WYKŁAD 2

2. Grupy, pierścienie i ciała

Def. 1: Niech A będzie niepustym zbiorem. *Działaniem wewnętrznym* w zbiorze A nazywamy funkcję $*: A \times A \to A$.

Uwaga: To, że w zbiorze A określono działanie wewnętrzne w szczególności oznacza, że:

(1) $\forall x, y \in A \quad *(x,y)$ istnieje,

(2) $\forall x, y \in A \quad *(x,y) \in A$.

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

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 $\mathbb{N}$:
$3 - 5 \notin \mathbb{N}$ oraz $1 \div 2 \notin \mathbb{N}$. Z drugiej strony, odejmowanie jest działaniem w $\mathbb{Z}$, a dzielenie w $\mathbb{Q} \setminus \{0\}$.

Def. 2: Niech A będzie niepustym zbiorem, a $*$ i $\circ$ działaniami w A.

(1) Mówimy, że $*$ jest *łączne*, jeśli
$$\forall x, y, z \in A \quad x * (y * z) = (x * y) * z$$

(2) Mówimy, że $*$ jest *przemienne*, jeśli
$$\forall x, y \in A \quad x * y = y * x$$

(3) Mówimy, że $*$ ma *element neutralny* e, jeśli
$$\forall x \in A \quad x * e = e * x = x$$

(4) Mówimy, że y jest *elementem odwrotnym* do x, jeśli
$$x * y = y * x = e$$

(5) Mówimy, że $\circ$ jest *rozdzielne względem* $*$, jeśli
$$\forall x, y, z \in A \quad x \circ (y * z) = x \circ y * x \circ z.$$

Przykłady: (1) Dodawanie i mnożenie liczb naturalnych jest 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.

(2) Rozważmy dodawanie i mnożenie liczb całkowitych. Każda liczba całkowita ma element odwrotny względem dodawania, ale 2 nie ma elementu odwrotnego względem mnożenia.

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

Def. 2: (1) <u>Strukturą algebraiczną</u> nazywamy system $(A, *_1, \dots, *_n)$, gdzie A jest niepustym zbiorem, a $*_1, \dots, *_n$ działaniami w A.
(2) <u>Grupą</u> nazywamy strukturę algebraiczną $(G, *)$, gdzie $*$ jest łączne, ma element neutralny i każdy element ma element odwrotny. Jeśli ponadto $*$ jest przemienne, $(G,*)$ nazywamy grupą <u>przemienną</u> (lub <u>abelową</u>).
(3) <u>Pierścieniem</u> nazywamy strukturę algebraiczną ~~(R, *, *)~~, $(R,+,\cdot)$, gdzie $(R,+)$ jest grupą abelową, a $\cdot$ jest łączne i rozdzielne względem $+$. Jeśli $\cdot$ jest przemienne, to $(R,+,\cdot)$ nazywamy <u>pierścieniem przemiennym</u>. Jeśli $\cdot$ ma element neutralny 1, to $(R,+,\cdot)$ nazywamy <u>pierścieniem z jedynką</u>. W tym wykładzie ograniczymy się do pierścieni przemiennych z jedynką, które będziemy krótko nazywać pierścieniami.
(4) <u>Ciałem</u> nazywamy pierścień przemienny z jedynką $(F,+,\cdot)$ w którym $0 \neq 1$ (gdzie 0 to element neutralny $+$ a 1 to element neutralny $\cdot$) i gdzie każdy $\neq 0$ element ma element odwrotny względem ~~mnoż~~ $\cdot$.

<u>Przykłady:</u> (1) $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ są przykładami grup. $(\mathbb{N},+)$ nie jest grupą. Podobnie $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$, gdzie $K^* = K \setminus \{0\}$, są grupami. $(\mathbb{N}^*,\cdot)$ i $(\mathbb{Z}^*,\cdot)$ nie są.
(2) $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ są przykładami pierścieni.
(3) $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ są ciałami. $(\mathbb{Z},+,\cdot)$ nie jest.

Def. 3: Niech $n \in \mathbb{N}$ i oznaczmy przez $\mathbb{Z}_n = \{0,1,\dots,n-1\}$. W zbiorze $\mathbb{Z}_n$ definiujemy <u>dodawanie modulo n</u>:

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

oraz <u>mnożenie modulo n</u>:

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

Tw. 1: (1) $(\mathbb{Z}_n, \oplus_n)$ jest grupą abelową
(2) $(\mathbb{Z}_n^*, \otimes_n)$ jest grupą abelową 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.

<u>Dowód:</u> 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.
Ustalmy $x \in \mathbb{Z}_n^*$. Chcemy pokazać, że istnieje $y \in \mathbb{Z}_n^*$ taki, że $x \otimes_n y = 1$, tzn.:

$$xy = 1 + qn$$

Jest to równoważne pokazaniu, że równanie

$$xy - qn = 1$$

ma rozwiązanie. Jest tak, ponieważ n jest pierwsze i $\mathrm{NWD}(x,n)=1$ □

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

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

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

Definicja	Notacja addytywna	Notacja multyplikatywna
działanie	$+$ dodawanie suma	$*$ mnożenie iloczyn
element neutralny	0 zero	1 jedynka
potęga	nx wielokrotność	x^n potęga
element odwrotny	$-x$ element przeciwny	x^{-1} element odwrotny

Tw. 2: Niech $(G,*)$ będzie grupą. Wówczas:

(1) e jest wyznaczony jednoznacznie (2) $\prod_{i=1}^m x_i * \prod_{j=1}^n x_{m+j} = \prod_{j=1}^{m+n} x_j$

(3) $x^{m+n} = x^m * x^n$ (4) $(x^m)^n = x^{mn}$

(5) element odwrotny jest wyznaczony jednoznacznie

(6) $(x_1^{n_1} * \ldots * x_k^{n_k})^{-1} = x_k^{-n_k} * \ldots * x_1^{-n_1}$ (7) $(x^{-1})^{-1} = x$

(8) $(x^{-1} * y * x)^n = x^{-1} * y^n * x$ (9) Jeśli $x*y = x*z$, to $y=z$.

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

$$e = e * e' = e'$$ □

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

$$xy + z = (x \cdot y) + z$$

$$\sum_{i=1}^n x_i = x_1 + \ldots + x_n, \quad \sum_{i=1}^0 x_i = 0$$

$$\prod_{i=1}^n x_i = x_1 \cdot \ldots \cdot x_n, \quad \prod_{i=1}^0 x_i = 1$$

$$nx = \sum_{i=1}^n x, \quad x^n = \prod_{i=1}^n x.$$

Tw. 3: Niech $(R,+,\cdot)$ będzie pierścieniem. Wówczas:

(1) $-(-x) = x$ (2) $-(x+y) = -x-y$ (3) $n(mx) = nmx$

(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) Jeśli $x+y = x+z$ to $y=z$ (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 $0x = 0$ □