O izomorfizmie

Dr Witold WIĘSŁAW

Izomorficzny — słowo pochodzenia greckiego oznaczające: tak samo zbudowany. Pojęcie izomorfizmu (wskazywanie na taką samą budowę różnych struktur matematycznych) jest charakterystycznym dla matematyki XX wieku narzędziem badawczym. Obok podajemy pierwszy z serii artykułów poświęconych temu pojęciu.

Zob. też *Sześć zadań — jedno rozwiązanie*, Delta 1/1974

Gdy przed kilkoma miesiącami Redakcja zaproponowała mi napisanie artykułu o izomorfizmie, pomyślałem sobie — nic prostszego, napiszę, wyślę.... O ludzka naiwności! Wydawałoby się, że nic prostszego, niż napisać artykuł popularny. Zacznijmy więc od początku. Jeżeli w trakcie wykładu okaże się, Drogi Czytelniku, że tempo wykładu jest zbyt szybkie, wróć do miejsca, od którego zacząłeś, i przeczytaj powtórnie.

Można by zacząć mniej więcej tak. Niech A będzie zbiorem niepustym. Każdą funkcję $f\colon A^n = \underbrace{A \times A \times \ldots \times A}_{n \text{ razy}} \to A$, która każdemu uporządkowanemu układowi $(a_1, \ldots, a_n)$ elementów zbioru A przyporządkowuje element $f(a_1, \ldots, a_n)$ zbioru A, nazywamy *działaniem* w zbiorze A. Zbiór A z wyróżnionymi działaniami $f_1, f_2, \ldots, f_m$ nazywamy *algebrą* i oznaczamy $\mathfrak{A} = \langle A; f_1, f_2, \ldots, f_m\rangle$. Jeżeli $\mathfrak{Z} = \langle B; g_1, g_2, \ldots, g_m\rangle$ jest drugą algebrą, w której działania g_j zależą od tej samej liczby zmiennych, co f_j, dla każdego $j = 1, 2, \ldots, m$, to funkcję różnowartościową $\varphi\colon A \to B$, odwzorowującą zbiór A na B, nazywamy izomorfizmem algebr $\mathfrak{A}$ i $\mathfrak{Z}$, jeżeli warunki

(1) $\quad g_i(\varphi(a_1), \varphi(a_2), \ldots, \varphi(a_{s_i})) = \varphi(f_i(a_1, a_2, \ldots, a_{s_i})),\ i = 1, 2, \ldots, m,$

spełnione są dla każdego układu $a_1, a_2, \ldots, a_{s_i}$ elementów zbioru A (s_i oznacza liczbę zmiennych działania f_i).

Przykłady

A. Niech $\mathfrak{A}$ i $\mathfrak{Z}$ będą grupami, tzn. możemy przyjąć, że $\mathfrak{A} = \langle A; f_1, f_2\rangle$, $\mathfrak{Z} = \langle B; g_1, g_2\rangle$, $f_1(a_1, a_2) = a_1a_2$ (mnożenie w A), $f_2(a) = a^{-1}$, $g_1(b_1, b_2) = b_1b_2$ (mnożenie w B), $g_2(b) = b^{-1}$. Wtedy warunki (1) odczytujemy jako „zwykłą" definicję izomorfizmu: $\varphi(a_1a_2) = \varphi(a_1)\varphi(a_2)$, $\varphi(a^{-1}) = (\varphi(a))^{-1}$, $\varphi\colon A \xrightarrow[\text{na}]{} B$ i φ jest funkcją różnowartościową.

B. Jeżeli $\mathfrak{A}$ i $\mathfrak{Z}$ są pierścieniami, to jednym z działań jest dodawanie a drugim mnożenie, tzn. $\mathfrak{A} = \langle A; f_1, f_2\rangle$, $\mathfrak{Z} = \langle B; g_1, g_2\rangle$, $f_1(a_1, a_2) = a_1 + a_2$, $f_2(a_1, a_2) = a_1a_2$, $g_1(b_1, b_2) = b_1 + b_2$, $g_2(b_1, b_2) = b_1b_2$. Stosując (1) w tym szczególnym przypadku, dostajemy znów klasyczną definicję izomorfizmu pierścieni.

Wyczuwam, że należy przerwać. W ten sposób na pewno nie wyjaśnię Czytelnikowi, czym jest izomorfizm, a już na pewno zniechęcę Go do matematyki. Zbyt to wszystko jest podręcznikowe.

Spróbujmy więc nieco inaczej. W tym celu przyjmijmy najpierw pojęcie grupy.

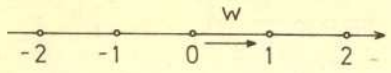
Grupą nazywamy niepusty zbiór G, wraz z ustaloną funkcją $G \times G \to G$, zwaną dalej działaniem, albo mnożeniem w grupie G, która każdej parze uporządkowanej (a, b) elementów z G przyporządkowuje element $ab \in G$, spełniającą następujące warunki:

1. działanie jest łączne, tzn. $a(bc) = (ab)c$ dla każdych $a, b, c \in G$;
2. istnieje element neutralny e w G, tzn. element spełniający warunek $ae = ea = a$ dla każdego $a \in G$;
3. każdy element $a \in G$ ma element odwrotny $a^{-1} \in G$, tzn. $aa^{-1} = a^{-1}a = e$.

Grupa przemienna to grupa, w której każda para elementów a, b spełnia $ab = ba$.

Jeżeli G jest grupą z działaniem $(a, b) \to ab$, a H — grupą z działaniem $(c, d) \to c * d$, to odwzorowanie $\varphi\colon G \to H$ zbioru G na zbiór H nazywamy izomorfizmem grup G i H, jeżeli warunek $\varphi(ab) = \varphi(a) * \varphi(b)$ spełniony jest dla każdego $a, b \in G$. Powyższy fakt zapisujemy krótko $G \simeq H$, co czytamy „grupa G jest izomorficzna z grupą H". Ażeby zdać sobie sprawę z istoty wprowadzonego pojęcia, rozważmy kilka przykładów.

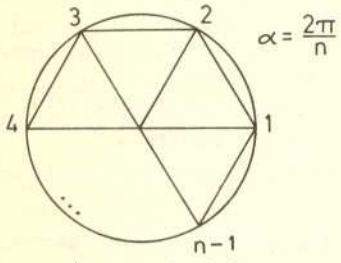
Przykład I. Niech Z^+ będzie zbiorem liczb całkowitych, z dodawaniem. Jest to grupa przemienna — elementem neutralnym jest zero, bo $a + 0 = 0 + a = a$ dla każdego $a \in Z^+$, a przemienność dodawania liczb jest faktem wszystkim dobrze znanym (element odwrotny do a nazywany jest w tej grupie na ogół elementem przeciwnym do a).



Rys. 1

$+ \pmod n$	0	1	2	...	$n-1$
0	0	1	2	...	$n-1$
1	1	2	3	...	0
2	2	3	4	...	1
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
$n-1$	$n-1$	0	1	...	$n-2$

Rys. 2



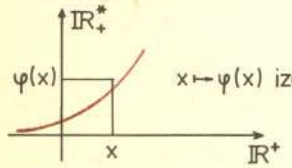
$$\vartheta_{k\alpha} \circ \vartheta_{l\alpha} = \begin{cases} \vartheta_{(k+l)\alpha} & 0 \leqslant k+l < n \\ \vartheta_{s\alpha} & n \leqslant k+l,\ k+l = nq+s,\ 0 \leqslant s < n \end{cases}$$

Rys. 3

$\circ$	ϑ_0	ϑ_α	$\vartheta_{2\alpha}$	...	$\vartheta_{(n-1)\alpha}$
ϑ_0	ϑ_0	ϑ_α	$\vartheta_{2\alpha}$	...	$\vartheta_{(n-1)\alpha}$
ϑ_α	ϑ_α	$\vartheta_{2\alpha}$	$\vartheta_{3\alpha}$	...	ϑ_0
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
$\vartheta_{(n-1)\alpha}$	$\vartheta_{(n-1)\alpha}$	.	.	.	$\vartheta_{(n-2)\alpha}$

Rys. 4

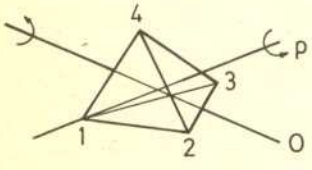
Zob. też *Urojony sprzymierzeniec*, Delta 3/1974



$\mathbb{R}_+^* = \{x \in \mathbb{R}: x > 0\}$

$\mathbb{R}^+$ – grupa addytywna liczb rzeczywistych

Rys. 5



$G = \{O_1, O_2, \cdots, O_{12}\}$

Rys. 6

Przykład II. Zbiór P przesunięć prostej o całkowite wielokrotności niezerowego wektora w jest grupą względem składania przesunięć (rys. 1). Jeżeli p_v oznacza przesunięcie o wektor v, a $nw = w+w+ \ldots +w$ (n razy) gdy n jest liczbą naturalną, $(-n)w = (-w)+(-w)+ \ldots +(-w)$ (n razy), to

$$p_{kw} \circ p_{lw} = p_{(k+l)w};\quad k,\ l \in Z^+. \tag{2}$$

Grupa Z^+ jest izomorficzna z P; wystarczy zdać sobie sprawę z tego, że każda liczba całkowita k wyznacza przesunięcie p_{kw} i na odwrót. Reszty dopełnia wzór (2) wraz z uwagą, że funkcja $k \to p_{kw}$ ze zbioru Z^+ na zbiór P jest różnowartościowa. Gdyby jednak ktoś chciał przeprowadzić drobiazgowy dowód, wystarczy określić $\varphi\colon Z^+ \to P$ wzorem $\varphi(k) = p_{kw}$ i sprawdzić, że φ jest izomorfizmem.

Przykład III. Niech Z_n^+ oznacza zbiór liczb $\{0, 1, \ldots, n-1\}$, w którym za działanie przyjmujemy *dodawanie modulo n*, tzn. $s = a+b \pmod n$, jeżeli s jest nieujemną resztą z dzielenia $a+b$ przez n. Np. $3+4 \pmod 5 = 2$, bo $3+4 = 7 = 5+2$, a $8+12 \pmod{14} = 6$, bo $8+12 = 20 = 14+6$. Czytelnik sprawdzi, że Z_n^+ jest grupą.

Przykład IV. Zbiór C_n obrotów n-kąta foremnego wokół jego środka jest grupą: elementem neutralnym jest obrót ϑ_0 o kąt 0, a elementem odwrotnym do ϑ_β jest obrót $\vartheta_{-\beta}$, tzn. $\vartheta_\beta^{-1} = \vartheta_{-\beta}$ (rys. 3). Tabelka (rys. 4) opisuje wyniki działań $\vartheta_{k\alpha} \circ \vartheta_{l\alpha}$ ($\vartheta_{k\alpha}$ w pierwszej kolumnie, $\vartheta_{l\alpha}$ w pierwszym wierszu).

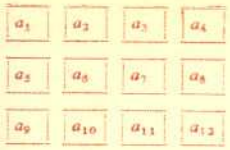
Przykład V. (Czytelnik, który nie zna liczb zespolonych, może, nie tracąc wiele, pominąć ten przykład). Niech E_n będzie zbiorem wszystkich rozwiązań równania $x^n - 1 = 0$ w zbiorze C liczb zespolonych. Można od razu zauważyć (bez znajdowania rozwiązań), że E_n jest grupą względem mnożenia. (Przy okazji: czy Czytelnik zna inny przykład wielomianu, którego pierwiastki tworzą grupę względem mnożenia?) Wynika to z poniższych równości: $(x_1x_2)^n = x_1^n x_2^n = 1 \cdot 1 = 1$, $(x^{-1})^n = (x^n)^{-1} = 1$, jeżeli tylko $x_1, x_2 \in E_n$. Ponieważ każdy wielomian stopnia $n \geqslant 1$, o współczynnikach z C, ma n pierwiastków w C (fakt ten tradycyjnie nazywany jest „zasadniczym twierdzeniem algebry", choć dawno już są w algebrze twierdzenia bardziej „zasadnicze"), więc grupa E_n ma n elementów. Są to liczby $1, \varepsilon_n, \varepsilon_n^2, \ldots, \varepsilon_n^{n-1}$, gdzie $\varepsilon_n = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$.

I tym razem można odwołać się do rys. 3, z tym jednak, że teraz koło leży na płaszczyźnie C liczb zespolonych, ma promień równy 1, a jego k-tym wierzchołkiem jest ε_n^{k-1} ($k = 1, 2, \ldots, n$).

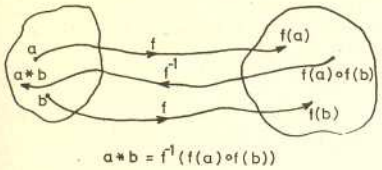
W trzech ostatnich przykładach rzuca się w oczy podobieństwo rozpatrywanych sytuacji. W każdym z przykładów wykonanie działania sprowadza się do dodania (modulo n) dwóch liczb. Mówiąc ściślej, wszystkie trzy grupy: Z_n^+, C_n, E_n są izomorficzne. Czytelnika, którego moje sugestie nie przekonały, zachęcam do sprawdzenia, że funkcja $\varphi\colon Z_n^+ \to C_n$, $\varphi(k) = \vartheta_{k\alpha}$ ($k = 0, 1, \ldots, n-1$) jest izomorfizmem grupy Z_n^+ z grupą C_n, a $\psi\colon C_n \to E_n$, $\psi(\vartheta_{k\alpha}) = \varepsilon_n^k$ ($k = 0, 1, \ldots, n-1$) jest izomorfizmem grupy C_n z grupą E_n.

Przykład VI. (rys. 5) Niech R^+ oznacza grupę addytywną liczb rzeczywistych (zbiór R z dodawaniem), a R_+^* — półoś liczb dodatnich. Sprawdzenie, że R^+ jest grupą względem dodawania, a R_+^* grupą względem mnożenia liczb, wymaga znajomości jedynie najprostszych własności liczb rzeczywistych. Ale fakt, że obie grupy są izomorficzne, jest (w pierwszej chwili) dość nieoczekiwany. Zamiast odwoływać się do intuicji, tym razem wspólnie przeprowadźmy dowód. Niech $\varphi(x) = 3^x$. Oczywiście $\varphi\colon R^+ \to R_+^*$ (rys. 5). Funkcja φ jest różnowartościowa, jako funkcja rosnąca i odwzorowuje R^+ na R_+^*, bo każda liczba dodatnia y ma logarytm $\log_3 y$. Wreszcie równość $\varphi(x+y) = 3^{x+y} = 3^x 3^y = \varphi(x)\,\varphi(y)$; $x, y \in R^+$ jest znaną własnością potęgowania liczb rzeczywistych, co równocześnie kończy dowód.

Przykład VII. Niech G oznacza zbiór wszystkich obrotów czworościanu foremnego. Bez trudu wskazujemy 12 obrotów: identycznościowy, 2 obroty wokół każdej osi P (rys. 6) przechodzącej przez wierzchołek czworościanu i środek przeciwległej ściany, tzn. $2 \cdot 4 = 8$ obrotów, 3 obroty wokół osi łączących środki nierównoległych krawędzi (np. oś Q na rys. 6). Wynika stąd, że grupa G ma co najmniej 12 elementów. Wykażemy teraz, że ma ich nie więcej niż 12, skąd wyniknie, że G jest zbiorem dwunastoelementowym. Niech $g \in G$ będzie dowolnym obrotem czworościanu i niech przeprowadza on pierwszy wierzchołek na j-ty, tzn. $g(1) = j$.



Rys. 7



$a * b = f^{-1}(f(a) \circ f(b))$

Rys. 8

Jeżeli $a \in G$ jest dowolnym obrotem przeprowadzającym pierwszy wierzchołek na j-ty, $a(1) = j$, to $b = a^{-1} \circ g$ pozostawia pierwszy wierzchołek na swoim miejscu: $b(1) = a^{-1} \circ g(1) = a^{-1}(g(1)) = a^{-1}(j) = 1$. Element G można zatem zapisać (co najmniej jednym sposobem) w postaci $g = a \circ b$, gdzie $a, b \in G$ i $a(1) = g(1)$, $b(1) = 1$. Wynika stąd, że liczba elementów zbioru G nie przekracza liczby wszystkich par uporządkowanych (a, b). Ponieważ a przeprowadza pierwszy wierzchołek na któryś z pozostałych, więc są cztery możliwości na a. Podobnie, są trzy możliwości na b. Oznacza to, że wszystkich możliwych par jest 12, tzn. G jest zbiorem mającym nie więcej niż 12 elementów. Można przekonać się łatwo, że grupa obrotów czworościanu foremnego nie jest przemienna. Czytelnik odnotuje, że są co najmniej dwie nieizomorficzne grupy dwunastoelementowe: przemienna grupa C_{12} (**Przykład IV**, $n = 12$) i (nieprzemienna) grupa G.

Czy każdy zbiór może być grupą? Aby uniknąć zbyt zawiłych rozważań, przeformułujmy postawione pytanie na nieco mniej ogólne zadanie.

W klasie jest 12 ławek (rys. 7). Czy zbiór A tych ławek można przekształcić w grupę? Wyjaśnienie zawarte jest na rysunku 8. Ponieważ grupy izomorficzne są równoliczne (mają tę samą liczbę elementów), a znamy przykłady grup dwunastoelementowych (np. grupa G z przykładu VII), więc postaramy się przekształcić zbiór A w grupę izomorficzną z G. Niech $a_1, a_2, \ldots, a_{12}$ będzie jakąkolwiek numeracją ławek, a $\vartheta_1, \vartheta_2, \ldots, \vartheta_{12}$ — ustaloną numeracją elementów grupy G. Określmy funkcję $f\colon A \to G$, ustalającą równoliczność tych zbiorów, wzorem $f(a_i) = \vartheta_i$ $(i = 1, 2, \ldots, 12)$. Aby znaleźć „iloczyn" $a * b$ dwóch ławek a i b, znajdujemy najpierw obroty $f(a)$, $f(b)$ przyporządkowane tym ławkom, wykonujemy działanie $f(a) \circ f(b)$, a następnie odczytujemy, jakiemu elementowi zbioru A został przyporządkowany element $f(a) \circ f(b)$. Jest nim $f^{-1}(f(a) \circ f(b))$ (funkcja f jest różnowartościowa!). W ten sposób dowolny zbiór A, równoliczny z grupą G, można przekształcić w grupę izomorficzną z grupą G. Jeżeli bowiem przepisać otrzymany warunek, będący definicją działania w A: $a * b = f^{-1}(f(a) \circ f(b))$, w postaci równoważnej: $f(a * b) = f(a) \circ f(b)$, to odczytamy, że f jest izomorfizmem grupy A (z działaniem „$*$") z grupą G (z superpozycją „$\circ$" jako działaniem). Przypomnijmy, że f było dowolną funkcją ustalającą równoliczność zbiorów A i G. Ale możemy przecież w dowolny sposób przenumerować ławki i powtórzyć konstrukcję, już z nową numeracją. Zmiana numeracji ławek to nic innego, jak permutacja zbioru A (permutacją zbioru skończonego nazywamy każdą funkcję różnowartościową odwzorowującą ten wzór w siebie). Ponieważ zbiór dwunastoelementowy A ma $12! = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 = 479001600$ permutacji, więc tym samym skonstruowaliśmy prawie pół miliarda izomorficznych, choć różnych grup!

Nasuwa się teraz spostrzeżenie, że izomorfizm pozwala zaniedbać własności fizyczne elementów grupy. Mówiąc poglądowo, grupy izomorficzne mają te same własności. Na przykład, jeżeli $\varphi\colon G \to H$ jest izomorfizmem grup G i H, oraz $g \in G$ jest elementem, który spełnia warunek $g^2 = e_G$ (e_G — element neutralny grupy G; podobne znaczenie ma e_H), $g \neq e_G$, to $\varphi(g) \neq e_H$ i $\varphi(g)^2 = e_H$. Istotnie, ponieważ $g \neq e_G$, więc $\varphi(g) \neq \varphi(e_G) = e_H$ (dlaczego?), bo φ jest funkcją różnowartościową; ponadto $\varphi(g)^2 = \varphi(g^2) = \varphi(e_G) = e_H$.

W sposób podobny do opisanego można mówić o izomorfizmie pierścieni, czy też izomorfizmie ciał, ale o tym może innym razem.

Zadania

1. Wykazać, że grupa n-elementowa nie może być izomorficzna z grupą m-elementową, jeśli $m \neq n$.

2. Podać przykład dwóch nieizomorficznych grup, które mają tę samą liczbę elementów.

3. Czy zbiór obrotów kuli wokół jej środka (będący grupą względem składania obrotów) jest grupą izomorficzną z grupą obrotów koła ze składaniem obrotów, jako działaniem?

4. Udowodnić, że relacja „być izomorficznym" jest zwrotna, symetryczna i przechodnia: $G \simeq G$; $G \simeq H \to H \simeq G$; $G \simeq H$ i $H \simeq N \Rightarrow G \simeq N$.

5. Wykazać, że grupa izomorficzna z grupą przemienną jest przemienna.

6. Podzbiór H grupy G nazywamy podgrupą grupy G, jeżeli jest grupą względem tego samego działania. Wykazać, że $\{1\}$, $\{-1, 1\}$ są jedynymi skończonymi podgrupami grupy $\boldsymbol{R}^*$ niezerowych liczb rzeczywistych (względem mnożenia liczb).

7. Wykazać, że $\{0\}$ jest jedyną skończoną podgrupą grupy $\boldsymbol{R}^+$.