Przykład teorii aksjomatycznej: grupy

Zbigniew MARCINIAK, Warszawa

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

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

Jak wiadomo, ojcowie bawią się kolejką również chętnie. Wprawdzie nie bardzo wypada sabierać dziecko sabawkę, ale gdy synek na chwilę odejdzie...

Oczywiście, potem należy zstąpić wszystko tak, jak było: w szczególności tor powinien wyglądać tak, jakby go nikto nie ruszał. Spotrzeszegawczy ojciec szczerze zaawansował, że istnieje cała gama ruchów torem, które ujmuje maszynarnie. Należy do nich np. przesunięcia w prawo i w lewo o całkowitą liczbę odcinków między podkładami: po takim przesunięciu tor „nakładają 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 półobrot. Również dobrze jest półobrot wokół punktu B.

Mamy więc nieskończonej szó GM bezkarnych ruchów torem kolejki. Ruchy te można składać, tzn. wykonywać po kolei jeden po drugim (np. wtedy, gdy dziecko ogląda dobranockie). Ponadto, jeśli synek przylapie nas w takim wykonywaniu jednego z ruchów \( R \in G_m \), sasse możemy uspokoić jego lamento wykonując ruch odwrotny, \( R^{-1} \in G_m \), przywracający stan poprzedni. Ponieważ uznaliśmy wcześniej, że słoženie każdej pary ruchów bezkarnych prowadzi do takiego ruchu, to mamy w naszym zbiorze \( G_m \) "ruch" identycznościowy \( R = R^{-1} \), który polega na tym, że nie robimy absolutnie nic.

Rozważmy teraz zupełnie inną sytuację. Wyobraźmy sobie urząd celny, znajdujący się na granicy dwóch, niesèrent sąsiedzkościowych państw \( A \) i \( B \). Konsekwentnie, obywatele państwa \( A \) oszczędzają będące literą \( a \), a obywatele z państwa \( B \) – literą \( b \) (\( a \in A \) i \( b \in B \)). Graniczny urząd celny wygląda mniej więcej tak:

\[
\begin{array}{c}
\times \\
A \\
\end{array} \begin{array}{c}
abaababab \\
\times \\
bababb \\
\end{array} \begin{array}{c}
B \\
\end{array}
\]

Przy kilku biurkach uredzają celnicy, którzy, bez sięgnięcia pośpiechu, przeglądają bagaże podróżnych.

Ci ostatni czekają w kolejkach. Typowa kolejka ma postać: \( abaabaab \). Wraz z upływem czasu petenci zaczynają się nieracjonalnie, dyskutować i wreszcie klócą się między sobą. Jeśli języki państw \( A \) i \( B \) dostatecznie się różnią (jak np. czeński i węgierski), to klótnie będą w zasadzie przebiegać w parach \( aa \) i \( bb \). Przyjmijmy (dość realistyczne) sałoszenie, że para, która jest bardzo zauważalna, jest w konsekwencji w zależności od miejsca, w którym znajduje się, więc staje się dla kolejki nieistotna. Zatem, po dostatecznie długim okresie oczekiwania, w kolejce następują kolejne skrócenia par \( aa \) i \( bb \), np. \( abaabaab \rightarrow abaabaab \rightarrow aababbaa \rightarrow abaab \). Ostatnia kolejka jest stabilna: ona będzie już stała spokojnie. Po kilku godzinach w urzędzie celnym pozostaną już tylko kolejki stabilne.

Oszacujemy litera \( G_s \) sześcian wszystkich kolejek stabilnych. W praktyce możemy obserwować składanie kolejek. W tym celu jeden z uredzających celników powinien ogłosić bryliferową przerwę na herbatkę.

Kolejka oczekująca przy jego biurku zwykle w takiej sytuacji przemieszcza się solidarnie na koniec innej, możliwie krótkiej i aktualnie obsługiwanej kolejki.

Oczywiście, prowadzi to zwykle do sytuacji konfliktowej, ale po malym zamieszaniu dochodzimy do kolejki stabilnej. W sześciornie \( G_s \) mamy więc określoną operację składania kolejek. Dalej, dla dowolnej kolejki stabilnej \( K \) istnieje „antykolejka” \( K^{-1} \), która w procesie skracania całkowicie anihiluje \( K \). Na dole \( K \) do kolejki \( K = abaab \) należy dostawić na końcu (lub na początku) \( K^{-1} = bababa \). Powstanie z nich kolejki pusta \( I \) (marzenie każdego urednika).

Oczywiście \( I \) też saliczymy do sześciornia \( G_s \).

W następnym przykładzie sążymy się pieniędzami.

W czasach, gdy ceny są co najmniej trzycentowe, utrzymywanie portfela w portfelu staje się istotne. Dla wygodę wszystkie banknoty powinny być ułożone w ten sam sposób, np. tak, by patronujące im osobistoci swocone były „busią” do nas i „młośkami” do dołu. Od dowolnego polożenia banknotu można dojść do opisanego wyżej przez wykonanie jednego z następujących cześci ruchów:

\[
\begin{array}{c}
\times \\
\text{Narodowy Bank Polski} \\
\end{array} \begin{array}{c}
1000 \\
\text{Tł} \\
\end{array} \begin{array}{c}
\times \\
\end{array}
\]

\[
R_1 = R_2 + R_3
\]

Rzecz

36
Oznaczmy zbiór tych ruchów $G_{4l} = \{I, R_1, R_2, R_3\}$. Wykonując machinalne manipulacje porządkujące nasz portfel w istocie składamy ruchy z tego zbioru. Łatwo s瑙ać, 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” = $I$.


\[ W \]

\[ Z \quad L \]

Mamy $G_7 = \{I, S_1, S_2, S_3\}$, gdzie $S_i$ oznacza skok o i pór roku, a $I$ oznacza „pogoda bez zmian”.
Oczywiście, ruchy se wakacje $G_7$ można składać, a każdy z nich może zostać rekompensowany innym, odpowiednio dobrym ruchem wakacje.

Łatwo s瑙ać, że wszystkie opisane wyżej sytuacje mają pewne cechy wspólne. Po pierwsze, są każdym razem mamy do czynienia z pewnym zbiorem $G = \{G_1, G_2, G_3, G_4\}$. 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 dojrzala do sformułowania kolejnej teorii matematycznej. Należy po prostu zaoferowane teoretyczne wspólne przyjąć za aksjomaty nowej teorii, po czym nadać jej nazwę.

Definicja: Grupa nazywamy zbiór $G$ wyposażony w działanie $*: G \times G \to G$ 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 dowolnych $G \in I$ istnieje taki element $X^{-1} \in G$, że $X \circ X^{-1} = X^{-1} \circ X = I$; (element odwrotny – „anty-X”),
3) działanie $*$ jest łączne: $(X \circ Y) \circ Z = X \circ (Y \circ Z)$.

(Ta ostatnia własność jest łatwa do przeczytania dla niefachowca, ale występowała ona także we wszystkich przykładach.) Oczywiście, $G_1, G_2, G_3, G_4, G_7$ są przykładami grup.

W ten sposób narodziła się nowa teoria matematyczna. Jakie korzyści nam to przyniesie? Otóż każde twierdzenie, które teraz wyprowadzimy z aksjomatów, grupę będzie automatycznie obowiązywać w świecie ruchów torem dziennej kolejki, w urzędzie celnym na granicy, podczas porządkowania pliku banknotów, jak też w czasie skoków wakacje segara 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 przeczą nam do głowy, ale które zapewne pojawią się w przyszłości. W końcu, usunięcie z wzajemnych przykładów srodkowej fabuły powoli nam w czasie poszukiwania i dowodzenia twierdzeń skoncentrować się właśnie na tych cechach sytuacji, które są najistotniejsze.

Powinniśmy zatem teraz sięgnąć i postarać się udowodnić możliwe wiele twierdzeń o grupach. Oczywiście, szaar 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 rozwój na cele praktyczne: interesujące są te twierdzenia, które mają ważne zastosowania. W szczególności, dowodzone twierdzenia są często rozwijanie problemów przychodzących spostrzegane teorii.

Dla przykładu, jeśli jeden z członków w opisywanym wyżej urzędzie granicznym jest miłośnikiem Trylogii, to może mu się przydać do głowy analogie problemu pana Podbiłyski: czy ustawić się kiedyś równolegle obok siebie trzy identycznie wyglądające koleje turystów (np. z Turcji), które – gdy nagle zostawione razem – znikną? (Inne formułowanie: czy istnieje takie $K \in G$ i $K \neq I$, że $K \circ K \circ K = I$! – zbadamy to później.)

Zdarsza się też, że dowodzimy twierdzeń, które są wprawdzie całkowicie bezwzględne, ale są to bardzo przyjemne. Trudno wprawdzie wytłumaczyć, co to dokładnie znaczy, ale matematycy to rozumięją.

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

Przed każdym, kto sabiera 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-usię są takie same? Oczywiście, fabuła opisująca sytuację nie powinna mieć tu najmniejszego znaczenia. To, co jest istotne, zostało odcenione w definicji: grupa to zbór wraz ze specymaleniem działaniem.

Konsekwentnie, dwie grupy uważamy za takie same, jeśli: 1) mają "taki sam" zbior i 2) mają "takie samo" działanie.

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

1) $f$ jest wzajemnie jednoznaczną (zbiori $G, H$ są równowolnicze...),
2) $f(a \circ b) = f(a) \circ f(b)$ dla $a, b \in G$ (...i $f$ zachowuje działanie).

Zobaczymy najprostszy przykład pary grup isomorficznych. W skole podstawowej sporo czasu (i nerwów) zabiera nauczenie słuchaczy szaad mnożenia liczb dodatnich i ujemnych. Bystrzejsi uczniowie szybko szenają, że regulki, które Pani dyktuje, nie mają nic wspólnego z liczbami: ważne jest tylko, jak "się mnożą snaki". W istocie, mamy tu do czynienia z grupą $G = \{+,-\}$, której działanie najlepiej opisać tabelką:

<table>
<thead>
<tr>
<th>$+$</th>
<th>$+$</th>
<th>$+$</th>
<th>$-$</th>
<th>$-$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$+$</td>
<td>$+$</td>
<td>$+$</td>
<td>$-$</td>
<td>$+$</td>
</tr>
<tr>
<td>$-$</td>
<td>$-$</td>
<td>$-$</td>
<td>$+$</td>
<td>$-$</td>
</tr>
</tbody>
</table>

Opisujemy 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:

A. B.

Każydzie kolejny użytkownik może po przeprowadzonej rozmowie (lub nieudanej próbie) bądź przywrócić stan poprzedni, bądź też wymienić stan aparatu na przeciwny. (Typowa przycisna zmiana: leworecurzący urzędnik korzysta z aparatu, który był w stanie A.) Możemy rozważyć grupę zmian stanu aparatu $G_0$. Składają się ona z dwóch elementów: $I = "poostaw po starem", Z = "zmień stan".

Łatwo szaować, że operacje te składają się wg tabelki:

<table>
<thead>
<tr>
<th>$I$</th>
<th>$Z$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$I$</td>
<td>$I$</td>
</tr>
<tr>
<td>$Z$</td>
<td>$I$</td>
</tr>
</tbody>
</table>

Grupy $G_\pm$ oraz $G_0$ są isomorficzne. Istotnie, przekształcenie $f : G_\pm \to G_0$, $f(+) = I$, $f(-) = Z$ jest wzajemnie jednoznacznym i zachowuje działanie: funkcja $f$ po prostu "słumacy" tabelkę grupy $G_\pm$ na tabelkę grupy $G_0$.

Docieklowy Czytelnik powinien sobie teraz sadać pytanie: a co z grupami $G_\phi$, $G_\phi$, $G_{\pm}$, $G_\phi$, które pojawiały się na początku: czy są wśród nich pary grup isomorficznych (a więc ile sporoś nich musimy wpisać do Mądrey K siègi)?

Najbardziej podejrzane wygląda para grup: $G_{\pm}$ (manipulacje banknotem) i $G_\phi$ (zmiany klimatu): obie mają przeciêœ cztery elementy.

Czy istnieje isomorfizm $f : G_{\pm} \to G_\phi$? Latwo 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 $G_{\pm}$. 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 $S_1, S_2, S_3$. Wobec dwóch $S_2$ ma własność: $S_i \circ S_j = I$. Zatem nie istnieje równowartościowe przekształcenie $f$, które zachowuje działanie. Wniosek: grupy $G_{\pm}$ i $G_\phi$ nie są isomorficzne.

Natomiast grupy $G_\phi$ (ruchy torem kolejki) i $G_\phi$ (kolejki do celnika) są isomorficzne. Zbudujemy isomorfizm $f : G_{\phi} \to G_\phi$ w następujący sposób: powiemy, jaki ruch torem kolejki odpowiada ka¿dej stabilnej kolejce stojącej w urzędzie celnym. Po pierwsze, "ko³ekę pustą" przekształcimy na "bersztoru". Jednosobową kółkę a przenosimy na $O_A = półbór toru wokół środka podkładu $A$ (rysunek na początku artykułu). Podobnie kolejkę $b$ przekształcimy na półbór $O_B$. A dalej... nie mamy jeszcze do wyboru: ponieważ $f$ musi zachowywać działanie, a każda kolejka stabilna jest iloczynem kolejek postaci $a$ i $b$, to odpowiadający jej ruch torem jest już sztetyzmowany. Np. $f(ab) = f(a \circ b) = f(a) \circ f(b) = O_A \circ O_B = mersunięcie toru w prawo o jeden odstęp między podkładami. Poostawiam Czytelnikom sprawdzenie, że $f$ jest przekształceniem wzajemnie jednoznacznym (wskazówka: znaleźć przekształcenie odwrotne).

Jeśli mamy szabać, czy dwie grupy $G$ i $H$ są isomorficzne, to próbujemy szybko szubować isomorfizm $f : G \to H$. Jeśli nam się to uda — to problem jest rozwiązany. Inaczej wygląda sytuacja, gdy nawet długo trwane wysiłki nie przynosiły powodzenia: nie stanowi to wszak dowodu, że taki izomorfizm nie istnieje. Jak taki dowód usyskać?
Kluczem do rozwiązywania są tzw. niemieckini: trzeba znaleźć taka własność grupy $G$, która zachowuje się przy izomorfizmach, ale która nie przysługuje grupie $H$. Na przykład, porównując grupy $G_1$ i $G_2$, wykorzystaliśmy fakt, że dla dowolnego $R \in G_1$, mamy $R \circ R = I$, a w grupie $G_2$ to nieprawda: $S_1 \circ S_1 = S_2 \neq I$.

Podręczniki teorii grup są pełne niemieckin. Grupa, która ma taka specjalną własność, opartuje się zwykle specjalnym przysmakiem. Mamy więc grupy skończone, periodyczne, abelowe, rozwijalne, nilpotentne, wolne, ... i tystań innych. A oto konkretny przykład.

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

Narwa ta pochodzi od nazwiska matematyka norweskiego, Nielsa Abela.

Łatwo sprawdzić, że grupy $G_1$, $G_2$, $G_3$, $G_4$ są abelowe. Natomiast grupa $G_5$ kolejek do celników (jak i izomorficzna z nią grupa $G_6$) nie jest abelowa: elementy $a$ i $b$ 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 nierozstrzygany. U dowodnił to A. Markow w 1958 roku. Wobec tego klasyfikacja grup wymaga dużej pomysłowości, a Modrą Księgą Wszystkich Grup pozostaje w strefie marzeń. Nie wyklucza to jednak istnienia "klasyfikacji cząstkowych".


W tym celu ostatecznie nasze wymagania w stosunku do funkcji $f : G \rightarrow H$.

Definicja: Przekształcenie $f : G \rightarrow H$ 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 różnovoścnowościowe: elementy grupy $G$ mogą się poszepiać. Im więcej zlepień, tym słabszym echem odbijają się własności $G$ w "luszcze" $H$.

Np. przekształcenie $f : G \rightarrow H$, 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 $G_6$ na grupę znaków $G_{12}$: kolejkę $K$ przekształcamy na $+$, gdy stoi w niej parzysta liczba potentów; w przeciwnym przypadku $f(K) = -$.

Grupa $G_4$ 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 $n$ symetrii osiowych; razem $2n$ elementów. Grupa $D_n$ nosi nazwę grupy dihedralnej.

Dla każdego $n \geq 3$ określmy homomorfizm $f_n$ grupy $G_4$ na grupę $D_n$. Po pierwsze, zamiast $G_4$ weźmiemy $G_{12}$ – wiemy już, że to jest sama grupa, tylko w innym przebraniu. Wstarczy teraz nawiąać tor kolejowy na s pulpę o obwodzie równym $n$ odstępu między podkładami i spojrzeć na ten swój z boku: ruchy torem staną się wtedy obrotami i symetriami n-kąta.

Zauważmy, że gdy $n$ równe, to grupy dihedralne $D_n$ są coraz większe. Chwytyają one więc coraz to więcej informacji o grupie $G_4$. Dlatego też grupę $G_4$ nazwaliśmy "tym ciekawym nieskończoną grupą dihedralną" i oznaczono: $D_{\infty}$. Można ją opisać bezpośrednio w języku geometrii jak następuje: $D_{\infty}$ jest grupą tych izometrii prostej euklidesowej, które przeprowadzają zbior punktów o wspólnej prostej kalkowej w siebie. Grupa ta jest bardzo podobna do $D_n$, jeśli prostą potraktować jak "\infty-kąt".


39
Skłono 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 jest istotnie. W latach siedemdziesiątych udało się uzyskać, za pomocą komputera, pełną listę 4-wymiarowych grup krystalograficznych.

Wróćmy do sytuacji ogólniej. 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 jadrem homomorfizmu \( f \): \( \ker(f) = \{ X \in G : f(X) = I \} \). Łatwo sprawdzić, że jest to podgrupa grupy \( G \).

Na przykład, dla rozwiniętego przes nas na początek homomorfizmu \( f : G \to G \), mamy \( \ker(f) = \{ K : K \to \text{kolejka parysztej długości} \} = \{ (ab)^n : n \in \mathbb{Z} \} \). Przekształcenie \( g \): \( \ker(f) \to \mathbb{Z} \), dane wzorem \( g(ab)^n = n \), ustala isomorfizm grupy \( \ker(f) \)

s grupą liczb całkowitych.

Można powiedzieć, że homomorfizm \( f : G \to H \)

„rozluźnia” 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 spolne.

Już sama znajomość obu kawałków daje sporo informacji o grupie \( G \). Np. mamy już dostatecznie wiele informacji o grupie \( G \), aby pomóc celnikowi, a także salome 

Ligusinusa Podbięty 

Mysichkisek: nie istnieje taka kolejka \( K \in G \setminus \{ I \} \), że \( K^3 = I \). Mamy bowiem \( f : G \to \{+, - \} \)

i \( \ker(f) = Z \). Ponadto \( f(K^3) = f(I) = + \).

Ale \( -3 = - > \), więc pozostaje \( f(K) = + > element neutralny w G \). Stąd \( K \in \ker(f) \to Z \). Jednak w grupie liczby całkowite (z dodawaniem) nie ma takiego elementu \( K \neq 0 \), by \( K + K + K = 0 \).

(Wniosek: celnik musi niestety pozostać w niewinie.)

Widzimyśmy przed chwilą, jak pozytyczną rzeczą są homomorfizmy badanej grupy w grupy zbadane wcześniejszej. Ale skąd brać takie przekształcenia?

Rada jest prosta – należy odwrócić kota ogonem.

Każdy homomorfizm \( f : G \to H \) wyznacza podgrupę elementów „znajdnanych” \( \ker(f) \subseteq G \). Zobowiązuję więc tak: w badanej grupie \( G \) wybierzemy sobie najpierw podgrupę \( K \) elementów „do sgniecenia”, a grupa \( H \) i homomorfizm \( f \) utworzą się same: mówiąc nieścieńst, \( H \) powstanie z \( G \) przez umiejętny sgniecenie \( K \), a \( f \) będzie po prostu odwzorowaniem sgniającym.

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 \( f(gzg^{-1}) = f(g)f(z)f(g^{-1}) = f(g) \circ I \circ f(g)^{-1} = I \), tj. \( gzg^{-1} \in K \). 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 \( gzg^{-1} \in K \).

Przeważnie podgrupy nie są normalne, np. dla

\( G = G \) nie jest normalna podgrupa \( K = \{ I, O \} \).

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 \( H = G / \ker(f) \). Ale obie grupy:

\( K \) i \( H \) mają mniejszych 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 nasywamy prostymi.

Klasifikacja skończonych grup prostych jest bardzo

zawieszana. Niektoży specjaliści nawet twierdzą,

że już jest sakocona. Wszyscy jednak wiedzą, że

istniejące dowody wymagają jeszcze wielu uzupełnień.