

IZOMORFIZMY GRUP

Piotr Słanina

22 kwietnia 2003

Definicja 1 Funkcję $\varphi : G \longrightarrow H$ nazywamy homomorfizmem grupy $(G, \cdot, {}^{-1}, 1)$ w grupę $(H, \cdot, {}^{-1}, 1)$ wtedy i tylko wtedy gdy

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$$

dla każdego $x, y \in G$.

Można wtedy powiedzieć, że grupy G i H są izomorficzne.

Definicja 2 Izomorfizmem nazywamy każdy homomorfizm, który jest różnowartościowy.

1 JAK SPRAWDZIĆ, ŻE DWIE GRUPY SĄ IZOMORFICZNE?

1.1 PODOBIENSTWO TABELI DZIAŁAŃ

Jeżeli dla dwóch różnych grup można w taki sposób ułożyć tabele działań, że w każdej z nich na odpowiednim miejscu znajduje się ten sam element, to te grupy są izomorficzne.

Izomorfizm ten jest zadany jako przyporządkowanie dowolnemu elementowi z pierwszej tabelki elementu z drugiej tabelki, który znajduje się na tym samym miejscu w tabelce II co jego przeciwobraz w pierwszej.

Przykład 1 Oto tabelki działań dla grup kolejno: $G_1 = \mathbb{Z}_6$, G_2 grupa obrotów sześciokąta, $G_3 = \mathbb{Z}_2 \times \mathbb{Z}_3$, $G_4 = U_7$ (grupa $(\{1, 2, 3, 4, 5, 6\}, \cdot, {}^{-1}, 1)$):

	+	0	1	2	3	4	5
	0	0	1	2	3	4	5
	1	1	2	3	4	5	0
G_1 :	2	2	3	4	5	0	1
	3	3	4	5	0	1	2
	4	4	5	0	1	2	3
	5	5	0	1	2	3	4

	◦	0 ⁰	60 ⁰	120 ⁰	180 ⁰	240 ⁰	300 ⁰
	0 ⁰	0 ⁰	60 ⁰	120 ⁰	180 ⁰	240 ⁰	300 ⁰
	60 ⁰	60 ⁰	120 ⁰	180 ⁰	240 ⁰	300 ⁰	0 ⁰
$G_2 :$	120 ⁰	120 ⁰	180 ⁰	240 ⁰	300 ⁰	0 ⁰	60 ⁰
	180 ⁰	180 ⁰	240 ⁰	300 ⁰	0 ⁰	60 ⁰	120 ⁰
	240 ⁰	240 ⁰	300 ⁰	0 ⁰	60 ⁰	120 ⁰	180 ⁰
	300 ⁰	300 ⁰	0 ⁰	60 ⁰	120 ⁰	180 ⁰	240 ⁰

	+	(0, 0)	(1, 1)	(0, 2)	(1, 0)	(0, 1)	(1, 2)
	(0, 0)	(0, 0)	(1, 1)	(0, 2)	(1, 0)	(0, 1)	(1, 2)
	(1, 1)	(1, 1)	(0, 2)	(1, 0)	(0, 1)	(1, 2)	(0, 0)
$G_3 :$	(0, 2)	(0, 2)	(1, 0)	(0, 1)	(1, 2)	(0, 0)	(1, 1)
	(1, 0)	(1, 0)	(0, 1)	(1, 2)	(0, 0)	(1, 1)	(0, 2)
	(0, 1)	(0, 1)	(1, 2)	(0, 0)	(1, 1)	(0, 2)	(1, 0)
	(1, 2)	(1, 2)	(0, 0)	(1, 1)	(0, 2)	(1, 0)	(0, 1)

	·	1	3	2	6	4	5
	1	1	3	2	6	4	5
	3	3	2	6	4	5	1
$G_4 :$	2	2	6	4	5	1	3
	6	6	4	5	1	3	2
	4	4	5	1	3	2	6
	5	5	1	3	2	6	4

Tu należy zwrócić uwagę na analogiczny układ elementów w każdej z tabel.

Uwaga Jeżeli elementy w tabelce działania grupy np. G_4 zapisać w innej kolejności:

	·	1	2	3	4	5	6
	1	1	2	3	4	5	6
	2	2	4	6	1	3	5
$G_4 :$	3	3	6	2	5	1	4
	4	4	1	5	2	6	3
	5	5	3	1	6	4	2
	6	6	5	4	3	2	1

to wtedy nie widać tego izomorfizmu; przy innym zapisaniu elementów w tabelce (takim, jak za pierwszym razem) widać jednak, że ten izomorfizm istnieje. Zatem należy wtedy próbować zapisać tabelę w inny sposób.

1.2 RÓWNOLICZNE GRUPY CYKLICZNE SĄ IZOMORFICZNE

Definicja 3 Jeżeli w grupie G istnieje element a taki, że każdy element tej grupy jest postaci $a^n, n \in \mathbb{Z}$ to G jest nazywana grupą cykliczną, a element a generatorem tej grupy.

Przykład 2 $(\mathbb{Z}, +, -, 0)$ jest cykliczna, bo jej generatorem jest 1 i każdą liczbę całkowitą można przedstawić jako potęgę jedynki (potęga w grupie działa następująco: $a^4 = a \circ a \circ a \circ a$, $a^{-3} = a^{-1} \circ a^{-1} \circ a^{-1}$), np. $7 = 1^7 = 1 + 1 + 1 + 1 + 1 + 1 + 1$, $-4 = 1^{-4} = 1^{-1} + 1^{-1} + 1^{-1} + 1^{-1} = -1 - 1 - 1 - 1$

Przykład 3 $(\mathbb{Q}, +, -, 0)$ nie jest cykliczna. Gdyby tak było, to istniałby jakiś jej generator a . Jednak za pomocą jego potęg można jedynie wygenerować elementy $\{\dots, -3a, -2a, -a, 0, a, 2a, 3a, \dots\}$. Nie można np. wygenerować $a/2$. Skoro zatem żaden z elementów nie może być generatorem, to \mathbb{Q} nie jest cykliczna. Bardzo podobnie można udowodnić, że $(\mathbb{R}, +, -, 0)$ nie jest cykliczna.

Przykład 4 Dla każdego $n \in \mathbb{N}$ grupa $(\mathbb{Z}_n, +_n, -_n, 0)$ jest cykliczna. Łatwo sprawdzić, że jej generatorem jest np. 1.

Grupy cykliczne o tej samej liczbie elementów są izomorficzne.

Przykład 5 Jeżeli zauważysz się, że np. \mathbb{Z}_6 i $\mathbb{Z}_2 \times \mathbb{Z}_3$ są cykliczne o generatorach odpowiednio 1 i $(1, 1)$, to z tego wynika, że te grupy są izomorficzne.

1.3 GRUPY p -ELEMENTOWE, GDZIE p JEST LICZBA PIERWSZĄ SĄ IZOMORFICZNE

Aby to udowodnić najpierw pokażę, że:

Twierdzenie 1 Każda p -elementowa grupa (p liczba pierwsza) jest cykliczna.

Dowód (nie wprost) niech grupa G nie jest cykliczna.

Zatem mogę wybrać taki element $a \neq 1$, który nie generuje całej grupy, czyli $H = \{1, a, a^2, a^3, \dots, a^{n-1}\} \neq G$ (warto tutaj zauważyć, że $|H| > 1$).

Ten zbiór jest podgrupą grupy G .

Z tw. Lagrange'a $|G| = |H| \cdot |G/H|$. Ponieważ $|G| > |H|$ więc $|G/H| > 1$ i ponieważ $|H| > 1$ czyli $|G|$ jest liczbą złożoną. \square

Zatem jeżeli udowodniliśmy, że jest to grupa cykliczna to z **1.2** wynika, że jakiegokolwiek grupy np. 17-toelementowe są cykliczne, czyli izomorficzne.

Uwaga To, że liczba elementów w grupie nie jest liczbą pierwszą wcale nie wynika, że grupa nie jest cykliczna, np. \mathbb{Z}_6 jest cykliczna.

1.4 BEZPOŚREDNIE WSKAZYWANIE IZOMORFIZMU MIĘDZY GRUPAMI

Przykład 6 Pokażemy izomorfizm pomiędzy grupami $(\mathbb{R} \times \mathbb{R}, +, -, 0)$ i $(\mathbb{C}, +, -, 0)$: Niech $\varphi((x, y)) = x + iy$ będzie funkcją odwzorowującą pierwszą grupę w drugą. Aby udowodnić że funkcja φ jest izomorfizmem należy pokazać, że:

1. Jest to homomorfizm grup:

$$\varphi((x_1, y_1) + (x_2, y_2)) = \varphi(x_1 + x_2, y_1 + y_2) = x_1 + x_2 + i(y_1 + y_2),$$

$$\varphi((x_1, y_1)) + \varphi((x_2, y_2)) = (x_1 + iy_1) + (x_2 + iy_2) = x_1 + x_2 + i(y_1 + y_2).$$

Zatem φ jest homomorfizmem.

2. Jest to funkcja "w" (czyli $\text{Im}(\varphi) = \mathbb{C}$):

Bierzemy dowolny element $x + iy \in \mathbb{C}$.

$$\varphi^{-1}(x + iy) = (x, y) \in \mathbb{R} \times \mathbb{R}.$$

Zatem obrazem φ jest całe \mathbb{C} .

3. Jest to funkcja różnowartościowa:

Weźmy dwa różne elementy z $\mathbb{R} \times \mathbb{R}$: $(x_1, y_1), (x_2, y_2)$. Jednak

$$\varphi((x_1, y_1)) = x_1 + iy_1 \neq x_2 + iy_2 = \varphi((x_2, y_2)),$$

co dowodzi różnowartościowości.

Stąd φ jest izomorfizmem danych grup, więc te grupy są izomorficzne.

2 JAK SPRAWDZIĆ, ŻE DWIE GRUPY NIE SĄ IZOMORFICZNE?

2.1 GRUPY RÓŻNEGO RZĘDU

Definicja 4 Rzędem grupy nazywamy ilość elementów w grupie.

Wskazując, że dwie grupy mają różną liczbę elementów łatwo wywnioskować, że nie może być pomiędzy nimi żadnej funkcji różnowartościowej.

Przykład 7 Grupa $(\mathbb{Q}, +, -, 0)$ nie jest izomorficzna ani z $(\mathbb{R}, +, -, 0)$ ani z $(\mathbb{R}/\mathbb{Q}, +, -, 0)$, bo $|\mathbb{Q}| = \aleph_0$ a $|\mathbb{R}/\mathbb{Q}| = |\mathbb{R}| \neq \aleph_0$.

Przykład 8 Grupa $S_3/\{e, (12)\}$ nie jest izomorficzna z $\mathbb{Z}_8/\mathbb{Z}_2$ z tych samych powodów.

2.2 OBSERWOWANIE RZĘDU ELEMENTÓW

Definicja 5 Rzędem rz elementu a w grupie nazywamy najmniejszą liczbę naturalną n , taką, że $a^n = e$. Jeżeli taka liczba nie istnieje, to rząd elementu jest nieskończony.

Przykład 9 $rz(\mathbb{Z}_9 \times \mathbb{Z}_3) = 27$. Rzędy pewnych elementów z tej grupy: $rz((3, 1)) = 3$, bo $(3, 1)^3 = (3, 1) + (3, 1) + (3, 1) = (0, 0) = e$. $rz((4, 2)) = 9$, bo $(4, 2)^9 = (0, 0) = e$, a ten element podnoszony do niższych potęg jest różny od e .

Przykład 10 Rzędem podgrupy $(3\mathbb{Z}, +, -, 0)$ grupy $(\mathbb{Z}, +, -, 0)$ jest ∞ . Rząd każdego niezerowego elementu z tej grupy również jest nieskończony, bo podnosząc dowolny element (niezerowy) do dowolnej potęgi uzyskamy jego wielokrotność, a nigdy 0.

Twierdzenie 2 Jeżeli w grupie G istnieje element rzędu n , a w grupie H element o tej własności nie istnieje, to G i H nie są izomorficzne.

(Twierdzenie to jest przydatne, gdy obydwie grupy mają taką samą liczbę elementów).

Dowód (Nie wprost) niech $x \in G \setminus \{0\}$ jest elementem rzędu n , $\varphi : G \rightarrow H$ izomorfizmem grup G i H .

Z definicji homomorfizmu $\varphi(x_1 \cdot x_2) = \varphi(x_1) \cdot \varphi(x_2)$, gdzie $\varphi : G \rightarrow H$. można w sposób indukcyjny wykazać, że dla dowolnego $k \in \mathbb{N}$ zachodzi również

$$\varphi(x_1 \cdot x_2 \cdot \dots \cdot x_k) = \varphi(x_1) \cdot \varphi(x_2) \dots \varphi(x_k),$$

a w szczególności gdy wszystkie $x := x_1 = x_2 = \dots = x_n$ mamy

$$\varphi(x \cdot x \cdot \dots \cdot x) = \varphi(x) \cdot \varphi(x) \dots \varphi(x),$$

czyli $\varphi(x^k) = \varphi(x)^k$.

Zauważmy, że jeżeli x^n jest różny od zera, to $\varphi(x^n)$ również musi być niezerowym elementem (własność izomorfizmu).

1. Jeśli $0 < k < n$ to

$$0 \neq \varphi(x^k) = \varphi(x)^k$$

2. Jeśli $k = n$ to

$$0 = \varphi(x^n) = \varphi(x)^n$$

Oznaczałoby to jednak że $\varphi(x)$ jako element z grupy H jest rzędu n , co przeczy założeniu. \square

Przykład 11 Grupa $(\mathbb{Z}_2 \times \mathbb{Z}_2, +_{2 \times 2}, \bar{}, 0)$ nie jest izomorficzna z $(\mathbb{Z}_4, +_{4, \bar{}}, 0)$, gdyż w tej drugiej grupie istnieje element, którego rząd wynosi 4 (jest to 1, bo $1^4 = 1 + 1 + 1 + 1 = 0$), a w $\mathbb{Z}_2 \times \mathbb{Z}_2$ każdy element jest rzędu 2 lub 1.

Przykład 12 Grupa ilorazowa $(\mathbb{Z}/6\mathbb{Z}, +, \bar{}, [0])$ i $(S_3, \circ, ^{-1}, e)$ nie są izomorficzne, bo w pierwszej z nich element $[1]$ jest rzędu 6. Elementami drugiej z nich są cykle o długości 1, 2 lub 3, więc żaden z nich nie ma rzędu 6.

2.3 INNE SPOSOBY

Pokażemy tylko jeden sposób inny od poprzednich, aby prześledzić różne techniki rozwiązywania takich problemów:

Przykład 13 Pokażemy, że $(\mathbb{Z}, +, \bar{}, 0)$ i $(\mathbb{Q}, +, \bar{}, 0)$ nie są izomorficzne. (Nie wprost) gdyby istniał taki izomorfizm φ , to musiałby istnieć obraz elementu 1: $\varphi(1) = q \in \mathbb{Q}$.

Jednak musiałby istnieć również przeciwobraz $q/2$, np. $\varphi^{-1}(q/2) = z \in \mathbb{Z}$.

Jednak stąd wynika, że:

$$1 = \varphi^{-1}(q) = \varphi^{-1}(q/2 + q/2) = \varphi^{-1}(q/2) + \varphi^{-1}(q/2) = z + z = 2z.$$

Jednak w zbiorze liczb całkowitych nie istnieje taki element z , aby $2z = 1$, co kończy dowód.

Zadanie 1 Udowodnić

$$\begin{aligned} (\mathbb{Z}_2 \times \mathbb{Z}_2, +_{2 \times 2}, \bar{}, (0, 0)) &\cong (\{1, 3, 5, 7\}, \cdot_8, ^{-1}, 0) \cong \\ &\cong (\{e, (12)(34), (13)(24), (14)(23)\}, \circ, ^{-1}, e). \end{aligned}$$

Zadanie 2 Udowodnić

$$(S_3, \circ, ^{-1}, e) \cong G_t,$$

gdzie G_t to grupa wszystkich przekształceń izometrycznych trójkąta.

Zadanie 3 Udowodnić

$$(Z_{12}, +_{12}, ^{-}, 0) \cong (Z_3 \times Z_4, +_{Z_3 \times Z_4}, ^{-}, 0)$$

Spróbować rozwiązać te zadania różnymi sposobami.

Zadanie 4 Udowodnić dla każdego $n \in \mathbb{N}$ zachodzi

$$(\mathbb{Z}, +, ^{-}, 0) \cong (n\mathbb{Z}, +, ^{-}, 0) \cong (\{\dots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \dots\}, \cdot, ^{-1}, 1)$$

Zadanie 5 Udowodnić

$$(\mathbb{Q} \times \mathbb{R} \times \mathbb{Z}, +, ^{-1}, (0, 0, 0)) \cong (\mathbb{Z} \times \mathbb{Q} \times \mathbb{R}, +, ^{-1}, (0, 0, 0))$$

Zadanie 6 Udowodnić, że następujące grupy nie są izomorficzne

$$\begin{aligned} & (S_6, \circ, ^{-1}, e), (Z_{120}, +, ^{-}, 0), \\ & (S_4, \circ, ^{-1}, e), (Z_{24}, +, ^{-}, 0), \\ & (Z_8, +_{8,8}, ^{-}, 0), (Z_4 \times Z_2, +_{4 \times 2, 4 \times 2}, ^{-}, (0, 0)) \end{aligned}$$

Zadanie 7 Sprawdź, czy grupa obrotów i symetrii trójkąta jest izomorficzna z Z_6 czy z S_3 .

Zadanie 8 Sprawdź, czy następujące grupy są izomorficzne:

$$\mathbb{Z}, \mathbb{Z} \times \mathbb{Z}_2,$$

$$\mathbb{Z}/5\mathbb{Z}, G,$$

gdzie G oznacza grupę obrotów pięciokąta,

$$(\{1, -1, i, -i\}, \cdot, ^{-1}, 1), \mathbb{Z}_4,$$

$$(\{1, 3, 5, 7, 9, 11, 13, 15\}, \cdot, ^{-1}, 1), (\{1, 3, 7, 9, 11, 13, 17, 19\}, \cdot, ^{-1}, 1).$$

Zadanie 9 Wskaż dwie grupy dwunastoelementowe, które nie są izomorficzne