Oznaczenia stosowane na wykładzie AlgT

Symbole logiczne

$\sim$, $\neg$ – negacja (nieprawda, że);
$\vee$ – alternatywa (lub);
$\wedge$ – koniunkcja (i);
$\Rightarrow$ – implikacja (jeżeli, to);
$\Leftrightarrow$ – równoważność (wtedy i tylko wtedy, gdy).

Oznaczenia zbiorów

$\mathbb{N}$ – zbiór liczb naturalnych $\{1, 2, 3, \ldots\}$;
$\mathbb{N}_0 = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \ldots\}$;
$\mathbb{Z}$ – zbiór liczb całkowitych;
$\mathbb{Q}$ – zbiór liczb wymiernych;
$\mathbb{R}$ – zbiór liczb rzeczywistych;
$\mathbb{R}_+$ – zbiór liczb rzeczywistych dodatnich;
$\mathbb{C}$ – zbiór liczb zespolonych;
$\mathbb{R}[x]$ – zbiór wielomianów o współczynnikach rzeczywistych;
$\mathbb{C}[x]$ – zbiór wielomianów o współczynnikach zespolonych;
$\mathbb{R}_k[x]$, $\mathbb{C}_k[x]$ – zbiory wielomianów stopnia co najwyżej k;
2^X – zbiór wszystkich podzbiorów zbioru X;
$Y^X = \{f : X \to Y\}$ – zbiór wszystkich funkcji o argumentach w X i wartościach w Y.

Działania algebraiczne

Niech A będzie niepustym zbiorem, $n \in \mathbb{N}_0$.

***Def*. Działaniem n-argumentowym** (wewnętrznym) w zbiorze A nazywamy każdą funkcję $f : A^n \to A$.

Przykłady.

Dodawanie i mnożenie to działania 2-argumentowe w zbiorach $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

Odejmowanie nie jest działaniem wewnętrznym w zbiorze $\mathbb{N}$, ale jest działaniem w zbiorach $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

Dzielenie nie jest działaniem wewnętrznym w powyższych zbiorach, ale jest działaniem np.
w zbiorach $\mathbb{Q} \setminus \{0\}$ i $\mathbb{R} \setminus \{0\}$.

Def. Niech $\mathcal{F}$ - układ działań w zbiorze $A \neq \emptyset$. Parę $(A, \mathcal{F})$ nazywamy **algebrą**.

Przykłady algebr: $(\mathbb{N}, +), (\mathbb{N}, +, \cdot), (\mathbb{Z}, +, \cdot), (\mathbb{Z}, -), (\mathbb{Q}, -), (\mathbb{Q}, +, -, \cdot), (\mathbb{R}, +), (\mathbb{R}, +, \cdot)$, $(2^{\mathbb{N}}, \cup, \cap), (\mathbb{R}^{\mathbb{R}}, \circ)$ – zbiór funkcji rzeczywistych z działaniem składania.

Działania binarne to działania 2-argumentowe $(A \neq \emptyset)$ $\quad f : A^2 \to A$.
Będziemy stosować oznaczenie: $f(x, y) = x \circ y$.

Def. Mówimy, że działanie $\circ$ w zbiorze A jest **przemienne**, jeśli $\forall a, b \in A \ a \circ b = b \circ a$.

Def. Mówimy, że działanie $\circ$ w zbiorze A jest **łączne**, jeśli $\forall a, b, c \in A \ (a \circ b) \circ c = a \circ (b \circ c)$.

Przykłady:
Działania dodawania i mnożenia liczb są łączne i przemienne.
Działanie odejmowania i dzielenia nie jest łączne ani przemienne.
Działanie składania w zbiorze funkcji $f : X \to X$ jest łączne, ale nie jest przemienne.
Działanie $x \circ y = x$ w zbiorze $\mathbb{R}$ jest łączne, ale nie jest przemienne, bo
$(a \circ b) \circ c = a \circ b = a$ oraz $a \circ (b \circ c) = a \circ b = a$, zaś $a \circ b = a$, gdy $b \circ a = b$.
Działanie $x \star y = x^2 + y^2$ w zbiorze $\mathbb{R}$ jest przemienne,
ale nie jest łączne, bo $(x^2 + y^2)^2 + z^2 \neq x^2 + (y^2 + z^2)^2$.
Działanie $x \diamond y = x + y^2$ w zbiorze $\mathbb{R}$ nie jest ani łączne, ani przemienne.

Def. Niech $\circ, \diamond$ - działania binarne w A.
Mówimy, że działanie $\circ$ jest **rozdzielne** względem działania $\diamond$, jeśli
$\forall a, b, c \in A \ a \circ (b \diamond c) = (a \circ b) \diamond (a \circ c)$ i $\forall a, b, c \in A \ (b \diamond c) \circ a = (b \circ a) \diamond (c \circ a)$.

Przykłady:
Mnożenie liczb jest rozdzielne względem dodawania.
Działanie sumy jest rozdzielne względem przecięcia, a działanie przecięcia jest rozdzielne względem sumy w algebrze zbiorów $(2^X, \cup, \cap)$.
Koniunkcja jest rozdzielna względem alternatywy, a alternatywa rozdzielna względem koniunkcji w algebrze zdań $(\{0, 1\}, \wedge, \vee)$.

Def. Element $e \in A$ nazywamy **elementem neutralnym** działania $\circ$ w zbiorze A, jeśli $\forall a \in A \ (e \circ a = a \circ e = a)$.

Uwaga. Jeśli istnieje element neutralny działania $\circ$ w zbiorze A to jest on wyznaczony jednoznacznie (czyli może istnieć tylko jeden element neutralny danego działania).

Przykłady:
Elementem neutralnym działania dodawania jest liczba 0 w zbiorach $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

W zbiorze $\mathbb{N}$ dodawanie nie ma elementu neutralnego.

W zbiorach $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ elementem neutralnym mnożenia jest liczba 1.

W algebrze funkcji $(X^X, \circ)$ elementem neutralnym składania jest funkcja identyczności id_X.

W algebrze zbiorów $(2^X, \cup, \cap)$ elementem neutralnym sumy jest $\emptyset$, a elementem neutralnym przecięcia jest zbiór X.

Nie każde działanie posiada element neutralny w danym zbiorze.

Działanie $x \sqcap y = max\{x, y\}$ nie posiada elementu neutralnego w zbiorze $\mathbb{R}$.

Def. Niech e będzie elementem neutralnym działania $\circ$ w zbiorze A.

Element $b \in A$ nazywamy **elementem odwrotnym** do elementu $a \in A$, jeśli $a \circ b = b \circ a = e$.

Jeśli taki element b istnieje, to element a nazywamy **odwracalnym**.

Przykłady:

W algebrze $(\mathbb{Z}, +, \cdot)$ elementem odwrotnym do liczby x względem dodawania jest liczba $-x$.

Względem mnożenia odwrotności istnieją jedynie dla 1 i dla -1.

W algebrach $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ odwracalne względem mnożenia są wszystkie liczby oprócz zera.

W algebrze funkcji $(X^X, \circ)$ odwracalne są jedynie bijekcje.

Grupy

Def. Algebrę $(G, \circ)$, gdzie $\circ$ - działanie binarne, nazywamy **grupą**, jeżeli

1. działanie $\circ$ jest łączne
2. istnieje element neutralny działania $\circ$
3. każdy element ze zbioru G jest odwracalny.

Grupę $(G, \circ)$ nazywamy **przemienną** (abelową), jeśli działanie $\circ$ jest przemienne.

Przykłady grup: $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$,

$(\mathbb{Z}_n, +_n) = (\{0, 1, \ldots, n-1\}$, dodawanie modulo $n)$,

D_n=(zbiór izometrii n-kąta foremnego, złożenie izometrii),

S_n=(permutacje zbioru n-elementowego, złożenie permutacji).

Pierścienie i ciała

Def. Algebrę $(P, \oplus, \odot)$, gdzie $\oplus, \odot$ - działania binarne, nazywamy **pierścieniem**, jeżeli

1. $(P, \oplus)$ jest grupą przemienną
2. działanie $\odot$ jest łączne
3. działanie $\odot$ jest rozdzielne względem działania $\oplus$.

Pierścień $(P, \oplus, \odot)$ nazywamy **przemiennym**, jeśli działanie $\odot$ jest przemienne.

Element neutralny działania $\oplus$ nazywamy **zerem pierścienia** (ozn. $\mathbf{0}$).

Jeśli istnieje element neutralny działania $\odot$, to nazywamy go **jedynką pierścienia** (ozn. $\mathbf{1}$).

Przykłady pierścieni: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{R}[x], +, \cdot)$ $(\mathbb{Z}_n, +_n, \cdot_n)$

Pierścień $(P, \oplus, \odot)$ nazywamy **ciałem**, jeśli $(P \setminus \{\mathbf{0}\}, \odot)$ jest grupą przemienną.

Przykłady ciał: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$.