

Działania wewnętrzne i zewnętrzne

Niech X będzie ustalonym niepustym zbiorem.

Def. Dwuargumentowym **działaniem wewnętrznym** w zbiorze X nazywamy funkcję $h: X \times X \rightarrow X$.

Jeśli $x \in X$ i $y \in X$, to $h(x, y) \in X$ nazywamy wynikiem działania h na argumentach x i y .

Wygodniejszy jest zapis działania $x * y$ zamiast $h(x, y)$.

Przykłady

1. dodawanie (+) i mnożenie ($\cdot$) są działaniami wewnętrznymi w zbiorach N, Z, W, R
2. odejmowanie nie jest działaniem wewnętrznym w N
3. działanie $m \otimes n = m^n$ jest działaniem wewnętrznym w N
4. zbiór obrotów kwadratu wokół jego środka przekształcających go na siebie. Oznaczmy O_k obrót o kąt $k \frac{\pi}{2}$. Wobec tego $X = \{O_0, O_1, O_2, O_3\}$. Jako działanie wewnętrzne rozpatrzmy składanie ($\circ$) obrotów. Możemy ułożyć następującą tabelkę działania

$\circ$	O_0	O_1	O_2	O_3
O_0	O_0	O_1	O_2	O_3
O_1	O_1	O_2	O_3	O_0
O_2	O_2	O_3	O_0	O_1
O_3	O_3	O_0	O_1	O_2

5. Działania $a \oplus b = \frac{a+b}{2}$, $a * b = a + b + 1$, $a \bullet b = a - b + ab$ są wewnętrznymi w R

Niech A i F będą dwoma ustalonymi niepustymi zbiorami.

Def. Dwuargumentowym **działaniem zewnętrznym** w zbiorze X nad zbiorem F nazywamy funkcję $g: F \times X \rightarrow X$.

Przykład. Niech X będzie zbiorem wektorów na płaszczyźnie a $F=R$. Działaniem zewnętrznym w zbiorze wektorów X nad zbiorem R jest mnożenie wektora przez liczbę rzeczywistą.

Uwaga. Ponieważ zbiory X i F nie muszą być różne, to działanie wewnętrzne jest szczególnym przypadkiem działania zewnętrznego.

Wybrane własności działania wewnętrznego

Niech $*$ będzie działaniem wewnętrznym w zbiorze X .

Def. Element $e \in X$ nazywamy elementem neutralnym działania $*$ gdy, $\forall x \in X \quad x * e = e * x = x$.

Tw. Jeżeli działanie wewnętrzne posiada element neutralny, to jest on jedyny.

Dow.(niewprost) Przypuśćmy, że działanie $*$ posiada dwa różne elementy neutralne $e_1 \neq e_2$.

$$e_1 = e_1 * e_2 = e_2 \text{ (sprzeczność)}$$

Pierwsza równość jest konsekwencją faktu, że e_2 jest elementem neutralnym a druga konsekwencją faktu, że e_1 jest elementem neutralnym.

Def. Działanie $*$ nazywamy przemennym, gdy $\forall x, y \in X \quad x*y = y*x$.

Def. Działanie $*$ nazywamy łącznym, gdy $\forall x, y, z \in X \quad (x*y)*z = x*(y*z)$

Element symetryczny (odwrotny, przeciwny)

Niech $*$ będzie działaniem wewnętrznym w zbiorze X posiadającym element neutralny e .

Def. Element $\tilde{x} \in X$ nazywamy elementem symetrycznym (odwrotnym , przeciwnym) do elementu $x \in X$, gdy $x * \tilde{x} = \tilde{x} * x = e$.

Tw. Jeżeli działanie łączne posiada element neutralny, to element symetryczny do danego elementu, (o ile istnieje) jest wyznaczony jednoznacznie.

Dow. (niewprost) Niech y_1 i y_2 będą elementami symetrycznymi do danego elementu x . Wówczas

$$y_1 = y_1 * e = y_1 * (x * y_2) = (y_1 * x) * y_2 = e * y_2 = y_2.$$

Podstawowe struktury algebraiczne

Grupa

Def. Niech $X \neq \emptyset$ będzie niepustym zbiorem a $*$ działaniem w zbiorze X . Parę $(X, *)$ nazywamy grupą jeżeli

1. $\forall x, y \in X \quad x*y \in X$ (działanie $*$ jest wewnętrzne)
2. $\forall x, y, z \in X \quad (x*y)*z = x*(y*z)$ (działanie $*$ jest łączne)
3. $\exists e \in X \quad \forall x \in X \quad x*e = e*x = x$ (istnieje element neutralny działania $*$ (jest on jedyny!))
4. $\forall x \in X \quad \exists \tilde{x} \in X \quad x * \tilde{x} = \tilde{x} * x = e$ (dla każdego elementu istnieje element symetryczny)

Jeżeli dodatkowo jest spełniony warunek

5. $\forall x, y \in X \quad x*y = y*x$. (przemienność działania $*$)

to grupę $(X, *)$ nazywamy grupą przemenną albo abelową¹.

Grupę o skończonej liczbie elementów nazywamy grupą skończoną. Jeżeli X jest grupą skończoną mającą n elementów, to mówimy, że rząd grupy X jest równy n , co zapisujemy $|X|=n$. Jeżeli grupa jest nieskończona, to piszemy $|X|=\infty$.

¹ Niels Abel (1802-1829) matematyk norweski

W grupie $(X, *)$ potrafimy rozwiązać równanie

$$a*x=b \quad (\text{rozwiązaniem jest } x = \tilde{a} * b)$$

oraz równanie

$$x*a=b \quad (\text{rozwiązaniem jest } x = b * \tilde{a})$$

Addytywny i multiplikatywny zapis działania

- Jeżeli działanie $(*)$ ma podobne własności do dodawania liczb, to działanie nazywamy addytywnym i używamy symbolu $(+)$. Element neutralny e działania addytywnego $(+)$ nazywamy zerem i oznaczamy $e=0$, natomiast element symetryczny do elementu x nazywamy elementem przeciwnym i oznaczamy $\tilde{x} = -x$.
- Jeżeli działanie $(*)$ ma podobne własności do mnożenia liczb, to działanie nazywamy multiplikatywnym i używamy symbolu $(\cdot)$. Element neutralny e działania multiplikatywnego $(\cdot)$ nazywamy jedynką i oznaczamy $e=1$, natomiast element symetryczny do elementu x nazywamy elementem odwrotnym i oznaczamy $\tilde{x} = x^{-1}$.

Przykłady grup

- $(\{-1,1\}, \cdot)$ (multiplikatywna) grupa abelowa
- $(\mathbb{R}, +)$ (addytywna) grupa abelowa
- $(\mathbb{R}, \cdot)$ nie jest grupą (multiplikatywną) bo 0 nie ma elementu odwrotnego
- $(\mathbb{R} \setminus \{0\}, \cdot)$ (multiplikatywna) grupa abelowa
- zbiór $X = \{O_0, O_1, O_2, O_3\}$ obrotów kwadratu wokół jego środka przekształcających go na siebie z działaniem składania $(\circ)$ obrotów jest grupą abelową.
- Zbiór $X = \{0,1,2,3\}$ z działaniem $a \oplus b = \text{"reszta z dzielenia } a+b \text{ przez } 4\text{"}$ jest grupą abelową

Podgrupa

Def. Niech $(X,*)$ będzie grupą a $Y \subset X$ podzbiorem zbioru X . Jeśli $(Y,*)$ jest grupą, to $(Y,*)$ nazywamy **podgrupą** grupy $(X,*)$.

Morfizmy (odwzorowania) grup

Niech $(X, \oplus)$ i $(Y, \otimes)$ będą grupami.

Def. Odwzorowanie $h: X \rightarrow Y$ nazywamy **homomorfizmem** grupy $(X, \oplus)$ w grupę $(Y, \otimes)$, gdy

$\forall x_1, x_2 \in X: h(x_1 \oplus x_2) = h(x_1) \otimes h(x_2)$. Gdy odwzorowanie h jest bijekcją, to $h: X \rightarrow Y$ nazywamy **izomorfizmem** grup $(X, \oplus)$ i $(Y, \otimes)$.

Przykłady

- Grupy $(\mathbb{R}^+, \cdot)$ i $(\mathbb{R}, +)$ są izomorficzne. Izomorfizm ustanawia funkcja $h(x) = \log(x)$.

Ciało

Intuicja. Ciałem nazywamy zbiór w którym potrafimy wykonywać 4 podstawowe działania (+),(-), ($\cdot$), ($:$)

Ponieważ odejmowanie to dodawanie elementu przeciwnego a dzielenie to mnożenie przez odwrotność wystarczy rozważać 2 działania (+) i ($\cdot$) .

Def. Niech $X \neq \emptyset$ będzie niepustym zbiorem a $\oplus$ i $\otimes$ działaniami X . Trójkę $(X, \oplus, \otimes)$ nazywamy **ciałem** jeżeli

1. $\forall x, y \in X \quad x \oplus y \in X$
2. $\forall x, y, z \in X \quad (x \oplus y) \oplus z = x \oplus (y \oplus z)$
3. $\exists 0 \in X \quad \forall x \in X \quad x \oplus 0 = x \oplus 0 = x$
4. $\forall x \in X \quad \exists -x \in X \quad x \oplus (-x) = (-x) \oplus x = 0$
5. $\forall x, y \in X \quad x \oplus y = y \oplus x$

(postulaty 1÷5 można krótko zapisać $(X, \oplus)$ jest grupą przemienną)

6. $\forall x, y \in X \quad x \otimes y \in X$
7. $\forall x, y, z \in X \quad (x \otimes y) \otimes z = x \otimes (y \otimes z)$
8. $\exists 1 \in X \quad \forall x \in X \quad x \otimes 1 = 1 \otimes x = x$
9. $\forall x \in X - \{0\} \quad \exists x^{-1} \in X \quad x \otimes (x^{-1}) = x^{-1} \otimes x = 1$

(postulaty 6÷9 można krótko zapisać $(X - \{0\}, \otimes)$ jest grupą)

10. $\forall x, y, z \in X \quad (x \oplus y) \otimes z = (x \otimes z) \oplus (y \otimes z) \quad \text{ i } \quad z \otimes (x \oplus y) = (z \otimes x) \oplus (z \otimes y)$

($\otimes$ jest rozdzielne względem $\oplus$).

Jeżeli ponadto

11. $\forall x, y \in X \quad x \otimes y = y \otimes x$ to ciało nazywamy **ciałem przemiennym**.

Przykłady ciał (sprawdzić na ćwiczeniach)

- przemienne ciało liczb wymiernych $(W, +, \cdot)$
- przemienne ciało liczb rzeczywistych $(R, +, \cdot)$
- $(A, +, \cdot)$ gdzie $A = \{a + b\sqrt{2} : a, b \in W\}$

Podciało

Def. Niech $(X, \oplus, \otimes)$ będzie ciałem a $Y \subset X$ podzbiorem zbioru X . Jeśli struktura $(Y, \oplus, \otimes)$ jest ciałem, to $(Y, \oplus, \otimes)$ nazywamy **podciałem** ciała $(X, \oplus, \otimes)$.

Łatwo pokazać, że ciało $(W, +, \cdot)$ jest podciałem ciała $(A, +, \cdot)$ gdzie $A = \{a + b\sqrt{2} : a, b \in W\}$ natomiast ciało $(A, +, \cdot)$ jest podciałem ciała $(R, +, \cdot)$.

Działania modulo w zbiorze liczb całkowitych $\mathbb{Z}$

Niech n będzie dowolną ustaloną liczbą naturalną. W zbiorze liczb całkowitych definiujemy 2 nowe działania $\oplus_n$ i $\otimes_n$ w następujący sposób:

$$a \oplus_n b = (a + b)_n = \text{reszta z dzielenia } (a+b) \text{ przez } n,$$

$$a \otimes_n b = (a \cdot b)_n = \text{reszta z dzielenia } (a \cdot b) \text{ przez } n.$$

Łatwo pokazać (ćwiczenia), że

$$(a \oplus_n b) \oplus_n c = (a + b + c)_n = a \oplus_n (b \oplus_n c)$$

$$(a \otimes_n b) \otimes_n c = (abc)_n = a \otimes_n (b \otimes_n c)$$

Morfizmy (odwzorowania) ciał

Niech $(X, \circ, \bullet)$ i $(Y, \oplus, \otimes)$ będą ciałami .

Def. Odwzorowanie $h: X \rightarrow Y$ nazywamy **homomorfizmem** ciała $(X, \circ, \bullet)$ w ciało $(Y, \oplus, \otimes)$, gdy

$$\forall x_1, x_2 \in X: \begin{aligned} h(x_1 \circ x_2) &= h(x_1) \oplus h(x_2) \\ h(x_1 \bullet x_2) &= h(x_1) \otimes h(x_2) \end{aligned}$$

Gdy odwzorowanie h jest bijekcją, to $h: X \rightarrow Y$ nazywamy **izomorfizmem** ciał $(X, \circ, \bullet)$ i $(Y, \oplus, \otimes)$.