- $x^2$  ma element odwrotny dla  $\cdot$  na  $\mathbb{R}^+$

**FAKT.** Niech  $\circ$  - działanie na  $X, e \in X$  - element neutralny  $x \in X$  - dowolny  $x$ . W działaniu łącznym liczba odwrotna może być co najwyżej jedna. Istnieje maksymalnie jeden element odwrotny do  $x$ .

D-d. Niech  $a, b$  ozn. el. odwrotne do  $x$   
 $(a \circ x) \circ b = a \circ (x \circ b)$  (z łączności)  
 $e \circ b = a \circ e$   
 $b = a$   $\square$

**Definicja 1.2.5.** Grupą nazywamy parę elementów  $(G, \circ)$ , gdzie  $G$  - zbiór.  $\circ$  działanie na  $G$ , takie że:

1.  $\circ$  jest działaniem na  $G$
2.  $\forall a, b, c \in G (a \circ b) \circ c = a \circ (b \circ c)$  - Łączność
3.  $\exists e \in G \forall a \in G a \circ e = e \circ a = a$  - Element neutralny
4.  $\forall a \in G \exists b \in G a \circ b = b \circ a = e$  - Element odwrotny

## 2 Wykład drugi

... tbd

## 3 Wykład trzeci

... tbd

## 4 Wykład czwarty - Pierścienie

**Przykład 4.0.1.**  $(\mathbb{Z}, +, -)$  - rozszerza grupę

**Definicja 4.0.1.** Pierścieniem nazywamy trójkę  $(P, \oplus, \odot)$ , gdzie  $P$  - zbiór,  $\oplus, \odot$  - działania na  $P$ , takie że:

1.  $(P, \oplus)$  - grupa przemienna (abelowa)
2. działanie na  $\odot$  jest łączne na  $P$
3.  $\forall_x \forall_{a,b} x \odot (a \oplus b) = (x \odot a) \oplus (x \odot b)$  oraz  $(a \oplus b) \odot x = a \odot x \oplus b \odot x$

**Przykład 4.0.2.**  $(\mathbb{Z}, +, -)$  jest pierścieniem, ponieważ:

- $(\mathbb{Z}, +)$  - grupa przemienna
- $\cdot$  jest łączne na  $\mathbb{Z}$
- Rozdzielność mnożenia względem dodawania

Rozważmy inne przykłady:

- $(\mathbb{R}, +, \cdot), (\mathbb{Q}, +, \cdot)$  - pierścienie
- $(\mathbb{N}, +, \cdot)$  - nie jest pierścieniem
- $(\mathbb{R}[x], +, \cdot)$  - (el neu.  $W(x) = 0$ , el odw.  $-W(x)$ ) - zbiór wielomianów o współczynnikach  $\mathbb{R}$

### 4.1 Oznaczenia

Działania na  $P$  oznaczamy  $+, \cdot$ , nazywamy dodawaniem i mnożeniem.

- Element neutralny  $+$  oznaczamy  $0$  i nazywamy zerem.
- Element przeciwny (odwrotny) do  $a$  to  $-a$ , bo  $(a + (-a)) = 0$
- Element neutralny  $\cdot$  (nie musi istnieć) oznaczamy  $1$  i nazywamy jedyneką
- Element odwrotny do  $a$  to  $a^{-1}$

Analogicznie do  $(\mathbb{Z}, +, \cdot)$

**Przykład 4.1.1.**

- Pierścień bez  $1$  to np.  $(2\mathbb{Z}, +, \cdot)$
- Istnieje pierścień z nieprzemiennym  $\cdot$  - mnożeniem (pierścień macierzy)

## 4.2 Własności

**FAKT.** Niech  $(P, +, \cdot)$  - pierścień. Wtedy:

1.  $\forall_{a \in P} a \cdot 0 = 0 \cdot a = a$   
D-d.  $a \cdot 0 = a \cdot (0 + 0) \stackrel{rd}{=} a \cdot 0 + a \cdot 0 \mid +(-(a \cdot 0))$   
 $a \cdot 0 - (a \cdot 0) = a \cdot 0 + a \cdot 0 - a \cdot 0$   
 $0 = a \cdot 0 \quad \square$
2.  $\forall_{a, b \in P} (-a) \cdot b = -(a \cdot b)$   
D-d.  $(-a) \cdot b = -(a \cdot b) \mid + (a \cdot b)$   
 $(-a) \cdot b + a \cdot b \stackrel{rd}{=} (-a + a) \cdot b = 0 \cdot b \stackrel{1}{=} 0$   
 $(-a) \cdot b + a \cdot b = 0 \mid +(-(ab))$   
 $(-a) \cdot b = -(ab)$
3.  $\forall_{a, b \in P} (-a) \cdot (-b) = a \cdot b$   
D-d. ćwiczenie
4.  $\forall_{a, -a \in P} (-1) \cdot a = -a$   
D-d. ćwiczenie

**Definicja 4.2.1.** Niech  $(P, +, \cdot)$  - pierścień oraz niech  $A \subseteq P$ . Zbiór niepusty  $A$  nazywamy podpierścieniem, gdy:

1.  $\forall_{a, b \in A} (a + b) \in A \wedge (-a) \in A$
2.  $\forall_{a, b \in A} (a \cdot b) \in A$  (odwrotność mnożenia nie jest wymagana)

**Przykład 4.2.1.** Niech  $P = (\mathbb{R}, +, \cdot)$ ,  $A = \mathbb{Z}$ .  $\mathbb{Z}$  jest podpierścieniem, ponieważ:

1.  $a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z} \wedge (-a) \in \mathbb{Z}$
2.  $a, b \in \mathbb{Z} \implies a \cdot b \in \mathbb{Z}$

$2\mathbb{Z}$  jest podpierścieniem  $(P, +, \cdot)$

$((0, \infty), +, \cdot)$  nie jest podpierścieniem bo  $7 \in (0, \infty)$ ,  $-7 \notin (0, \infty)$

**Oznaczenie**  $A \leq P$  oznaczamy, że  $A$  jest podpierścieniem  $P$

**Własności** Jeśli  $(P, +, \cdot)$  - pierścień oraz  $A \leq P$  to  $(A, +, \cdot)$  jest pierścieniem.

D-d.  $\leftarrow$  ćwiczenie.  $(P, +, \cdot)$  posiada dwa podpierścienie  $P \leq P$  i  $\{0\} \leq P$

## 4.3 Produkt

Niech  $(P, +, \cdot), (R, \oplus, \odot)$  - pierścienie

Na zbiorze  $P \times R$  definiujemy działania:

1.  $(p_1, r_1) +_b (p_2, r_2) = (p_1 + p_2, r_1 \oplus r_2)$
2.  $(p_1, r_1) \cdot_b (p_2, r_2) = (p_1 \cdot p_2, r_1 \odot r_2)$

D-d. Sprawdzić listę własności z definicji pierścienia.

**Przykład 4.3.1.**  $\mathbb{Z} \times \mathbb{Z}$ 

$$(3, 5) + (7, 8) = (3 + 7, 5 + 8) = (10, 13)$$

Element neutralny  $(0, 0) \in \mathbb{Z} \times \mathbb{Z}$

Element przeciwny  $-(a, b) = (-a, -b)$

**Definicja 4.3.1.** Niech  $n \in (\mathbb{N})^+$   $\mathbb{Z}_n = (\{0, 1, 2, \dots, n-1\}, +_n, \cdot_n)$ .

**FAKT.**  $\mathbb{Z}_n$  jest pierścieniem skończonym.

D-d.

1.  $(\{0, 1, \dots, n-1\}, +_n)$  - grupa przeciwna  $(\mathbb{C}_n)$
2. Łączność -  $(a \cdot_n (b \cdot_n c)) = (a \cdot b \cdot c) \bmod(n)$
3. Rozdzielność -  $L = a \cdot_n (x +_n y) = (a(x + y)) \bmod(n)$   
 $P = a \cdot_n x +_n a \cdot_n y = (ax + ay) \bmod(n)$   
 $L = P$  z rozdzielności dodawania w  $(\mathbb{Z}, +, \cdot)$

**Definicja 4.3.2.** Niech  $(P, +, \cdot), (R, \oplus, \odot)$  - pierścienie. Funkcję  $f_{P \rightarrow R}$  nazywamy homomorfizmem, gdy:

1.  $\forall_{a,b \in P} f(a + b) = f(a) \oplus f(b)$
2.  $\forall_{a,b \in P} f(a \cdot b) = f(a) \odot f(b)$

**Przykład 4.3.2.**

1.  $(P, +, \cdot)$  oraz  $f(a) = a : P \rightarrow P$  to  $f$  jest homomorfizmem.
2.  $(P, +, \cdot)$  oraz  $g(a) = - : P \rightarrow P$  to  $g$  jest homomorfizmem.

$$\text{D-d. } g(a + b) = 0 = 0 + 0 = g(a) + g(b) \wedge g(a \cdot b) = 0 \cdot 0 = g(a) \cdot g(b)$$

**Przykład 4.3.3.**  $\varphi_n(k) = k \bmod(n) : (\mathbb{Z}) \rightarrow 0, 1, \dots, n-1$ 

$\varphi_n$  jest homomorficzna dla pierścieni  $(\mathbb{Z}, +, \cdot), ((\mathbb{Z})_n, +_n, \cdot_n)$ , ponieważ:

1.  $\varphi_n(a + b) = (a + b) \bmod(n)$   
 $(a \bmod(n) + b \bmod(n)) \bmod(n) = \varphi_n(a) +_n \varphi_n(b)$
2. ćwiczenie (dla mnożenia)

**FAKT.** Niech  $(P, +, \cdot), (R, \oplus, \odot)$  - pierścienie. Oraz  $f_{P \rightarrow R}$  homomorfizm. Wtedy:

1.  $f(0_P) = 0_R$

$$\begin{aligned} \text{D-d. } f(0_P) &= f(0_P + 0_P) = f(0_P) + f(0_P) \\ f(0_P) &= f(0_P) + f(0_P) \mid + (-f(0_P)) \\ 0_R &= f(0_P) \quad \square \end{aligned}$$

2.  $f(-a) = -f(a)$

$$\begin{aligned} \text{D-d. } f(-a) + f(a) &=^{hom.} f((-a) + a) = f(0) = 1 \mid 0 \mid + (-f(a)) \\ f(-a) &= -f(a) \end{aligned}$$

3.  $f(1_P) = 1_R$ , o ile istnieje
4.  $f(a^{-1}) = f(a)^{-1}$ , o ile istnieje

## 4.4 Zastosowanie

**Reguła podzielności przez 3** Notacja.  $a, b, c$  - cyfry  $0, \dots, 9$ ,  $a|b$  -  $a$  dzieli  $b$

$$\overline{abc} = 100a + 10b + c$$

$$\overline{933} = 933$$

$$\text{Przypadek: } 3|\overline{abc} \iff 3|(a+b+c)$$

$$3|\overline{abcd} \iff \overline{abcd} \pmod{3} = 0$$

$$\varphi_3(\overline{abcd}) = 0$$

$$\varphi_3(1000a + 100b + 10c + d) \stackrel{hom}{=}$$

$$\varphi_3(1000a) + \varphi_3(100b) + \varphi_3(10c) + \varphi_3(d)$$

$$\varphi_3(10)^3 + \varphi_3(10)^2 + \varphi_3(10) + \varphi_3(a) + \varphi_3(b) + \varphi_3(c) + \varphi_3(d) =$$

$$\varphi_3(a) + \varphi_3(b) + \varphi_3(c) + \varphi_3(d) = \varphi_3(a+b+c+d)$$