Matematyka dyskretna - teoria

Jan Rodziewicz-Bielewicz, Wydział Informatyki ZUT

May 15, 2022

8 Struktury algebraiczne

Definicja 47. **Działaniem (wewnętrznym)** w zbiorze A nazywamy dowolne odwzorowanie iloczynu kartezjańskiego $A \times A$ w zbiór A - czyli parze uporządkowanej $(a, b) \in A \times A$ przyporządkowany zostaje dokładnie 1 element ze zbioru A.

Definicja 48. **Grupą** nazywamy parę $(G, \cdot)$, składającą się ze zbioru G oraz działania $\cdot$ spełniającego warunki:

1. łączność $\underset{a,b,c \in G}{\forall} (a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. istnienie elementu neutralnego e: $\underset{a \in G}{\forall} a \cdot e = e \cdot a = a$
3. istnienie elementów odwrotnych: $\underset{a \in G}{\forall} \underset{a^{-1} \in G}{\exists} a \cdot a^{-1} = a^{-1} \cdot a = e$

Definicja 49. Grupę nazywamy **abelową** (przemienną), jeśli działanie $\cdot$ jest przemienne:

$$\underset{a,b,c \in G}{\forall} a \cdot b = b \cdot a$$

Uwaga Symbol "$\cdot$" nie musi oznaczać mnożenia liczb, może to być dowolnie zdefiniowane działanie (jest to tzw. notacja multiplikatywna). Dla uproszczenia zapisu symbol działania zwykle się pomija i zapisuje ab zamiast $a \cdot b$. Spotykana jest też notacja addytywna - działanie grupowe oznaczane jest symbolem $+$, i zamiast mówić o elementach odwrotnych do elementu a mówi się o elementach przeciwnych $-a$.

Definicja 50. Niech $(G, \cdot)$ będzie grupą. Jeśli zbiór G jest skończony, to liczbę jego elementów nazywamy **rzędem grupy** i oznaczamy $rz\ G$ lub krótko $|G|$. Jeśli zbiór G jest nieskończony, to grupa ma rząd nieskończony i piszemy $|G| = \infty$.

Definicja 51. Niech $(G, \cdot)$ będzie grupą. Niepusty podzbiór H zbioru G nazywamy podgrupą grupy G, jeżeli spełniony jest warunek:

$$\underset{a,b \in H}{\forall} ab^{-1} \in H$$

Fakt bycia podgrupą zapisuje się następująco: $H < G$.
Uwaga Zgodnie z twierdzeniem Lagrange'a, jesli grupa G jest skończona, to rząd podgrupy jest dzielnikiem rzędu grupy.

Definicja 52. Niech G_1 i G_2 będą grupami. **Homomorfizmem** grupy G_1 w grupę G_2 nazywamy odwzorowanie $\phi : G_1 \to G_2$, spełniające warunek:

$$\underset{a,b \in G_1}{\forall} \phi(ab) = \phi(a)\phi(b)$$

Definicja 53. Niech ϕ będzie homomorfizmem grup (pierścieni, ciał). ϕ nazywamy:

1. **monomorfizem**, gdy jest odwzorowaniem różnowartościowym,
2. **epimorfizmem**, gdy jest odwzorowaniem "na",
3. **izomorfizmem**, gdy jest bijektywny (jednocześnie monomorfizm i epimorfizm),

4. **endomorfizmem**, gdy działa ze struktury A (np. grupy) do tej samej struktury,
5. **automorfizmem**, gdy jest jednocześnie endomorfizmem i izomorfizmem.

Definicja 54. **Jądrem** homomorfizmu grup (pierścieni, ciał) $\phi : G_1 \to G_2$ nazywamy zbiór:

$$\ker \phi = \{g \in G_1 : \phi(g) = e_{G_2}\}$$

gdzie e_{G_2} oznacza element neturalny grupy G_2.

Definicja 55. **Obrazem** homomorfizmu grup (pierścieni, ciał) $\phi : G_1 \to G_2$ nazywamy zbiór:

$$\operatorname{im} \phi = \phi(G_1) = \{h \in G_2 : \underset{g \in G_1}{\exists} \phi(g) = h\}$$

Definicja 56. Mówimy, że grupy (pierścienie, ciała) G_1 i G_2 są **izomorficzne** jeżeli istnieje izomorfizm między nimi. Oznaczamy to w poniższy sposób:

$$G_1 \cong G_2$$

Uwaga Izomorfizm między grupami (pierścieniami, ciałami) zachowuje własności struktury np. odwrotności elementów.

Twierdzenie 119. Niech G_1 i G_2 są grupami (pierścieniami, ciałami) oraz $\phi : G_1 \to G_2$ homomorfizmem grup (pierścieni, ciał). ϕ jest izomorfizmem wtedy i tylko wtedy, gdy $\ker \phi = \{e\}$ i $\operatorname{im} \phi = G_2$.

Definicja 57. Niech G będzie dowolną grupą i niech $g \in G$. **Potęgę** elementu a o wykładniku $k \in \mathbb{Z}$ określamy wzorem:

$$g^k = \begin{cases} g \cdot \ldots \cdot g, \ (k \text{ czynników}), \text{ gdy } k > 0 \\ e, \ \text{gdy } k = 0 \\ g^{-1} \cdot \ldots \cdot g^{-1}, \ (|k| \text{ czynników}), \text{ gdy } k < 0 \end{cases}$$

Dla tak określonych potęg oraz $k, l \in \mathbb{Z}$ zachodzą równości:

1. $a^k \cdot a^l = a^{k+l}$
2. $(a^k)^l = a^{kl}$
3. Jeśli $ab = ba$, to $(ab)^k = a^k \cdot b^k$

Twierdzenie 120. Dla każdego $a \in G$ zbiór $\langle a \rangle := \{a^k \in G : k \in \mathbb{Z}\}$ jest podgrupą grupy G.

Definicja 58. Podgrupę $\langle a \rangle$ nazywamy **podgrupą generowaną przez element** a. Jeżeli istnieje element $a \in G$, taki że $G = \langle a \rangle$ to G nazywamy **grupą cykliczną**, a nazywamy wtedy **generatorem**.

Definicja 59. Niech $a \in G$. Jeżeli istnieje liczba naturalna k, taka że $a^k = e$, to najmniejszą spośród takich liczb nazywamy **rzędem elementu** a i oznaczamy $rz(a)$ lub $rz\ a$. Jeżeli taka liczba nie istnieje, to mówimy że element a ma rząd nieskończony, co oznaczamy $rz\ a = \infty$.

References

[1] Larisa Dobryakova, *Matematyka dyskretna.* Lulu, 2012.

[2] Jerzy Rutkowski, *Algebra abstrakcyjna w zadaniach.* Wydawnictwo Naukowe PWN, 2002.

[3] Kenneth A. Ross, Charles R. B. Wright, *Matematyka dyskretna.* Wydawnictwo Naukowe PWN, 1999.