Algebra - Notatki z wykladu

Rafal Wlodarczyk

INA 1 Sem.

1 Wyklad Pierwszy

1.1 Symbole

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

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

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

Własność
Dla $\mathbb{N}$ $W(n) \forall_x (x|n) \implies x = 1 \vee x = n$
Jest to definicja liczb pierwszych.

1.2 Definicje

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

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 przemiennym, 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 oznaczają elementy neutralne. Działanie $\circ$ na X:

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

Zatem: $a = b \quad \square$

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)
$e \circ b = a \circ e$
$b = a \quad \square$

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. $(\mathbb{Z}, +, \cdot)$ - 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. $(\mathbb{Z}, +, \cdot)$ 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 jedynką
- 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. $\forall_{a \in P} a \cdot 0 = 0 \cdot a = 0$
   D-d. $a \cdot 0 = a \cdot (0 + 0) =^{rd} a \cdot 0 + a \cdot 0| + (-(a \cdot 0))$
   $a \cdot 0 - (a \cdot 0) = a \cdot 0 + a \cdot 0 - a \cdot 0$
   $0 = a \cdot 0 \quad \square$

2. $\forall_{a,b \in P} (-a) \cdot b = -(a \cdot b)$
   D-d. $(-a) \cdot b = -(a \cdot b)| + (a \cdot b)$
   $(-a) \cdot b + a \cdot b =^{rd} (-a + a) \cdot b = 0 \cdot b =^1 0$
   $(-a) \cdot b + a \cdot b = 0| + (-(ab))$
   $(-a) \cdot b = -(ab)$

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 podpieścieniem, 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 $A \leqslant P$ oznaczamy, że A jest podpierścieniem P

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

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

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 $n \in (N)^+$ $\mathbb{Z}_n = (\{0,1,2,\ldots,n-1\}, +_n, \cdot_n)$.

FAKT. $\mathbb{Z}_n$ jest pierścieniem skończonym.
D-d.

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

Definicja 4.3.2. Niech $(P,+,\cdot), (R, \oplus, \odot)$ - pierścienie. Funkcję $f_{P \to R}$ 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 $f(a) = a : P \to P$ to f jest homomorfizmem.
2. $(P,+,\cdot)$ oraz $g(a) = - : P \to P$ to g jest homomorfizmem.

   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. $\varphi_n(k) = k(mod(n)) : (Z) \to 0,1,\ldots,n-1$
φ_n jest homomorficzna dla pierścieni $(\mathbb{Z},+,\cdot), ((Z)_n, +_n, \cdot_n)$, ponieważ:

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

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

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

   D-d. $f(0_P) = f(0_P + 0_P) = f(0_P) + f(0_P)$
   $f(0_P) = f(0_P) + f(0_P) | + (-f(0_P))$
   $0_R = f(0_P)$ $\square$
2. $f(-a) = -f(a)$

   D-d. $f(-a) + f(a) =^{hom.} f((-a)+a) = f(0) =^1 0 | + (-f(a))$
   $f(-a) = -f(a)$
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 $0, \ldots, 9$, $a|b$ - a dzieli b
$\overline{abc} = 100a + 10b + c$
$\overline{933} = 933$
Przypadek: $3|\overline{abc} \iff 3|(a+b+c)$
$3|\overline{(abcd)} \iff \overline{abcd}(mod(3)) = 0$
$\varphi_3(\overline{abcd}) = 0$
$\varphi_3(1000a + 100b + 10c + d) =^{hom}$
$\varphi_3(1000a) + \varphi(100b) + \varphi(10c) + \varphi(d)$
$\varphi_3(10)^3 + \varphi_3(10)^2 + \varphi(10)^1 + \varphi(a) + \varphi(b) + \varphi(c) + \varphi(d) =$
$\varphi_3(a) + \varphi(b) + \varphi(c) + \varphi(d) = \varphi_3(a+b+c+d)$

5 Wykład piąty

tbd...

6 Wykład szósty

6.1 Liczby naturalne

$\mathbb{N} = \{0, 1, 2, 3, ...\}$

Definicja 6.1.1. Zasada dobrego uporządkowania (WO) Dla dowolnego $\emptyset \neq X \in \mathbb{N}$:

$$(\exists_{a \in X} \forall_{b \in X}) a \leqslant b$$

Każdy niepusty podzbiór $\mathbb{N}$ ma element najmniejszy.
$\mathbb{R}(0, 1)$ NIE spełnia WO

Definicja 6.1.2. Zasada Indukcji:
Dla dowolnego $A \in \mathbb{N}$ zachodzi:

$$[(0 \in A) \wedge ((\forall_K) K \in A \implies k+1 \in A)] \implies A = \mathbb{N}$$

Twierdzenie 6.1.1. Zasada indukcji wynika z zasady dobrego uporządkowania.
D-d. Nie wprost załóżmy że zasada indukcji nie jest prawdziwa. To znaczy, że poprzednik jest fałszywy a następnik prawdziwy.

$$0 \in A(\forall_K k \in A \implies k+1 \in A) \wedge A \neq \mathbb{N}$$

Wtedy niech $X = \mathbb{N} - A = A^c$
- $X \neq \emptyset, X \leqslant \mathbb{N}$
Z zasady WO $\exists_a \in X$, element najmniejszy w X
$a \neq 0$, bo $0 \in A, a \in X$
$a \in X$, to $a \notin A$
$a - 1 \in A \implies a = a - 1 + 1 \in A$
Dwa ostatnie punkty dają sprzeczność, zatem założenie nie wprost jest fałszywe, a twierdzenie prawdziwe.

Przykład 6.1.1. $\forall_n 1 + 3 + 5 + \cdots + 2n + 1 = (n + 1)^2$
D-d. Niech $A = \{n \in \mathbb{N}, 1 + 3 + ... + 2n + 1 = (n + 1)^2\}$
Dla $n = 0, L = 2 \cdot 0 + 1 = (0 + 1)^2 = P$
Niech $k \in a\ \forall_{k>a}$, wtedy z założenia indukcyjnego:
$1 + 3 + ... + 2k + 1 = (k + 1)^2$
$1 + 3 + ... + 2k + 1 + 2(k + 1) + 1 = (k + 1)^2 + 2k + 3 = k^2 + 2k + 1 + 2k + 3 = (k + 2)^2$
Wtedy z zasady indukcji matematycznej wynika że $A = \mathbb{N}$
Wobec tego $\forall n \in \mathbb{N}\ 1 + 3 + \cdots + 2n + 1 = (n + 1)^2 \quad \square$

Twierdzenie 6.1.2. W liczbach naturalnych nie ma nieskończonego malejącego ciągu.
D-d. Zakładamy nie wprost, że istnieje ciąg l. naturalnych:
$\{a_n\}_{n\in\mathbb{N}}$ tak, że $\forall_{k\in\mathbb{N}} a_k \in \mathbb{N}$
$a_k > a_{k+1}$
Niech $X = \{a_1, a_2, ...\}$, Mamy

1. $X \leqslant N$
2. $X \neq 0$
3. X nie ma elementu najmniejszego, bo
   niech $a \in X$ to $a = a_k, k \in \mathbb{N}$, ale wtedy
   $a_{k+1} < a_k = a$, zatem a nie jest najmniejszy.

1,2,3 są sprzeczne z zasadą dobrego uporządkowania. $\square$

Definicja 6.1.3. Niech $a, b \in \mathbb{N}$. Największym wspólnym dzielnikiem a i b nazywamy liczbę:

$$NWD(a, b) = max\{k \in \mathbb{N} : k|a \wedge k|b\}$$

NWD(15,12)=3
Algorytm euklidesa, rokzład liczb na czynniki pierwsze.

Przykład 6.1.2. Algorytm Euklidesa:
Większą zapisujemy resztą z dzielenia przez mniejszą:
Np. $(45, 12) \implies (12, 45mod12) = (12, 9) \implies (9, 12mod9) = (9, 3) \implies (3, 0)$
W momencie kiedy dowolna z liczb to 0 algorytm się kończy.
Wynikiem jest druga liczba, w tym wypadku 3.

FAKT. Aby obliczyć $NWD(a, b)$, wykonujemy do momentu gdy $a = 0 \vee b = 0$:
$(a, b) = ([min(a, b)], [max(a, b)]\%[min(a, b)])$

FAKT. Dla dowolnych $a, b \in \mathbb{N}$ algorytm Euklidesa, zaczynający od pary (a, b) zatrzymuje się.
D-d. Zakładamy nie wprost, że algorytm nie zatrzymuje się. Więc istnieje nieskończony ciąg par:
$(a_0, b_1) \implies (a_1, b_1) \implies (a_2, b_2) \implies \ldots$
Wtedy $a_0 + b_0, a_1 + b_1, a_2 + b_2, ...$ jest nieskończonym malejącym ciągiem liczb naturalnych.
Jest to sprzeczne z twierdzeniem 6.1.2, które mówi że w $\mathbb{N}$ nie ma nieskończonego malejącego ciągu. A zatem fakt jest prawdziwy $\square$.

Obserwacja. $a, b \in \mathbb{N}$, $r = a \mod b$, to $a = b\omega + r$
D-d: Niech $k \in 1, ..., n - 1$, wtedy należy dowieść, że:

$\forall_m (m|a_k \wedge m|b_k) \iff m|a_{k+1} \wedge m|b_{k+1}$
$\rightarrow$: Niech $m|a_k, b_k$, wtedy:
$m|b_k = a_k + 1$
$b_{k+1} = a_k \mod b_k$. Istnieje liczba naturalna w, taka że:
$a_k = b_k \cdot w + b_{k+1}$
$\leftarrow$: Ćwiczenie.

Niech Z_0 - zbiór wspólnych dzielników liczb a_0, b_0
(*) $Z_0 = Z_n$ - $NWD(a,b) = max(Z_0) = max(Z_n) = NWD(a_n, 0) = a_n$