Grupa

Jeśli $X = \{1, \ldots, n\}$, to S_X jest zbiorem permutacji n-elementowego zbioru; oznaczamy go jako S_n.

Zainteresowanemu Czytelnikowi polecamy *Wstęp do teorii grup* Czesława Bagińskiego.

Ustalmy zbiór X, np. $X = \{1, 2, \ldots, 2019\}$. Niech S_X oznacza zbiór funkcji odwracalnych z X w X. Funkcje z S_X można składać i odwracać, nie wychodząc poza S_X. W zbiorze S_X istnieje też funkcja identycznościowa. Tytułowe *grupy* są abstrakcyjnym sposobem wyrażenia powyższych własności zbioru S_X.

Grupa to zbiór G wraz z *działaniem mnożenia*, czyli funkcją $G \times G \to G$ oznaczaną $(g_1, g_2) \mapsto g_1 \cdot g_2$, elementem neutralnym $1_G \in G$ oraz działaniem odwracania $g \to g^{-1}$. Działania mnożenia i odwracania oraz element neutralny są częścią definicji grupy i wymagamy, by spełniały one wszystkie naturalne własności z przykładu S_X (patrz margines).

Te „naturalne własności" sprowadzają się do trzech:
- $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$,
- $g \cdot g^{-1} = g^{-1} \cdot g = 1_G$,
- $1_G \cdot g = g \cdot 1_G = g$ dla wszystkich $g_1, g_2, g_3, g \in G$.

Nie wymagamy, by $g_1 \cdot g_2 = g_2 \cdot g_1$. Faktycznie, już dla $n \geqslant 3$ istnieją permutacje $g_1, g_2 \in S_n$ takie, że $g_1 g_2 \neq g_2 g_1$ (czy Czytelnik umie je znaleźć?). Grupy spełniające warunek $g_1 g_2 = g_2 g_1$ dla wszystkich elementów g_1, g_2 nazywamy *przemiennymi*.

Przykładowo, zbiór S_X, w którym „mnożenie" to składanie funkcji, odwracanie to odwracanie funkcji, a jedynka to funkcja identycznościowa, jest grupą. Zbiór $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ ze zwykłym mnożeniem i odwracaniem także jest grupą, podobnie zbiór $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. Zbiór $\mathbb{Z} \setminus \{0\}$ z mnożeniem i dzieleniem *nie* jest grupą, bo odwrotność liczby całkowitej zwykle nie jest liczbą całkowitą. Jeśli p jest liczbą pierwszą, to zbiór $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ z mnożeniem modulo p *jest* grupą, bo z algorytmu Euklidesa wynika, że dla każdej liczby $a \in \{1, \ldots, p-1\}$ istnieją liczby całkowite r, s takie, że $ar + ps = 1$; reszta z dzielenia r przez p jest odwrotnością a. Grupą jest także zbiór $\mathbb{Z}$, w którym „mnożenie" to dodawanie, zaś „odwrotność" to $a \mapsto -a$. Podobnie, zbiór $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ z dodawaniem modulo n jest grupą. Notabene, twierdzenie o generatorze z teorii liczb mówi, że grupa $\mathbb{Z}_p^*$ jest *izomorficzna* z grupą $\mathbb{Z}_{p-1}$. Wreszcie, jeszcze bardziej egzotyczne grupy pojawiają się w kryptografii (patrz „Krzywe eliptyczne w kryptografii", Δ_{18}^8).

– Jasiu, ile to pięć razy siedem?
– A jaka jest struktura grupy, psze Pani?

Izomorfizm grup G i H to bijekcja $\varphi\colon G \to H$ taka, że zachodzi $\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$ dla wszystkich $g_1, g_2 \in G$. Wspomniany izomorfizm np. dla $p = 5$ można łatwo wskazać: jest to funkcja $\varphi\colon \mathbb{Z}_4 \to \mathbb{Z}_5^*$ zadana wzorem $\varphi(i) = 2^i \mod 5$. Konkretniej mówiąc: $(\varphi(0), \varphi(1), \varphi(2), \varphi(3)) = (1, 2, 4, 3)$. Liczba 2 zwana jest *generatorem* grupy $\mathbb{Z}_5^*$.

Podgrupa grupy G to podzbiór $H \subset G$ taki, że działania wykonywane na elementach z H dają w wyniku element z H. Formalnie mówiąc, dla każdych $h_1, h_2 \in H$ zachodzi $h_1 \cdot h_2 \in H$ oraz $h_1^{-1} \in H$. Jedno z podstawowych twierdzeń teorii grup mówi, że każda grupa G jest podgrupą S_X dla odpowiednio dużego zbioru X. Definicja grupy nie odchodzi więc zbyt daleko od przykładu S_X. Jeśli H jest podgrupą G, to zbiór G/H powstaje z G przez utożsamienie elementów g i hg dla każdych $g \in G$, $h \in H$. Prawdziwy jest następujący elegancki wzór: $|G/H| = |G|/|H|$, a zatem liczność podgrupy jest zawsze dzielnikiem liczności grupy.

Czytelnik Uważny powinien sprawdzić, że $\{1_G\}$ jest podgrupą, i zauważyć analogię pomiędzy grupami prostymi a liczbami pierwszymi.

Specjalną klasą podgrup są **podgrupy normalne**. Podgrupa $H \subset G$ jest normalna, jeśli zachodzi $g \cdot h \cdot g^{-1} \in H$ dla każdych $g \in G$, $h \in H$. Ten dziwaczny warunek pozwala wprowadzić na zbiorze G/H strukturę grupy. W każdej grupie G podgrupami normalnymi są G i $\{1_G\}$. Grupy, które nie mają innych podgrup normalnych, nazywane są *prostymi*, np. grupa $\mathbb{Z}_p$ jest prosta (gdyż rozmiar podgrupy musi być dzielnikiem rozmiaru grupy), a grupa $\mathbb{Z}$ nie jest. W XX wieku sklasyfikowano wszystkie grupy proste. Tworzą one 18 „rodzin" i 26 „nieoczekiwanych" grup sporadycznych. Te ostatnie święcą dziś triumfy w matematycznych modelach teorii strun, w ramach tzw. *moonshine theory*.

Dlaczego jednak grupy pojawiają się w innych gałęziach matematyki i fizyki? Okazuje się, że grupy dobrze obrazują (odwracalne) działania na obiektach. Grupa S_X w naturalny sposób *działa* na zbiorze X: jeśli weźmiemy element $x \in X$ oraz $f \in S_X$, to możemy otrzymać nowy element $f(x)$.

Jak poprzednio, tworzymy z tego abstrakcyjną definicję: **działanie grupy G na zbiorze X** jest to odwzorowanie $G \times X \to X$, zapisywane jako $(g, x) \mapsto g \cdot x$, takie że $1_G \cdot x = x$ oraz $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$.

Grupa S_3 działa na wierzchołkach trójkąta równobocznego ABC, permutując je. Działanie to można utożsamić z „geometrycznym" działaniem przez odbicia względem symetralnych boków trójkąta oraz obroty względem środka ciężkości. Na wierzchołkach tego trójkąta działa również na przykład grupa $\mathbb{Z}_3$ – działanie $k \in \mathbb{Z}_3$ na wierzchołku x to jego (wspomniany już) obrót o kąt $k \cdot 120°$.

To właśnie działania grup czynią grupy tak interesującymi i wszechobecnymi obiektami w matematyce. Żeby zobaczyć to lepiej, rozważmy przypadek, gdy X ma dodatkową strukturę, np. gdy niektóre pary elementów X połączymy, otrzymując graf $\Gamma = (X, E)$. W tej sytuacji możemy zadać następujące pytania:

- Które elementy $g \in S_X$ spełniają warunek $g \cdot \Gamma = \Gamma$? Zbiór takich elementów nazywamy **stabilizatorem** Γ. Stabilizator jest naturalnie podgrupą S_X. Oznaczamy go G_Γ.
- Które grafy można otrzymać z Γ przez permutowanie wierzchołków? Zbiór takich grafów nazywamy **orbitą** Γ przy działaniu G i oznaczamy $G \cdot \Gamma$.
- Jeśli popatrzymy na zbiór $\mathcal{M}$ wszystkich możliwych grafów o wierzchołkach X, to ile jest orbit? Zbiór orbit oznaczamy przez $\mathcal{M}/G$.

Warto sprawdzić, że jedyne grafy ze stabilizatorem równym S_X to graf pełny oraz graf pusty. Zachodzi też równanie $|G_\Gamma| \cdot |G \cdot \Gamma| = |G|$. Wynika stąd, że im większa orbita, tym mniejszy stabilizator, a ponadto: liczby $|G_\Gamma|$, $|G \cdot \Gamma|$ są dzielnikami G. Znacznie bardziej skomplikowane jest sprawdzenie, ile jest orbit, czyli ile elementów ma zbiór $\mathcal{M}/G$. Tym niemniej czasem można powiedzieć coś o orbitach, mając bardzo niewiele danych:

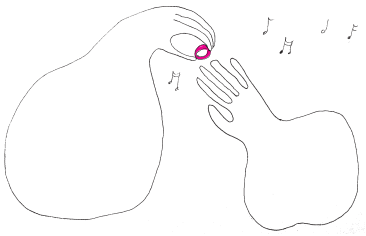
Lemat. *Jeśli p jest pierwsza, grupa G ma p^k elementów i działa na zbiorze $\mathcal{M}$, który ma niepodzielną przez p liczbę elementów, to istnieje element stały, tzn. $\Gamma \in \mathcal{M}$ taki, że $g \cdot \Gamma = \Gamma$ dla wszystkich $g \in G$.*

Dowód. Faktycznie, $\mathcal{M}$ jest sumą orbit, a rozmiar każdej orbity dzieli $|G| = p^k$. Jeśli żadna orbita nie jest jednoelementowa, to rozmiar każdej jest podzielny przez p, zatem i $|\mathcal{M}|$ jest podzielna przez p. Sprzeczność. A więc istnieje Γ takie, że $G \cdot \Gamma = \{\Gamma\}$. □

Zamiast grafów można podobnie analizować inne obiekty. Jeśli będziemy patrzeć na przestrzenie liniowe, to otrzymamy *teorię reprezentacji*, jeśli na *ciała* (patrz poniżej), to teorię Galois, itd. Wreszcie, aby lepiej zrozumieć same grupy, warto badać działania grup na grupach.

Joachim JELISIEJEW

Pierścień



Kolejnym fundamentalnym pojęciem algebraicznym są pierścienie. Zostały one wprowadzone pod koniec XIX wieku z nadzieją na pomoc w udowodnieniu Wielkiego Twierdzenia Fermata. Jak wiadomo, zostało to uczynione dopiero w 1995 roku, więc przez długi czas nadzieja ta była płonna.

Modelowym przykładem pierścienia jest zbiór liczb całkowitych $\mathbb{Z}$. Formalnie, **pierścień przemienny** R to zbiór z działaniami dodawania, odejmowania i mnożenia, przy czym spełnione są naturalne własności: R z dodawaniem i odejmowaniem jest grupą, jest rozdzielność mnożenia względem dodawania, a mnożenie jest łączne i przemienne i posiada jedynkę.

Inne przykłady pierścieni przemiennych to $\mathbb{Q}$ lub $\mathbb{R}$ z naturalnymi działaniami. Przykład z innej półki: jeśli X jest przestrzenią metryczną (patrz str. 6) lub ogólniej przestrzenią topologiczną, to zbiór $C(X, \mathbb{R})$ wszystkich ciągłych funkcji z X do $\mathbb{R}$ jest pierścieniem przemiennym.

Ideał w pierścieniu przemiennym A jest to podgrupa $I \subset A$ taka, że $a \cdot i \in I$ dla wszystkich $a \in A$ oraz $i \in I$. Ten warunek gwarantuje, że w zbiorze A/I da się sensownie mnożyć; tzn. że A/I jest pierścieniem przemiennym. W tym sensie ideał odpowiada podgrupie normalnej. Ideał $I \subsetneq A$ jest **maksymalny**, jeśli nie istnieje ideał $J \subsetneq A$ taki, że $I \subsetneq J$. Każde A posiada przynajmniej dwa ideały: A oraz $\{0\}$. Mówimy, że A jest **ciałem**, jeśli nie posiada żadnych innych ideałów, np. $\mathbb{Q}$, $\mathbb{R}$ są ciałami, lecz $\mathbb{Z}$ nie jest ciałem.

W pierścieniu $\mathbb{Z}$ jedyne ideały są postaci $n\mathbb{Z} = \{n \cdot a \mid a \in \mathbb{Z}\}$. Ideał $n\mathbb{Z}$ jest maksymalny, jeśli $|n|$ jest liczbą pierwszą.

Jeśli X jest przestrzenią topologiczną i $x \in X$, to podzbiór

$$\mathfrak{m}_x = \{f \in C(X, \mathbb{R}) |\ f(x) = 0\}$$

jest ideałem maksymalnym. Co więcej, jeśli X jest zwartą przestrzenią (dla przestrzeni metrycznej zwartość oznacza, że każdy ciąg zawiera podciąg zbieżny), są to jedyne ideały maksymalne w $C(X, \mathbb{R})$. Zatem jeśli ktoś roztargniony zgubi swoją ulubioną przestrzeń topologiczną X, ale będzie pamiętać, jaki jest pierścień B funkcji ciągłych na tej przestrzeni, to może zrekonstruować X. Mianowicie, punktami X będą ideały maksymalne w B, a zbiory domknięte to zbiory ideałów maksymalnych postaci $V(E) = \{\mathfrak{m} \mid \mathfrak{m} \supset E\}$, gdzie $E \subset B$ jest podzbiorem.

W latach pięćdziesiątych Alexandre Grothendieck zaproponował, by tę operację „odzyskiwania" X z B przeprowadzać dla dowolnego pierścienia B; niekoniecznie pochodzącego od X. Doprowadziło to do powstania *teorii schematów*, która ostatecznie miała wielki udział m.in. w dowodzie Wielkiego Twierdzenia Fermata. Po stu latach pierścienie miały swój rewanż!

Joachim JELISIEJEW

Rozwiązanie zadania M 1597.
Zauważmy, że

$$a + \sqrt{a^2+1} = \frac{1}{\sqrt{b^2+1}+b} = \sqrt{b^2+1} - b,$$
$$b + \sqrt{b^2+1} = \frac{1}{\sqrt{a^2+1}+a} = \sqrt{a^2+1} - a.$$

Dodając stronami te dwie równości, uzyskujemy $a + b = -(a + b)$, czyli $a + b = 0$.

Łatwo sprawdzić, że liczby a, b spełniające założenia zadania rzeczywiście istnieją (np. $a = b = 0$), więc znaleziona wartość 0 istotnie jest osiągalna.