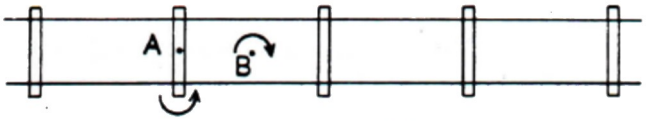
Przykład teorii aksjomatycznej: grupy

Zbigniew MARCINIAK, Warszawa

Teorie aksjomatyczne nie spadają matematykom z nieba – są one zwykle wspólnym uogólnieniem wielu obserwacji.

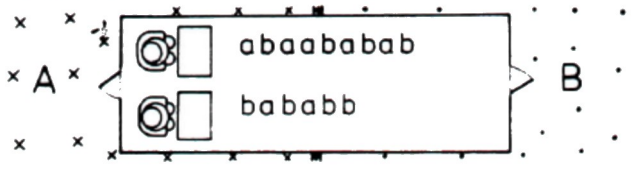
Na przykład, wyobraźmy sobie dziecko bawiące się kolejką elektryczną. Dla prostoty załóżmy, że zabawka ta nie jest zbyt skomplikowana: kolejka ma tylko jeden prosty (ale za to długi) tor.



Jak wiadomo, ojcowie bawią się kolejką równie chętnie. Wprawdzie nie bardzo wypada zabierać dziecku zabawkę, ale gdy synek na chwilę odejdzie... Oczywiście, potem należy zostawić wszystko tak, jak było: w szczególności tor powinien wyglądać tak, jakby go nikt nie ruszał. Spostrzegawczy ojciec szybko zauważy, że istnieje cała gama ruchów torem, które ujdą mu bezkarnie. Należą do nich np. przesunięcia w prawo i w lewo o całkowitą liczbę odstępów między podkładami: po takim przesunięciu tor „nakłada się na siebie", więc wygląda jak nietknięty. Istnieją jeszcze inne operacje dające podobny skutek: np. można przycisnąć tor do podłogi w środku długości dowolnego podkładu (punkt A na obrazku), a następnie wykonać wokół tego punktu półobrót. Równie dobry jest półobrót wokół punktu B.

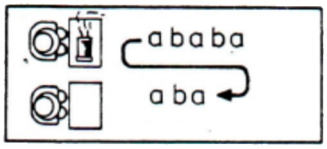
Mamy więc nieskończony zbiór $G_{\#}$ bezkarnych ruchów torem kolejki. Ruchy te można składać, tzn. wykonywać po kolei jeden po drugim (np. wtedy, gdy dziecko ogląda dobranockę). Ponadto, jeśli synek przyłapie nas w trakcie wykonywania jednego z ruchów $R \in G_{\#}$, zawsze możemy uspokoić jego lament wykonując ruch odwrotny, $R^{-1} \in G_{\#}$, przywracający stan poprzedni. Ponieważ uznaliśmy wcześniej, że złożenie każdej pary ruchów bezkarnych prowadzi do takiego ruchu, to mamy w naszym zbiorze $G_{\#}$ „ruch" identycznościowy $I = R \circ R^{-1}$, który polega na tym, że nie robimy absolutnie nic.

Rozważymy teraz zupełnie inną sytuację. Wyobraźmy sobie urząd celny, znajdujący się na granicy dwóch, niezbyt zaprzyjaźnionych państw A i B. Konsekwentnie, obywateli państwa A oznaczać będziemy literą a, a obywateli z państwa B – literą b ($a \in A$ i $b \in B$). Graniczny urząd celny wygląda mniej więcej tak:



Przy kilku biurkach urzędują celnicy, którzy, bez zbędnego pośpiechu, przeglądają bagaże podróżnych. Ci ostatni czekają w kolejkach. Typowa kolejka ma postać: *abaababab*. Wraz z upływem czasu petenci zaczynają się niecierpliwić, dyskutować i wreszcie kłócić między sobą. Jeśli języki państw A i B dostatecznie się różnią (jak np. czeski i węgierski), to kłótnie będą w zasadzie przebiegać w parach *aa* i *bb*. Przyjmijmy (dość realistyczne) założenie, że para, która jest bardzo zajęta kłótnią, przestaje pilnować „swojego miejsca", a więc staje się dla kolejki nieistotna. Zatem, po dostatecznie długim okresie oczekiwania, w kolejce następują kolejne skrócenia par *aa* i *bb*, np. *abaababab* → *abbabab* → *aabab* → *bab*. Ostatnia kolejka jest stabilna: ona będzie już stała spokojnie. Po kilku godzinach w urzędzie celnym pozostaną już tylko kolejki stabilne.

Oznaczmy literą $G_\$$ zbiór wszystkich kolejek stabilnych. W praktyce możemy obserwować składanie kolejek. W tym celu jeden z urzędujących celników powinien ogłosić bezterminową przerwę na herbatkę. Kolejka oczekujących przy jego biurku zwykle w takiej sytuacji przemieści się solidarnie na koniec innej, możliwie krótkiej i aktualnie obsługiwanej kolejki.



Oczywiście, prowadzi to zwykle do sytuacji konfliktowej, ale po małym zamieszaniu dochodzimy do kolejki stabilnej. W zbiorze $G_\$$ mamy więc określoną operację składania kolejek. Dalej, dla dowolnej kolejki stabilnej K istnieje „antykolejka" K^{-1}, która w procesie skracania całkowicie anihiluje K. Np. do kolejki $K = ababab$ należy dostawić na końcu (lub na początku) $K^{-1} = bababa$. Powstanie z nich kolejka pusta I (marzenie każdego urzędnika). Oczywiście I też zaliczymy do zbioru $G_\$$.

W następnym przykładzie zajmiemy się pieniędzmi. W czasach, gdy ceny są co najmniej trzycyfrowe, utrzymanie porządku w portfelu staje się istotne. Dla wygody wszystkie banknoty powinny być ułożone w ten sam sposób, np. tak, by patronujące im osobistości zwrócone były „buzią" do nas i „nóżkami" do dołu. Od dowolnego położenia banknotu można dojść do opisanego wyżej przez wykonanie jednego z następujących czterech ruchów:

Oznaczmy zbiór tych ruchów $G_{zl} = \{I, R_1, R_2, R_3\}$. Wykonując machinalne manipulacje porządkujące nasz portfel w istocie składamy ruchy z tego zbioru. Łatwo zauważyć, że każdy ruch ma swój antyruch, przywracający stan poprzedni. Może się też zdarzyć, że banknot od początku leżał jak należy – wtedy wykonujemy na nim „ruch pusty" = I.

W ostatnim przykładzie przyjrzymy się zegarowi klimatycznemu. Ma on tylko jedną wskazówkę, która może wskazywać na jedną z czterech pór roku: wiosna, lato, jesień, zima. Wskazówka ta może się posuwać (ale tylko w kierunku „zgodnym z ruchem wskazówek zegara"). Ruch tego zegara ilustruje zmiany pogody. Np. w marcu mamy typowe sekwencje: zima–wiosna–zima–lato–zima, a w październiku: lato–jesień–lato–jesień. Oznaczmy przez $G_?$ zbiór ruchów tej wskazówki.

Mamy $G_? = \{I, S_1, S_2, S_3\}$, gdzie S_i oznacza skok o i pór roku, a I oznacza „pogoda bez zmian". Oczywiście, ruchy ze zbioru $G_?$ można składać, a każdy z nich może zostać zrekompensowany innym, odpowiednio dobranym ruchem wskazówki.

Łatwo zauważyć, że wszystkie opisane wyżej sytuacje mają pewne cechy wspólne. Po pierwsze, za każdym razem mamy do czynienia z pewnym zbiorem G $(= G_\#, G_\$, G_{zl}, G_?)$. W zbiorze tym mamy określone działanie składania jego elementów. Działanie to ma w każdym z przykładów bardzo podobne własności.

To, że dostrzegamy analogię między wieloma, na pozór zupełnie różnymi sytuacjami, stanowi sygnał, że sytuacja dojrzała do zdefiniowania kolejnej teorii matematycznej. Należy po prostu zaobserwowane cechy wspólne przyjąć za aksjomaty nowej teorii, po czym nadać jej nazwę.

Definicja: Grupą nazywamy zbiór G wyposażony w działanie

$$\circ : G \times G \to G$$

mające następujące własności:
1) zbiór G zawiera element I, taki że $I \circ X = X \circ I = X$ dla dowolnego $X \in G$; (element neutralny – identyczność),
2) dla dowolnego $X \in G$ istnieje taki element $X^{-1} \in G$, że $X \circ X^{-1} = X^{-1} \circ X = I$; (element odwrotny – „anty-X"),
3) działanie $\circ$ jest łączne: $(X \circ Y) \circ Z = X \circ (Y \circ Z)$.

(Ta ostatnia własność jest łatwa do przeoczenia dla niefachowca, ale występowała ona także we wszystkich przykładach.) Oczywiście, $G_\#$, $G_\$$, G_{zl}, $G_?$ są przykładami grup.

W ten sposób narodziła się nowa teoria matematyczna. Jakie korzyści nam to przyniesie? Otóż każde twierdzenie, które teraz wyprowadzimy z aksjomatów, grupy będzie automatycznie obowiązywać w świecie ruchów torem dziecinnej kolejki, w urzędzie celnym na granicy, podczas porządkowania pliku banknotów, jak też w czasie skoków wskazówki zegara klimatycznego. Zamiast czterech twierdzeń wystarczy udowodnić jedno! Co więcej, twierdzenie uzyskane z aksjomatów będzie też prawdziwe w setkach innych sytuacji, które wprawdzie w tej chwili nie przychodzą nam do głowy, ale które zapewne pojawią się w przyszłości. W końcu, usunięcie z rozważanych przykładów zbędnej fabuły pozwoli nam w czasie poszukiwania i dowodzenia twierdzeń skoncentrować się wyłącznie na tych cechach sytuacji, które są najistotniejsze.

Powinniśmy zatem teraz siąść i postarać się udowodnić możliwie wiele twierdzeń o grupach. Oczywiście, zdań prawdziwych, które można wydedukować z naszych aksjomatów, jest nieskończenie wiele. Powstaje zatem naturalne pytanie: w którą stronę powinien podążać rozwój teorii, by jej tworzenie miało sens?

Większość teorii matematycznych orientuje się w swym rozwoju na cele praktyczne: interesujące są te twierdzenia, które mają ważne zastosowania. W szczególności, dowodzone twierdzenia są często rozwiązaniami problemów przychodzących spoza tworzonej teorii.

Dla przykładu, jeśli jeden z celników w opisywanym wyżej urzędzie granicznym jest miłośnikiem *Trylogii*, to może mu z czasem przyjść do głowy analog problemu pana Podbipięty: czy ustawią się kiedyś równolegle obok siebie trzy identycznie wyglądające kolejki turystów (np. z Turcji), które – gdy nagle zestawione razem – znikną? (Inne sformułowanie: czy istnieje takie $K \in G_\$$ i $K \neq I$, że $K \circ K \circ K = I$?! – zbadamy to później.)

Zdarza się też, że dowodzimy twierdzeń, które są wprawdzie całkowicie bezużyteczne, ale są za to bardzo ładne. Trudno wprawdzie wytłumaczyć, co to dokładnie znaczy, ale matematycy to rozumieją.

Wymienione wyżej cele mają wyraźnie charakter taktyczny. Jednakże każda dobrze rozwijająca się teoria ma też przed sobą cel strategiczny: podanie pełnej klasyfikacji opisywanych przez nią obiektów.

Posiadanie takiej klasyfikacji jest istotnie sytuacją idealną. Wyobraźmy sobie np., że jesteśmy w posiadaniu Mądrej Księgi pt. GRUPY, która zawiera po prostu spis wszystkich istniejących na świecie grup. Powiedzmy, że każda grupa byłaby opisana na oddzielnej stronie, wraz z jej własnościami. Aby rozwiązać dowolny problem praktyczny dotyczący grup, wystarczyłoby odszukać odpowiednią stronę w tej księdze.

Przed każdym, kto zabiera się do pisania takiej księgi, pojawiają się natychmiast dwa problemy. Po pierwsze, zawarta w niej lista grup nie powinna mieć luk – każda grupa powinna się tam znaleźć. Po drugie, lista ta nie powinna mieć powtórzeń.

Stajemy zatem przed koniecznością udzielenia odpowiedzi na pytanie: kiedy dwie grupy uznać za takie same? Oczywiście, fabuła opisująca sytuację nie powinna mieć tu najmniejszego znaczenia. To, co jest istotne, zostało odcedzone w definicji: grupa to zbiór wraz ze specjalnym działaniem. Konsekwentnie, dwie grupy uznamy za takie same, jeśli: 1) mają „taki sam" zbiór i 2) mają „takie samo" działanie.

Definicja: Grupy G i H są takie same (izomorficzne), jeśli istnieje takie przekształcenie $f : G \to H$, że:

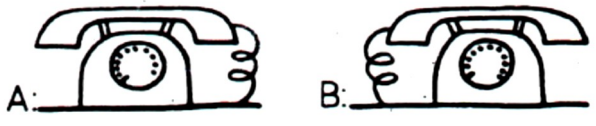
1) f jest wzajemnie jednoznaczne (zbiory G, H są równoliczne...),

2) $f(a \circ b) = f(a) \circ f(b)$ dla $a, b \in G$ (...i f zachowuje działanie).

Zobaczymy najprostszy przykład pary grup izomorficznych. W szkole podstawowej sporo czasu (i nerwów) zabiera nauczenie słuchaczy zasad mnożenia liczb dodatnich i ujemnych. Bystrzejsi uczniowie szybko zauważają, że regułki, które Pani dyktuje, nie mają nic wspólnego z liczbami: ważne jest tylko, jak „się mnożą znaki". W istocie, mamy tu do czynienia z grupą $G_\pm = \{+, -\}$, której działanie najlepiej opisać tabelką:

$\cdot$	$+$	$-$
$+$	$+$	$-$
$-$	$-$	$+$

Opiszemy jeszcze jedną grupę. Można ją odnaleźć w większości naszych biur. W typowym pokoju urzędniczym znajduje się jeden telefon do wspólnego użytkowania przez cały personel. Zwykle znajduje się on w jednym z następujących stanów:



Każdy kolejny użytkownik może po przeprowadzonej rozmowie (lub nieudanej próbie) bądź przywrócić stan poprzedni, bądź też zmienić stan aparatu na przeciwny. (Typowa przyczyna zmiany: leworęczny urzędnik korzysta z aparatu, który był w stanie A.) Możemy rozważyć grupę zmian stanu aparatu $G_\bullet$. Składa się ona z dwóch elementów: I = „zostaw po staremu", Z = „zmień stan". Łatwo zauważyć, że operacje te składają się wg tabelki:

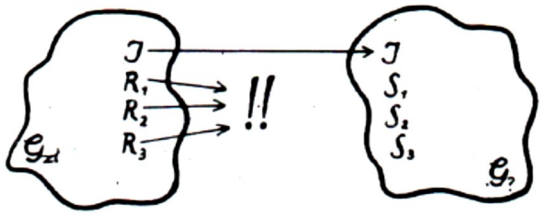
$\cdot$	I	Z
I	I	Z
Z	Z	I

Grupy $G_\pm$ oraz $G_\bullet$ są izomorficzne. Istotnie, przekształcenie $f : G_\pm \to G_\bullet$: $f(+) = I$, $f(-) = Z$ jest wzajemnie jednoznaczne i zachowuje działanie: funkcja f po prostu „tłumaczy" tabelkę grupy $G_\pm$ na tabelkę grupy $G_\bullet$.

Dociekliwy Czytelnik powinien sobie teraz zadać pytanie: a co z grupami $G_\#$, $G_\$$, $G_{zł}$, $G_?$, które pojawiły się na początku: czy są wśród nich pary grup izomorficznych (a więc ile spośród nich musimy wpisać do Mądrej Księgi)?

Najbardziej podejrzanie wygląda para grup: $G_{zł}$ (manipulacje banknotem) i $G_?$ (zmiany klimatu): obie mają przecież po cztery elementy.

Czy istnieje izomorfizm $f : G_{zł} \to G_?$? Łatwo sprawdzić, że element neutralny musi być przekształcony na element neutralny: $f(I) = I$. Zauważmy dalej, że dla $i = 1, 2, 3$ mamy $R_i \circ R_i = I$ w $G_{zł}$. Zatem musi być $I = f(I) = f(R_i \circ R_i) = f(R_i) \circ f(R_i)$. Ponadto $f(R_i)$ musi być jednym z elementów S_1, S_2, S_3. Wśród nich tylko S_2 ma własność: $S_i \circ S_i = I$. Zatem nie istnieje różnowartościowe przekształcenie f, które zachowuje działanie. Wniosek: grupy $G_{zł}$ i $G_?$ nie są izomorficzne.



Natomiast grupy $G_\#$ (ruchy torem kolejki) i $G_\$$ (kolejki do celnika) są izomorficzne. Zbudujemy izomorfizm $f : G_\$ \to G_\#$ w następujący sposób: powiemy, jaki ruch torem kolejki odpowiada każdej stabilnej kolejce stojącej w urzędzie celnym. Po pierwsze, „kolejkę pustą" przekształcimy na „bezruch toru". Jednoosobową kolejkę a przenosimy na O_A = = półobrót toru wokół środka podkładu A (rysunek na początku artykułu). Podobnie kolejkę b przekształcamy na półobrót O_B. A dalej... nie mamy już żadnego wyboru: ponieważ f musi zachowywać działanie, a każda kolejka stabilna jest iloczynem kolejek postaci a i b, to odpowiadający jej ruch torem jest już zdeterminowany. Np. $f(ab) = f(a \circ b) = f(a) \circ f(b) = O_A \circ O_B$ = przesunięcie toru w prawo o jeden odstęp między podkładami. Pozostawiam Czytelnikom sprawdzenie, że f jest przekształceniem wzajemnie jednoznacznym (wskazówka: znaleźć przekształcenie odwrotne).

Jeżeli mamy zbadać, czy dwie grupy G i H są izomorficzne, to próbujemy zwykle zbudować izomorfizm $f : G \to H$. Jeśli nam się to uda – to problem jest rozwiązany. Inaczej wygląda sytuacja, gdy nawet długotrwałe wysiłki nie przynoszą powodzenia: nie stanowi to wszak dowodu, że taki izomorfizm nie istnieje. Jak taki dowód uzyskać?

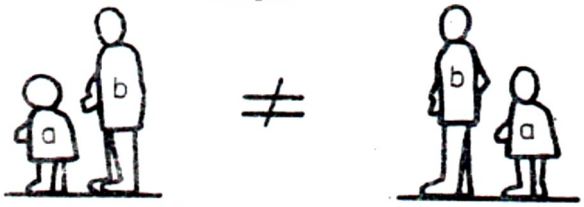
Kluczem do rozwiązania są tzw. niezmienniki: trzeba znaleźć taką własność grupy G, która zachowuje się przy izomorfizmach, ale która nie przysługuje grupie H. Na przykład, porównując grupy $G_{\text{zł}}$ i $G_?$ wykorzystaliśmy fakt, że dla dowolnego $R \in G_{\text{zł}}$ mamy $R \circ R = I$, a w grupie $G_?$ to nieprawda: $S_1 \circ S_1 = S_2 \neq I$.

Podręczniki teorii grup są pełne niezmienników. Grupę, która ma taką specjalną własność, opatruje się zwykle specjalnym przymiotnikiem. Mamy więc grupy skończone, periodyczne, abelowe, rozwiązalne, nilpotentne, wolne,... i tysiące innych. A oto konkretny przykład.

Definicja: Grupa G jest *abelowa*, jeśli $x \circ y = y \circ x$ zachodzi dla dowolnych $x, y \in G$.

Nazwa ta pochodzi od nazwiska matematyka norweskiego, Nielsa Abela.

Łatwo sprawdzić, że grupy $G_{\text{zł}}$, $G_?$, $G_\pm$, $G_\bullet$ są abelowe. Natomiast grupa $G_\$$ kolejek do celników (jak i izomorficzna z nią grupa $G_\#$) nie jest abelowa: elementy ab i ba są różne, o czym dobrze wie każdy, kto choć raz stał w kolejce.



Czy można zlecić zadanie porównywania grup komputerom? Potrzebny byłby do tego program komputerowy, który dla każdej pary grup potrafi w skończonym czasie rozstrzygnąć, czy grupy te są izomorficzne. Niestety, programu takiego nie ma i być nie może: nasz problem jest nierozstrzygalny. Udowodnił to A. Markow w 1958 roku. Wobec tego klasyfikacja grup wymaga dużej pomysłowości, a Mądra Księga Wszystkich Grup pozostaje w strefie marzeń. Nie wyklucza to jednak istnienia „klasyfikacji cząstkowych".

Jak wobec tego radzić sobie z nowo pojawiającym się okazem grupy G? Oczywiście, trzeba zacząć od porównania go ze znanymi grupami. Wobec niekompletności listy grup poznanych wcześniej, poszukiwanie izomorfizmu $G \to H$ ($H \in$ Katalog-Grup-Znanych) byłoby objawem nieuzasadnionego optymizmu. Będziemy więc szukać grup H, które choć trochę przypominają grupę G. W tym celu osłabimy nasze wymagania w stosunku do funkcji $f : G \to H$.

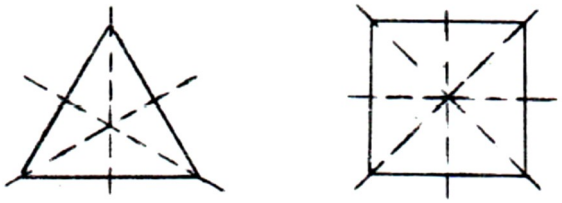
Definicja: Przekształcenie $f : G \to H$ jest *homomorfizmem* grup, jeśli f zachowuje działanie, tj. $f(X \circ Y) = f(X) \circ f(Y)$ dla dowolnych $X, Y \in G$.

W szczególności, przekształcenie f nie musi być różnowartościowe: elementy grupy G mogą się pozlepiać. Im więcej zlepień, tym słabszym echem odbijają się własności G w „lustrze" H.

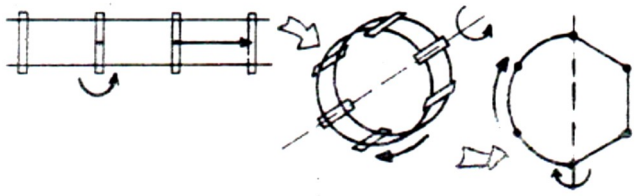
Np. przekształcenie $f : G \to H$, dane wzorem $f(X) = I$ dla wszystkich $X \in G$ jest homomorfizmem, który „zapamiętał" tylko to, że G ma element neutralny.

Łatwo wskazać homomorfizm grupy kolejek $G_\$$ na grupę znaków $G_\pm$: kolejkę K przekształcamy na $+$, gdy stoi w niej parzysta liczba petentów; w przeciwnym przypadku $f(K) = -$.

Grupa $G_\$$ dopuszcza także wiele innych ciekawych homomorfizmów. Niech np. D_n oznacza grupę wszystkich izometrii własnych n-kąta foremnego. Składa się ona z n obrotów wokół środka symetrii oraz z n symetrii osiowych: razem $2n$ elementów. Grupa D_n nosi nazwę grupy dihedralnej.



Dla każdego $n \geq 3$ określimy homomorfizm f_n grupy $G_\$$ na grupę D_n. Po pierwsze, zamiast $G_\$$ weźmiemy $G_\#$ – wiemy już, że to jest ta sama grupa, tylko w innym przebraniu. Wystarczy teraz nawinąć tor kolejowy na szpulkę o obwodzie równym n odstępom między podkładami i spojrzeć na ten zwój z boku: ruchy torem staną się wtedy obrotami i symetriami n-kąta.



Zauważmy, że gdy n rośnie, to grupy dihedralne D_n są coraz większe. Chwytają one więc coraz to więcej informacji o grupie $G_\$$. Dlatego też grupę $G_\$$ nazywa się zwykle *nieskończoną grupą dihedralną* i oznacza: D_∞. Można ją opisać bezpośrednio w języku geometrii jak następuje: D_∞ jest grupą tych izometrii prostej euklidesowej, które przeprowadzają zbiór punktów o współrzędnej całkowitej w siebie. Grupa ta jest bardzo podobna do D_n, jeśli prostą potraktować jak „∞-kąt".

Grupa D_∞ jest przykładem grupy krystalograficznej. Grupy te są grupami symetrii nieskończonych, nie zagęszczających się nigdzie siatek krystalicznych, leżących w przestrzeni euklidesowej. Wymiar grupy – to wymiar przestrzeni, w której leży wspomniana siatka. Np. D_∞ ma wymiar 1: kryształek elementarny jest tu odcinkiem. Grupy krystalograficzne mają ważne zastosowania praktyczne i dlatego matematycy od dawna starali się uzyskać ich klasyfikację. Jeszcze w końcu XIX wieku udało się to zrobić w wymiarach $n \leq 3$. Liczba tych grup jest skończona i wynosi: 2 dla $n = 1$, 17 dla $n = 2$ i 230 dla $n = 3$.

Skłoniło to Davida Hilberta do postawienia pytania, czy w każdym wymiarze jest tylko skończenie wiele grup krystalograficznych (18 problem Hilberta). W roku 1910 Bieberbach udowodnił, że tak istotnie jest. W latach siedemdziesiątych udało się uzyskać, za pomocą komputera, pełną listę 4-wymiarowych grup krystalograficznych.

Wróćmy do sytuacji ogólnej. Jeśli $f : G \to H$ jest homomorfizmem, ale nie jest izomorfizmem, to f przekształca niektóre elementy $X \in G$ w element neutralny $I \in H$; konsekwentnie f gubi o nich informację. Zbiór tych „poszkodowanych" elementów nazywamy jądrem homomorfizmu f : $\ker(f) = \{X \in G : f(X) = I\}$. Łatwo sprawdzić, że jest to podgrupa grupy G.

Na przykład, dla rozważanego przez nas na początku homomorfizmu $f : G_\sharp \to G_\pm$ mamy $\ker(f) = \{K : K$ – kolejka parzystej długości$\} = \{(ab)^n : n \in \mathbf{Z}\}$. Przekształcenie $g : \ker(f) \to \mathbf{Z}$, dane wzorem $g((ab)^n) = n$, ustala izomorfizm grupy $\ker(f)$ z grupą liczb całkowitych.

Można powiedzieć, że homomorfizm $f : G \to H$ „rozłupuje" grupę G na dwa mniejsze kawałki: $\ker(f)$ oraz H. Aby opisać G, należy opisać te kawałki oraz sposób, w jaki są one ze sobą splecione.

Już sama znajomość obu kawałków daje sporo informacji o grupie G. Np. mamy już dostatecznie wiele informacji o grupie $G_\sharp$, aby pomóc celnikowi, dręczonemu ślubem Longinusa Podbipięty z Mysichkiszek: nie istnieje taka kolejka $K \in G_\sharp \setminus \{I\}$, że $K^3 = I$. Mamy bowiem $f : G_\sharp \to \{+, -\}$ i $\ker(f) = Z$. Ponadto $f(K)^3 = f(K^3) = f(I) = +$. Ale $-^3 = -$, więc pozostaje $f(K) = + =$ element neutralny w $G_\pm$. Stąd $K \in \ker(f) \cong \mathbf{Z}$. Jednak w grupie liczb całkowitych (z dodawaniem) nie ma takiego elementu $K \neq 0$, by $K + K + K = 0$. (Wniosek: celnik musi niestety pozostać w cnocie.)

Widzieliśmy przed chwilką, jak pożyteczną rzeczą są homomorfizmy badanej grupy w grupy zbadane wcześniej. Ale skąd brać takie przekształcenia?

Rada jest prosta – należy odwrócić kota ogonem.

Każdy homomorfizm $f : G \to H$ wyznacza podgrupę elementów „zgniatanych" $\ker(f) \subseteq G$. Zrobimy więc tak: w badanej grupie G wybierzemy sobie najpierw podgrupę K elementów „do zgniecenia", a grupa H i homomorfizm f wytworzą się same: mówiąc nieściśle, H powstanie z G przez umiejętne zgniecenie K, a f będzie po prostu odwzorowaniem zgniatającym.

Jest tylko jedna trudność: nie każda podgrupa $K \subseteq G$ nadaje się na jądro homomorfizmu! Jeśli $K = \ker(f)$ dla pewnego homomorfizmu f, to dla dowolnych $x \in K$ i $g \in G$ mamy $f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g) \circ I \circ f(g)^{-1} = I$, tj. $gxg^{-1} \in K$. To jest specjalna własność przysługująca podgrupie $K \subseteq G$.

Definicja: Podgrupa $K \subseteq G$ nazywa się *normalna*, jeśli dla dowolnych $x \in K$ i $g \in G$ mamy $gxg^{-1} \in K$.

Przeważnie podgrupy nie są normalne, np. dla $G = G_\#$ nie jest normalna podgrupa $K = \{I, O_A\}$. Jeśli jednak K jest podgrupą normalną w G, to innych przeszkód już nie ma: istnieje homomorfizm f określony na grupie G, taki że $\ker(f) = K$.

Szczególnie uporczywy bój o klasyfikację toczy się w klasie grup skończonych. Oczywiście tu pełna klasyfikacja jest możliwa: w końcu dla zbioru n-elementowego można określić działanie tabelką i takich tabelek jest tylko skończenie wiele. Problem polega jednak na tym, że „skończenie wiele" nie znaczy „niewiele". Możemy jednak zastosować tu technikę homomorfizmów, opisaną wyżej. Jeśli tylko uda nam się znaleźć właściwą podgrupę normalną $K \subseteq G$, to opis grupy G redukuje się do opisu K oraz grupy ilorazowej H (= G ze zgniecionym K). Ale obie grupy: K i H mają mniej elementów niż G, więc prowadząc klasyfikację indukcyjnie można założyć, że o nich wiemy już wszystko.

W najgorszej sytuacji jesteśmy wtedy, gdy badana grupa G nie ma podgrup normalnych różnych od $\{I\}$ i całej G: takie grupy nazywamy *prostymi*.

Klasyfikacja skończonych grup prostych jest bardzo zaawansowana. Niektórzy specjaliści nawet twierdzą, że już jest zakończona. Wszyscy jednak wiedzą, że istniejące dowody wymagają jeszcze wielu uzupełnień.