Działania algebraiczne

Niech $A \neq \emptyset,\ n \in \mathbb{N} \cup \{0\}$.

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

- $n = 0$ – działanie 0-argumentowe oznacza konkretny element zbioru A, czyli wyróżnioną stałą np. 0, 1;
- $n = 1$ – działanie unarne, czyli funkcja o argumentach i wartościach w zbiorze A;
- $n = 2$ – działanie binarne (algebraiczne).

Jeśli zbiór A składa się z n elementów, to można zdefiniować w tym zbiorze n^{n^2} różnych działań binarnych.
Dla działania dwuargumentowego $\star$ stosujemy oznaczenie $x \star y := \star(x, y)$.

Przykład: Dodawanie (+) jest działaniem wewnętrznym między innymi w zbiorach: liczb naturalnych, liczb całkowitych parzystych, liczb wymiernych, ale nie jest działaniem w zbiorze liczb nieparzystych czy niewymiernych.
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. *Jeżeli $\mathcal{F}$ jest układem działań w zbiorze $A \neq \emptyset$, to parę $(A, \mathcal{F})$ nazywamy* ***algebrą*** *(strukturą algebraiczną).*

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.

Własności działań binarnych

Def. *Mówimy, że działanie $\star$ w zbiorze A jest* ***przemienne****, jeśli*

$$\forall x, y \in A \;\; x \star y = y \star x.$$

Def. *Mówimy, że działanie $\star$ w zbiorze A jest* ***łączne****, jeśli*

$$\forall x, y, z \in A \;\; x \star (y \star z) = (x \star y) \star z.$$

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 zbiorów 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*** $\star$*, jeśli*

$$\forall a \in A \ \ a \star e = e \star a = a.$$

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 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* $\star$ *w* A. *Element* $a \in A$ *nazywamy* ***odwracalnym*** *w* A*, jeśli istnieje element* $b \in A$ *taki, że* $a \star b = b \star a = e$*, wtedy* b *nazywamy* ***elementem odwrotnym do*** a ***względem działania*** $\star$.

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.

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** ($\mathbf{1}$).

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

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

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