

WSTĘP DO ALGEBRY

NOTATKI

„Studenci mogą się z tym nigdy więcej nie spotkać, więc warto to zrobić.”

MACIEJ MIKOŁAJCZAK
Kraków, 2025

Spis treści

1. Struktury algebraiczne	2
---------------------------	---

1. Struktury algebraiczne

Definicja 1. Działaniem wewnętrznym w zbiorze A nazywamy dowolne odwzorowanie $h : A \times A \rightarrow A$. Zbiór A nazywamy grupoidem lub magmą.

Propozycja 1. Dla każdego działania istnieje co najwyżej jeden element neutralny, a dla każdego łącznego działania istnieje co najwyżej jeden element odwrotny.

Dowód. Jeśli e_1, e_2 to elementy neutralne, to $e_1 = e_1 e_2 = e_2$.

Jeśli a', a'' są elementami odwrotnymi a , to $a' = a' e = a' a a'' = a''$. $\square$

Definicja 2. Działaniem zewnętrznym w zbiorze A nazywamy dowolne odwzorowanie $g : F \times A \rightarrow A$, gdzie elementy F nazywamy operatorami.

Definicja 3. Działanie zewnętrzne $\cdot : F \times A \rightarrow A$ jest rozdzielne względem działania wewnętrznego $\circ : A \times A \rightarrow A$, jeśli

$$\forall a, b \in A \quad \forall p \in F \quad p \cdot (a \circ b) = (p \cdot a) \circ (p \cdot b).$$

Definicja 4. Działanie zewnętrzne $\cdot : F \times A \rightarrow A$ jest łączne względem łącznego działania wewnętrznego $\circ : F \times F \rightarrow F$, jeśli

$$\forall a \in A \quad \forall p, q \in F \quad (p \circ q) \cdot a = p \cdot (q \cdot a).$$

Definicja 5. Działania zewnętrzne $\cdot : F_1 \times A \rightarrow A$ i $\circ : F_2 \times A \rightarrow A$ są przemienne, jeśli

$$\forall a \in A \quad \forall p \in F_1, q \in F_2 \quad p \cdot (q \circ a) = q \circ (p \cdot a).$$

Definicja 6. Strukturą algebraiczną na zbiorze A nazywamy układ

$$(A, F_1, \dots, F_m, h_1, \dots, h_n, g_1, \dots, g_m),$$

gdzie $h_i : A \times A \rightarrow A$ to działania wewnętrzne, a $g_j : F_j \times A \rightarrow A$ to działania zewnętrzne.

Definicja 7. Mając zadane struktury algebraiczne

$$(A, F_1, \dots, F_m, h_1, \dots, h_n, g_1, \dots, g_m), (A', F_1, \dots, F_m, h'_1, \dots, h'_n, g'_1, \dots, g'_m)$$

o takiej samej liczbie działań i tych samych zbiorach operatorów mówimy, że odwzorowanie $\Phi : A \rightarrow A'$ jest homomorfizmem, jeśli

$$h'_i(\Phi(a), \Phi(b)) = \Phi(h_i(a, b)),$$

$$g'_j(p, \Phi(a)) = \Phi(g_j(p, a)).$$

Definicja 8. Dla homomorfizmu $\Phi : A \rightarrow B$ definiujemy jego obraz $\text{Im}(\Phi) = \Phi(A)$ jako strukturę algebraiczną z działaniami indukowanymi z B .

Propozycja 2. Obraz homomorfizmu $\Phi : A \rightarrow B$ jest zamknięty na wszystkie działania struktury B .

Dowód. Jeśli $\circ$ jest działaniem wewnętrznym w B odpowiadającym $\cdot$ w A , to mamy $\Phi(a) \circ \Phi(b) = \Phi(a \cdot b)$, a więc wynik należy do $\text{Im}(\Phi)$. Podobnie dla działań zewnętrznych. $\square$

Propozycja 3. Jeśli $\Phi : A \rightarrow B$ jest homomorfizmem a $C \subseteq B$ podzbiorem zamkniętym na działania, to $\Phi^{-1}(C)$ jest podzbiorem A zamkniętym na działania.

Dowód. Jeśli $\circ$ jest działaniem wewnętrznym w B odpowiadającym $\cdot$ w A , to dla $a = \Phi(c), b = \Phi(c')$ mamy $\Phi(a \cdot b) = c \circ c' \in C$, a więc $a \cdot b \in \Phi^{-1}(C)$. Podobnie dla działań zewnętrznych. $\square$

Definicja 9. Niech $\{A_i\}_{i \in I}$ będą strukturami algebraicznymi o tych samych operatorach i liczbie działań. Produktem $\prod_{i \in I} A_i$ nazywamy strukturę o tych samych operatorach i liczbie działań wraz z epimorfizmami $\pi_j : \prod_{i \in I} A_i \rightarrow A_j$ takimi, że dla dowolnej struktury B i homomorfizmów $g_i : B \rightarrow A_i$ istnieje jedyny homomorfizm $\Psi : B \rightarrow \prod_{i \in I} A_i$ taki, że $\pi_i \circ \Psi = g_i$.

Definicja 10. Niech $\{A_i\}_{i \in I}$ będą strukturami algebraicznymi o tych samych operatorach i liczbie działań. Koproduktem $\coprod_{i \in I} A_i$ nazywamy strukturę o tych samych operatorach i liczbie działań wraz z monomorfizmami $p_j : A_j \rightarrow \coprod_{i \in I} A_i$ takimi, że dla dowolnej struktury B i homomorfizmów $g_i : A_i \rightarrow B$ istnieje jedyny homomorfizm $\Psi : \coprod_{i \in I} A_i \rightarrow B$ taki, że $\Psi \circ p_i = g_i$.

Uwaga. Produkt i koprodukt to uogólnienia odpowiednio iloczynu kartezjańskiego i sumy rozłącznej.

Propozycja 4. Dla struktur algebraicznych A, B i homomorfizmu $\Phi : A \rightarrow B$ oraz relacji równoważności R na B relacja Φ^*R zadana przez

$$x(\Phi^*R)y \iff \Phi(x)R\Phi(y)$$

jest relacją równoważności. Możemy zapisać skrótowo $\Phi^*R = (\Phi \times \Phi)^{-1}(R)$ – przeciwobraz par w relacji R .

Definicja 11. Jądrem odwzorowania $\Phi : A \rightarrow B$ nazywamy relację

$$\ker(\Phi) = \{(x, y) \in A \times A : \Phi(x) = \Phi(y)\},$$

która jest relacją równoważności.

Uwaga. Odwzorowanie

$$A/\ker(\Phi) \ni [x] \rightarrow \Phi(x) \in B$$

jest iniekcją, czyli bijekcją na obraz $\Phi(A)$.

Twierdzenie 1 (Pierwsze twierdzenie o izomorfizmie). Dla dowolnego homomorfizmu $\Phi : A \rightarrow B$ relacja $\ker(\Phi)$ jest zgodna z działaniami oraz $\text{Im}(\Phi) \cong A/\ker(\Phi)$.

Definicja 12. Zbiór uporządkowany $(I, \leq)$ nazywamy skierowanym, jeśli dla każdych $i, j \in I$ istnieje $k \in I$ takie, że $i \leq k, j \leq k$.

Definicja 13. Niech $(I, \leq)$ będzie zbiorem skierowanym. Rozważmy struktury algebraiczne $\{A_i\}_{i \in I}$, które mają równe liczby działań i te same zbiory operatorów wraz z homomorfizmami $f_{ij} : A_i \rightarrow A_j$ spełniającymi dla wszystkich $i \leq j$ następujące warunki:

- f_{ii} jest identycznością na A_i .
- $f_{ik} = f_{jk} \circ f_{ij}$ dla wszystkich $i \leq j \leq k$.

Para (A_i, f_{ij}) nazywana jest systemem prostym na I .

Definicja 14. Niech $(I, \leq)$ będzie zbiorem skierowanym. Rozważmy struktury algebraiczne $\{A_i\}_{i \in I}$, które mają równe liczby działań i te same zbiory operatorów wraz z homomorfizmami $f_{ij} : A_j \rightarrow A_i$ spełniającymi dla wszystkich $i \leq j$ następujące warunki:

- f_{ii} jest identycznością na A_i .
- $f_{ik} = f_{ij} \circ f_{jk}$ dla wszystkich $i \leq j \leq k$.

Para (A_i, f_{ij}) nazywana jest systemem odwrotnym na I .

Definicja 15. Granicą prostą $\varinjlim A_i$ systemu prostego (A_i, f_{ij}) nad I nazywamy strukturę o tej samej liczbie działań i tym samym zbiorze operatorów wraz z homomorfizmami $\phi_i : A_i \rightarrow \varinjlim A_i$

takimi, że $\phi_i = \phi_j \circ f_{ij}$ dla $i \leq j$ oraz spełniającą następujący warunek uniwersalny: dla dowolnej struktury B i homomorfizmów $\psi_i : A_i \rightarrow B$ takich, że $\psi_i = \psi_j \circ f_{ij}$ istnieje jedyny homomorfizm $\Psi : \varinjlim A_i \rightarrow B$ taki, że $\Psi \circ \phi_i = \psi_i$ dla każdego $i \in I$.

Definicja 16. Granicą odwrotną $\varprojlim A_i$ systemu odwrotnego (A_i, f_{ij}) nad I nazywamy strukturę o tej samej liczbie działań i tym samym zbiorze operatorów wraz z homomorfizmami $\phi_i : \varprojlim A_i \rightarrow A_i$ takimi, że $\phi_i = f_{ij} \circ \phi_j$ dla $i \leq j$ oraz spełniającą następujący warunek uniwersalny: dla dowolnej struktury B i homomorfizmów $\psi_i : B \rightarrow A_i$ takich, że $\psi_i = f_{ij} \circ \psi_j$ istnieje jedyny homomorfizm $\Psi : B \rightarrow \varprojlim A_i$ taki, że $\phi_i \circ \Psi = \psi_i$ dla każdego $i \in I$.

Definicja 17. Pierścień przemienny z jedyneką i bez dzielników zera nazywamy całkowitym.

Pierścień z jedyneką, w którym każdy element różny od zera jest odwracalny nazywamy pierścieniem z dzieleniem.

Ciałem nazywamy pierścień przemienny z dzieleniem.

Twierdzenie 2 (Wedderburn). Dowolny skończony pierścień z dzieleniem jest ciałem.

Propozycja 5. Pierścień skończony bez dzielników zera R jest pierścieniem z dzieleniem. Zatem skończony pierścień całkowity jest ciałem.

Dowód. Dla ustalonego $a \in R^*$ można zdefiniować odwzorowanie $R^* \ni b \rightarrow ab \in R^*$, które jest iniekcją (bo inaczej $a(b_1 - b_2) = 0$), a więc również surjekcją, bo prowadzi ze skończonego zbioru w siebie. Zatem istnieje takie $b \in R^*$, że $ab = e$. Podobnie istnieje $b' \in R^*$ takie, że $b'a = e$. Wtedy $b = eb = b'ab = b'e = b'$. Zatem znaleźliśmy element odwrotny. $\square$

Uwaga. W pierścieniu całkowitym możemy rozważać relację równoważności $(n, d) \sim (m, b) \iff nb = md$, gdzie b, d są niezerowe. Klasy takiej relacji tworzą ciało ułamków nad tym pierścieniem.

Definicja 18. Lewy moduł nad pierścieniem z jedyneką R (lewy R -moduł) to układ $(M, R, +, \cdot)$ złożony z grupy abelowej $(M, +)$ oraz działania zewnętrznego $\cdot : R \times M \rightarrow M$ spełniającego następujące warunki:

- $r \cdot (u + v) = ru + rv$ dla $r \in R, u, v \in M$.
- $(r + s) \cdot v = rv + sv$ dla $r, s \in R, v \in M$.
- $(rs) \cdot v = r(sv)$ dla $r, s \in R, v \in M$.
- $1 \cdot v = v$ dla $v \in M$.

Jeśli przedostatni warunek zastąpimy $(sr) \cdot v = r(sv)$, to otrzymamy prawy R -moduł. Jednocześnie lewy i prawy R -moduł to po prostu R -moduł.

Definicja 19. R -algebrą nad pierścieniem przemiennym R nazywamy R -moduł A z dodatkowym dwuliniowym działaniem $A \times A \ni (x, y) \rightarrow xy \in A$.

Uwaga. Zależnie od własności dodatkowego działania R -algebry mówimy o algebrze łącznej, przemiennej, z dzieleniem i tak dalej.

Definicja 20. Algebrę nazywamy alternatywną, jeśli dla dowolnych a, b zachodzi $a(ab) = (aa)b$ oraz $(ba)a = b(aa)$ (osłabiona łączność).

Algebra jest potęgowo łączna, jeśli potęga $\underbrace{a \cdot a \cdot \dots \cdot a}_{k \text{ razy}}$ jest poprawnie określona (nie zależy od nawiasowania).

Twierdzenie 3 (Artin, Zorn). Dowolna skończona algebra alternatywna jest ciałem.

Twierdzenie 4 (Artin). Każda algebra alternatywna jest potęgowo łączna. Ponadto dowolny iloczyn zawierający dwa elementy nie zależy od ustawienia nawiasów.

Definicja 21. Kwarternionami nazywamy liczby postaci $a + bi + cj + dk$, gdzie $a, b, c, d \in \mathbb{R}$ a i, j, k to jednostki urojone. Mamy $i^2 = j^2 = k^2 = -1$ oraz $ik = -j$, $ki = j$, $ji = -k$, $ij = k$, $kj = -i$, $jk = i$. Do tego mamy rozdzielność dodawania względem mnożenia. Kwarterniony powstają z liczb zespolonych analogicznie jak one powstają z rzeczywistych.