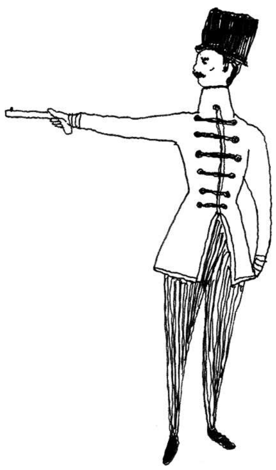
Pojedynek, symetrie i potwór – klasyfikacja grup prostych

Gabriela MAJEWSKA[*]

Śmierć młodego geniusza. 30 maja 1832 roku w Paryżu zginął w pojedynku młody matematyk, Evariste Galois. Nie ma pewności, czy pojedynek ten miał podłoże polityczne, czy też Galois bronił honoru pewnej młodej damy. W pożegnalnym liście poprosił on, by jego notatki wysłać Jacobiemu albo Gaussowi. Żaden z tych wielkich matematyków nigdy nie zobaczył jednak zapisków Galois.

Jedną z wersji tych zdarzeń zawiera powieść Leopolda Infelda *Wybrańcy bogów*. Infeld, wybitny polski fizyk, napisał ją w celach zarobkowych, gdy za młodu był nieetatowym współpracownikiem Einsteina.



Czternaście lat później inny znany matematyk, Liouville, opublikował wyniki Galois razem z komentarzami. Co jednak było w nich aż tak interesującego? Galois zajmował się problemem istnienia wzorów na pierwiastki równań danych przez wielomiany. Większość Czytelników zna wzór na pierwiastki równania drugiego stopnia, słynne *be kwadrat minus cztery a ce*, a nieliczni słyszeli również o wzorach Cardano na rozwiązania równania stopnia trzeciego, czy Ferrariego, które stosujemy przy równaniach stopnia czwartego. Czy można w podobny sposób opisać rozwiązania dowolnego równania stopnia piątego?

Galois zauważył, że mimo iż na mocy Zasadniczego Twierdzenia Algebry równanie piątego stopnia ma aż pięć pierwiastków, to pierwiastki te nie są całkowicie niezależne – tworzą one grupy, a w każdej takiej grupie można zaobserwować pewne zależności, symetrie między pierwiastkami. Geniusz Galois polegał na tym, że skupił się on na tych symetriach, a nie na samych pierwiastkach.

Zmianę kolejności elementów w zbiorze nazywamy permutacją. Galois zainteresował fakt, że jeśli użyjemy najpierw jednej permutacji, a potem drugiej, to możemy tej parze przypisać trzecią permutację, która da ten sam efekt. Galois nazwał taki system łączenia permutacji *grupą permutacji*. Kluczowym pomysłem jego pracy było rozkładanie grup permutacji na prostsze grupy, które współczesny matematyk, Mark Ronan (*Symmetry and the Monster*, Oxford University Press, 2006), nazywa *atomami symetrii*. Nazwa ta jest trafna – *atom* pochodzi od greckiego *niepodzielny*, więc to określenie pasuje do grup, których na prostsze rozłożyć się nie da. Mniej romantyczna nazwa tych atomów to *grupy proste*.

Zamiast objaśniać, co to jest grupa prosta, łatwiej jest pokazać, co to znaczy, że grupa nie jest prosta. Oto przykład.

Trójkąt równoboczny można z powrotem położyć na tym samym miejscu na 6 sposobów. Te przemieszczenia, zwane *grupą izometrii własnych* trójkąta równobocznego, to trzy symetrie względem prostych zawierających wysokości i trzy obroty o 0°, 120° i 240° względem punktu ich przecięcia. Te obroty tworzą mniejszą, trójelementową grupę obrotów, symetrie zaś grupy nie tworzą. Możemy natomiast rozważyć grupę dwuelementową, której elementami będą: zbiór $\mathcal{R}$ obrotów i zbiór $\mathcal{S}$ symetrii. Działanie w tej grupie określa tabelka

$\times$	$\mathcal{R}$	$\mathcal{S}$
$\mathcal{R}$	$\mathcal{R}$	$\mathcal{S}$
$\mathcal{S}$	$\mathcal{S}$	$\mathcal{R}$

bowiem złożenie dowolnego przekształcenia z $\mathcal{R}$ z dowolnym przekształceniem z $\mathcal{R}$ daje przekształcenie z $\mathcal{R}$, złożenie dowolnego przekształcenia z $\mathcal{R}$ z dowolnym przekształceniem z $\mathcal{S}$ daje przekształcenie z $\mathcal{S}$ i tak dalej.

Można więc powiedzieć, że grupę izometrii własnych trójkąta równobocznego rozłożyliśmy na grupę trój- i dwuelementową.

Powiemy, że zbiór permutacji P *generuje* grupę G, jeśli dowolną permutację z G możemy przedstawić jako złożenie potęg elementów zbioru P, gdzie *potęga* permutacji p to jej wielokrotne złożenie. Grupa G jest cykliczna, jeśli generuje ją jeden element. *Rzędem grupy G* nazywamy liczbę jej elementów, zaś rząd elementu p to moc grupy generowanej przez ten element. Pierwsze atomy symetrii, jakie udało się znaleźć, to grupy cykliczne o rzędach będących liczbami pierwszymi. Jakie są inne atomy? Czy możemy te atomy w jakiś sposób sklasyfikować?

Grupy Liego, które powstały w związku z jego badaniami nad równaniami różniczkowymi, oraz pomysł Killinga na *układ okresowy* tych grup nadały kierunek poszukiwaniom. Udało się sklasyfikować istniejące atomy, umieszczając je w odpowiednich rodzinach. Okazało się jednak, że na tym nie koniec.

Puszka Pandory. W opowiadaniu *Uncle Petros and Goldbach's Conjecture* autorstwa Apostolosa Doxiadisa pojawia się matematyk, który przez całą swoją karierę próbuje rozwiązać pewien stary problem. Mianowicie, czy każdą parzystą liczbę większą od 2 możemy przedstawić jako sumę dwóch liczb pierwszych? Jest to jedno z pytań, na które do tej pory nie udało się znaleźć odpowiedzi, chociaż poszukiwania trwają od dawna. Co sprawia, że niektóre problemy matematyczne są tak ciężkie do rozwiązania? Czy, tak jak w tym przypadku, trudność polega na tym, że nie wiemy, jak się do tego zabrać, czy może po prostu droga do rozwiązania jest długa i stroma?

[*] doktorantka, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

Rozwiązanie zadania F 832.
W ośrodku sprężystym lokalne zaburzenia gęstości rozprzestrzeniają się z prędkością dźwięku c. Dla wody $c = 1500$ m/s. Zmiana prędkości wody wywołana zamknięciem zaworu w czasie Δt dotrze na odległość $l = c\Delta t$, zatrzymana zostanie masa wody $m = l\rho S$, gdzie S jest polem przekroju rury, a $\rho = 10^3$ kg/m^3 oznacza gęstość wody. Zmiana pędu wody wynosi mu. Ciśnienie p wody na zawór wyniesie więc

$$p = \frac{1}{S}\frac{mu}{\Delta t} = \rho cu.$$

Dla prędkości $u = 1$ m/s ciśnienie jest równe $p = 1{,}5 \cdot 10^6$ Pa $= 15$ atm.

Do tej drugiej grupy problemów zdecydowanie należy zaliczyć (przynajmniej dziś) twierdzenie Feita-Thompsona o nieparzystym rzędzie. Jego sformułowanie jest bardzo proste:

Jeśli atom symetrii nie jest cykliczną grupą o rzędzie będącym liczbą pierwszą, to jego rząd jest parzysty.

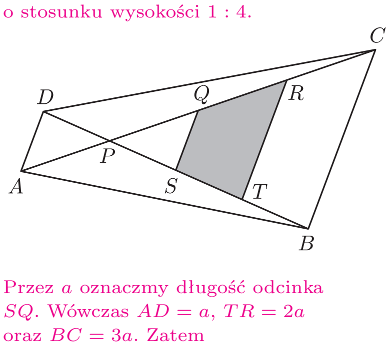
Dowód miał jednak 255 stron i zajął cały numer *Pacific Journal of Mathematics*. Dlaczego jednak twierdzenie to było tak ważne przy poszukiwaniu atomów symetrii?

Cauchy udowodnił, że jeśli rząd grupy dzieli się przez liczbę pierwszą p, to w grupie tej istnieje element rzędu p. Jeśli więc rząd atomu symetrii jest liczbą parzystą, to atom ten musi zawierać element rzędu 2. Taki element (a dokładniej mnożenie przez niego) zachowuje się podobnie jak symetria lustrzana. Jeśli odbijemy przedmiot raz, to znajdzie się on po drugiej stronie lustra, a jeśli odbijemy go ponownie, to wróci na swoje miejsce. Składając tę symetrię z innymi, możemy otrzymać symetrię względem innego lustra. Znajdą się jednak takie symetrie, które utrzymają lustro w tym samym miejscu. Podgrupę permutacji niezmieniających wybranego lustra będziemy nazywać *przekrojem poprzecznym*. Do czego potrzebny jest nam jednak taki twór?

Pomysł jest prosty. Zamiast szukać atomów symetrii, spróbujmy zrozumieć ich przekroje poprzeczne. Zacznijmy od przekrojów znanych nam atomów i pokażmy, że nie mogą istnieć inne, mające te same przekroje. Okazało się jednak, że to nie takie proste.

Nowe atomy. W połowie XIX wieku, kiedy opublikowane zostały prace Galois, wielu matematyków zainteresowało się teorią grup, a w szczególności grupami permutacji. Powstało wtedy pojęcie *tranzytywnej* (*przechodniej*) grupy permutacji. Grupa ta, działając na zbiorze obiektów, spełniała warunek, że dowolnie wybrany obiekt możemy zamienić miejscami z dowolnym innym obiektem. W podobny sposób możemy zdefiniować grupy wielokrotnie przechodnie. Grupa k-przechodnia to taka, która dla dwóch dowolnych podzbiorów złożonych z k obiektów zawiera przekształcenie, które zamienia miejscami odpowiednie pary tych obiektów. Badając grupy 5-przechodnie, francuski matematyk Mathieu wpadł na ślad dwóch nowych atomów, które oznaczył odpowiednio $M12$ i $M24$. Nie udało mu się jednak udowodnić istnienia tych grup. W końcu, ponad 70 lat później, na seminarium w Hamburgu, niemiecki matematyk Ernst Witt zdefiniował 24 symbole, których grupa symetrii to właśnie $M24$.

Rozwiązanie zadania M 1384.
Z twierdzenia Talesa wynika, że $AD \parallel SQ \parallel TR \parallel BC$, więc $STRQ$ i $ABCD$ są trapezami o stosunku wysokości $1:4$.



Przez a oznaczmy długość odcinka SQ. Wówczas $AD = a$, $TR = 2a$ oraz $BC = 3a$. Zatem

$$\frac{[STRQ]}{[ABCD]} = \frac{(a+2a)\cdot h}{2} \cdot \frac{2}{(a+3a)\cdot 4h} = 3/16.$$

Interesujące jest, że atomy Mathieu nie należą do żadnej ze znanych rodzin atomów. Skoro jednak znaleźliśmy kilka samotnych atomów (takie samotne atomy zostały nazwane *grupami sporadycznymi*), to czy może być ich więcej?

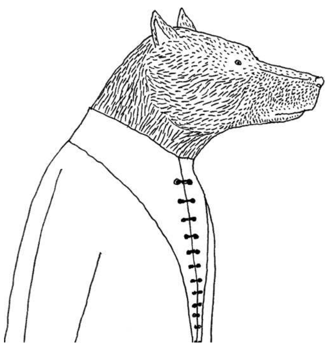
Odpowiedź brzmi: tak. Korzystając z opisanych wcześniej przekrojów poprzecznych, matematycy Janko i Thompson odnaleźli grupy, nazwane na cześć Janko $J1$, $J2$ i $J3$.

Radio i sieci. Pierwsze odkryte grupy sporadyczne miały nadspodziewanie dużo elementów. Na przykład, najmniej liczna spośród grup odkrytych przez Mathieu miała ich 7920. Powstało pytanie, jakie to obiekty mogą mieć tak liczne i nietypowe grupy symetrii.

Inspiracja przyszła od strony radia. W czasach pierwszych transmisji radiowych często zdarzało się, że dźwięki zakłócane były przez szumy, mimo że stacje radiowe starały się zachowywać jak najwyższą jakość transmisji. Szukając rozwiązania problemu, Claude Shannon z Bell Labs zaproponował, by sygnał radiowy wysyłany był jako seria krótkich dźwięków kodujących informację w taki sposób, żeby niewielkie zakłócenia mogły być natychmiast poprawiane, co zwiększyłoby jakość przekazu.

Dogodnym modelem takich sytuacji są gęsto upakowane sieci o ustalonej odległości między węzłami, na dodatek w wielowymiarowej przestrzeni.

Badając przestrzeń o wymiarze równym 24, matematyk John Leech zdefiniował nową sieć tego typu (nazywaną kratą Leecha). Doszedł on również do wniosku, że jest to struktura na tyle ciekawa, że warto sprawdzić, co kryje grupa jej symetrii. Udało mu się przekonać innego matematyka, Johna Conwaya, by zajął się badaniem możliwości otrzymania z niej kolejnych atomów symetrii, co doprowadziło Conwaya do uzyskania trzech nowych atomów $Co1$, $Co2$ i $Co3$.



Potwór Fischera. Matematyk Bernd Fischer postanowił zająć się problemem, którego sformułowanie było proste: jakie grupy permutacji, generowane przez permutacje rzędu 2, zachowują się podobnie jak transpozycje? *Transpozycja* to permutacja, która zamienia miejscami dwa ustalone elementy. Łatwo jest wykazać, że złożenie dwóch transpozycji ma albo rząd 2, albo rząd 3. Te permutacje, tak zbliżone do transpozycji, nazywamy *transpozycjami Fischera*. Fischerowi udało się udowodnić następujące twierdzenie:

Jeśli atom symetrii (albo coś bardzo do niego podobnego) jest generowany przez transpozycje Fischera, to może on być tylko jednym z 6 typów obiektów.

Analizując te typy obiektów, Fischer uzyskał trzy nowe interesujące grupy, blisko związane z grupami Mathieu $M22$, $M23$, $M24$. Oznaczył je jako $Fi22$, $Fi23$ i $Fi24$. $Fi22$ i $Fi23$ są atomami, zaś $Fi24$ zawiera olbrzymi atom rozmiaru 1 255 205 709 190 661 721 292 800.

Możemy porównać transpozycje Fischera do luster, które odbijają część obiektów, a resztę pozostawiają niezmienioną. Jeśli ustawimy dwa lustra pod kątem α, to złożenie odbić w tych lustrach będzie obrotem o kąt 2α. Jeśli rząd złożenia dwóch symetrii lustrzanych ma być równy 2 lub 3, to kąty pomiędzy lustrami mogą być tylko równe $90°$ lub $60°$. Rozważając pewne specyficzne zbiory tych luster, czyli układy generatorów, Fischer udowodnił podane wcześniej twierdzenie.

Następny krok można przedstawić jako dopuszczenie ustawienia luster pod kątem $45°$. To doprowadziło Fischera do większego atomu, który zdawał się zawierać $Fi22$. Dzięki temu udało mu się stworzyć nowy atom symetrii, który nazwał M^{22}. Dodatkowo zauważył, że M^{22} może być przekrojem poprzecznym innego atomu symetrii, który z powodu powiązań z $Fi24$ został oznaczony jako M^{24}. Istniało podejrzenie, że pomiędzy M^{22} a M^{24} ukrywa się trzecia grupa, więc Conway, z którym Fischer podzielił się swoimi spostrzeżeniami, nazwał te trzy grupy odpowiednio Małym Potworem, Średnim Potworem i Super Potworem. Gdy później okazało się, że Średni Potwór nie może istnieć, nazwy zmieniono na *Mały Potwór* i *Potwór*.

Potwór okazał się być grupą, której rząd wynosi

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \cdot 10^{53}.$$

Naukowcom z Cambridge udało się udowodnić, że Potwór nietrywialnie działa na przestrzeni o wymiarze 196 883. Najoszczędniejsza forma, w jakiej udało się zawrzeć pełne informacje o tej grupie, ma postać tabeli o 194 wierszach i tyluż kolumnach. Aby ją wypełnić (obliczyć), potrzeba było roku pracy, w którą zaangażowano wszystkie (ówczesne) komputery uniwersytetu w Birmingham.

Jako że dwie podgrupy Potwora również okazały się atomami symetrii, to w sumie udało się odnaleźć 25 atomów niezrzeszonych w znanych wcześniej rodzinach. W 1975 roku Janko udowodnił istnienie jeszcze jednego atomu, $J4$, który wkrótce został dokładniej opisany. Od tego czasu liczba tych ważnych grup już się nie zmieniła i się nie zmieni.

Rozwiązanie zadania M 1386. Załóżmy przeciwnie, że $x_1, \ldots, x_n$ to pierwiastki rzeczywiste naszego wielomianu. Wówczas

$$x^n + a_{n-3}x^{n-3} + a_{n-4}x^{n-4} + \ldots + a_0 = (x - x_1)(x - x_2) \cdot \ldots \cdot (x - x_n).$$

Porównując współczynniki przy x^{n-1} i x^{n-2}, dostajemy

$$0 = \sum_{i=1}^{n} x_i, \qquad 0 = \sum_{1 \leqslant i < j \leqslant n} x_i x_j.$$

Stąd

$$x_1^2 + \ldots + x_n^2 = \left(\sum_i x_i\right)^2 - 2\sum_{i<j} x_i x_j = 0,$$

więc $x_1 = \ldots = x_n = 0$. Zatem $a_{n-3} = \ldots = a_0 = 0$, co jest sprzeczne z założeniem.