

Notatki z algebry abstrakcyjnej: definicje i twierdzenia

Informatyka, WPPT

Bartosz Chodorowski <chomzee@ethernet.pl>

16 kwietnia 2008 r.

Definicja 1 (Grupa) $\{G, \nabla\}$ nazywamy grupą jeśli:

- 0) ∇ jest działaniem w G
- 1) ∇ jest działaniem łącznym,
- 2) istnieje element neutralny e , czyli $(\exists e \in G)(\forall a \in G)(a \nabla e = e \nabla a = a)$
- 3) dla każdego elementu z G istnieje element odwrotny, czyli: $(\forall a \in G)(\exists a^{-1} \in G)(a^{-1} \nabla a = a \nabla a^{-1} = e)$

Definicja 2 (Grupa abelowa) Grupę $\{G, \nabla\}$, w której działanie ∇ jest przemienne, czyli $(\forall a, b \in G)(a \nabla b = b \nabla a)$, nazywamy grupą abelową.

Twierdzenie 1 Element neutralny w grupie wyznaczony jest jednoznacznie.

Twierdzenie 2 Dla każdego a z grupy element odwrotny a^{-1} jest wyznaczony jednoznacznie.

Twierdzenie 3 (Prawo skracania w grupie) Niech $\{G, \nabla\}$ będzie grupą, $a, b, c \in G$. Wówczas:

- 1) $a \nabla b = a \nabla c \Rightarrow b = c$
- 2) $b \nabla a = c \nabla a \Rightarrow b = c$

Twierdzenie 4 (Własności grup) Niech $\{G, \nabla\}$ będzie grupą, $a, b \in G$. Wówczas:

- 1) $(a \nabla b)^{-1} = b^{-1} \nabla a^{-1}$
- 2) $(a^{-1})^{-1} = a$

Definicja 3 (Podgrupa) Podgrupą H grupy $\{G, \nabla\}$ nazywamy niepusty podzbiór G , który jest grupą ze względu na działanie ∇ .

Twierdzenie 5 Niepusty podzbiór H grupy $\{G, \nabla\}$ jest jej podgrupą wtedy i tylko wtedy gdy zachodzi implikacja:

$$a, b \in H \Rightarrow a \nabla b^{-1} \in H$$

Definicja 4 (Potęga elementu) Niech $\{G, \nabla\}$ będzie grupą, $k \in \mathbb{Z}$, $g \in G$

$$g^k \stackrel{\text{def}}{=} \begin{cases} \underbrace{g \nabla g \nabla \dots \nabla g}_{k \text{ razy}} & \text{dla } k > 0 \\ \underbrace{g^{-1} \nabla g^{-1} \nabla \dots \nabla g^{-1}}_{k \text{ razy}} & \text{dla } k < 0 \\ e & \text{dla } k = 0 \end{cases}$$

Twierdzenie 6 (Własność potęgowania) Niech $\{G, \nabla\}$ będzie grupą, $a \in G$, $k, l \in \mathbb{Z}$. Wówczas:

$$a^k \nabla a^l = a^{k+l}$$

Definicja 5 (Wielokrotność elementu w grupie) Niech $\{G, \nabla\}$ będzie grupą addytywną. Wówczas potęgę g^k nazywamy wielokrotnością elementu g i oznaczamy kg .

Definicja 6 (Grupa cykliczna) Niech G będzie grupą, $a \in G$. Grupą cykliczną generowaną przez element a nazywamy zbiór:

$$\langle a \rangle \stackrel{\text{def}}{=} \{a^k : k \in \mathbb{Z}\}$$

Twierdzenie 7 Dla każdego $a \in G$ zbiór $\langle a \rangle$ jest podgrupą grupy G .

Definicja 7 (Rząd grupy) Jeśli $\{G, \nabla\}$ jest grupą skończoną, to $\text{rz } G = \text{ilość elementów w } G$. Jeśli $\{G, \nabla\}$ jest grupą nieskończoną, to $\text{rz } G = \infty$

Definicja 8 (Rząd elementu grupy) Niech G będzie grupą, $g \in G$.

$$\text{rz } g \stackrel{\text{def}}{=} \text{rz } \langle g \rangle$$

Twierdzenie 8 Niech G będzie grupą, $a \in G$, $\text{rz } a = n$. Wówczas:

$$\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$$

Twierdzenie 9 Niech G będzie grupą oraz $a \in G$. Jeżeli istnieje liczba naturalna n taka, że $a^n = e$ oraz $a^k \neq e$ dla $k = 1, 2, \dots, n-1$, to $\text{rz } a = n$.
Jeżeli taka liczba nie istnieje, to $\text{rz } a = \infty$.

Definicja 9 (Warstwa) Niech $\{G, \nabla\}$ będzie grupą, H podgrupą G , $a \in G$. Warstwą lewostronną elementu a względem podgrupy H nazywamy zbiór:

$$aH \stackrel{\text{def}}{=} \{a \nabla h : h \in H\}$$

Warstwa prawostronna:

$$Ha \stackrel{\text{def}}{=} \{h \nabla a : h \in H\}$$

Twierdzenie 10 Jeżeli H jest podgrupą G , to każde dwie warstwy lewostronne względem H są albo rozłączne albo równe.

Wniosek: każdy element grupy należy do dokładnie jednej lewostronnej warstwy względem H .

Definicja 10 (Indeks podgrupy) Jeżeli liczba warstw lewostronnych względem podgrupy H jest skończona, to tę liczbę nazywamy indeksem podgrupy H w grupie G . W przeciwnym razie indeks jest nieskończony.

Twierdzenie 11 (Lagrange'a) Jeżeli H jest podgrupą grupy skończonej G , to rząd grupy G jest iloczynem rzędu podgrupy H i indeksu podgrupy H w grupie G .

Definicja 11 (Dzielnik normalny) Podgrupę H grupy G nazywamy dzielnikiem normalnym jeśli:

$$(\forall a \in G)(aH = Ha)$$

Twierdzenie 12 Podgrupa H grupy G jest jej dzielnikiem normalnym wtedy i tylko wtedy gdy:

$$(\forall g \in G)(\forall h \in H)(ghg^{-1} \in H)$$

Definicja 12 (Działanie na warstwach) Niech $\{G, \nabla\}$ będzie grupą, H podgrupą G , $a, b \in G$. Definiujemy działanie $\circ$ na warstwach:

$$aH \circ bH \stackrel{\text{def}}{=} (a \nabla b)H \quad (1)$$

Twierdzenie 13 Niech H będzie dzielnikiem normalnym grupy G . Wówczas wzór (1) określa działanie w zbiorze warstw i zbiór warstw jest grupą ze względu to działanie (grupa ilorazowa).

Definicja 13 (Homomorfizm) Niech $\{G_1, \circ\}, \{G_2, \nabla\}$ będą grupami. Funkcję $\varphi : G_1 \rightarrow G_2$ taką, że:

$$(\forall a, b \in G_1)(\varphi(a \circ b) = \varphi(a) \nabla \varphi(b))$$

nazywamy homomorfizmem.

Definicja 14 (Izomorfizm) Homomorfizm różnowartościowy i „na” nazywamy izomorfizmem.

Definicja 15 (Obraz i jądro homomorfizmu) Niech G_1, G_2 będą grupami, e_2 elementem neutralnym w G_2 , $\varphi : G_1 \rightarrow G_2$ homomorfizmem.

Obrazem homomorfizmu nazywamy zbiór:

$$\text{Im } \varphi \stackrel{\text{def}}{=} \{a \in G_2 : (\exists g \in G_1)(a = \varphi(g))\}$$

Jądrem homomorfizmu nazywamy zbiór:

$$\ker \varphi \stackrel{\text{def}}{=} \{a \in G_1 : \varphi(a) = e_2\}$$

Twierdzenie 14 (Własności homomorfizmu) Niech G_1, G_2 będą grupami, $\varphi : G_1 \rightarrow G_2$ homomorfizmem. Wówczas:

- 1) $\varphi(e_1) = e_2$
- 2) $\varphi(a^{-1}) = (\varphi(a))^{-1}$
- 3) $\ker \varphi$ jest podgrupą grupy G_1

Twierdzenie 15 Grupy cykliczne mające ten sam rząd są izomorficzne.

Twierdzenie 16 Niech G będzie grupą cykliczną rzędu n . Wówczas G jest izomorficzna z addytywną grupą $\mathbb{Z}_n$.

Twierdzenie 17 (Cayley’a) Każda grupa $\{G, \nabla\}$ zanurza się izomorficznie w swojej grupie symetrycznej $\{S_G, \circ\}$, czyli G jest izomorficzna z pewną podgrupą grupy wszystkich permutacji zbioru G .

Uwaga:

$S_G = S(G)$ – zbiór wszystkich bijekcji (permutacji) G na siebie.
W $S(G)$ działaniem jest złożenie $\circ$.

Definicja 16 (Pierścień) $\{R, \oplus, \odot\}$ jest pierścieniem jeśli:

- 0) $\oplus, \odot$ są poprawnie określonymi działaniami w R
- 1) R jest grupą abelową ze względu na $\oplus$
- 2) działanie $\odot$ jest łączne
- 3) zachodzi rozdzielność $\odot$ względem $\oplus$, to znaczy:

$$(\forall a, b, c \in R)(a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c))$$

oraz

$$(\forall a, b, c \in R)((b \oplus c) \odot a = (b \odot a) \oplus (c \odot a))$$

$\oplus$ nazywamy dodawaniem

$\odot$ nazywamy mnożeniem

Definicja 17 (Dzielnik zera) Element $a \neq 0$ pierścienia $\{R, \oplus, \odot\}$ nazywamy lewostronnym dzielnikiem zera jeśli:

$$(\exists b \in R)(b \neq 0 \wedge a \odot b = 0)$$

Definicja 18 (Pierścień całkowity) *Pierścień przemienny, bez dzielników zera i z jedyneką (elementem neutralnym mnożenia) nazywamy pierścieniem całkowitym.*

Definicja 19 (Odejmowanie w pierścieniu) *Niech $a, b \in R$.*

$$a - b \stackrel{\text{def}}{=} a \oplus (-b), \text{ gdzie } -b \text{ jest elementem odwrotnym do } b \text{ ze względu na } \oplus$$

Twierdzenie 18 *Niech R będzie pierścieniem, $a \in R$, 0 elementem neutralnym ze względu na $\oplus$. Wówczas:*

$$0a = a0 = 0$$

Twierdzenie 19 (Własności pierścieni) *Niech R będzie pierścieniem, $a \in R$. Wówczas:*

$$1) (-a)b = a(-b) = -ab$$

$$2) (-a)(-b) = ab$$

Twierdzenie 20 *Jeżeli w pierścieniu R nie ma dzielników zera, $a, b, c \in R$, $a \neq 0$, to zachodzą własności:*

$$1) ab = ac \Rightarrow b = c$$

$$2) ba = ca \Rightarrow b = c$$

Definicja 20 (Podpierścień) *Niepusty podzbiór S pierścienia $\{R, \oplus, \odot\}$ nazywamy podpierścieniem, gdy $\{S, \oplus, \odot\}$ sam jest pierścieniem.*

Twierdzenie 21 *Niepusty podzbiór S pierścienia R jest jego podpierścieniem wtedy i tylko wtedy gdy:*

$$(a, b \in S) \Rightarrow ((a - b \in S) \wedge (ab \in S))$$

Definicja 21 (Ciało) *Pierścień $\{K, \oplus, \odot\}$ nazywamy ciałem, gdy:*

$$1) K \text{ zawiera więcej niż 1 element}$$

$$2) K \setminus \{0\} \text{ jest grupą ze względu na } \odot$$

$$3) \odot \text{ jest przemienne}$$

Definicja 22 (Podciało) *Niepusty podzbiór L ciała $\{K, \oplus, \odot\}$ nazywamy podciałem, gdy $\{L, \oplus, \odot\}$ sam jest ciałem.*

Twierdzenie 22 *Niepusty podzbiór L ciała K jest jego podciałem wtedy i tylko wtedy gdy:*

$$1) L \text{ zawiera więcej niż 1 element}$$

$$2) a, b \in L \Rightarrow a - b \in L$$

$$3) a, b \in L \setminus \{0\} \Rightarrow ab^{-1} \in L \setminus \{0\}$$