Algebra I

Wykład I

Grzegorz Bobiński (UMK)

Oznaczenie

Jeśli $X \subseteq \mathbb{R}$, to

$$X_+ := \{x \in X : x > 0\} \qquad \text{i} \qquad X_- := \{x \in X : x < 0\}.$$

1 Struktury algebraiczne i ich homomorfizmy

1.1 Działania w zbiorach i ich własności

Definicja

Działaniem w zbiorze X nazywamy każdą funkcję postaci $X \times X \to X$.

Przykłady

- Dodawanie liczb naturalnych, całkowitych, wymiernych, rzeczywistych, zespolonych.
- Odejmowanie liczb całkowitych, wymiernych, rzeczywistych, zespolonych.
- Mnożenie liczb naturalnych, całkowitych, wymiernych, rzeczywistych, zespolonych.
- Dzielenie niezerowych liczb wymiernych, rzeczywistych, zespolonych.
- Dodawanie macierzy ustalonego rozmiaru.
- Mnożenia macierzy kwadratowych ustalonego rozmiaru funkcji.
- Składanie funkcji o tej samej dziedzinie i przeciwdziedzinie.

Oznaczenia

Działania będziemy zwykle oznaczać symbolami takimi jak $*$, $+$ lub $\cdot$.

Jeśli $*$ jest działaniem w zbiorze X oraz $x, y \in X$, to

$$x * y := *(x, y).$$

Jeśli działanie oznaczamy symbolem $+$, to nazywamy je dodawaniem.

Jeśli działanie oznaczamy symbolem $\cdot$, to nazywamy je mnożeniem i piszemy często xy zamiast $x \cdot y$.

Definicja

Działanie $*$ w zbiorze X nazywamy łącznym, jeśli

$$\forall_{x,y,z \in X} \ (x * y) * z = x * (y * z).$$

Zbiór X wraz łącznym działaniem $*$ nazywamy półgrupą.

Uwaga

Jeśli $(X, *)$ jest półgrupą oraz $x_1, \ldots, x_n \in X$, to wynik działania

$$x_1 * \cdots * x_n$$

nie zależy od kolejności wykonywania działań.

Przykłady

- Działanie dodawania liczb rzeczywistych jest łączne.
- Działanie odejmowania liczb rzeczywistych nie jest łączne.
- Działanie mnożenia liczb rzeczywistych jest łączne.
- Działanie dzielenia niezerowych liczb rzeczywistych nie jest łączne.
- Działania dodawania i mnożenia macierzy są łączne.
- Działanie składania funkcji jest łączne.

Definicja

Działanie $*$ w zbiorze X nazywamy przemiennym, jeśli

$$\forall_{x,y \in X}\ x * y = y * x.$$

Półgrupę $(X, *)$ taką, że działanie $*$ jest przemienne, nazywamy półgrupą przemienną.

Uwaga

Jeśli $(X, *)$ jest półgrupą przemienną oraz $x_1, \ldots, x_n \in X$, to

$$x_1 * \cdots * x_n = x_{\sigma(1)} * \cdots * x_{\sigma(n)},$$

dla dowolnej permutacji σ zbioru $\{1, \ldots, n\}$.

Przykłady

- Działania dodawania i mnożenia liczb rzeczywistych są przemienne.
- Działanie odejmowania liczb rzeczywistych nie jest przemienne.
- Działanie dzielenia niezerowych liczb rzeczywistych nie jest przemienne.
- Działanie dodawania macierzy jest przemienne.
- Działanie mnożenia macierzy nie jest przemienne.
- Działanie składania funkcji nie jest przemienne.

Definicja

Niech $*$ będzie działaniem w zbiorze X.

Mówimy, że element $e \in X$ jest elementem neutralnym dla działania $*$, jeśli

$$\forall_{x \in X}\ x * e = x = e * x.$$

Półgrupę (przemienną), która posiada element neutralny, nazywamy monoidem (przemiennym).

Uwaga

Jeśli e_1 i e_2 są elementami neutralnymi dla działania $*$ w zbiorze X, to $e_1 = e_2$.

Dowód

Mamy

$$e_1 = e_1 * e_2 = e_2. \quad \square$$

Notacja

Jeśli działanie oznaczamy symbolem $+$ i posiada ono element neutralny, to oznaczamy go symbolem 0 i nazywamy zerem.

Jeśli działanie oznaczamy symbolem $\cdot$ i posiada ono element neutralny, to oznaczamy go symbolem 1 i nazywamy jedynką.

Przykłady

- $(\mathbb{N}, +)$ jest monoidem (przemiennym).
- $(\mathbb{N}_+, +)$ jest półgrupą (przemienną), która nie jest monoidem.

Definicja

Niech e będzie elementem neutralnym dla działania $*$ w zbiorze X.

Jeśli $x \in X$, to mówimy, że $y \in X$ jest elementem odwrotnym (względem działania $*$) do x, jeśli

$$x * y = e = y * x.$$

W powyższej sytuacji x nazywamy elementem odwracalnym (względem działania $*$).

Monoid, w którym każdy element jest odwracalny, nazywamy grupą.

Grupę, w której działanie jest przemienne, nazywamy grupą abelową.

Uwaga

Niech x będzie elementem monoidu $(X, *)$. Jeśli y_1 i y_2 są elementami odwrotnymi do x, to $y_1 = y_2$.

Dowód

Mamy

$$y_1 = y_1 * e = y_1 * (x * y_2) = y_1 * x * y_2 = (y_1 * x) * y_2 = e * y_2 = y_2. \quad \square$$

Notacja

Niech x będzie elementem zbioru X.

Jeśli $(X, +)$ jest monoidem, to element odwrotny (o ile istnieje) do x oznaczamy $-x$ i nazywamy go elementem przeciwnym.

Jeśli $(X, \cdot)$ jest monoidem, to element odwrotny (o ile istnieje) do x oznaczamy x^{-1}.

Przykłady (grup)

- $\mathbb{Z} := (\mathbb{Z}, +)$.
- $\mathbb{Q} := (\mathbb{Q}, +)$.
- $\mathbb{R} := (\mathbb{R}, +)$.
- $\mathbb{C} := (\mathbb{C}, +)$.
- $\mathbb{Q}^\times := (\mathbb{Q} \setminus \{0\}, \cdot)$.
- $\mathbb{R}^\times := (\mathbb{R} \setminus \{0\}, \cdot)$.
- $\mathbb{C}^\times := (\mathbb{C} \setminus \{0\}, \cdot)$.
- $\mathbb{T}_n := (\{z \in \mathbb{C} : z^n = 1\}, \cdot)$ $(n \in \mathbb{N}_+)$.
- $\mathbb{Z}_n := (\{0, \ldots, n-1\}, +_n)$ $(n \in \mathbb{N}_+)$.
- $\mathbb{Z}_n^\times := (\{k \in \{0, \ldots, n-1\} : \gcd(k, n) = 1\}, \cdot_n)$ $(n \in \mathbb{N}_+)$.
- $\mathbb{M}_{m,n}(\mathbb{Z}) := (\mathbb{M}_{m,n}(\mathbb{Z}), +)$ $(m, n \in \mathbb{N}_+)$.
- $\mathbb{M}_{m,n}(\mathbb{Q}) := (\mathbb{M}_{m,n}(\mathbb{Q}), +)$ $(m, n \in \mathbb{N}_+)$.
- $\mathbb{M}_{m,n}(\mathbb{R}) := (\mathbb{M}_{m,n}(\mathbb{R}), +)$ $(m, n \in \mathbb{N}_+)$.
- $\mathbb{M}_{m,n}(\mathbb{C}) := (\mathbb{M}_{m,n}(\mathbb{C}), +)$ $(m, n \in \mathbb{N}_+)$.
- $\mathrm{GL}_n(\mathbb{Q}) := (\{A \in \mathbb{M}_n(\mathbb{Q}) : \det A \neq 0\}, \cdot)$ $(n \in \mathbb{N}_+)$.
- $\mathrm{GL}_n(\mathbb{R}) := (\{A \in \mathbb{M}_n(\mathbb{R}) : \det A \neq 0\}, \cdot)$ $(n \in \mathbb{N}_+)$.
- $\mathrm{GL}_n(\mathbb{C}) := (\{A \in \mathbb{M}_n(\mathbb{C}) : \det A \neq 0\}, \cdot)$ $(n \in \mathbb{N}_+)$.
- $S_X := (\{\sigma : X \to X : \sigma \text{ jest bijekcją}\}, \circ)$ (X zbiór).
- $S_n := S_{\{1,\ldots,n\}}$ $(n \in \mathbb{N}_+)$, n-ta grupa symetryczna.

Terminologia

Działanie w abstrakcyjnej półgrupie/monoidzie/grupie będziemy zwykle domyślnie oznaczać symbolem $\cdot$.

Dlatego będziemy zwykle identyfikować półgrupę/monoid/grupę ze zbiorem, na którym jest zdefiniowana struktura półgrupy (monoidu, grupy).

Innymi słowy, będziemy pisać np. „Niech X będzie grupą" zamiast „Niech $(X, \cdot)$ będzie grupą".

Ponadto element neutralny będziemy zwykle oznaczać 1, a element odwrotny do elementu x przez x^{-1}.

Lemat 1.1

Niech G będzie grupą.

(1) $1^{-1} = 1$.

(2) Jeśli $g \in G$, to

$$(g^{-1})^{-1} = g.$$

Dowód

(1) Z definicji $a := 1^{-1}$ jest elementem takim, że

$$1 \cdot a = 1 = a \cdot 1.$$

Z definicji elementu neutralnego wiemy, że

$$1 \cdot 1 = 1 = 1 \cdot 1,$$

więc $1^{-1} = a = 1$.

(2) Z definicji $a := (g^{-1})^{-1}$ jest elementem takim, że

$$g^{-1} \cdot a = 1 = a \cdot g^{-1}.$$

Z definicji elementu g^{-1} wiemy, że

$$g^{-1} \cdot g = 1 = g \cdot g^{-1},$$

więc $(g^{-1})^{-1} = a = g$.

Lemat 1.1

Niech G będzie grupą.

(1) $1^{-1} = 1$.

(2) Jeśli $g \in G$, to
$$(g^{-1})^{-1} = g.$$

(3) Jeśli $g, h \in G$, to
$$(gh)^{-1} = h^{-1}g^{-1}.$$

(4) Przyporządkowanie
$$G \ni g \mapsto g^{-1} \in G$$
jest bijekcją.

Dowód (kont.)

(4) Niech $\Phi\colon G \to G$ będzie funkcją daną wzorem
$$\Phi(g) := g^{-1} \qquad (g \in G).$$
Z (2) wynika, że
$$\Phi \circ \Phi = \mathrm{Id}_G,$$
a więc Φ jest bijekcją ($\Phi^{-1} = \Phi$).

(3) Z definicji $a := (gh)^{-1}$ jest elementem takim, że
$$a \cdot gh = 1 = gh \cdot a.$$
Ale
$$h^{-1}g^{-1} \cdot gh = h^{-1} \cdot 1 \cdot h = 1.$$
Podobnie $gh \cdot h^{-1}g^{-1} = 1$, więc $(gh)^{-1} = a = h^{-1}g^{-1}$. □

Definicja

Niech x będzie elementem półgrupy X.

Jeśli $n \in \mathbb{N}_+$, to

$$x^n := \begin{cases} x & \text{jeśli } n = 1, \\ x^{n-1}x & \text{jeśli } n > 1. \end{cases}$$

Jeśli X jest monoidem, to

$$x^0 := 1.$$

Jeśli X jest grupą oraz $n \in \mathbb{Z}_-$, to

$$x^n := (x^{-1})^{-n}.$$

Notacja

Jeśli działanie oznaczamy symbolem $+$, to piszemy nx zamiast x^n.

Lemat 1.2

(1) Jeśli X jest monoidem/grupą i $n \in \mathbb{N}/n \in \mathbb{Z}$, to

$$1^n = 1.$$

(2) Jeśli X jest półgrupą/monoidem/grupą, $x \in X$ i $n, m \in \mathbb{N}_+/n, m \in \mathbb{N}/n, m \in \mathbb{Z}$, to

$$x^{n+m} = x^n x^m \qquad \text{oraz} \qquad (x^n)^m = x^{nm}.$$

Dowód

Ćwiczenie. □

Definicja

Niech X będzie zbiorem z działaniami $*$ i $\#$.
Mówimy, że działanie $*$ jest rozdzielne względem działania $\#$, jeśli

$$\forall_{x,y,z\in X}\ x*(y\#z) = (x*y)\#(x*z)$$

i

$$\forall_{x,y,z\in X}\ (x\#y)*z = (x*z)\#(y*z).$$

Definicja

Pierścieniem nazywamy zbiór R wraz z dwoma działaniami $+$ i $\cdot$ takimi, że:

(1) $(R,+)$ jest grupą abelową;

(2) $(R,\cdot)$ jest monoidem przemiennym;

(3) $\cdot$ jest rozdzielne względem $+$.

Jeśli dodatkowo

(4) $0 \neq 1$;

(5) $(R\setminus\{0\},\cdot)$ jest grupą (abelową),

to $(R,+,\cdot)$ nazywamy ciałem.

Uwaga

Działania w pierścieniu będziemy oznaczać symbolami $+$ i $\cdot$.
Jeśli R jest pierścieniem, to zakładamy, że $\cdot$ w R ma wyższy priorytet niż $+$, a więc np.

$$rs + t := (r\cdot s) + t.$$

Definicja

Jeśli R jest pierścieniem, to

(1) $(R, +)$ nazywamy grupą addytywną pierścienia R,

(2) $(R, \cdot)$ nazywamy monoidem multiplikatywnym pierścienia R.

Przykłady (pierścieni)

- $\mathbb{Z} := (\mathbb{Z}, +, \cdot)$.
- $\mathbb{Q} := (\mathbb{Q}, +, \cdot)$.
- $\mathbb{R} := (\mathbb{R}, +, \cdot)$.
- $\mathbb{C} := (\mathbb{C}, +, \cdot)$.
- $\mathbb{Z}_n := (\{0, 1, \ldots, n-1\}, +_n, \cdot_n)$ $(n \in \mathbb{N}_+)$.
- Pierścień $R[T]$ wielomianów o współczynnik w R (R pierścień).
- Pierścień $R[[T]]$ szeregów formalnych o współczynnikach w R (R pierścień).
- Pierścień R^X funkcji $X \to R$ (R pierścień).
  Przypomnijmy, że jeśli $f, g \colon X \to R$, to
  $$(f + g)(x) := f(x) + g(x) \qquad \text{i} \qquad (f \cdot g)(x) := f(x) \cdot g(x).$$
- Jeśli $R_1, \ldots, R_n$ są pierścieniami, to zbiór $R_1 \times \cdots \times R_n$ z dodawaniem i mnożeniem po współrzędnych jest pierścieniem.
  W szczególności, jeśli R jest pierścieniem oraz $n \in \mathbb{N}_+$, to zbiór $R^n := R \times \cdots \times R$ (n razy) z dodawaniem i mnożeniem po współrzędnych jest pierścieniem.
  Zauważmy, że $R^n = R^{[1,n]}$.

Przykłady (grup)

- $R := (R, +)$ (R pierścień).
- $R^\times := (\{r \in R : r \text{ jest odwracalny}\}, \cdot)$ (R pierścień).
- $\mathbb{M}_{m,n}(R) := (\mathbb{M}_{m,n}(R), +)$ ($m, n \in \mathbb{N}$, R pierścień).
- $\mathrm{GL}_n(F) := (\{A \in \mathbb{M}_n(F) : \det A \neq 0\}, \cdot)$ ($n \in \mathbb{N}$, F ciało).

  Ogólniej:

  $\mathrm{GL}_n(R) := (\{A \in \mathbb{M}_n(R) : \det A \in R^\times\}, \cdot)$ ($n \in \mathbb{N}$, R pierścień).

Lemat 1.3

Jeśli R jest pierścieniem, to

$$\forall_{r \in R}\ 0 \cdot r = 0 = r \cdot 0$$

oraz

$$\forall_{r,s \in R}\ (-r)s = -(rs) = r(-s).$$

Dowód

Mamy ciągi równości

$$0 \cdot r = 0 \cdot r + 0 \cdot r - 0 \cdot r = (0 + 0) \cdot r - 0 \cdot r = 0 \cdot r - 0 \cdot r = 0$$

oraz

$$(-r)s = (-r)s + rs - rs = (-r + r)s - rs = 0 \cdot s - rs = 0 - rs = -rs. \quad \square$$