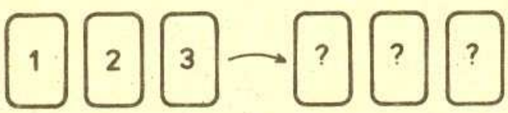
O klasyfikacji grup skończonych

Dr Zbigniew MARCINIAK

Na jakiej podstawie jesteśmy skłonni uznać pewne przedmioty za bardziej symetryczne od innych ?

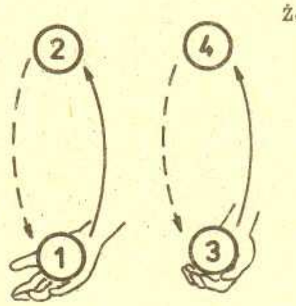
Możemy postąpić np. tak: dla każdej z oglądanych figur F rozważmy zbiór $Sym(F)$ wszystkich ruchów sztywnych (izometrii euklidesowych), które nakładają F na F. Ten z przedmiotów uznamy za bardziej symetryczny, którego zbiór symetrii $Sym(F)$ jest „bogatszy", tj. ma więcej elementów. Nawet jeśli figura F jest pozbawiona wszelkiej symetrii, to i tak zbiór $Sym(F)$ jest niepusty: przekształcenie identycznościowe nakłada F na F. Jest oczywiste, że składając przekształcenia należące do zbioru $Sym(F)$, a także odwracając przekształcenie z $Sym(F)$, nadal pozostaniemy w tym zbiorze.

Jeśli X nie jest figurą geometryczną, lecz po prostu zbiorem pewnych przedmiotów, to rozważanie izometrii nie ma sensu, ale zbiór $Per(X)$ wszystkich wzajemnie jednoznacznych przekształceń X na X (zwanych permutacjami) ma te same własności, które zauważyliśmy wyżej dla zbiorów symetrii.
Oto przykłady permutacji:

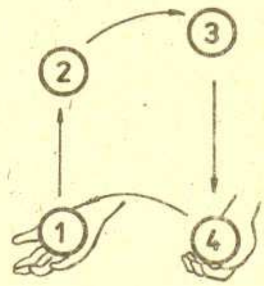


Gra w 3 karty: Która permutacja zmyli widza ?

Żonglerka



Ta permutacja jest łatwa...



...a ta trudna do wykonania.

Wspólne własności zbiorów symetrii i zbiorów permutacji można wysłowić jak następuje. Dany jest zbiór G z działaniem $\cdot$ (u nas składanie przekształceń), które ma następujące własności:

1. G zawiera element e neutralny ze względu na działanie $\cdot$:

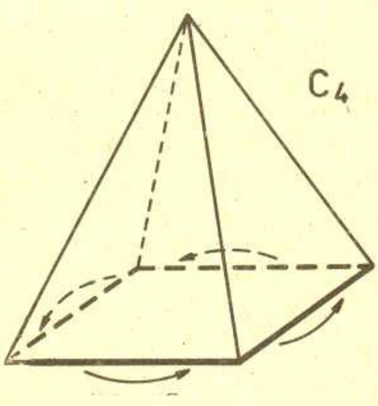
$$e \cdot a = a \cdot e = a \quad \text{dla dowolnego} \quad a \in G\,.$$

2. Każdy element $a \in G$ ma w zbiorze G element odwrotny a':

$$a \cdot a' = a' \cdot a = e\,.$$

3. Działanie $\cdot$ jest łączne:

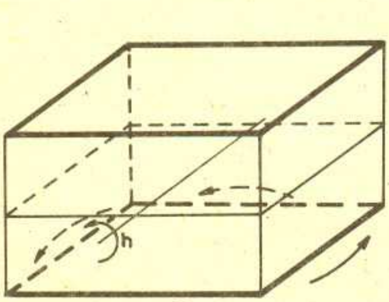
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \text{dla dowolnych} \quad a, b, c \in G\,.$$



Zbiór G, wyposażony w działanie $\cdot$ spełniające powyższe aksjomaty, nazywamy grupą. Na ogół działanie grupowe nazywa się mnożeniem, a element neutralny – jedynką (na wzór grupy multiplikatywnej dodatnich liczb rzeczywistych). Panuje też zwyczaj nazywania działania dodawaniem, a elementu neutralnego zerem, gdy chcemy krótko zasygnalizować, iż grupa jest przemienna (tj. $a \cdot b = b \cdot a$ dla dowolnych $a, b \in G$).

Wszystkie rozważane dalej grupy będą skończone, tzn. zbiór G będzie miał zawsze skończenie wiele elementów (liczbę elementów grupy nazywamy rzędem grupy i oznaczamy $|G|$). Np. jeśli zbiór X składa się z n kolejnych liczb: $1, 2, \ldots, n$, to grupa $Per(X)$ ma, jak nietrudno obliczyć, $n!$ elementów. Grupę tę oznaczamy S_n.

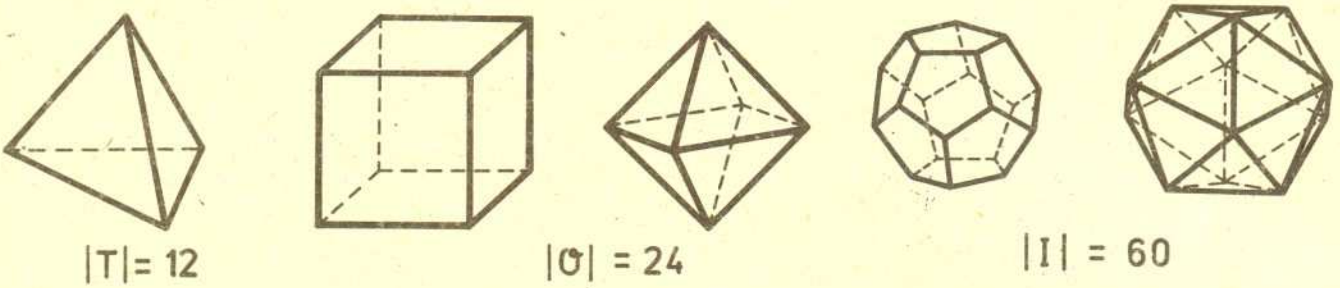
D_4



Ciekawych przykładów grup skończonych dostarczają nam wielościany w przestrzeni trójwymiarowej. Oznaczmy przez $O(W)$ grupę tych obrotów przestrzeni, które przeprowadzają wielościan W na siebie. Gdy W_1 jest ostrosłupem prawidłowym nieforemnym, którego podstawą jest n-kąt foremny, to grupa $O(W_1)$ ma n elementów i składa się z obrotów ostrosłupa wokół jego osi. Nosi ona nazwę grupy cyklicznej C_n.

Gdy W_2 jest graniastosłupem (ale nie sześcianem), którego podstawą jest ten sam n-kąt foremny, to jego grupa obrotów $O(W_2)$ ma $2n$ elementów: n „starych" obrotów podstawy oraz n nowych obrotów, będących złożeniem starych obrotów z półobrotem h, stawiającym graniastosłup „do góry nogami". Grupa $O(W_2)$ nosi nazwę grupy diedralnej D_n (grupy dwuścianu).

Grupy cykliczne C_n i diedralne D_n tworzą dwie nieskończone serie typowych grup obrotów przestrzeni 3-wymiarowej. Oprócz nich mamy jeszcze trzy grupy wyjątkowe, związane z bryłami platońskimi. Dla czworościanu dostajemy 12-elementową grupę T. Dla sześcianu i dla ośmiościanu foremnego mamy grupę 24-elementową, oznaczaną tradycyjnie przez $\mathcal{O}$. Wreszcie dla dwunastościanu i dla dwudziestościanu foremnego mamy grupę I o 60 elementach. (Zachęcam Czytelników do odszukania tych wszystkich obrotów dla każdej z brył.)



Zauważmy, że grupa $\mathcal{O}$ ma 4! elementów, podobnie jak grupa S_4. Może to ta sama grupa, tyle że w „geometrycznym przebraniu" ?

Dwie grupy G_1, G_2 uznamy za takie same (izomorficzne), jeśli istnieje wzajemnie jednoznaczne przekształcenie $f : G_1 \to G_2$, które zachowuje mnożenie:

$$f(x \cdot y) = f(x) \cdot f(y) \quad \text{dla dowolnych} \quad x, y \in G.$$

Nietrudno dowieść, że grupa $\mathcal{O}$ jest istotnie izomorficzna z grupą S_4. W tym celu należy zauważyć, że każdy obrót sześcianu permutuje zbiór czterech przekątnych, przechodzących przez jego środek. Co więcej, każdy obrót sześcianu jest wyznaczony przez tę permutację jednoznacznie.

Nie należy jednak sądzić, że każde dwie grupy, które mają tyle samo elementów, są izomorficzne. Np. grupy S_3 i C_6 mają po 6 elementów, ale są różne: w C_6 mnożenie jest przemienne, a w S_3 – nie (sprawdź !).

Głównym zadaniem teorii grup skończonych jest ich pełna klasyfikacja.
Grupa $G = \{g_1, \ldots, g_n\}$ jest w pełni opisana przez swoją tabelkę mnożenia, która podaje wynik pomnożenia każdych dwóch jej elementów. Tabelka ta jest więc kwadratem o boku n. Takich tabelek jest skończenie wiele. Dla małych liczb n możemy je wszystkie bez trudu wypisać, ale dla dużych n zadanie robi się kłopotliwe: większość tabelek nie chce spełniać aksjomatów grupy ! Trzeba więc szukać innych sposobów.

Inną możliwość stwarza następujące twierdzenie Cayleya: każda grupa skończona rzędu n jest podgrupą w grupie permutacji S_n. (Mnożenie z lewej strony przez $g \in G$ miesza elementy grupy G, określając w ten sposób ich permutację.)

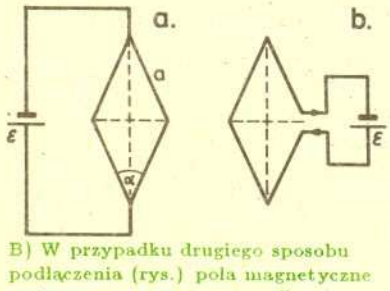
Dla klasyfikacji grup rzędu n należałoby opisać wszystkie podgrupy w grupie S_n. Niestety, jest to również zadanie beznadziejne dla dużych n. Twierdzenie Cayleya daje nam jednak możliwość wygodnego reprezentowania grup skończonych za pomocą liczb, np. w pamięci komputera.

Właściwa droga do klasyfikacji grup rozpoczyna się od następującego odkrycia: niektóre grupy skończone są zbudowane z dwóch grup o mniejszej liczbie elementów. Aby znaleźć taki rozkład dla grupy G, wystarczy wskazać w niej podgrupę normalną H, tj. taki podzbiór $H \subset G$, który:
1. jest podgrupą, tzn. H wraz z mnożeniem pochodzącym z G spełnia aksjomaty grupy, oraz
2. dla dowolnych elementów $x \in G$ i $h \in H$ element xhx' pozostaje w H (warunek normalności).
Jeśli $H \neq \{e\}$ i $H \neq G$, to G jest zbudowana z pary grup. Jedną z nich jest sama H, a drugą – tzw. grupa ilorazowa G/H, która ma dokładnie $|G|/|H|$ elementów.

Uznamy, że badanie takiej grupy G zostało zredukowane do zbadania mniejszych grup H i G/H. Pozostaje jednak problem opisu tych grup G, które nie mają podgrup normalnych H różnych od $\{e\}$ i G. Takie grupy nazywamy grupami prostymi.

Które z grup opisanych wyżej były proste ? Grupa cykliczna C_n jest prosta tylko wtedy, gdy n jest liczbą pierwszą. Grupy diedralne nie są proste: zawierają podgrupy normalne C_n. Grupy permutacji S_n także nie są proste: zawierają one podgrupy normalne A_n, składające się ze wszystkich permutacji parzystych.

Rozwiązanie zadania F 258.
A) Środek rombu jest środkiem symetrii tego obwodu. Sposób podłączenia tego obwodu do źródła prądu sprawia, że każdemu elementowi jednego boku możemy przyporządkować odpowiedni element boku równoległego, który będzie wytwarzać pole o tej samej wartości, ale przeciwnie skierowane. Oznacza to, że indukcja w środku rombu jest równa zeru.



B) W przypadku drugiego sposobu podłączenia (rys.) pola magnetyczne wytworzone przez poszczególne boki zsumują się dając w środku rombu pole różne od zera. Indukcję pola w punkcie O, jaką daje pojedynczy bok, oznaczmy przez B'. Całkowita indukcja w tym punkcie wyniesie $B = 4B'$. Na podstawie prawa Biota – Savarta możemy obliczyć natężenie pola magnetycznego w punkcie O, pochodzące od jednego z boków:

$$H' = \frac{I}{4\pi r}(\sin \angle AOD + \sin \angle DOB),$$

ponieważ $\angle AOD = \alpha/2$, $\angle DOB = \\ = \alpha$, $r = a\sqrt{3}/4$, więc

$$H' = \frac{I}{2\pi\sqrt{3}a}(\sqrt{3} + 1).$$

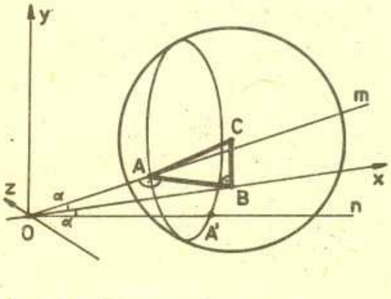
Znając opór drutu $R = \rho 4s/S$ obliczymy natężenie prądu w obwodzie:

$$I = \frac{\varepsilon}{R} = \frac{\varepsilon S}{4\rho a}.$$

Stąd

$$B = \mu_0 4B' = \frac{\mu_0 \varepsilon S}{2\pi\rho a^2}(\sqrt{3} + 1)/\sqrt{3}.$$

Rozwiązanie zadania M 528. Ustalmy początek układu współrzędnych w punkcie przecięcia prostych m, n, oś x – jako dwusieczną kąta między prostymi, oś z – w płaszczyźnie wyznaczonej przez proste m, n (które przecinają się pod kątem 2α).



Środek kuli ma współrzędne $C = (x, y, 0)$. A jest punktem styczności sfery z prostą m, B – rzutem prostopadłym C na płaszczyznę xz.

W takim razie $AC^2 = CB^2 + BA^2$; oznaczając przez R promień kuli, mamy $AC = R$, $CB = y$, $BA = x \sin\alpha$, stąd
$$R^2 = y^2 + x^2 \sin^2\alpha,$$
a to jest równanie elipsy.

Permutacja miesza naturalną kolejność liczb; np. $\sigma \in S_5$ może przekształcać 12345 w 21435. Liczby te możemy ponownie uporządkować, zamieniając miejscami niektóre pary liczb sąsiednich. Jeśli liczba tych zamian jest parzysta, to permutacja też nazywa się parzysta. Taka jest np. permutacja σ z powyższego przykładu:

2 1 4 3 5

Zadanie: wykaż, że grupa T obrotów czworościanu foremnego jest izomorficzna z grupą A_4.

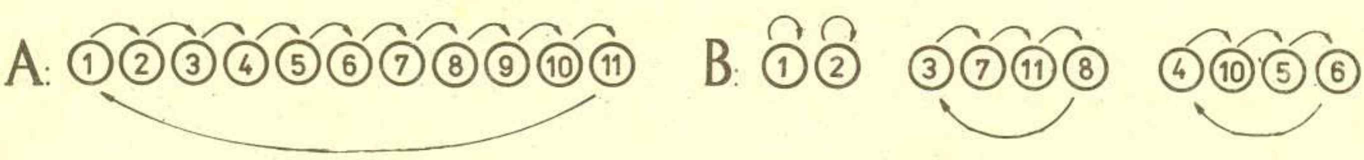
Można udowodnić, że dla $n \geq 5$ grupa A_n jest prosta. Mamy więc już dwie nieskończone serie grup prostych: C_p, gdzie p – liczba pierwsza, oraz A_n dla $n \geq 5$. Odkryto jeszcze 16 innych serii skończonych grup prostych. Podobnie jak seria A_n została wykryta w grupach permutacji S_n, tak te nowe serie zostały wykryte za pomocą grup macierzy.

Macierz dla algebraika to po prostu kwadratowa tablica składająca się z liczb. Najważniejszą cechą macierzy jest to, że je można mnożyć. Dla geometry – macierz to bardzo ekonomiczny sposób zakodowania przekształcenia afinicznego (zachowującego proste) przestrzeni n-wymiarowej, które zachowuje punkt $(0, 0, \ldots, 0)$. W tej interpretacji mnożenie macierzy dokładnie odpowiada składaniu przekształceń, a zbiór macierzy odpowiadających przekształceniom odwracalnym tworzy grupę – $\mathrm{GL}(n,\mathbf{R})$. Jest to grupa Liego – o nich też możesz poczytać w tym numerze *Delty*.

Oczywiście, grupa $\mathrm{GL}(n,\mathbf{R})$ jest nieskończona. Weźmy więc zamiast nieskończonego zbioru liczb rzeczywistych skończony zbiór reszt $F_q = \{0, 1, 2, \ldots, q-1\}$ dla ulubionej liczby pierwszej q. Liczby ze zbioru F_q można, podobnie jak liczby rzeczywiste, dodawać i mnożyć biorąc zawsze wynik modulo q. Rozważając macierze o współczynnikach ze zbioru F_q otrzymujemy grupę skończoną $\mathrm{GL}(n, q)$. Wspomniane wyżej grupy 16 nowych serii powstają z grup $\mathrm{GL}(n, q)$ przez proste operacje algebraiczne. Są one ściśle związane z tzw. prostymi grupami Liego i dlatego noszą wspólną nazwę grup skończonych typu Lie.

Wszystkie grupy proste, wspomniane dotąd, uchodzą za typowe. Oprócz nich istnieją jeszcze tzw. grupy sporadyczne, odkrywane ad hoc i nie mieszczące się w żadnym schemacie. Były one znajdowane pojedynczo, w ciągu kilku dziesięcioleci.

Znamy obecnie 26 grup sporadycznych. Każda z nich ma swoją nazwę, zwykle pochodzącą od nazwiska jej odkrywcy–konstruktora. Mamy więc 5 grup Mathieu: M_{11}, M_{12}, M_{22}, M_{23}, M_{24} – zostały odkryte w 1860 r., z których najmniejsza M_{11} ma 7 920 elementów, a największa – M_{24}: 244 823 040 elementów. Grupę M_{11} można reprezentować w komputerze jako podgrupę permutacji 11 liczb, generowaną przez dwa elementy:



Dalej mamy 4 grupy Janko: $J1$ – 1966 r., $J2$, $J3$ – 1969 r., $J4$ – 1980 r.; grupy Higmana–Simsa: HS – 1968 r., McLaughlina: Mc – 1969 r., Suzuki: Suz – 1969 r., Rudvalisa: Ru – 1973 r., Helda: He – 1969 r., Lyonsa: Ly – 1972 r., O'Nana: ON – 1976 r., trzy grupy Conwaya: .1, .2, .3 – 1969 r., trzy grupy Fishera: $M(22)$, $M(23)$ i $M(24)'$ – 1971 r. oraz w końcu cztery grupy Griessa: F_5, F_3, F_2, F_1 – 1976 r.

Rozwiązanie zadania M 527. W końcu dostajemy los, który albo wygrywa, albo przegrywa. Ze względu na symetrię prawdopodobieństwo otrzymania każdego z takich losów jest takie samo. Zatem szukane prawdopodobieństwo wynosi $k/(n-m)$, czyli jest takie jak w sytuacji, w której usunięto by wszystkie losy uprawniające do następnego ciągnienia. Znajdują się one w różnych loteriach wyłącznie w celach propagandowych.

Największą pośród grup sporadycznych jest grupa F_1, która ma
$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 =$$
$$= 808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000 \text{ elementów.}$$

Początkowo nosiła ona nazwę potwora (*monster*), ale gdy jej odkrywca, R. Griess, znalazł jej ładną interpretację geometryczną, przemianował ją na przyjaznego olbrzyma (*friendly giant*). Grupa ta została odkryta jako podgrupa w grupie macierzy stopnia 196 883.

W lutym 1981 roku specjaliści uznali, że dowód twierdzenia o klasyfikacji grup prostych został zakończony – innych grup prostych nie ma ! Twierdzenie to jest efektem pracy setek matematyków. Jego dowód składa się z wielu fragmentów, rozrzuconych w około 500 pracach zajmujących łącznie około 10 000 stron druku. Oczywiście, prace nad uproszczeniem dowodu trwają.