Algebra wyższa

Elżbieta Adamus
Wydział Matematyki Stosowanej
Akademia Górniczo-Hutnicza w Krakowie

Kraków 2024

References

[1] Z. Furdzik, J. Maj-Kluskowa, A. Kulczycka, M. Sękowska, *Nowoczesna matematyka dla inżynierów. Część I - Algebra*, Wydawnictwo AGH, Kraków, 1993

[2] B. Gleichgewicht, *Algebra*, PWN, Warszawa, 1983, wydanie III zmienione

[3] T. Jurlewicz, Z. Skoczylas, *Algebra i geometria analityczna. Definicje, twierdzenia, wzory*, Oficyna Wydawnicza GiS, Wrocław, 2020, wydanie XXII

[4] T. Jurlewicz, Z. Skoczylas, *Algebra liniowa. Definicje, twierdzenia, wzory*, Oficyna Wydawnicza GiS, Wrocław, 2015, wydanie VIII poprawione

[5] A. I. Kostrikin, *Wstęp do algebry, tomy 1,2*, Wydawnictwo Naukowe PWN, 2004.

Elżbieta Adamus
Wydział Matematyki Stosowanej
Akademia Górniczo-Hutnicza w Krakowie

Algebra
Wykład nr 1
Data: .....

TEMAT: *Zbiory i relacje. Działania i wybrane struktury algebraiczne*

1.1 Notacja

Przyjmujemy następująca notację.

$\mathbb{N} = \{1, 2, 3, \ldots\}$	zbiór liczb naturalnych
$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$	
$\mathbb{Z}$	zbiór liczb całkowitych
$\mathbb{Q}$	zbiór liczb wymiernych
$\mathbb{R}$	zbiór liczb rzeczywistych

$\mathbb{C}$ - liczby zespolone

Oznaczenia kwantyfikatorów

$\forall$	kwantyfikator ogólny (duży)	*dla każdego*
$\exists$	kwantyfikator szczegółowy (mały)	*istnieje*
$\exists!$		*istnieje dokładnie jeden*

Symbol sumy i iloczynu

Niech $n \in \mathbb{N}$ oraz niech $a_1, a_2, \ldots, a_m, a_{m+1}, \ldots, a_n$ to dowolny ciąg liczb.

Sumę $a_1 + a_2 + \ldots + a_n$ oznaczamy symbolem $\sum_{i=1}^{n} a_i$. Symbol i to wskaźnik sumowania lub indeks sumowania, m to dolna granica sumowania, zaś n to górna granica sumowania.

Zauważmy że dla dowolnego $m \in \mathbb{N}$, $m < n$ oraz $c \in \mathbb{R}$ zachodzą równości
$a_1 + a_2 + \ldots + a_n = (a_1 + a_2 + \ldots + a_m) + (a_{m+1} + a_{m+2} + \ldots + a_n)$ oraz
$c(a_1 + a_2 + \ldots + a_n) = ca_1 + ca_2 + \ldots + ca_n$, czyli

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{m} a_i + \sum_{i=m+1}^{n} a_i, \qquad c\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} ca_i.$$

Przykład 1.1.1. $\sum_{i=1}^{6} i = 1 + 2 + 3 + 4 + 5 + 6 = 21$
$\sum_{i=5}^{9} \frac{i}{i+2} = \frac{5}{7} + \frac{6}{8} + \frac{7}{9} + \frac{8}{10} + \frac{9}{11}$
$\sum_{i=0}^{n} \left(\frac{1}{2}\right)^i = 1 + \frac{1}{2} + \frac{1}{4} + \ldots + \left(\frac{1}{2}\right)^n = \frac{1-\left(\frac{1}{2}\right)^{n+1}}{1-\frac{1}{2}}$

Iloczyn $a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1} \cdot a_n$ oznaczamy symbolem $\prod_{i=1}^{n} a_i$. Symbol i to wskaźnik iloczynu, m to dolny wskaźnik iloczynu, zaś n to górny wskaźnik iloczynu.

Przykład 1.1.2. $\prod_{i=0}^{6}(9-j) = 9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3$
$\prod_{i=1}^{n} i = 1\cdot 2\cdot 3\cdot \ldots \cdot (-1)\cdot n = n!$
$\underbrace{x\cdot x\cdot \ldots \cdot x}_{n\ razy} = \prod_{i=1}^{n} x$

1.2 Zbiory i relacje

Definicja 1.2.1. *Parą uporządkowaną* (a,b) nazywamy zbiór $\{\{a\},\{a,b\}\}$ podzbiorów zbioru $\{a,b\}$.

Twierdzenie 1.2.2. Dwie pary $(a,b),(c,d)$ są równe wtedy i tylko wtedy, gdy $a = c \wedge b = d$.

Możemy zdefiniować n-kę uporządkowaną:

$$(a_1,a_2,a_3) := ((a_1,a_2),a_3)$$
$$(a_1,a_2,a_3,a_4) := ((a_1,a_2,a_3),a_4)$$
$$\ldots$$
$$(a_1,a_2,\ldots,a_{n-1},a_n) := ((a_1,a_2,\ldots,a_{n-1}),a_n)$$

Można uzasadnić, że

$$(a_1,a_2,\ldots a_n) = (b_1,b_2,\ldots,b_n) \Leftrightarrow \forall i\in\{1,2,\ldots,n\}\ a_i = b_i.$$

Definicja 1.2.3. *Iloczynem kartezjańskim* zbiorów A i B nazywamy zbiór

$$A\times B := \{(a,b) :\ a\in A \wedge b\in B\}.$$

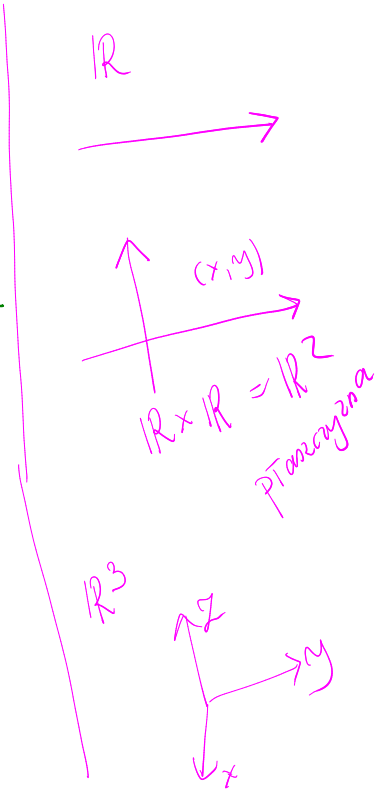
Analogicznie definiujemy
$A_1\times A_2\times\ldots\times A_n := \{(a_1,a_2,\ldots a_n) :\ a_1\in A_1 \wedge a_2\in A_2 \wedge\ldots\wedge a_n\in A_n\}$.
Oznaczamy $A^2 = A\times A$ oraz $A^n = \underbrace{A\times A\times\ldots\times A}_{n-razy}$.

Przykład 1.2.4. Wyznacz $A\times B$, $B\times A$, B^2.

i) $A=\{3,4,5\}$, $B=\{5,7\}$
$A\times B = \{(3,5),(3,7),(4,5),(4,7),(5,5),(5,7)\}$
$B\times A = \{(5,3),(5,4),(5,5),(7,3),(7,4),(7,5)\}$ $\quad A\times B \neq B\times A$
$B^2 = \{(5,5),(5,7),(7,5),(77)\}$

ii) przedziały $A=(0,1)\subset\mathbb{R}$, $B=(1,2)\subset\mathbb{R}$
$A\times B = \{(x,y) : 0<x<1 \wedge 1<y<2\}$
$B\times A = \{(x,y) : 1<x<2 \wedge 0<y<1\}$

iii) $A=B=\mathbb{R}$
$A\times B = B\times A = A^2 = B^2$
Oznaczamy $\mathbb{R}^2 = \mathbb{R}\times\mathbb{R} = \{(x,y) :\ x,y\in\mathbb{R}\}$ - płaszczyzna rzeczywista



Definicja 1.2.5. Niech A, B będą dowolnymi zbiorami. Każdy podzbiór $R \subseteq A \times B$ nazywamy *dwuargumentową relacją* w iloczynie kartezjańskim $A \times B$. Gdy $A = B$, to mówimy o dwuargumentowej relacji w zbiorze A.

Dla $(x, y) \in A \times B$ piszemy $xRy \Leftrightarrow (x, y) \in R$.

Przykład 1.2.6. i) Relacja równości $=$ w zbiorze $\mathbb{N}$

ii) Relacja $\leq$ w zbiorze $\mathbb{N}$ (lub $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$)

iii) Relacja inkluzji $\subseteq$ w zbiorze potęgowym $\mathcal{P}(A) = \{B : B \subseteq A\}$

iv) Relacja podzielności $|$ w zbiorze $\mathbb{N}$, tj. $m|n \Leftrightarrow \exists k \in \mathbb{N} \quad n = mk$

Definicja 1.2.7. Niech $R \subset A \times A$ będzie relacją w zbiorze A. Relację R nazywamy

i) *zwrotną*, jeżeli $\forall x \in A \quad xRx$,

ii) *przeciwzwrotną*, jeżeli $\forall x \in A \quad \sim (xRx)$,

iii) *symetryczną*, jeżeli $\forall x, y \in A \quad xRy \Rightarrow yRx$,

iv) *przeciwsymetryczną*, jeżeli $\forall x, y \in A \quad xRy \Rightarrow \sim (yRx)$,

v) *antysymetryczną*, jeżeli $\forall x, y \in A \quad (xRy \wedge yRx) \Rightarrow x = y$,

vi) *przechodnią*, jeżeli $\forall x, y, z \in A \quad (xRy \wedge yRz) \Rightarrow xRz$,

vii) *spójną*, jeżeli $\forall x, y \in A \quad xRy \vee yRx \vee x = y$.

Definicja 1.2.8. Niech A będzie zbiorem niepustym.

i) Relację $R \subset A \times A$ nazywamy *relacją równoważności* w zbiorze A, jesli jest ona zwrotna, symetryczna i przechodnia.

ii) Niech R będzie relacją równoważności w zbiorze A, zaś $x \in A$. Zbiór

$$[x]_R := \{y \in A : xRy\}$$

nazywamy *klasą równoważności* lub *klasą abstrakcji* relacji równoważności R wyznaczoną przez element x. Element x nazywamy *reprezentantem* klasy równoważności $[x]_R$.

iii) Niech R będzie relacją równoważności w zbiorze A. Zbiór

$$A/R := \{[x]_R : x \in A\}$$

nazywamy *zbiorem ilorazowym* zbioru A przez relację R.

Twierdzenie 1.2.9. Niech A będzie zbiorem niepustym, zaś R relacją równoważności w zbiorze A. Wówczas dla dowolnych $x, y \in A$

i) $x \in [x]_R$,

ii) $[x]_R = [y]_R \Leftrightarrow xRy$,

iii) $[x]_R \neq [y]_R \Rightarrow [x]_R \cap [y]_R = \varnothing$.

Dowód. iii) $[x]_R \cap [y]_R = \varnothing \Leftrightarrow \exists z \in [x]_R \cap [y]_R \Leftrightarrow \exists z : z \in [x]_R \wedge z \in [y]_R \Leftrightarrow zRx \wedge zRy \Leftrightarrow zRx \wedge yRz \Rightarrow xRy$. Na mocy ii) mamy, że $[x]_R = [y]_R$. $\square$

Uwaga 1.2.10. Określenie relacji równoważności w danym zbiorze A jest równoznaczne z dokonaniem podziału tego zbioru na niepuste i rozłączne zbiory, których suma mnogościowa równa jest temu zbiorowi. Taki podział nazywamy *rozbiciem* zbioru A.

$$A = \bigcup_{x \in A} [x]_R$$

Przykład 1.2.11. i) $A = \mathbb{Z}$, $n \in \mathbb{N}$ ustalone $\quad xRy \Leftrightarrow n|(x-y)$

$xRy \Leftrightarrow \exists k \in \mathbb{Z} : kn = x - y \Leftrightarrow \exists k \in \mathbb{Z} : y = x + kn$

Jest to relacja równoważności zwana *relacją przystawania modulo n*.

Piszemy $x \equiv y \ (mod\, n)$ lub $x \equiv_n y$.

$\mathbb{Z}/_{\equiv_n} = \{[0], [1], \ldots, [n-1]\}$ zbiór reszt modulo n

ii) $A = \mathbb{Z} \times \mathbb{Z}^*$, gdzie $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$, $\quad (x,y)R(u,v) \Leftrightarrow xv = yu$

$(x,y)R(x,y) \Leftrightarrow xy = yx$

$(x,y)R(u,v) \Leftrightarrow xv = yu \Leftrightarrow uy = vx \Leftrightarrow (u,v)R(x,y)$

przechodniość - ĆWICZENIE

Jest to relacja równoważności. Liczba wymierna $\frac{x}{y}$ to klasa abstrakcji.

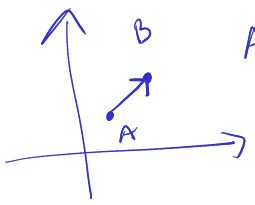
$[(x,y)]_R = \{(u,v) \in \mathbb{Z} \times \mathbb{Z}^* : (x,y)R(u,v)\} = \{(u,v) \in \mathbb{Z} \times \mathbb{Z}^* : xv = yu\} = \{(u,v) \in \mathbb{Z} \times \mathbb{Z}^* : \frac{x}{y} = \frac{u}{v}\}$

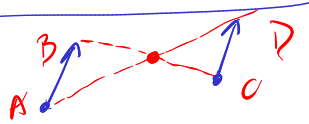
$\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^* /_R$

Działania $+, \cdot$ w $\mathbb{Q}$ nie zależą od wyboru reprezentanta.

iii) Wektory zaczepione i wektory swobodne płaszczyzny euklidesowej

Wektor swobodny to klasa abstrakcji wektorów zaczepionych.





Definicja 1.2.12. Niech A będzie zbiorem, zaś $R \subset A \times A$ relacją w A.

i) Relację R nazywamy *relacją częściowo porządkującą* lub *porządkiem częściowym* w zbiorze A, jeżeli jest ona zwrotna, antysymetryczna i przechodnia. Mówimy wówczas, że zbiór A jest *częściowo uporządkowany*.

ii) Relację R nazywamy *porządkiem liniowym* w zbiorze A, jeśli jest ona porządkiem częściowym i jest spójna. Mówimy wówczas, że zbiór A jest *liniowo uporządkowany*.

Dwa elementy $x, y \in A$ nazywamy *porównywalnymi* jeśli xRy lub yRx. Jeśli zbiór jest liniowo uporządkowany, to każde dwa elementy tego zbioru są porównywalne.

Oznaczamy symbolem $\leq$ ustalony porządek częściowy.
Wówczas piszemy $x < y$, gdy $x \leq y$ oraz $x \neq y$.
Relacja $<$ jest przeciwzwrotna, asymetryczna i przechodnia. Nazywamy ją *silnym porządkiem częściowym*.

Przykład 1.2.13. i) $\mathcal{P}(A) = \{B : B \subseteq A\}$ z relacją inkluzji $\subseteq$

$A \subseteq A$ zwrotna
$A \subseteq B \ \wedge \ B \subseteq A \ \Leftrightarrow \ A = B$ antysymetria
$A \subseteq B \ \wedge \ B \subseteq C \ \Leftrightarrow \ A \subseteq C$ przechodnia

Jest to porządek częściowy, który nie jest porządkiem liniowym.

Jeśli $A \cap B = \varnothing$, to ani $A = B$, ani $A \subseteq B$, ani $B \subseteq A$.

ii) $(\mathbb{R}, \leq)$ zbiór liniowo uporządkowany

$\forall x, y \in \mathbb{R} \quad x \leq y \ \vee \ y \leq x \ \vee x = y$
Wszystkie liczby rzeczywiste są porównywalne.

1.3 Działania wewnętrzne i ich własności

Niech A będzie zbiorem niepustym.

Definicja 1.3.1. Dowolną funkcję $h : A \times A \to A$ nazywamy *działaniem wewnętrznym* w zbiorze A. Wartość funkcji $h(a, b) \in A$ nazywamy *wynikiem* działania dla pary argumentów $a, b \in A$.

Przykład 1.3.2. i) Dodawanie jest działaniem wewnętrznym w $\mathbb{N}$.

ii) Odejmowanie nie jest działaniem wewnętrznym w $\mathbb{N}$.

iii) Dodawanie nie jest działaniem wewnętrznym w $\mathbb{R} \setminus \mathbb{Q}$.

Własności działań wewnętrznych

Definicja 1.3.3. Niech $* : A \times A \to A$ będzie działaniem wewnętrznym.

i) Działanie $*$ nazywamy *przemiennym*, jeśli $\forall\, a, b \in A \quad a * b = b * a$.

ii) Działanie $*$ nazywamy *łącznym*, jeśli $\forall\, a, b, c \in A \quad (a * b) * c = a * (b * c)$.

iii) Element $e \in A$ nazywamy *elementem neutralnym* działania $*$, jeśli $\forall\, a \in A \quad a * e = e * a = a$.

Przykład 1.3.4. i) Dodawanie jest działaniem wewnętrznym łącznym i przemiennym w $\mathbb{R}$. 0 jest elementem neutralnym.

ii) Mnożenie jest działaniem wewnętrznym łącznym i przemiennym w $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. 1 jest elementem neutralnym.

Twierdzenie 1.3.5. Jeżeli element neutralny istnieje to jest jedyny.

Dowód. Przypuśćmy, że istnieją $e_1, e_2 \in A$ będące elementami neutralnymi w A. Wówczas $e_2 = e_1 * e_2 = e_1$. □

Przykład 1.3.6. Niech X to dowolny zbiór.

i) Zbiór pusty $\varnothing$ jest elementem neutralnym w $\big(P(X), \cup\big)$.

ii) Zbiór X jest elementem neutralnym w $\big(P(X), \cap\big)$.

Definicja 1.3.7. Niech $* : A \times A \to A$ będzie działaniem wewnętrznym, posiadającym element neutralny $e \in A$. Dla dowolnego $a \in A$ każdy element $a' \in A$ taki, że $a * a' = a' * a = e$, nazywamy *elementem symetrycznym* do a względem działania $*$.

Przykład 1.3.8. i) W $(\mathbb{R}, +)$ elementem symetrycznym do 5 jest -5 (tzw. element przeciwny).

ii) W $(\mathbb{R}^*, \cdot)$ elementem symetrycznym do 5 jest $\frac{1}{5}$ (tzw. element odwrotny).

iii) W $(\mathbb{R}, \circ)$, gdzie $x \circ y = x + y + 1$, elementem neutralnym jest -1, zaś elementem symetrycznym do x jest $-2 - x$.

Twierdzenie 1.3.9. Jeżeli działanie wewnętrzne jest łączne oraz posiada element neutralny, to każdy element posiada co najwyżej jeden element symetryczny.

Dowód. Rozważmy zbiór A z działaniem łącznym $\circ$. Niech e będzie elementem neutralnym działania $\circ$. Niech a', a'' to dwa elementy symetryczne do $a \in A$. Wówczas

$$\begin{aligned} a \circ a' = e \;\Rightarrow\; a'' \circ (a \circ a') &= a'' \circ e \\ (a'' \circ a) \circ a' &= a'' \\ e \circ a' &= a'' \\ a' &= a'' \end{aligned}$$

□

1.4 Podstawowe struktury algebraiczne

Niech G będzie zbiorem niepustym, zaś $* : G \times G \to G$ działaniem wewnętrznym w G.

Definicja 1.4.1. i) Parę $(G, *)$ nazywamy *półgrupą*, jeżeli działanie jest łączne.

ii) Parę $(G, *)$ nazywamy *monoidem*, jeżeli działanie jest łączne i posiada element neutralny.

iii) Parę $(G, *)$ nazywamy *grupą*, jeżeli działanie jest łączne, posiada element neutralny oraz każdy element G posiada element symetryczny względem $*$ w G.

Jeśli dodatkowo działanie $*$ jest przemienne, to mówimy o *półgrupie przemiennej, monoidzie przemiennym, grupie przemiennej (abelowej).*

Przykład 1.4.2. Oznaczmy $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

	$(\mathbb{N}, +)$	$(\mathbb{Z}, \cdot)$	$(\mathbb{Q}, +)$	$(\mathbb{Q}, \cdot)$	$(\mathbb{R}^*, +)$	$(\mathbb{R}^*, \cdot)$
wewnętrzność	✓	✓	✓	✓	nie $-1+1=0$ $0 \notin \mathbb{R}^*$	✓
łączność	✓	✓	✓	✓		✓
przemienność	✓	✓	✓	✓		✓
el. neutralny	brak $0 \notin \mathbb{N}$	✓ $1 \in \mathbb{Z}$	✓ $0 \in \mathbb{Q}$	✓ $1 \in \mathbb{Q}$		✓ $1 \in \mathbb{R}^*$
el. symetryczny		brak $2 \cdot b = 1$ $b = \frac{1}{2} \notin \mathbb{Z}$	✓ $a + a' = 0$ $a' = -a \in \mathbb{Q}$	brak $a \cdot a' = 1$ $a' = \frac{1}{a}$ nie dla $a = 0$		✓ $a \cdot a' = 1$ $a' = \frac{1}{a}$ $\forall a \in \mathbb{R}^*$
	półgrupa przemienna bez el. neutr.	monoid przemienny	grupa abelowa	monoid przemienny		grupa abelowa

Przykład 1.4.3. Niech $X = \{1, 2, 4, \ldots, 2^n, \ldots\}$, $n \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$, zaś działanie $\circ$ to mnożenie liczb. Czy $(X, \circ)$ jest półgrupą/grupą (abelową)?

Jeśli $a, b, c \in X$, to istnieją $k, m, n \in \mathbb{N}_0$ takie, ze $a = 2^n, b = 2^m, c = 2^k$.