

2. WYKŁAD 2: GRUPY, PIERŚCIEŃ I CIAŁA.

Definicja 2.1. Niech A będzie niepustym zbiorem. **Działaniem wewnętrznym** (lub, krótko, **działaniem**) w zbiorze A nazywamy funkcję $*$: $A \times A \rightarrow A$. Niech ponadto B będzie niepustym zbiorem. **Działaniem zewnętrznym** w zbiorze A nazywamy funkcję $*$: $B \times A \rightarrow A$.

Uwaga 2.2. To, że w zbiorze A określono działanie wewnętrzne $*$ w szczególności oznacza, że:

- (1) $\forall x, y \in A [*(x, y) \text{ istnieje}]$,
- (2) $\forall x, y \in A [*(x, y) \in A]$.

Zamiast $*(x, y)$ będziemy na ogół pisać $x * y$.

Podobnie, jeśli $B \neq \emptyset$, to to, że w zbiorze A określono działanie zewnętrzne $\diamond$ w szczególności oznacza, że:

- (1) $\forall a \in B \forall x \in A [\diamond(a, x) \text{ istnieje}]$,
- (2) $\forall a \in B \forall x \in A [\diamond(a, x) \in A]$.

Zamiast $\diamond(a, x)$ będziemy na ogół pisać $a \diamond x$.

Na tym wykładzie będziemy zajmować się prawie wyłącznie działaniami wewnętrznymi.

Przykłady:

- (1) Dodawanie liczb naturalnych jest działaniem w zbiorze $\mathbb{N}$.
- (2) Mnożenie liczb naturalnych jest działaniem w zbiorze $\mathbb{N}$.
- (3) Odejmowanie i dzielenie nie są działaniami w zbiorze $\mathbb{N}$: $3 - 5 \notin \mathbb{N}$ oraz $1 \div 2 \notin \mathbb{N}$. Z drugiej strony, odejmowanie jest działaniem w $\mathbb{Z}$, a dzielenie jest działaniem w $\mathbb{Q} \setminus \{0\}$.
- (4) Mnożenie wektorów na płaszczyźnie przez skalary rzeczywiste jest przykładem działania wewnętrznego.

Definicja 2.3. Niech A będzie niepustym zbiorem, a $*$ i $\circ$ działaniami w A .

- (1) Mówimy, że $*$ jest **łącznie**, jeżeli

$$\forall x, y, z \in A [x * (y * z) = (x * y) * z].$$

- (2) Mówimy, że $*$ jest **przemienne**, jeżeli

$$\forall x, y \in A [x * y = y * x].$$

- (3) Mówimy, że $*$ ma **element neutralny** e , jeżeli

$$\forall x \in A [x * e = e * x = x].$$

- (4) Mówimy, że y jest **elementem odwrotnym** do x , jeżeli

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

- (5) Mówimy, że $\circ$ jest **rozdzielne względem** $*$, jeżeli

$$\forall x, y, z \in A [x \circ (y * z) = x \circ y * x \circ z].$$

Przykłady:

- (5) Dodawanie i mnożenie liczb naturalnych są łączne i przemienne. 0 jest elementem neutralnym dodawania, a 1 jest elementem neutralnym mnożenia. Ponadto mnożenie jest rozdzielne względem dodawania. 1 nie ma elementu odwrotnego względem dodawania, a 2 nie ma elementu odwrotnego względem mnożenia.
- (6) Rozważmy dodawanie i mnożenie liczb całkowitych. Każda liczba całkowita ma element odwrotny względem dodawania, ale 2 nie ma elementu odwrotnego względem mnożenia.

- (7) Rozważmy dodawanie i mnożenie liczb wymiernych. Każda liczba wymierna ma element odwrotny względem dodawania i każda niezerowa liczba wymierna ma element odwrotny względem mnożenia.

Definicja 2.4. (1) **Algebrą** nazywamy system $(A, *_1, \dots, *_n, B_1, \dots, B_m, \diamond_1, \dots, \diamond_m)$, gdzie A jest niepustym zbiorem, $*_1, \dots, *_n$ działaniami wewnętrznymi w zbiorze A , a $\diamond_1, \dots, \diamond_m$ działaniami zewnętrznymi w zbiorze A (wraz z odpowiadającymi im zbiorami $B_1, \dots, B_m$).

- (2) **Grupą** nazywamy algebrę $(G, *)$, gdzie $*$ jest łączne, ma element neutralny i każdy element w zbiorze G ma element odwrotny. Jeżeli ponadto $*$ jest przemienne, to grupę $(G, *)$ nazywamy **przemienią** (lub **abelową**).
- (3) **Pierścieniem** nazywamy algebrę $(R, +, \cdot)$, gdzie $(R, +)$ jest grupą abelową, a $\cdot$ jest łączne i rozdzielne względem $+$. Jeżeli $\cdot$ jest przemienne, to $(R, +, \cdot)$ nazywamy **pierścieniem przemiennym**. Jeżeli $\cdot$ ma element neutralny 1, to $(R, +, \cdot)$ nazywamy **pierścieniem z jedyneką**. W tym wykładzie ograniczymy się do pierścieni przemiennych z jedyneką, które będziemy krótko nazywać **pierścieniami**.
- (4) **Ciałem** nazywamy pierścień przemienny z jedyneką $(F, +, \cdot)$, w którym $0 \neq 1$, przy czym 0 oznacza element neutralny $+$, a 1 to element neutralny $\cdot$ i taki, że każdy $\neq 0$ element ma element odwrotny względem $\cdot$.

Przykłady:

- (8) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ są przykładami grup przemiennych. $(\mathbb{N}, +)$ nie jest grupą. Podobnie $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, gdzie $A^* = A \setminus \{0\}$, są grupami przemiennymi. $(\mathbb{N}^*, \cdot)$ i $(\mathbb{Z}^*, \cdot)$ nie są grupami.
- (9) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ są przykładami pierścieni.
- (10) $(\mathbb{Q}^+, \cdot)$, $(\mathbb{R}^+, \cdot)$ są przykładami ciał. $(\mathbb{Z}, +, \cdot)$ nie jest ciałem.

Definicja 2.5. Niech $n \in \mathbb{N}$ i oznaczmy przez $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$. W zbiorze $\mathbb{Z}_n$ definiujemy **dodawanie modulo n** :

$$x \oplus_n y = \text{reszta z dzielenia } x + y \text{ przez } n$$

oraz **mnożenie modulo n** :

$$x \otimes_n y = \text{reszta z dzielenia } x \cdot y \text{ przez } n.$$

Przykłady:

- (11) Sprawdzamy, że $2 \oplus_5 2 = 4$, $2 \oplus_5 4 = 1$, $2 \oplus_5 3 = 0$, $3 \oplus_6 5 = 2$ i $98 \oplus_{100} 2 = 0$.
- (12) Podobnie, $2 \otimes_5 2 = 4$, $2 \otimes_5 4 = 3$, $2 \otimes_5 3 = 1$, $3 \otimes_6 2 = 0$ i $98 \otimes_{100} 2 = 96$.

Twierdzenie 2.6. Niech $n \in \mathbb{N}$.

- (1) $(\mathbb{Z}_n, \oplus_n)$ jest grupą przemienną.
- (2) $(\mathbb{Z}_n^*, \otimes_n)$ jest grupą przemienną, o ile n jest liczbą pierwszą.
- (3) $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ jest pierścieniem.
- (4) $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ jest ciałem, o ile n jest liczbą pierwszą.

Dowód. Sprawdzenie wszystkich aksjomatów jest dość czasochłonne, ale proste. Ograniczymy się do pokazania, że jeśli n jest liczbą pierwszą, to każdy element $x \in \mathbb{Z}_n^*$ ma element odwrotny względem $\otimes_n$.

Ustalmy $x \in \mathbb{Z}_n^*$. Chcemy pokazać, że istnieje $y \in \mathbb{Z}_n^*$ taki, że $x \otimes_n y = 1$, to znaczy

$$xy = 1 + qn,$$

dla pewnej liczby całkowitej $q \in \mathbb{Z}$. Jest to równoważne pokazaniu, że równanie

$$xy - qn = 1$$

ma rozwiązanie w liczbach całkowitych. Ponieważ n jest liczbą pierwszą, a zatem $NWD(x, n) = 1$, równanie to istotnie ma rozwiązanie wobec Twierdzenia 1.9. $\square$

W dowolnej grupie $(G, *)$ wprowadzamy oznaczenie

$$\prod_{i=1}^n x_i = x_1 * \dots * x_n.$$

W szczególności $\prod_{i=1}^n x = x^n$. Tradycyjnie używamy w teorii grup dwóch równoległych terminologii: addytywnej i mnożymy, według następującego schematu:

Definicja	Notacja addytywna	Notacja mnożymy
działanie	$+$ dodawanie suma	$\cdot$ mnożenie iloczyn
element neutralny	0 zero	1 jedyńska
potęga	nx wielokrotność	x^n potęga
element odwrotny	$-x$ element przeciwny	x^{-1} element odwrotny

Twierdzenie 2.7. *Niech $(G, *)$ będzie grupą. Wówczas:*

- (1) *element neutralny e jest wyznaczony jednoznacznie;*
- (2) $\prod_{i=1}^m x_i * \prod_{j=1}^n x_j = \prod_{j=1}^{m+n} x_j$, dla $x_1, \dots, x_{m+n} \in G$;
- (3) $x^{m+n} = x^m x^n$, dla $x \in G$;
- (4) $(x^m)^n = x^{mn}$, dla $x \in G$;
- (5) *element odwrotny jest wyznaczony jednoznacznie;*
- (6) $(x_1^{n_1} * \dots * x_k^{n_k})^{-1} = x_k^{-n_k} * \dots * x_1^{-n_1}$, dla $x_1, \dots, x_k \in G$;
- (7) $(x^{-1})^{-1} = x$, dla $x \in G$;
- (8) $(x^{-1} * y * x)^n = x^{-1} * y^n * x$, dla $x, y \in G$;
- (9) *jeżeli $x * y = x * z$, to $y = z$.*

Dowód. Udowodnimy dla przykładu część (1): jeśli e i e' są dwoma elementami neutralnymi, to wówczas

$$e = e * e' = e'.$$

$\square$

W dowolnym pierścieniu $(R, +, \cdot)$ wprowadzamy oznaczenia:

$$\begin{aligned} xy + z &= (x \cdot y) + z, \\ \sum_{i=1}^n x_i &= x_1 + \dots + x_n, \sum_{i=1}^0 x_i = 0, \\ \prod_{i=1}^n x_i &= x_1 \cdot \dots \cdot x_n, \prod_{i=1}^0 x_i = 1, \\ nx &= \sum_{i=1}^n x, x^n = \prod_{i=1}^n x. \end{aligned}$$

Twierdzenie 2.8. *Niech $(R, +, \cdot)$ będzie pierścieniem, niech $x, y, z \in R$, $n, m \in \mathbb{N}$. Wówczas:*

- (1) $-(-x) = x$;
- (2) $-(x + y) = -x - y$;
- (3) $n(mx) = nm x$;
- (4) $nx + mx = (n + m)x$;
- (5) $0x = x0 = 0$;
- (6) $(-1)x = -x$;
- (7) $(-x)y = -(xy) = x(-y)$;
- (8) $(-x)(-y) = xy$;
- (9) $x(y - z) = xy - xz$;
- (10) $(x - y)z = xz - yz$;
- (11) *jeżeli $x + y = x + z$, to wówczas $y = z$;*
- (12) $x^n x^m = x^{n+m}$;
- (13) $(x^n)^m = x^{nm}$;
- (14) $(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k$.

Dowód. Udowodnimy dla przykładu część (5):

$$0x + 0x = (0 + 0)x = 0x$$

a zatem $0x = 0$.

□