

## Wykład 3

### Struktury algebraiczne

#### III. Struktury algebraiczne

Strukturą algebraiczną nazywamy zbiór wraz z pewnymi działaniami w tym zbiorze. Strukturę algebraiczną zapisujemy wymieniając zbiór oraz działania np.  $(\mathbb{N}, +, \cdot)$  jest strukturą algebraiczną złożoną z  $\mathbb{N}$  i dwóch działań dodawania i mnożenia. Działań w strukturze algebraicznej może być skończenie lub nieskończenie wiele.

W dalszym ciągu działanie  $\circ$  będzie działaniem binarnym.

Dowolną strukturę  $(G, \circ)$  nazywamy **grupoidem**.

Grupoid  $(G, \circ)$  nazywamy **półgrupą** jeśli działanie  $\circ$  jest łączne.

Półgrupę  $(G, \circ)$  nazywamy **grupą** jeśli  $\circ$  ma element neutralny i każdy element jest odwracalny.

Inaczej mówiąc  $(G, \circ)$  jest grupą jeśli:

$$(1) \forall a, b, c \in G \quad a \circ (b \circ c) = (a \circ b) \circ c,$$

$$(2) \text{Istnieje } e \in G, \text{ że } \forall a \in A \quad e \circ a = a \circ e = a,$$

$$(3) \forall a \in G \quad \exists a' \in G \quad aa' = a'a = e.$$

jeśli dodatkowo

$$(4) \forall a, b \in G \quad a \circ b = b \circ a$$

to grupę nazywamy **przemiennej** lub **abelową**.

#### Przykłady

$(\mathbb{N}, +)$  jest półgrupą i nie jest grupą,

$(\mathbb{Z}, +)$  jest grupą abelową,

$(\mathbb{R} \setminus \{0\}, \cdot)$  jest grupą abelową,

$(S_n, \circ)$  jest grupą i jeśli  $n > 2$  to jest to grupa nieabelowa.

Zbiór  $A = \{e, a, b, c\}$  z działaniem  $\circ$  określonym w tabelce:

$\circ$	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$e$	$c$	$b$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$b$	$a$	$e$

jest grupą abelową. Każdy element jest odwrotny sam do siebie.

**Twierdzenie 1** *Każdy element grupy posiada dokładnie jeden element odwrotny.*

**Dowód** Z definicji grupy wynika, że każdy element posiada element odwrotny. Przypuśćmy, że pewien element  $a$  posiada dwa elementy odwrotne  $a'$  i  $a''$ .

Wtedy, jeśli  $e$  oznacza element neutralny, mamy:

$$\begin{aligned}a \circ a' &= a' \circ a = e \\ a \circ a'' &= a'' \circ a = e\end{aligned}$$

Korzystając z powyższych równości i z łączności działania, otrzymujemy:

$$a' = a' \circ e = a' \circ (a \circ a'') \stackrel{(1)}{=} (a' \circ a) \circ a'' = e \circ a'' = a''.$$

Co oznacza, że element odwrotny jest dokładnie jeden. ■

Element odwrotny do  $a$  oznaczamy przez  $a^{-1}$ .

**Twierdzenie 2** *Jeśli  $(G, \circ)$  jest grupą to:*

- (i)  $\forall a \in G \quad (a^{-1})^{-1} = a,$
- (ii)  $\forall a, b \in G \quad (a \circ b)^{-1} = b^{-1} \circ a^{-1}.$

**Dowód**

- (i) Ponieważ  $a \circ a^{-1} = a^{-1} \circ a = e$  to element  $a$  jest odwrotny do  $a^{-1}$  i ponieważ element odwrotny jest wyznaczony jednoznacznie to  $(a^{-1})^{-1} = a.$
- (ii) Wystarczy sprawdzić, że element  $b^{-1} \circ a^{-1}$  jest odwrotny do  $a \circ b.$  ■

**Zadanie** Wyznaczyć elementy odwrotne do elementów grupy  $(S_3, \circ).$

**Twierdzenie 3** *Jeśli  $(G, \circ)$  jest grupą to:*

- (i)  $a \circ x = b \circ x \Rightarrow a = b,$
- (ii)  $x \circ a = x \circ b \Rightarrow a = b.$

**Dowód**

- (i) Jeśli  $a \circ x = b \circ x$  to mnożąc to równanie obustronnie z prawej strony przez  $x^{-1}$  otrzymujemy:

$$\begin{aligned}(a \circ x) \circ x^{-1} &= (b \circ x) \circ x^{-1} \\ a \circ (x \circ x^{-1}) &= b \circ (x \circ x^{-1}) \\ a \circ e &= b \circ e \\ a &= b\end{aligned}$$

- (ii) Analogicznie jak poprzedni punkt. ■

**Twierdzenie 4** *Jeśli  $(G, \circ)$  jest grupą i  $a, b \in G$  to równanie  $a \circ x = b$  ma dokładnie jedno rozwiązanie w zbiorze  $G.$*

**Dowód** Nietrudno jest zauważyć, że element  $a^{-1} \circ b$  jest rozwiązaniem równania i że jest to jedyne rozwiązanie tego równania. ■

Jeśli grupa jest abelowa to działanie binarne często zapisujemy przy pomocy znaku  $+$ , element odwrotny do  $a$  nazywamy przeciwnym i zapisujemy go w postaci  $-a$ , a element neutralny oznaczamy przez  $0$ .

System algebraiczny  $(R, \oplus, \odot)$  nazywamy **pierścieniem** jeśli  $\odot, \oplus$  są działaniami binarnymi oraz:

- (1)  $(R, \oplus)$  jest grupą abelową,
- (2)  $(R, \odot)$  jest półgrupą,
- (3) działanie  $\odot$  jest rozdzielne względem  $\oplus$ .

Dodatkowo jeśli:

- (4) działanie  $\odot$  jest przemienne to pierścień nazywamy **pierścieniem przemennym**, a jeśli mnożenie  $\odot$  posiada element neutralny to pierścień nazywamy **pierścieniem z jedyneką** (element neutralny działania  $\odot$  będziemy zwykle nazywać jedyneką pierścienia i oznaczać go będziemy zwykle przez  $1$ ).

Przykładami pierścieni przemennych z jedyneką są  $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ . Później poznamy również przykłady pierścieni nieprzemennych.

Ponieważ struktura  $(R, \oplus)$  jest grupą abelową to istnieje element neutralny działania  $\oplus$  i każdy element jest odwracalny względem tego działania. Element neutralny oznaczać będziemy przez  $0$ , a element odwrotny do  $x$  nazywać będziemy elementem przeciwnym i oznaczać go będziemy przez  $-x$ .