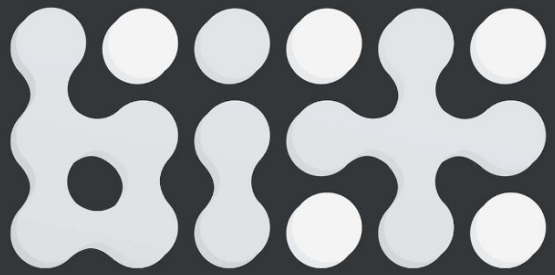

Algebra Komputerowa

Powtórzenie Podstaw Algebry

Filip Zieliński

2025

Spis Treści

KOŁO NAUKOWE

Działanie Wewnętrzne

KOŁO NAUKOWE

Definicja

Niech X będzie ustalonym niepustym zbiorem. Dwuargumentowym **działaniem wewnętrznym** na zbiorze X nazywamy dowolne odwzorowanie $h : X \times X \to X$. Dla elementów $x, y \in X$ wartość $h(x, y)$ nazywamy wynikiem działania h na argumentach x, y.

Definicja

Niech X będzie ustalonym niepustym zbiorem. Dwuargumentowym **działaniem wewnętrznym** na zbiorze X nazywamy dowolne odwzorowanie $h : X \times X \to X$. Dla elementów $x, y \in X$ wartość $h(x, y)$ nazywamy wynikiem działania h na argumentach x, y.

Przykład

Działaniami wewnętrznymi są np.

- $h(x, y) = \frac{x+y}{2}$, dla $X = \mathbb{Q}$
- $h(x, y) = 2^{xy}$, dla $X = \mathbb{N}$
- $h(f, g) = f \circ g$, dla $X = \mathcal{F}(\mathbb{R}, \mathbb{R})$

Działaniem wewnętrznym **nie jest** np.

- $h(x, y) = x + y$, dla $X = \{a \in \mathbb{N} : 2 \mid a \vee 3 \mid a\}$

Działanie Zewnętrzne

Definicja

Dwuargumentowym **działaniem zewnętrznym** w niepustym zbiorze X nad niepustym zbiorem F nazywamy odwzorowanie $g : F \times X \to X$.

Definicja

Dwuargumentowym **działaniem zewnętrznym** w niepustym zbiorze X nad niepustym zbiorem F nazywamy odwzorowanie $g : F \times X \to X$.

Przykład

Działaniami zewnętrznymi są np.

- $g(\alpha, [x, y]) = [\alpha\dot{x}, \alpha\dot{y}]$, dla $F = \mathbb{R}, X = \mathbb{R}^2$
- $g(a, x) = nx$, dla $F = \mathbb{Z}, X = \mathbb{R}$
- $g(a, b) = ab$, dla $F = \mathbb{Z}, X = \{b \in \mathbb{Z} : 3 \mid b\}$

Działaniem zewnętrznym **nie jest** np.

- $g(a, b) = a + b$, dla $F = \mathbb{R}, X = \mathbb{Q}$

Konwencja

Zwyczajowo działania oznaczamy symbolami :

$+, \star, \cdot, \circ, \oplus, \otimes$

Natomiast wynik działania oznaczamy odpowiednio przez:

$x + y, x \star y, x \cdot y, x \circ y, x \oplus y, x \otimes y$

Definicja

Niepusty zbiór G z działaniem wewnętrznym $\oplus$ nazywamy **Półgrupą** jeżeli spełnione są następujące warunki

1. $\forall x, y, z \in G \quad (x \oplus y) \oplus z = x \oplus (y \oplus z)$ *(łączność)*
2. $\exists e \in G : \forall x \in G \quad x \oplus e = e \oplus x = x$ *(el. neutralny)*
3. $\forall x \in G \, \exists x' \in G \quad x \oplus x' = x' \oplus x = e$ *(el. odwrotne)*
4. $\forall x, y \in G \quad x \oplus y = y \oplus x$ *(przemienność)*

Definicja

Niepusty zbiór G z działaniem wewnętrznym $\oplus$ nazywamy **Monoidem** jeżeli spełnione są następujące warunki

1. $\forall x, y, z \in G \quad (x \oplus y) \oplus z = x \oplus (y \oplus z)$ *(łączność)*
2. $\exists e \in G : \forall x \in G \quad x \oplus e = e \oplus x = x$ *(el. neutralny)*
3. $\forall x \in G \, \exists x' \in G \quad x \oplus x' = x' \oplus x = e$ *(el. odwrotne)*
4. $\forall x, y \in G \quad x \oplus y = y \oplus x$ *(przemienność)*

Definicja

Niepusty zbiór G z działaniem wewnętrznym $\oplus$ nazywamy **Grupą** jeżeli spełnione są następujące warunki

1. $\forall x, y, z \in G \quad (x \oplus y) \oplus z = x \oplus (y \oplus z)$ *(łączność)*
2. $\exists e \in G : \forall x \in G \quad x \oplus e = e \oplus x = x$ *(el. neutralny)*
3. $\forall x \in G \, \exists x' \in G \quad x \oplus x' = x' \oplus x = e$ *(el. odwrotne)*
4. $\forall x, y \in G \quad x \oplus y = y \oplus x$ *(przemienność)*

Definicja

Niepusty zbiór G z działaniem wewnętrznym $\oplus$ nazywamy **Grupą abelową** jeżeli spełnione są następujące warunki

1. $\forall x, y, z \in G \quad (x \oplus y) \oplus z = x \oplus (y \oplus z)$ *(łączność)*
2. $\exists e \in G : \forall x \in G \quad x \oplus e = e \oplus x = x$ *(el. neutralny)*
3. $\forall x \in G \, \exists x' \in G \quad x \oplus x' = x' \oplus x = e$ *(el. odwrotne)*
4. $\forall x, y \in G \quad x \oplus y = y \oplus x$ *(przemienność)*

Definicja

Niepusty zbiór G z działaniem wewnętrznym $\oplus$ nazywamy **Grupą abelową** jeżeli spełnione są następujące warunki

1. $\forall x,y,z \in G \quad (x \oplus y) \oplus z = x \oplus (y \oplus z)$ *(łączność)*
2. $\exists e \in G : \forall x \in G \quad x \oplus e = e \oplus x = x$ *(el. neutralny)*
3. $\forall x \in G \, \exists x' \in G \quad x \oplus x' = x' \oplus x = e$ *(el. odwrotne)*
4. $\forall x,y \in G \quad x \oplus y = y \oplus x$ *(przemienność)*

Konwencja addytywna

Element neutralny grupy G oznaczamy często jako **0**. W szczególności jeśli mowa o "dodawaniu", oznaczanym przez $+, \oplus$ Elementy symetryczne nazywamy "przeciwnymi" i oznaczamy $-a$. Zapis $a - b$ należy rozumieć jako $a + (-b)$

Przykład

Półgrupą jest np.

- $(\mathbb{N} \setminus \{0\}, +)$

Monoidem jest np.

- $(\mathbb{Z}, \cdot)$

Grupą jest np.

- $(Bij(\mathbb{R}, \mathbb{R}), \circ)$ - Zbiór funkcji bijektywnych z $\mathbb{R}$ w $\mathbb{R}$ ze składaniem odwzorowań.

Grupą Abelową jest np.

- $(\mathbb{Z}, +)$

Przykład

Półgrupą jest np.

- $(\mathbb{N} \setminus \{0\}, +)$

Monoidem jest np.

- $(\mathbb{Z}, \cdot)$

Grupą jest np.

- $(Bij(\mathbb{R}, \mathbb{R}), \circ)$ - Zbiór funkcji bijektywnych z $\mathbb{R}$ w $\mathbb{R}$ ze składaniem odwzorowań.

Grupą Abelową jest np.

- $(\mathbb{Z}, +)$

Konwencja

Jeżeli działanie w grupie wynika z kontekstu, możemy je pomijać w zapisie i utożsamiać grupę ze zbiorem.

Podgrupa

Definicja

Niech $(G, +)$ będzie grupą. Niepusty podzbiór $H \subseteq G$ nazywamy podgrupą grupy G jeżeli zachodzi warunek

$$\forall x, y \in H \quad x - y \in H$$

Podgrupa

Definicja

Niech $(G, +)$ będzie grupą. Niepusty podzbiór $H \subseteq G$ nazywamy podgrupą grupy G jeżeli zachodzi warunek

$$\forall x, y \in H \quad x - y \in H$$

Przykład

Podgrupami $(\mathbb{Z}, +)$ są np.
$2\mathbb{Z} = \{a \in \mathbb{Z} : 2 \mid a\}, \quad \{\mathbf{0}\}$
Podgrupami $(\mathbb{R} \setminus \{0\}, \cdot)$ są np.
$\mathbb{Q} \setminus \{0\}, \quad \mathbb{R} \setminus \{0\}$

Podgrupa

Definicja

Niech $(G, +)$ będzie grupą. Niepusty podzbiór $H \subseteq G$ nazywamy podgrupą grupy G jeżeli zachodzi warunek

$$\forall x, y \in H \quad x - y \in H$$

Przykład

Podgrupami $(\mathbb{Z}, +)$ są np.
$2\mathbb{Z} = \{a \in \mathbb{Z} : 2 \mid a\}, \quad \{\mathbf{0}\}$
Podgrupami $(\mathbb{R} \setminus \{0\}, \cdot)$ są np.
$\mathbb{Q} \setminus \{0\}, \quad \mathbb{R} \setminus \{0\}$

Konwencja

oznaczenie $H < G$ należy rozumieć jako *"H jest pogrupą G"*.

Definicja

Homomorfizmem między grupą $(G, \oplus)$ oraz grupą $(H, \otimes)$ nazywamy dowolne odwzorowanie $h : G \to H$, spełniające warunek

$$\forall x, y \in G \quad h(x \oplus y) = h(x) \otimes h(y)$$

Homomorfizmy Grup

KOŁO NAUKOWE

Definicja

Homomorfizmem między grupą $(G, \oplus)$ oraz grupą $(H, \otimes)$ nazywamy dowolne odwzorowanie $h : G \to H$, spełniające warunek

$$\forall x, y \in G \quad h(x \oplus y) = h(x) \otimes h(y)$$

Przykład

Homomorfizmem grup $(\mathbb{Z}, +), (\mathbb{R}, \cdot)$ jest np.

- $h(x) = e^x$

Homomorfizmem grup $(\mathbb{Z}, +), (\mathbb{Z}, +)$ jest np.

- $h(x) = 2x$

Definicja

Zbiór R z dwoma działaniami $\oplus, \otimes$ nazywamy **Pierścieniem** , jeżeli zachodzą następujące warunki

1. $(R, \oplus)$ jest grupą abelową
2. $(R, \otimes)$ jest półgrupą
3. $\forall x, y, z \in R \quad x \otimes (y \oplus z) = x \otimes y \oplus x \otimes z \wedge$
   $(x \oplus y) \otimes z = x \otimes z \oplus y \otimes z$ *(rozdzielność mn. wzg. dod.)*

Definicja

Zbiór R z dwoma działaniami $\oplus, \otimes$ nazywamy **Pierścieniem z jedynką** , jeżeli zachodzą następujące warunki

1. $(R, \oplus)$ jest grupą abelową
2. $(R, \otimes)$ jest monoidem
3. $\forall x, y, z \in R \quad x \otimes (y \oplus z) = x \otimes y \oplus x \otimes z \wedge$
   $(x \oplus y) \otimes z = x \otimes z \oplus y \otimes z$ *(rozdzielność mn. wzg. dod.)*

Definicja

Zbiór R z dwoma działaniami $\oplus, \otimes$ nazywamy **Pierścieniem przemiennym z jedynką**, jeżeli zachodzą następujące warunki

1. $(R, \oplus)$ jest grupą abelową
2. $(R, \otimes)$ jest monoidem przemiennym
3. $\forall x, y, z \in R \quad x \otimes (y \oplus z) = x \otimes y \oplus x \otimes z \wedge$
   $(x \oplus y) \otimes z = x \otimes z \oplus y \otimes z$ *(rozdzielność mn. wzg. dod.)*

Przykład

Pierścieniem jest np.

- $(5\mathbb{Z}, +, \cdot)$

Pierścieniem z jedynką jest np.

- $(\mathcal{M}_2(\mathbb{R}), +, \cdot)$

Pierścieniami przemiennymi z jedynką są np.

- $(\mathbb{Z}, +, \cdot)$
- $(\mathbb{R}[x], +, \cdot)$
- $(\mathbb{Z}_n, +, \cdot)$
- $(\mathbb{R}[x_1, \ldots, x_n], +, \cdot)$

Obserwacja

Dla dowolnego pierścienia $(R, \oplus, \otimes)$ zachodzi:

$$\forall x \in R \quad x \otimes \mathbf{0} = \mathbf{0} \otimes x = \mathbf{0}$$

Obserwacja

Dla dowolnego pierścienia $(R, \oplus, \otimes)$ zachodzi:

$$\forall x \in R \quad x \otimes \mathbf{0} = \mathbf{0} \otimes x = \mathbf{0}$$

Dowód.

Przeprowadzimy dowód, że $x \otimes \mathbf{0} = 0$. Załóżmy nie wprost, że istnieje $x \in R$ takie, że $x \otimes \mathbf{0} = y, y \neq \mathbf{0}$. Możemy zapisać $y = x \otimes \mathbf{0} = x \otimes (\mathbf{0} \oplus \mathbf{0}) = x \otimes \mathbf{0} \oplus x \otimes \mathbf{0} = y \oplus y$. Dostaliśmy zatem $y = y \oplus y$ co po obustronnym dodaniu $-y$ prowadzi do $y = \mathbf{0}$ co jest sprzeczne z założeniem. Dowód faktu, że $\mathbf{0} \otimes x = \mathbf{0}$ można przeprowadzić analogicznie. □

Konwencja

Jeżeli $(R, \oplus, \otimes)$ jest pierścieniem, to zwyczajowo działanie $\oplus$ nazywamy dodawaniem, a $\otimes$ mnożeniem. Dodatkowo, jeżeli $(R, \otimes)$ jest monoidem, to jego element neutralny nazywamy "jedynką" i oznaczamy $\mathbf{1}$.

Podpierścienie

Definicja

Niepusty podzbiór S pierścienia $(R, \oplus, \ominus)$ nazywamy podpierścieniem R, jeżeli $(S, \oplus)$ jest podgrupą (addytywną) $(R, \oplus)$ oraz zbiór S jest zamknięty ze względu na mnożenie. Dodatkowo, jeżeli, R jest pierścieniem z jedynką dodaje się warunek $\mathbf{1} \in S$.

Przykład

Podpierścieniem pierścienia $\mathbb{R}$ są np.

- $\mathbb{Q}$
- $\mathbb{Z}$

Pierścienie z Dzielnikami Zera

KOŁO NAUKOWE

Definicja

Niech $(R, \oplus, \otimes)$ będzie pierścieniem. Wtedy $a, b \in R, a, b \neq 0$ są **dzielnikami zera** wtedy i tylko wtedy gdy $a \otimes b = 0$.

Definicja

Pierścień, w którym nie występują dzielniki zera, nazywamy **Pierścieniem całkowitym**.

Przykład

1. W pierścieniu $\mathbb{Z}_6$ elementy $2, 3$ są dzielnikami zera, ponieważ $2, 3 \neq \mathbf{0} \wedge 2 \cdot 3 = 6 = \mathbf{0}$.
2. Pierścień $\mathbb{Z}$ jest pierścieniem całkowitym.

Definicja

Niech $(R, +, \cdot)$ oraz $(S, \oplus, \otimes)$ będą dowolnymi pierścieniami. Homomorfizmem pierścieni R, S nazywamy dowolne odwzorowanie $h : R \to S$ takie, że:

$$\forall a, b \in R \quad h(a + b) = h(a) \oplus h(b)$$
$$\forall a, b \in R \quad h(a \cdot b) = h(a) \otimes h(b)$$

Definicja

Niech $(R, +, \cdot)$ oraz $(S, \oplus, \otimes)$ będą dowolnymi pierścieniami. Homomorfizmem pierścieni R, S nazywamy dowolne odwzorowanie $h : R \to S$ takie, że:

$$\forall a, b \in R \quad h(a + b) = h(a) \oplus h(b)$$
$$\forall a, b \in R \quad h(a \cdot b) = h(a) \otimes h(b)$$

Dodatkowo, jeśli, R,S są pierścieniami z jedynką, musi zachodzić

$$h(\mathbf{1}_R) = \mathbf{1}_S$$

Przykład

Homomorfizmem pierścieni $\mathbb{Z}, \mathbb{Z}[x]$ jest np.

- $h(a) = a$

Homomorfizmem pierścieni $\mathbb{Z}, \mathbb{Z}_n$ jest np.

- $h(a) = a \pmod{n}$

Definicja

Pierścień z jednością $(K, \oplus, \otimes)$ nazywamy ciałem, jeżeli $(K \setminus \{\mathbf{0}\}, \otimes)$ jest grupą abelową.

Przykład

Ciałami są np.

- $\mathbb{R}$
- $\mathbb{Q}$
- $\mathbb{C}$
- $\mathbb{Z}_p$, dla p będącego liczbą pierwszą

Konwencja

Elementy symetryczne w działaniu "mnożenia" nazywamy elementami odwrotnymi i oznaczamy a^{-1}

Obserwacja

Dowolne ciało $(K, \oplus, \otimes)$ jest pierścieniem całkowitym.

Obserwacja

Dowolne ciało $(K, \oplus, \otimes)$ jest pierścieniem całkowitym.

Dowód.

Załóżmy nie wprost, że istnieją $a, b \in K, a, b \neq \mathbf{0}$ takie, że $a \otimes b = \mathbf{0}$. z tego wynika, że $a^{-1} \otimes a \otimes b = a^{-1} \otimes \mathbf{0}$ z czego wynika $\mathbf{1} \otimes b = \mathbf{0}$ co jest równoważne z $b = \mathbf{0}$, co jest sprzecze z założeniem. □

Podciała

Definicja

Niech K będzie ciałem. Niepusty podzbiór L zbioru K nazywamy podciałem, gdy L jest podpierścieniem K oraz zachodzi

$$\forall a \in L \setminus \{\mathbf{0}\} \quad a^{-1} \in L$$

Przykład

Podciałem $\mathbb{C}$ są np.

- $\mathbb{R}$
- $\mathbb{Q}$
- $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$

Definicja

Niech $(R, +, \cdot)$ oraz $(S, \oplus, \otimes)$ będą dowolnymi ciałami. Homomorfizem ciał R i S nazywamy dowolne odwzorowanie $h : R \to S$ spełniające

$$\forall a, b \in R \quad h(a + b) = h(a) \oplus h(b)$$
$$\forall a, b \in R \quad h(a \cdot b) = h(a) \otimes h(b)$$

Definicja

Homomorfizm (grup, pierścieni, ciał) nazwiemy

- *monomorfizmem*, gdy jest iniektywny
- *epimorfizmem*, gdy jest surjektywny
- *izomorfizmem*, gdy jest bijektywny
- *endomorfizmem*, gdy dziedzina jest równa przeciwdziedzinie
- *automorifzmem*, gdy jest to endomorfizm bijektywny

Niech $f : X \to Y$ będzie dowolnym odwzorowaniem z X do Y.

Definicja

Obrazem zbioru $A \subseteq X$ przez odwzorowanie f nazywamy zbiór $\{y \in Y \mid \exists x \in A : f(x) = y\}$ i oznaczamy przez $f(A)$.

Definicja

Przeciwobrazem zbioru $B \subseteq Y$ przez odwzorowanie f nazywamy zbiór $\{x \in X \mid f(x) \in B\}$ i oznaczamy przez $f^{-1}(B)$.

Niech $f : X \to Y$ będzie dowolnym odwzorowaniem z X do Y.

Definicja

Obrazem odwzorowania f nazywamy zbiór $f(X)$ i oznaczamy przez Im_f.

W przypadku gdy przeciwdziedzina dziedziny tworzy strukturę z elementem neutralnym oznaczanym przez $\mathbf{0}$ definiujemy dodatkowo *jądro odwzorowania*

Definicja

Jądrem odwzorowania f nazywamy zbiór $f^{-1}(\mathbf{0})$ i oznaczamy przez Ker_f.

Przykład

Niech $f : \mathbb{Z} \to \mathbb{Z}_7$ będzie zadane wzorem $f(a) = a \pmod 7$. Wtedy

- $f(\{1, 9, 15\}) = \{1, 2\}$
- $f^{-1}(1) = \{7k + 1 \mid k \in \mathbb{Z}\}$
- $Im_f = f(\mathbb{Z}) = \mathbb{Z}_7$
- $Ker_f = f^{-1}(0) = \{7k \mid k \in \mathbb{Z}\}$

Niech A, B będą dowolnymi niepustymi zbiorami.

Definicja

Iloczynem Kartezjańskim A, B nazywamy zbiór $\{(a, b) \mid a \in A \wedge b \in B\}$ i oznaczamy przez $A \times B$.

Definicja

n-tą potęgą zbioru A rozumiemy jako $\underbrace{A \times A \times \ldots \times A}_{n} = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in A\}$ i oznaczamy przez A^n.

Niech $(G, +)$ będzie grupą oraz niech A, B będą dowolnymi niepustymi podzbiorami G.

Definicja

Sumą Algebraiczną zbiorów A, B nazywamy zbiór $\{a + b \mid a \in A \wedge b \in B\}$ i oznaczamy przez $A + B$.

Jeżeli zachodzi własność, że dla każdego $c \in A + B$ istnieje dokładnie jedna para a, b taka, że $a \in A, b \in B$ oraz $c = a + b$, to mówimy o **Sumie Prostej** zbiorów A, B. Zwyczajowo, sumę prostą zbiorów A, B oznaczamy przez $A \oplus B$.

Niech $(G, +)$ będzie grupą oraz niech A, B będą dowolnymi niepustymi podzbiorami G.

Definicja

Sumą Algebraiczną zbiorów A, B nazywamy zbiór $\{a + b \mid a \in A \wedge b \in B\}$ i oznaczamy przez $A + B$.

Jeżeli zachodzi własność, że dla każdego $c \in A + B$ istnieje dokładnie jedna para a, b taka, że $a \in A, b \in B$ oraz $c = a + b$, to mówimy o **Sumie Prostej** zbiorów A, B. Zwyczajowo, sumę prostą zbiorów A, B oznaczamy przez $A \oplus B$. Zauważmy, że istnieje naturalny izomorfizm $\phi : A \times B \to A \oplus B$ zadany przez $\phi(a, b) = a + b$. Z tego powodu, często w literaturze suma prosta (wewnętrzna) jest nierozróżnialna z iloczynem kartezjańskim.

Pytania, wątpliwości, uwagi ?