$\theta\beta\ell\iota c\mathbb{Z}\varepsilon$ 2016

Koło Naukowe Matematyków UAM
oraz
Koło Matematyki i Informatyki Stosowanej UAM

wrzesień 2016 r.

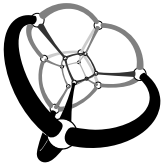
Wydawca: Koło Naukowe Matematyków UAM
Kontakt: konferencjaoblicze@gmail.com
Skład tekstu: Jędrzej Garnek
Korekta: Aleksandra Kaim
Druk: Wieland Drukarnia Cyfrowa

Odpowiedzialność za treść tekstów ponoszą ich autorzy.
ISBN: 978-83-946301-0-2

Projekt Potęga matematyki realizowany dzięki środkom finansowym otrzymanym od Miasta Poznań.

POZnań

Wykonawca projektu:
Poznańska Fundacja Matematyczna



http://oblicze.wmi.amu.edu.pl

Poznań, wrzesień 2016

Spis treści

Symbolem ♣ oznaczono artykuły przystępne również dla licealistów.

Podsumowanie

Trzecia edycja $\theta\beta\ell\imath c\mathbb{Z}a$ odbyła się w dniach 13-15 maja 2016 na Wydziale Matematyki i Informatyki UAM. Wzięło w niej udział około 120 osób z całej Polski. Organizatorem konferencji było Koło Naukowe Matematyków UAM oraz Koło Matematyki i Informatyki Stosowanej UAM. Konferencję rozpoczynał wykład dra Bartłomieja Bzdęgi pt. *„Twierdzenia o strażakach"* oraz wykład prof. UAM dra hab. Kaziemierza Świrydowicza pt. *„O logikach nieklasycznych"*. W ciągu trzech dni uczestnicy mieli możliwość wysłuchania ponad 50 referatów z najróżniejszych dziedzin matematyki, a także wzięcia udziału w sesji plakatowej. W konkursach na najlepszy referat i plakat zwyciężyli:

Najlepsze referaty:

- I miejsce – *„Najlepszy trik karciany na świecie - rzecz o potędze permutacji"* - Kamil Szymon Jadeszko (Politechnika Białostocka),
- II miejsce – *„Big Data a Analiza Danych Funkcjonalnych"* - Maria Skupień (Politechnika Krakowska),
- III miejsce – *„Obiekty de Bruijna odporne na przewracanie"* - Maciej Biesek (Uniwersytet im. Adama Mickiewicza).

Najlepsze plakaty:

- I miejsce – *„Zbiory Gerszgorina i Brauera danej macierzy"* - Alicja Wróbel,
- II miejsce – *„Grupy warkoczy"* - Agnieszka Stelmaszyk, Tomasz Śmierzchalski,
- III miejsce – *„Tam, gdzie matematyka, sztuka i magia łączą swoje siły czyli zaskakujące fakty o origami"* - Barbara Ciesielska, Agnieszka Kowalczyk.

Zwycięzcy konkursu referatów oraz plakatów

Podczas tej edycji $\theta\beta\ell\iota c\mathbb{Z}a$ po raz pierwszy odbyła się również sesja dedykowana dla licealistów. Mogli oni wysłuchać referatów dotyczących między innymi opisu piękna za pomocą matematyki, teorii warkoczy oraz sztuczek karcianych. W sesji tej wzięło udział około 20 licealistów oraz nauczycieli z poznańskich szkół, m.in. z Liceum Ogólnokształcącego św. Marii Magdaleny w Poznaniu, VII oraz VIII Liceum Ogólnokształcącego w Poznaniu.

Organizatorzy

W przygotowanie konferencji zaangażowane były w szczególności następujące osoby:

- organizatorzy konferencji:

  Katarzyna Donaj, Katarzyna Taczała, Aleksandra Kaim, Eliza Jackowska, Tomasz Dwojak, Andrzej Kokosza, Paweł Płaczek, Karolina Rogusz, Zofia Nowacka,

Mieczysław Krawiarz, Jędrzej Garnek, Kamil Sikorski, Rafał Bystrzycki, Agnieszka Stelmaszyk.

Organizatorzy konferencji $\theta\beta\ell\iota c\mathbb{Z}\varepsilon$ 2016

- pomocnicy:

  Gabriela Pałka, Ewelina Bukowska, Viktoriya Olechnowicz, Konrad Zierko, Joanna Kowalska, Justyna Tabor,

- Aleksandra Luberecka, która udokumentowała konferencję zdjęciami,
- Magdalena Kuchta, która wykonała dla nas plakat.

O kołach naukowych

Koło Naukowe Matematyków UAM

Koło Naukowe Matematyków UAM działa na Wydziale Matematyki i Informatyki od 1993 r. Celem działania Koła jest przede wszystkim poszerzanie wiedzy matematycznej poza zakres materiału obowiązującego na studiach. Członkowie Koła przygotowują referaty i odczyty na tematy, które ich interesują oraz prezentują je pozostałym członkom. Od czasu do czasu rozwiązują też ciekawe zadania, przygotowując się do konkursów matematycznych. Oprócz tego, Koło Naukowe Matematyków organizuje wykłady popularyzatorskie dla studentów prowadzone przez pracowników naukowych Uniwersytetu. Członkowie Koła służą także pomocą innym studentom w zrozumieniu i przyswajaniu wiadomości ze studiów.

Koło Naukowe Matematyki i Informatyki Stosowanej UAM

Koło Naukowe Matematyki i Informatyki Stosowanej powstało w 2014 roku z inicjatywy studentów Wydziału Matematyki i Informatyki. To grupa ludzi, których połączyła wspólna pasja i chęć robienia czegoś więcej. Więcej niż tylko uczenia się suchej teorii dla zdania egzaminu. Jesteśmy studentami, którzy poszukują zastosowań informatyki i wyższej matematyki w realnych problemach. Pasjonuje nas sposób w jaki matematyka osadzona jest w rzeczywistości, a informatyka rozwiązuje jej trudne problemy. Naszym celem jest stworzenie młodego i dynamicznego środowiska naukowego, w którym będziemy rozwijać matematyczne zainteresowania korzystając z wiedzy naszych kolegów, pracowników naukowych wydziału oraz instytucji działających na rynku. W naszych planach jest nawiązanie kontaktu z firmami oraz kołami studenckimi, ponieważ wierzymy że zdobyta w okresie studiów wiedza pozwoli nam na znalezienie ciekawej i satysfakcjonującej pracy po studiach.

Historia $\theta\beta\ell\iota c\mathbb{Z}a$

Pomysł zorganizowania $\theta\beta\ell\iota c\mathbb{Z}a$ narodził się w 2013 roku podczas jednej z wrocławskich konferencji dla studentów. Studenci poznańskich uczelni – Dominika Kubijk, Katarzyna Taczała (studentki UAM) oraz Paweł Rogalski (ówcześnie student Politechniki Poznańskiej) – stwierdzili, że podobna inicjatywa przydałaby się również w naszym mieście.

Logo konferencji – $\theta\beta\ell\iota c\mathbb{Z}\varepsilon$ – miało kojarzyć się z matematyką zarówno dosłownie, jak i wizualnie, a ponadto przypominać o różnych obliczach matematyki. Konferencja z założenia miała być organizowana przez studentów i dla studentów, a także nie mieć ograniczeń tematycznych. W realizację pomysłu szybko zaangażowały się również inne osoby. Pierwsza konferencja $\theta\beta\ell\iota c\mathbb{Z}\varepsilon$ została zorganizowana w dniach 9-11.05.2014 roku na Wydziale Matematyki i Informatyki pod szyldem UAM oraz Politechniki Poznańskiej. Wzięło w niej udział około 30 osób.

W kolejnej edycji (która odbyła się w dniach 8-10.05.2015) uczestniczyło już znacznie więcej osób, bo aż 80. W dwóch pierwszych edycjach uczestnicy mieli możliwość wysłuchania referatów na tak odległe tematy, jak np.:

- związki teorii grafów losowych z sieciami społecznościowymi,
- zastosowania teorii gier w polityce,
- fizyczne motywacje pojęcia rozmaitości różniczkowej,
- matematyczne podstawy gry w Monopoly.

Sponsorzy i partnerzy

Za wsparcie konferencji dziękujemy w pierwszej kolejności:

- **władzom Wydziału Matematyki i Informatyki UAM**, które wsparły konferencję finansowo oraz udostępniły budynek wydziału na czas konferencji.
- **Poznańskiej Fundacji Matematycznej**, która umożliwiła zorganizowanie sesji licealnej, wydanie niniejszej publikacji oraz pomogła w ufundowaniu nagród dla referentów. Otrzymane wsparcie pochodziło z projektu **Potęga matematyki** realizowanego dzięki środkom finansowym otrzymanym od **Miasta Poznań**.
- **fundacji Science To Business**, która pomagała nam w technicznej obsłudze przedsięwzięcia.

Podczas konferencji wykorzystaliśmy również środki zdobyte w konkursie inicjatyw studenckich „Kowadło", organizowanym przez **Samorząd Studencki UAM**.

Nagrody dla referentów i autorów plakatów zostały ufundowane przez firmę **Wolfram**, **Polskie Towarzystwo Matematyczne**, **European Mathematical Society** oraz **Poznańską Fundację Matematyczną**. **Miasto Poznań** ufundowało puchary dla autorów najlepszego referatu oraz plakatu.


Science2Business
foundation


Poznańska
Fundacja
Matematyczna


European Mathematical Society
Publishing House


WOLFRAM
COMPUTATION MEETS KNOWLEDGE


POZnan


rok zał. 1919
ptm

Obiekty de Bruijna odporne na przewracanie

Maciej Biesek
Uniwersytet im. Adama Mickiewicza w Poznaniu
Wydział Matematyki i Informatyki

Obiekty de Bruijna są ciekawym zagadnieniem kombinatorycznym, a – jak twierdzą badacze – na ich ślad można natrafić nawet w źródłach średniowiecznych. Celem niniejszego referatu jest zaprezentowanie Czytelnikowi szczególnego rodzaju obiektów de Bruijna – obiektów odpornych na przewracanie, sposobu ich tworzenia oraz unikatowych zastosowań. Zanim jednak to nastąpi, wymagane jest wprowadzenie podstawowych informacji o klasycznych obiektach de Bruijna, począwszy od grafów, poprzez ciągi, a na macierzach kończąc. Oprócz formalnych definicji przedstawię również sposoby generowania tych obiektów, ich własności oraz praktyczne zastosowania.

1.1 Obiekty de Bruijna

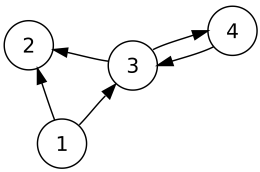
1.1.1 Graf de Bruijna

Pierwszym obiektem, który poznamy będzie graf de Bruijna. Zanim jednak to nastąpi, konieczne jest zrozumienie, czym jest graf skierowany.

Definicja 1.1. Grafem skierowanym (**digrafem**) D nazywamy parę $D = (V, E)$, gdzie V jest niepustym zbiorem wierzchołków grafu, a E pewnym zbiorem uporządkowanych par tych

wierzchołków, nazywanym zbiorem krawędzi skierowanych (lub zbiorem łuków) grafu D.

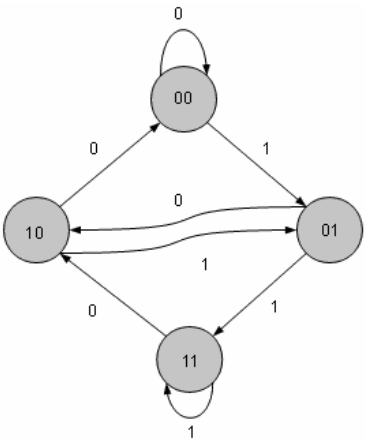
Przykład takiego grafu widzimy na rysunku 1.1.



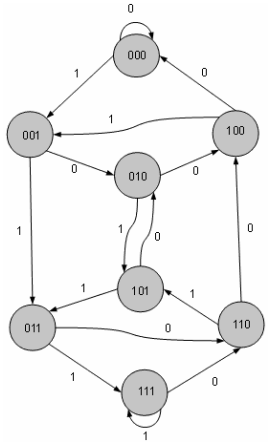
Rysunek 1.1: Graf skierowany

Definicja 1.2. Grafem de Bruijna o danych parametrach n oraz k nazywamy skierowany graf etykietowany $G_B = (V, E)$. Wierzchołki odpowiadają wszystkim słowom długości $n-1$ nad alfabetem mocy k. Krawędź pomiędzy dwoma dowolnymi wierzchołkami $u, v \in V$ istnieje wtedy i tylko wtedy, gdy ostatnie $n-2$ znaków słowa u zgadza się z pierwszymi $n-2$ znakami słowa v. Wówczas krawędź ta zostaje oetykietowana ostatnim znakiem v.

Definicja nie jest banalna, więc aby lepiej ją zrozumieć, spójrzmy na rysunki 1.2 oraz 1.3. Po lewej stronie znajduje się graf de Bruijna, dla $n = 3$ oraz $k = 2$. Wszystkie słowa długości $n-1$ (czyli w tym przypadku długości 2) nad alfabetem mocy 2 to: 00, 01, 10 i 10. To właśnie one będą wierzchołkami tego grafu. Według definicji, krawędź pomiędzy dwoma wierzchołkami istnieje wtedy, gdy ostatnie $n-2$ (w tym przypadku jeden ostatni) znaki słowa pierwszego są takie same jak pierwsze $n-2$ słowa drugiego. Etykietujemy ją wówczas ostatnim znakiem drugiego wierzchołka. Wracając do naszego przykładu, wybieramy dowolny wierzchołek, niech to będzie 10. Teraz prowadzimy krawędź z etykietą 0 do wierzchołka 00 (ponieważ ostatni znak 10 jest taki sam, jak pierwszy 00) oraz krawędź z etykietą 1 do wierzchołka 01. Powtarzając ten krok dla pozostałych wierzchołków, otrzymamy graf pokazany na rysunku 1.2. Analogiczną analizę rysunku 1.3 pozostawiam Czytelnikowi jako proste ćwiczenie.



Rysunek 1.2:
G_B dla $n = 3$, $k = 2$



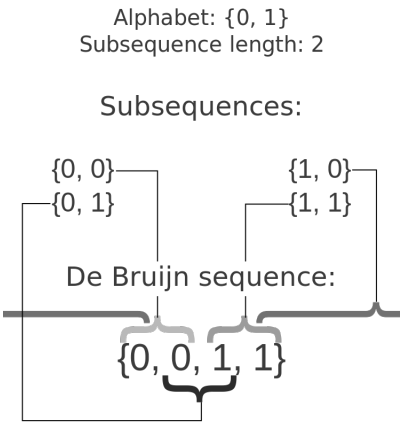
Rysunek 1.3:
G_B dla $n = 4$, $k = 2$

W dalszej części potrzebna będzie nam następująca własność: każdy graf de Bruijna posiada obchód Eulera, to znaczy zamknięty spacer zawierający każdą krawędź dokładnie jeden raz.

1.1.2 Ciąg de Bruijna

Definicja 1.3. Ciągiem de Bruijna rzędu n nad alfabetem mocy k nazywamy cykliczny ciąg długości k^n, w którym każdy podciąg długości n występuje dokładnie raz. Oznaczamy go jako $B(k, n)$.

Zobaczmy to na przykładzie. Wszystkie możliwe podciągi długości 2 nad alfabetem $\Sigma = \{0, 1\}$ to: 00, 01, 10 i 11. Jak łatwo zauważyć na Rysunku 1.4, każdy z nich występuje w ciągu $B(2, 2)$ dokładnie raz. Analogicznie dla ciągu $B(2, 3)$, który jest postaci 01000111 – wszystkie podciągi długości 3 nad alfabetem Σ to: 010, 100, 000, 001, 011, 111, 110, 101. Każdy z nich występuje w tym ciągu dokładnie jeden raz.



Rysunek 1.4: $B(2, 2)$

Oba poznane do tej pory obiekty są ze sobą ściśle powiązane: istnieje bijektywna odpowiedniość między ciągami etykiet na obchodach Eulera w grafie de Bruijna, a ciągami de Bruijna. Dzięki temu, mając graf, możemy w łatwy sposób wyznaczyć ciąg de Bruijna: wystarczy w grafie znaleźć obchód Eulera (np. za pomocą algorytmu Fleury'ego), zapisując etykiety kolejno odwiedzanych krawędzi. Ciąg etykiet jest ciągiem de Bruijna, który chcieliśmy znaleźć.

1.1.3 Macierz de Bruijna

Macierze de Bruijna są uogólnieniem ciągów de Bruijna na dwa wymiary.

Definicja 1.4. Macierzą de Bruijna ($M_{DB}(r, v; n, m)_d$) nazywamy macierz wymiaru $r \times v$ nad alfabetem mocy d, w której każde okno rozmiaru $n \times m$ występuje dokładnie raz.

Oknem nazywamy podmacierz, która powstaje przez wybranie sąsiadujących ze sobą elementów macierzy.

Macierz de Bruijna $M_{DB}(4,4;2,2)_2$ z oknem o wymiarach 2×2 wygląda następująco:

$$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

Kolorami zaznaczono przykładowe okna tej macierzy. Nie są to oczywiście jedyne możliwości wyboru takich podmacierzy. Jak podaje definicja, żadne z okien rozmiaru 2×2 nie występuje w tej macierzy więcej niż raz.

1.1.4 Zastosowania

Obiekty de Bruijna znalazły zastosowanie w wielu różnych dziedzinach życia.

Grafy de Bruijna z łatwością mogą zostać wykorzystane do generowania słów dowolnej długości nad alfabetem ustalonej mocy. Wiąże się z tym kolejne ich zastosowanie, a mianowicie sekwencjonowanie (czyli odczytywanie kolejności par nukleotydowych w cząsteczce) łańcuchów DNA.

Ciągi de Bruijna znalazły z kolei zastosowanie w kryptografii. Użyteczna jest tu szczególnie jedna, istotna własność tych ciągów – żaden podciąg nie występuje w nim więcej niż raz. Dzięki temu, każdy k-elementowy podciąg może odpowiadać innemu znakowi zakodowanej wiadomości.

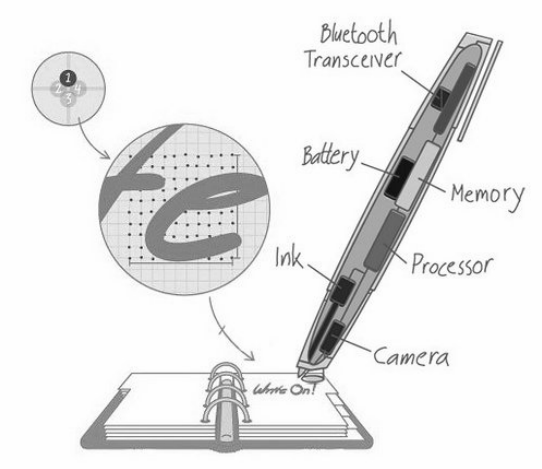
Oprócz powyższych zastosowań, obiekty de Bruijna, ze względu na swoje wyjątkowe własności, są również przedmiotem wielu badań teoretycznych.

1.2 Obiekty de Bruijna odporne na przewracanie

Obiekty de Bruijna odporne na przewracanie są szczególną odmianą obiektów de Bruijna.

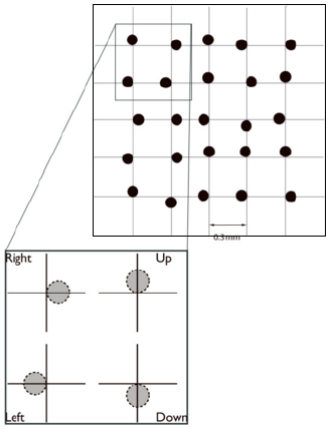
1.2.1 Macierz de Bruijna odporna na przewracanie

Motywacją do badań nad tymi obiektami jest problem określania lokalizacji na kartce papieru przez długopis cyfrowy. Jak taki długopis działa? Poniżej znajduje się schematyczny rysunek, przedstawiający jego budowę.

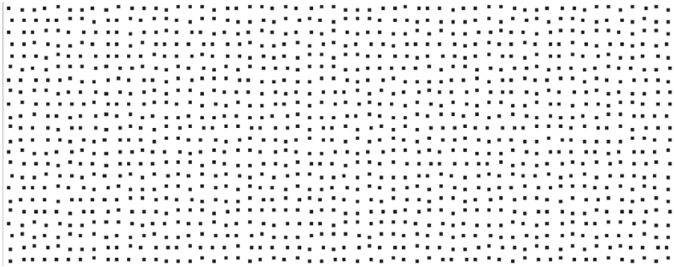


Rysunek 1.5: Budowa długopisu cyfrowego

Urządzenie składa się z baterii, nadajnika bluetooth, pamięci RAM, procesora, wkładu oraz kamery. To właśnie kamera ma niebagatelne znaczenie w trakcie korzystania z długopisu – podczas pisania po uprzednio zakropkowanym papierze sczytuje mały obszar arkusza i na tej podstawie urządzenie jest w stanie poprawnie się na nim zlokalizować. Kropka może zajmować jedną z czterech pozycji – powyżej linii, poniżej, na lewo od niej lub też na prawo. Rozkładowi kropek możemy przyjrzeć się bliżej na rysunku 1.6. Fragment zakropkowanego arkusza papieru został przedstawiony na ilustracji 1.7.



Rysunek 1.6: Rozkład kropek na papierze cyfrowym



Rysunek 1.7: Papier cyfrowy (digital paper), wykorzystywany przez Anoto

Długopis cyfrowy podczas pisania po takim właśnie arkuszu sczytuje jego mniejszy fragment. Jednak aby korzystanie z urządzenia miało sens, kamera musi być niewrażliwa na kąt trzymania długopisu i położenie kartki. Chcemy bowiem, aby po obrocie kartki (lub długopisu) urządzenie nadal potrafiło poprawnie się na niej zlokalizować.

Układ kropek na danym arkuszu możemy zapisać jako ma-

cierz. W tym celu przyjmujemy następujące oznaczenia: kropkę „w górę" kodujemy jako 0, kropkę „w prawo" jako 1, kropkę „w dół" jako 2 oraz kropkę „w lewo" jako 3. Jak się okazuje, gdybyśmy w ten sposób zakodowali kropki z Rysunku 1.7, otrzymana macierz byłaby fragmentem macierzy de Bruijna odpornej na przewracanie z oknem wymiaru 6×6.

Czym jest jednak ten przewrót?

Definicja 1.5. Relacją przewrócenia (**przewrotem**) macierzy nazywamy złożenie relacji obrotu macierzy z relacją przesunięcia wartości jej elementów.

Oznacza to, że podczas jednokrotnego przewracania macierzy dokonujemy przemieszczania jej elementów o kąt 90 stopni, przy jednoczesnej zmianie ich wartości, zgodnie z wcześniej zdefiniowaną funkcją przesunięcia.

Niech alfabet będzie postaci $\Sigma = \{0, 1, 2, 3\}$, a funkcja przesunięcia $f : \Sigma \to \Sigma$ będzie zdefiniowana w następujący sposób:

$$f(x) = (x + 1) \mod 4\,, \text{dla}\, x \in \{0, 1, 2, 3\}.$$

Wówczas przewrotem macierzy $A = \begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix}$ jest macierz:

$$A^* = \begin{bmatrix} 3 & 1 \\ 0 & 2 \end{bmatrix}.$$

Prześledźmy ten przykład. Element 0 zajmuje pozycję $A(1, 1)$, w wyniku relacji przewrotu będzie miał wartość $f(0) = 1$ i znajdzie się na pozycji $A(1, 2)$. Podobnie będzie z elementem 1, początkowo zajmującym pozycję $A(1, 2)$. W wyniku relacji jego wartość zostanie zmieniona na $f(1) = 2$, a znajdzie się na pozycji $A(2, 2)$. Analogicznie postępujemy z kolejnymi elementami macierzy.

Relacja przewrotu macierzy jest relacją równoważności, która dzieli zbiór macierzy na rozłączne klasy abstrakcji, przy czym dowolne dwie macierze znajdują się w jednej klasie abstrakcji wtedy i tylko wtedy, gdy jedną z nich można uzyskać poprzez pewną stałą liczbę obrotów i zmian wartości drugiej. Oznacza

to, że w jednej klasie abstrakcji znajdują się te same macierze, z dokładnością do relacji przewrotu macierzy.

Uzbrojeni w powyższe narzędzia możemy przejść do definicji macierzy de Bruijna odpornej na przewracanie.

Definicja 1.6. Macierzą de Bruijna odporną na przewracanie nazywamy macierz de Bruijna, której wszystkie okna danego rozmiaru pochodzą z różnych klas abstrakcji relacji przewracania macierzy. Oznaczamy ją jako: $M^r_{DB}(r,v)_d$, gdzie $r \times v$ jest wymiarem okna, a d– liczbą elementów alfabetu.

1.2.2 Ciąg de Bruijna odporny na przewracanie

Ciąg de Bruijna odporny na przewracanie jest uproszczeniem idei macierzy na obiekt jednowymiarowy. Podobnie jak w przypadku macierzy, tak i tutaj stosownym wydaje się zacząć od zdefiniowania relacji.

Definicja 1.7. Relacją przewrócenia ciągu nazywamy zmianę wartości jego wszystkich elementów, zgodnie z ustaloną funkcją.

Tak jak poprzednio, alfabet definiujemy jako $\Sigma = \{0,1,2,3\}$, a funkcję zmiany wartości $f : \Sigma \to \Sigma$ jako:

$$f(x) = (x+1) \mod 4\,, dla\, x \in \{0,1,2,3\}.$$

Wówczas przewrotem ciągu 0123 jest ciąg 1230. Poddając przykład analizie, nietrudno zauważyć, że produktem przewrotu ciągu $A_n = a_1a_2...a_n$ będzie $B_n = f(a_1)f(a_2)...f(a_n)$.

Podobnie jak było w przypadku macierzy, tak i tutaj relacja przewrotu jest relacją równoważności i dzieli zbiór ciągów na rozłączne klasy abstrakcji, przy czym dowolne dwa ciągi znajdują się w tej samej klasie abstrakcji wtedy i tylko wtedy, gdy jeden z nich może zostać uzyskany przez dokonanie pewnej liczby przewrotów drugiego. Oznacza to, że w każdej klasie abstrakcji znajdują się te same ciągi, z dokładnością do przewrotu.

Teraz, kiedy wiemy już, jak pojęcia poznane w poprzednim podrozdziale odnoszą się do jednowymiarowych obiektów, możemy zdefiniować ciąg de Bruijna odporny na przewracanie.

Definicja 1.8. Ciągiem de Bruijna odpornym na przewracanie nazywamy ciąg de Bruijna rzędu n nad alfabetem mocy k, którego wszystkie podciągi długości n pochodzą z różnych klas abstrakcji relacji przewracania ciągu. Oznaczamy go jako: $B^r(k, n)$

1.2.3 Zastosowania

Macierze de Bruijna odporne na przewracanie są wykorzystywane w widzeniu komputerowym. Wyobraźmy sobie robota przemysłowego, który porusza się po długim korytarzu w jedną i w drugą stronę. Podstawowym problemem jest to, że robot powinien wiedzieć gdzie się znajduje. Frank Sinden uznał, że pole pod urządzeniem można traktować jako macierz de Bruijna. Dzięki temu, że każda podmacierz rozmiaru $n \times m$ występuje w niej wyłącznie jeden raz, robot doskonale wie, na którym polu się znajduje. Ze względu na to, że wszystkie okna tej macierzy pochodzą z różnych klas abstrakcji robot jest w stanie poprawnie się zlokalizować nawet po obrocie, więc nie jest ograniczony do poruszania się wyłącznie w jednym kierunku. Według podobnej zasady działa wspomniany już długopis cyfrowy. Skutkiem tego, że wszystkie okna danego rozmiaru macierzy utworzonej z zakodowanych kropek pochodzą z różnych klas abstrakcji, było rozwiązanie problemu powtarzalności kropkowanych arkuszy. W konsekwencji – każda generowana kartka jest inna. Jakie ma to znaczenie? Pozwala powrócić do dokumentu, który był wypełniany kilka miesięcy temu, a system poprawnie zinterpretuje to, co użytkownik zapisał przy pomocy długopisu cyfrowego. Co więcej, nie dość, że będzie wiedział, o który dokument chodzi, to również bez trudu zorientuje się na której jego stronie dokonano zmian. Dzięki temu możliwe było zastosowanie systemu wykorzystującego długopisy cyfrowe na szeroką skalę. Dziś są one używane m.in. do przeprowadzania ankiet, prowadzenia do-

kumentacji medycznej oraz obsługi formalnej sieci transportu.

Ciągi de Bruijna odporne na przewracanie do tej pory nie znalazły praktycznego zastosowania. Niemniej, podobnie zresztą jak ich dwuwymiarowe odpowiedniki, stanowią ciekawy materiał do badań teoretycznych. Za przykład takich rozważań można podać problem wymiaru macierzy, czy też problem długości ciągu – od lat matematycy próbują bezskutecznie wskazać i udowodnić dokładne oszacowania.

Iloczyn Kroneckera

Katarzyna Donaj
Uniwersytet im. Adama Mickiewicza w Poznaniu
Wydział Matematyki i Informatyki

2.1 Wstęp

Macierze to jedne z najprostszych struktur w matematyce. Mimo to są wykorzystywane w wielu dziedzinach nauki. Poniższy artykuł ma na celu wprowadzenie do informatyki kwantowej, poprzez pokazanie zastosowania w niej iloczynu Kroneckera.

2.2 Iloczyn Kroneckera

Definicja 2.1. Dla $A \in M_{m,n}(K)$ oraz $B \in M_{l,k}(K)$ definiujemy **iloczyn tensorowy** $A \otimes B$ za pomocą formuły opisanej w tym rozdziale. Macierz $A \otimes B$ można zapisać w postaci blokowej, w której blok (i, j) jest iloczynem skalara a_{ij} oraz macierzy B, czyli

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{bmatrix}.$$

Przykład 2.2. *Weźmy przykładowe macierze:*

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, \qquad B = \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix}.$$

Ich iloczyn Kronekera jest postaci:

$$A \otimes B = \begin{bmatrix} 1 \cdot B & 2 \cdot B \\ 3 \cdot B & 4 \cdot B \end{bmatrix} = \begin{bmatrix} 5 & 6 & 10 & 12 \\ 7 & 8 & 14 & 16 \\ 15 & 18 & 20 & 24 \\ 21 & 24 & 28 & 32 \end{bmatrix}.$$

Po poznaniu głównego przedmiotu naszych rozważań, przejdźmy do jego własności:

(1) $(\alpha A) \otimes (\beta B) = \alpha\beta(A \otimes B)$, dla dowolnych α, β

(2) Jeżeli $A, B \in M_{m,n}(K)$ oraz $C \in M_{p,q}(K)$, to

$$(A + B) \otimes C = A \otimes C + B \otimes C.$$

(3) $(A \otimes B) \otimes C = A \otimes (B \otimes C)$

(4) $(A \otimes B)^T = A^T \otimes B^T$

(5) Jeżeli $A, B \in M_{m,m}(K)$, to:

$$\operatorname{tr}(A \otimes B) = \operatorname{tr} A \cdot \operatorname{tr} B$$

(6) Macierze identycznościowe $I_m \in M_{m,m}(K), I_n \in M_{n,n}(K), I_{mn} \in M_{mn,mn}(K)$ spełniają równość:

$$I_m \otimes I_n = I_{mn}.$$

(7) Dla macierzy $A \in M_{m,n}(K), B \in M_{p,q}(K), C \in M_{n,r}(K)$ oraz $D \in M_{q,s}(K)$:

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$$

(8) Jeżeli A i B są nieosobliwe, to:

$$(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}.$$

(9) Jeżeli A i B są macierzami ortogonalnymi, to macierz

$$A \otimes B$$

też jest macierzą ortogonalną.

Iloczyn Kroneckera bywa często stosowany na przykład w informatyce kwantowej. Jest to dziedzina łącząca informatykę i mechanikę kwantową, zajmująca się wykorzystaniem własności układów kwantowych do przesyłania i obróbki informacji. Pokażę to od matematycznej strony.

2.3 Notacja Diraca

Najczęściej w informatyce kwantowej posługujemy się notacją Diraca. Polega ona na przedstawianiu wektorów kolumnowych za pomocą symbolu *ket* $|\phi\rangle$ oraz wektorów wierszowych za pomocą symbolu *bra* $\langle\phi|$.
Zapis $|k\rangle$, gdzie $k \in \mathbb{N}$ oraz k jest przeważnie zapisane w systemie binarnym, oznacza wektor kolumnowy posiadający wartość 1 na k-tej pozycji, licząc od zera oraz 0 na wszystkich pozostałych miejscach. Zatem zapisy $|0\rangle, |1\rangle, |10\rangle, |011\rangle$ oznaczają następujące wektory:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

$$|10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \qquad |110\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

Iloczyn Kroneckera w notacji Diraca:

$$|0\rangle \otimes |11\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \cdot 0 \\ 1 \cdot 0 \\ 1 \cdot 0 \\ 1 \cdot 1 \\ 0 \cdot 0 \\ 0 \cdot 0 \\ 0 \cdot 0 \\ 0 \cdot 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |011\rangle .$$

.

2.4 Rejestr kwantowy

Definicja 2.3 (Kubit)**. Kubit (bit kwantowy)** ψ jest to dwupoziomowy układ kwantowy. Reprezentuje go wektor w dwuwymiarowej, zespolonej przestrzeni Hilberta:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle ,$$

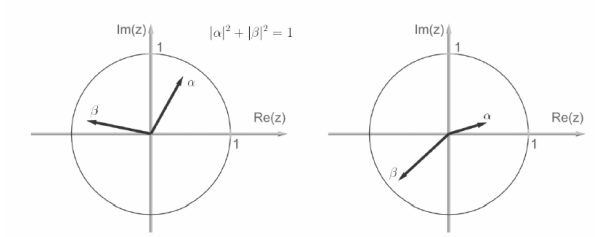
gdzie $|\alpha|^2 + |\beta|^2 = 1$ oraz $\alpha, \beta \in \mathbb{C}$.

Obserwacja(odczyt) bitu kwantowego daje w wyniku 0 lub 1 z prawdopodobieństwem odpowiednio $|\alpha|^2$ i $|\beta|^2$.
Następujące wektory

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

tworzą bazę standardową(obliczeniową) w dwuwymiarowej, zespolonej przestrzeni stanu kubitu. Liczby α i β nazywamy amplitudami stanów bazowych odpowiednio $|0\rangle$ oraz $|1\rangle$.

Reprezentację graficzną kubitu znaleźć można na rysunku 2.1.



(a) Stan kubitu (b) Inny stan kubitu

Rysunek 2.1: Reprezentacja kubitu.

Stan $|\phi\rangle$ dwóch kubitów jest **splątany**, jeśli nie można go przedstawić w postaci iloczynu Kroneckera pojedynczych kubitów, czyli:

$$|\phi\rangle \neq (\alpha_0 |0\rangle + \beta_0 |1\rangle) \otimes (\alpha_1 |0\rangle + \beta_1 |1\rangle),$$

gdzie $|\alpha_0|^2 + |\beta_0|^2 = 1$, $|\alpha_1|^2 + |\beta_1|^2 = 1$.
Stan, który nie jest splątany nazywamy **rozkładalnym**.

Definicja 2.4. Rejestr kwantowy to uporządkowany układ m kubitów o długości m. Może być on rozpatrywany jako układ izolowany złożony z wielu układów składowych.

W przypadku rejestru kwantowego, składającego się jedynie z dwóch kubitów $|q_0\rangle = \alpha_0 |0\rangle + \beta_0 |1\rangle$ i $|q_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle$, stan rejestru opisywany jest przez iloczyn Kroneckera:

$$|q_0\rangle \otimes |q_1\rangle = (\alpha_0 |0\rangle + \beta_0 |1\rangle) \otimes (\alpha_1 |0\rangle + \beta_1 |1\rangle) =$$

$$= \alpha_0\alpha_1 |0\rangle \otimes |0\rangle + \alpha_0\beta_1 |0\rangle \otimes |1\rangle + \beta_0\alpha_1 |1\rangle \otimes |0\rangle + \beta_0\beta_1 |1\rangle \otimes |1\rangle =$$

$$= \alpha_0\alpha_1 |00\rangle + \alpha_0\beta_1 |01\rangle + \beta_0\alpha_1 |10\rangle + \beta_0\beta_1 |11\rangle .$$

2.5 Bramki kwantowe

Definicja 2.5. Macierz unitarna to macierz kwadratowa o elementach rzeczywistych lub zespolonych, która pomnożona przez swoje sprzężenie hermitowskie daje macierz jednostkową:

$$UU^{\dagger} = U^{\dagger}U = I_n,$$

gdzie n jest wymiarem macierzy U.

Definicja 2.6. Bramką kwantową nazywamy dowolną operację przeprowadzającą kubity w inne stany.

Każda bramka kwantowa jest reprezentowana przez macierz unitarną. Przejścia między stanami są obliczane poprzez pomnożenie stanu z lewej strony przez macierz unitarną:

$$U \cdot |\phi\rangle .$$

Przykładowe bramki kwantowe:

(1) Bramka negacji:

$$NOT = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Bramka negacji zamienia ze sobą amplitudy prawdopodobieństw stanów bazowych:

Przykład 2.7. *Działanie bramki NOT na* $|\phi\rangle = \frac{1}{5}|0\rangle + \frac{2\sqrt{6}}{5}|1\rangle$*:*

$$\begin{aligned} NOT\,|\phi\rangle &= NOT\big(\frac{1}{5}|0\rangle + \frac{2\sqrt{6}}{5}|1\rangle\big) \\ &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\big(\frac{1}{5}|0\rangle + \frac{2\sqrt{6}}{5}|1\rangle\big) = \\ &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} \frac{1}{5} \\ \frac{2\sqrt{6}}{5} \end{bmatrix} = \frac{2\sqrt{6}}{5}|0\rangle + \frac{1}{5}|1\rangle . \end{aligned}$$

(2) Bramka $\sqrt{NOT}$:

$$\sqrt{NOT} = \frac{1}{2}\begin{bmatrix} 1-i & 1+i \\ 1+i & 1-i \end{bmatrix}$$

Złożenie ze sobą dwóch bramek $\sqrt{NOT}$ daje bramkę NOT.

(3) Bramka sterowanej negacji:

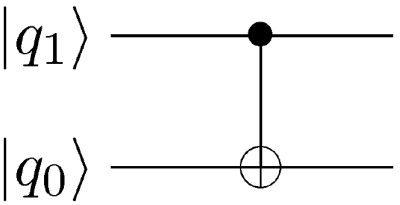
$$CNot = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Jest to dwukubitowa (w przeciwieństwie do innych przytoczonych przykładów) bramka kwantowa. Wykonuje ona operację sterowanej negacji na mniej znaczącym kubicie, natomiast starszy (bardziej znaczący) kubit jest kubitem sterującym.
Bramka ta odwraca drugi młodszy (docelowy) kubit wtedy i tylko wtedy, gdy kubit sterujący jest równy $|1\rangle$:

$$CNot\,|00\rangle = |00\rangle\,, \qquad CNot\,|01\rangle = |01\rangle\,,$$

$$CNot\,|10\rangle = |11\rangle\,, \qquad CNot\,|11\rangle = |10\rangle\,.$$

Na schematach oznaczamy tę bramkę następująco:



Rysunek 2.2: Symbol bramki CNot.

(4) Bramka Hadamarda:

$$H = \frac{\sqrt{2}}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Bramka ta ma podstawowe znaczenie dla obliczeń kwantowych, ponieważ przekształca stan bazowy $|0\rangle$ w równomierną superpozycję stanów bazowych:

$$H|0\rangle = \frac{\sqrt{2}}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{\sqrt{2}}{2} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle$$

(5) Bramka fazy:

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix}.$$

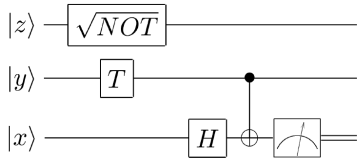
Odpowiada ona obrotowi o $\frac{\pi}{4}$.

2.6 Obwód kwantowy

Definicja 2.8. Obwodem kwantowym nazywamy odwzorowanie w dwuwymiarowej, zespolonej przestrzeni Hilberta, które można przedstawić w postaci złożenia skończonej liczby bramek kwantowych.

Dokonamy symulacji działania przykładowego obwodu kwantowego. Na rysunku 2.3 przedstawiony został obwód kwantowy na trzykubitowym rejestrze. Składa się on z czterech etapów obliczeń i kończy operacją pomiaru stanu jednego kubitu. Schematy obwodów kwantowych są analizowane od strony lewej do prawej. W pierwszym etapie bramki $\sqrt{NOT}$ i T działają odpowiednio na kubitach z oraz y.

W drugim etapie bramka Hadamarda działa na kubicie x. W trzecim etapie pojawia się bramka sterowanej negacji, działająca na kubicie x, gdzie kubitem sterującym jest kubit y. W ostatnim etapie obliczeń pomiarowi podlega kubit x. Ta operacja pomiaru jest przykładem pomiaru podzbioru kubitów, należących do



Rysunek 2.3: Schemat przykładowego obwodu kwantowego.

rejestru.
Symulacja pracy obwodu kwantowego wykonywana jest według następujących reguł:

(1) W miejscach w obwodzie, w których nie występują żadne bramki, zostaną umieszczone bramki o macierzy jednostkowej I.

(2) Połączeniu równoległemu bramek kwantowych odpowiada bramka opisana przez iloczyn tensorowy macierzy poszczególnych bramek. Obowiązuje przy tym kolejność od najbardziej znaczącego kubitu. Zatem w naszym przykładzie pierwszemu etapowi obliczeń odpowiada bramka o macierzy

$$\sqrt{NOT} \otimes T \otimes I,$$

drugiemu etapowi obliczeń bramka o macierzy

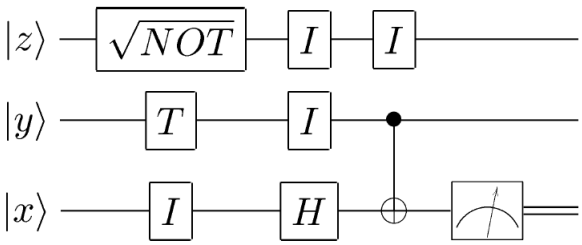
$$I \otimes I \otimes H,$$

itd.

(3) Połączeniu szeregowemu bramek odpowiada bramka opisywana przez zwykły iloczyn macierzy poszczególnych bramek. U nas jest to

$$(\sqrt{NOT} \otimes T \otimes I) \cdot (I \otimes I \otimes H) \cdot (I \otimes CNot).$$

(4) Stan otrzymany na wyjściu etapu obliczeń lub na wyjściu całego obwodu kwantowego jest równy iloczynowi macierzy



Rysunek 2.4: Schemat z zaznaczonymi jawnie bramkami I.

etapu lub obwodu stanu wejściowego - jeśli wewnątrz obwodu nie występowały operacje pomiaru stanu. Rezultatem otrzymanym dla naszego obwodu, po podaniu na jego wejściu stanu $|001\rangle$ byłby zatem stan

$$((\sqrt{NOT} \otimes T \otimes I) \cdot (I \otimes I \otimes H) \cdot (I \otimes CNot)) \cdot |001\rangle \,.$$

Korzystając z własności (7) otrzymujemy:

$$((\sqrt{NOT}) \otimes T \otimes I) \cdot (I \otimes I \otimes H) \cdot (I \otimes CNot)) \cdot |001\rangle =$$

$$= ((\sqrt{NOT} \otimes T \otimes H) \cdot (I \otimes CNot)) \cdot |001\rangle =$$

$$= (\sqrt{NOT} \otimes ((T \otimes H) \cdot CNot)) \cdot |001\rangle \,.$$

Po podstawieniu dostajemy:

$$(\sqrt{NOT} \otimes ((T \otimes H) \cdot CNot)) \cdot |001\rangle = \ldots = \frac{\sqrt{2}}{4} \begin{bmatrix} 1-i \\ i-1 \\ 0 \\ 0 \\ 1+i \\ -i-1 \\ 0 \\ 0 \end{bmatrix} .$$

Bibliografia

[1] Banaszak G., Gajda W. , *Elementy algebry liniowej cz.2*, Wydawnictwa Naukowo-Techniczne, Warszawa 2002

[2] Hirvensalo M., *Algorytmy kwantowe*, Wydawnictwa Szkolne i Pedagogiczne, Warszawa 2004

[3] Nowotniak R., *Wykorzystanie metod ewolucyjnych sztucznej inteligencji w projektowaniu algorytmów kwantowych*, praca magisterska, Politechnika Łódzka, Wydział Fizyki Technicznej, Informatyki i Matematyki Stosowanej

[4] Seber G. A. F., *Multivariate observations*, Wiley, New York 1984

Kobiety w matematyce

Katarzyna Donaj, Gabriela Pałka
Uniwersytet im. Adama Mickiewicza w Poznaniu
Wydział Matematyki i Informatyki

3.1 Wstęp

Jest wielu wybitnych mężczyzn cenionych za osiągnięcia związane z matematyką. Chyba każdy zna nazwiska: Pitagoras, Archimedes, Cauchy, Newton, Lagrange, Borsuk, Rejewski, Zygalski, Różycki. Nasuwa się pytanie: czy kobiety również miały swoje dokonania w matematyce? Matematyka zawdzięcza bardzo wiele twierdzeń kobietom, które nie zawsze uzyskały należną im sławę. Postaramy się przedstawić krótko kilka z nich.

3.2 Hypatia z Aleksandrii (370 - 415)

Pierwsza kobieta w dziejach nauki to mężczennica. Zamiast szukać mężczyzny, a potem wychowywać dzieci, zajmowała się matematyką, fizyką i astronomią. Przypisuje się jej wynalezienie aerometru, astrolabium i planisfery. Napisała komentarze do prac Apoloniusza i Diofantosa, mimo iż ludzie mówili jej, że zajęcia takie przystoją tylko ladacznicom. Święty (wtedy jeszcze tylko arcybiskup) Cyryl doradził, by zołzę ukamienować. Na pocieszenie Hypatia ma dziś kra-

ter na Księżycu i to z widocznej strony. Dziś jest uznawana za symbol nietolerancji religijnej i seksistowskiej.

3.3 Maria Gaetana Agnesi (1718 - 1799)

Była włoską matematyczką, lingwistką i filozofką, autorką pierwszego włoskiego podręcznika do rachunku różniczkowego i całkowego.

Córkę profesora matematyki Pietro Agnesiego uważano za „cudowne dziecko" i poliglotkę. Gdy miała 15 lat, ojciec zaczął zapraszać do domu wybitnych uczonych, przed którymi odczytywała swoje prace i broniła tez dotyczących zawiłych kwestii filozoficznych.

Od 20 roku życia zajmowała się niemal wyłącznie badaniami matematycznymi, m.in. nad krzywymi stożkowymi oraz krzywą, którą nazywamy dziś lokiem Agnesi. Gdy w 1750 zachorował jej ojciec, papież Benedykt XIV przekazał jej katedrę matematyki i filozofii naturalnej na Uniwersytecie w Bolonii. Była drugą kobietą-wykładowcą na tym uniwersytecie. W 1762 opracowała przegląd prac naukowych Josepha Louisa Lagrange'a.

3.4 Sophie Germain (1776 - 1831)

Koniecznie chciała zostać matematykiem. Dopuściła się nawet oszustwa. Ponieważ było niemożliwe, aby uczęszczała na zajęcia w Ecole Politechnique, więc namówiła jednego ze studentów, by przynosił jej notatki i tematy prac domowych oraz podrzucał wykładowcom wykonane przez nią prace. Znana była z tego, że udowodniła, iż równanie $x^n + y^n = z^n$ nie ma rozwiązań w liczbach całkowitych niepodzielnych przez n,

gdy n jest nieparzystą liczbą pierwszą, mniejszą od stu. Członkowie Akademii Paryskiej przyznali Sophie Germain w 1816 roku Grand Prix za pracę o wytrzymałości metali. Ale sprawiedliwości nie stało się zadość – na tablicy wymieniającej wszystkich laureatów tej nagrody, umieszczonej na wieży Eiffla pominięto jej nazwisko.

3.5 Ada Lovelace (1815 - 1852)

Brytyjska matematyczka i poetka, znana przede wszystkim z publikacji na temat mechanicznego komputera Charlesa Babbage'a, zwanego maszyną analityczną. Praca zawiera notatki, wśród nich pierwszy opublikowany algorytm napisany z zamiarem wykonania na maszynie. Z tego powodu uważana jest za pierwszą programistkę. Lovelace często kwestionowała podstawowe założenia przez łączenie poezji i nauki. Wierzyła, że intuicja i wyobraźnia są kluczowe do efektywnego korzystania z matematycznych i naukowych konceptów. Ceniła metafizykę na równi z matematyką, widząc w obu narzędzia do poznawania otaczającego nas świata. Łącząc poezję z matematyką, Ada opisywała swoje podejście jako „naukę poetycką", a siebie jako „analityka i metafizyka".

3.6 Zofia Kowalewska (1850 - 1891)

Panna o nazwisku Korwin-Krukowska wzięła ślub, aby mogła swobodnie przebywać w męskim towarzystwie, co było konieczne do uprawiania nauki. Małżeństwo to było fikcyjne, żeby nie przeszkadzało jej w nauce. Potem poznała cieszącego się w młodości bardzo złą reputacją starca będącego na dodatek tytanem matematyki – Karla Weierstrassa. Natychmiast wkradła się w jego łaski prezentując to, na co okazał się najbardziej łasy – duże wykształcenie i pomysłowość w matematyce. Do tego stopnia go sobie zjednała, że zaczął forsować pomysł, by za udowodnione przez nią twierdzenie o rozwiązalności równań różniczkowych cząstkowych dać jej doktorat. Pomimo sprzeciwu m.in. Darboux, Kowalewska w 1874 roku doktorat otrzymała. Owe twierdzenie znajdujemy w literaturze jako twierdzenie Cauchy'ego-Kowalewskiej.

3.7 Grace Chisholm Young (1868 - 1944)

W 1994 roku minęło sto lat od chwili, gdy pierwsza kobieta uzyskała doktorat z matematyki w normalnym (czyli męskim) trybie. Była to żona brytyjskiego matematyka Williama Younga. Doktorat uzyskała w Niemczech (w Getyndze), a jej praca dotyczyła rachunku różniczkowego funkcji rzeczywistych wielu zmiennych. Wcześniej Grace ukończyła studia matematyczne na Uniwersytecie w Cambridge. Egzaminy wstępne zdała w wieku 17 lat, ale aż 4 lata musiała czekać, zanim dopuszczo-

no ją do podjęcia tych studiów. Ukończyła je zdając egzaminy końcowe z pierwszą notą, jednak nie uzyskała tytułu magistra, który kobietom wówczas nie przysługiwał.

3.8 Krystyna Kuperberg (1944 - . . .)

Jest to współczesna amerykańska matematyczka pochodzenia polskiego. Krystyna Kuperberg obroniła pracę magisterską z topologii w 1966 roku pod kierunkiem Karola Borsuka. Otrzymała tytuł Full Professor (profesor zwyczajny) w roku 1984. Wykładała w Oklahoma State University, Courant Institute 1987, oraz w Uniwersytecie Paryskim w Orsay. W roku 1987 rozwiązała pewien dawny, bardzo trudny problem Knastera. W późnych latach 80. zajęła się zagadnieniem punktów stałych i topologicznymi aspektami układów dynamicznych. W roku 1993 obaliła tzw. przypuszczenie Seiferta (dotyczące pewnej właściwości pól wektorowych na powierzchni sfery). Pracę tę kontynuowała wspólnie z synem. W 1995 roku otrzymała prestiżową Nagrodę im. Alfreda Jurzykowskiego, a w roku 1996 – Research Excellence Award od College of Sciences and Mathematics Auburn University. Jest aktywną działaczką amerykańskiego środowiska matematycznego.

3.9 Maryam Mirzakhani (1977 - . . .)

Żyjąca obecnie irańska matematyczka w 1999 roku ukończyła matematykę na Uniwersytecie Technologicznym Szarif w Teheranie. W 2004 roku uzyskała doktorat na Uniwersytecie Harvarda. Jest profesorem matematyki Uniwersytetu Stanforda. Jej badania obejmują przestrzeń Teichmüllera, geometrię hiperboliczną,

hipotezę ergodyczną i geometrię symplektyczną.

W 2014 roku, jako pierwsza kobieta w historii, została uhonorowana Medalem Fieldsa za wkład w badania dynamiki i geometrii powierzchni Riemanna. Mirzakhani nie jest typem matematyka, który myśli szybko i błyskawicznie rozwiązuje kolejne problemy. Potrafi długo się zastanawiać, wgłębiać w temat przez całe lata, powoli go rozgryzając.

3.10 Zakończenie

Opis sylwetek zasłużonych matematyczek zakończymy cytatem Zofii Kowalewskiej – największej matematyczki XIX wieku:

„Wielu, którzy nigdy nie mieli okazji dowiedzieć się czegoś więcej o matematyce, myli ją z arytmetyką, uważając ją za nudną i jałową. W rzeczywistości zaś jest to nauka wymagająca największej wyobraźni."

Bibliografia

[1] Dokrzewska K., *Kobiety i matematyka*, `mif.pg.gda.pl/kmd/materialy/seminarium9/historiaikultura/kobiety.pdf`

[2] *Kobiety mają pod górkę*, Wrocławski Portal Matematyczny, `matematyka.wroc.pl/doniesienia/kobiety-mają-pod-górkę`

[3] *Biographies of Women Mathematicians*, `agnesscott.edu/lriddle/women/women.htm`

Zmodyfikowane i sferyczne funkcje Bessela – własności różniczkowo-całkowe

Magdalena Figiel, Anna Futa
Uniwersytet Marii Curie-Skłodowskiej
Wydział Matematyki, Fizyki i Informatyki

4.1 Wstęp

Funkcje Bessela (nazywane również funkcjami walcowymi) są jednym z przykładów funkcji specjalnych. Stanowią one rozwiązanie równania różniczkowego Bessela.

W pierwszej kolejności zaprezentowany zostanie krótki rys historyczny i równanie różniczkowe Bessela. Następnie zdefiniowane zostaną zmodyfikowane funkcje Bessela I i II rodzaju oraz wybrane własności różniczkowe i całkowe tych funkcji. Kolejno przedstawione zostaną sferyczne funkcje Bessela oraz własności tych funkcji.

Na koniec zaprezentowane zostaną wybrane zastosowania zmodyfikowanych i sferycznych funkcji Bessela w zagadnieniach matematyki i fizyki.

4.2 Historia

Funkcje Bessela po raz pierwszy pojawiły się w XVIII wieku w wyniku badań nad problemami fizycznymi.

W roku 1732 szwajcarski matematyk Daniel Bernoulli rozważał zagadnienie drgań zwisającego giętkiego i ważkiego łańcucha o dolnym końcu swobodnym. W konsekwencji otrzymał on równanie różniczkowe

$$\frac{d^2y}{dx} + \frac{1}{x} \cdot \frac{dy}{dx} + \frac{k^2 \cdot y}{x} = 0,$$

które może być przekształcone do postaci, jaką uzyskał Bessel około 100 lat później.

W 1824 roku niemiecki naukowiec F. W. Bessel badając problem związany z eliptycznym ruchem planet skorzystał z równania Laplace'a. Po przejściu na współrzędne biegunowe oraz dokonując pewnych przekształceń uzyskał on równanie różniczkowe liniowe jednorodne drugiego rzędu dane wzorem:

$$\frac{d^2y}{dx^2} + \frac{1}{x} \cdot \frac{dy}{dx} + \left(1 - \frac{n^2}{x^2}\right) \cdot y = 0. \tag{4.1}$$

Równanie (4.1) nazywamy równaniem Bessela rzędu całkowitego n [1].

4.3 Definicja funkcji Bessela

Równanie (4.1) w oparciu o teorię równań różniczkowych liniowych ma dwa liniowo niezależne rozwiązania. Rozwiązania te nazywamy funkcjami Bessela lub funkcjami walcowymi [5].

Funkcję Bessela I rodzaju określamy wzorem

$$J_n(x) = \sum_{r=0}^{\infty} \frac{(-1)^r \cdot (\frac{1}{2}x)^{n+2r}}{r! \cdot \Gamma(n + r + 1)}. \tag{4.2}$$

W przypadku, gdy wskaźnik n nie jest liczbą całkowitą, mamy

$$J_{-n}(x) = \sum_{r=0}^{\infty} \frac{(-1)^r \cdot (\frac{1}{2}x)^{-n+2r}}{r! \cdot \Gamma(-n + r + 1)}. \tag{4.3}$$

Jeżeli n nie jest liczbą całkowitą, to funkcje $J_n(x)$ oraz $J_{-n}(x)$ są dwoma liniowo niezależnymi rozwiązaniami równania (4.1). Wówczas rozwiązanie ogólne równania Bessela ma postać

$$y = A \cdot J_n(x) + B \cdot J_{-n}(x),$$

gdzie A i B są dowolnymi stałymi [2].

4.4 Zmodyfikowane funkcje Bessela I i II rodzaju

Niech $x \in \mathbb{C}$. Jeżeli dokonamy podstawienia $x := \pm xi$ w równaniu (4.1), to otrzymamy

$$\frac{d^2y}{dx^2} + \frac{1}{x} \cdot \frac{dy}{dx} - \left(1 + \frac{n^2}{x^2}\right) \cdot y = 0. \tag{4.4}$$

Równanie (19.5) określamy jako zmodyfikowane równanie różniczkowe Bessela [3].

Zmodyfikowaną funkcję Bessela I rodzaju rzędu n określamy wzorem

$$I_n(x) = \sum_{r=0}^{\infty} \frac{(\frac{1}{2}x)^{n+2r}}{r! \cdot \Gamma(n + r + 1)}. \tag{4.5}$$

Zatem prawdziwa jest następująca zależność:

$$I_n(x) = i^{-n} \cdot J_n(ix). \tag{4.6}$$

4.4.1 Relacje rekurencyjne

Zmodyfikowane funkcje Bessela dowolnych rzędów można wyrazić poprzez funkcje niższego rzędu. Poniższe wzory znane są pod nazwą związków rekurenycjnych dla zmodyfikowanych funkcji Bessela. Dowody tych zależności przeprowadza się analogicznie, dlatego też zostanie zaprezentowany jeden z nich.

Twierdzenie 4.1. *[1] Jeżeli n jest dowolną liczbą rzeczywistą oraz $x \neq 0$, to*

i) $\frac{d}{dx}\left(x^n \cdot I_n(x)\right) = x^n \cdot I_{n-1}(x)$,

ii) $\frac{d}{dx}\left(x^{-n} \cdot I_n(x)\right) = x^{-n} \cdot I_{n+1}(x)$,

iii) $I_n^{'}(x) = I_{n-1}(x) - \frac{n}{x} \cdot I_n(x)$,

iv) $I_n^{'}(x) = \frac{n}{x} \cdot I_n(x) + I_{n+1}(x)$,

v) $I_n^{'}(x) = \frac{1}{2} \cdot \left(I_{n-1}(x) + I_{n+1}(x)\right)$,

vi) $I_{n-1}(x) - I_{n+1}(x) = \frac{2n}{x} \cdot I_n(x)$.

Dowód. (i) Korzystając z zależności $\frac{d}{dx}\left(x^n \cdot J_n(x)\right) = x^n \cdot J_{n-1}(x)$, zachodzącej dla funkcji Bessela I rodzaju oraz dokonując podstawienia $x := xi$ mamy

$$\frac{d}{d(ix)}\left(i^n \cdot x^n \cdot J_n(ix)\right) = i^n \cdot x^n \cdot J_{n-1}(ix).$$

Następnie, przy użyciu wzoru (4.6) dostajemy

$$\frac{1}{i} \cdot \frac{d}{dx}\left(i^n \cdot x^n \cdot i^n \cdot I_n(x)\right) = i^n \cdot x^n \cdot i^{n-1} \cdot I_{n-1}(x).$$

Dzieląc obustronnie przez i^{2n-1} ostatecznie otrzymujemy

$$\frac{d}{dx}\left(x^n \cdot I_n(x)\right) = x^n \cdot I_{n-1}(x).$$

□

Pierwsze pięć własności pozwala na wyrażenie pochodnych zmodyfikowanych funkcji Bessela przez funkcje Bessela, zaś ostatnia własność daje możliwość wyrażenia funkcji dowolnego rzędu n poprzez funkcje niższych rzędów.

Funkcją zmodyfikowaną II rodzaju nazywamy funkcję postaci:

$$K_n(x) = \frac{\pi}{2} \cdot \frac{I_{-n}(x) - I_n(x)}{\sin(n\pi)}, \tag{4.7}$$

gdy n nie jest całkowite.

W sytuacji, gdy n jest całkowite, licznik i mianownik funkcji $K_n(x)$ zerują się, więc funkcja ta jest nieokreślona. W tym przypadku funkcję $K_n(x)$ możemy zdefiniować następującym warunkiem

$$K_n(x) = \lim_{v \to n} K_v(x).$$

Funkcję $K_v(x)$ nazywamy również funkcją MacDonalda. Bez względu na to czy n jest całkowite, funkcja ta jest rozwiązaniem zmodyfikowanego równania Bessela. Dla n będącego liczbą całkowitą funkcje $K_n(x)$ i $K_{-n}(x)$ są niezależnymi rozwiązaniami równania Bessela [4].

4.4.2 Reprezentacja całkowa zmodyfikowanych funkcji Bessela

Funkcje Bessela w prosty sposób mogą zostać wyrażone poprzez całki oznaczone, bądź krzywoliniowe zawierające zmienną x jako parametr. Wyrażenia dane za pomocą całek krzywoliniowych są zwykle prawdziwe w szerszym obszarze zmienności x i wskaźnika n niż wyrażenia w postaci całek oznaczonych. Z kolei, całki oznaczone spotykane są częściej w zastosowaniach.

Twierdzenie 4.2. *[1] Dla $n > -\frac{1}{2}$ prawdziwe są następujące zależności:*

$$i)\ \ I_n(x) = \frac{1}{\sqrt{\pi} \cdot \Gamma(n+\frac{1}{2})} \cdot \left(\frac{x}{2}\right)^n \cdot \int_{-1}^{1} e^{-xt} \cdot (1-t^2)^{n-\frac{1}{2}} dt\ ,$$

$$ii)\ \ K_n(x) = \frac{\sqrt{\pi}}{\Gamma(n+\frac{1}{2})} \cdot \left(\frac{x}{2}\right)^n \cdot \int_{1}^{\infty} e^{-xt} \cdot (t^2-1)^{n-\frac{1}{2}} dt\ , \quad x > 0.$$

W celu wyprowadzenia wzorów całkowych dla funkcji zmodyfikowanych należy skorzystać z reprezentacji całkowej funkcji $J_n(x)$ [6].

4.5 Sferyczne funkcje Bessela

Szczególnym rodzajem funkcji Bessela są sferyczne funkcje Bessela I i II rodzaju. Funkcje te nazywamy również funkcjami kulistymi. Są one bezpośrednio zależne od funkcji Bessela I i II rodzaju.

Rozważmy równanie

$$x^2 \cdot \frac{d^2y}{dx^2} + 2x \cdot \frac{dy}{dx} + \left[k^2 \cdot x^2 - l \cdot (l+1)\right] \cdot y = 0. \tag{4.8}$$

Powyższe równanie jest modyfikacją równania Bessela w sytuacji, gdy

$$\begin{cases} 1 - 2 \cdot \alpha = 2, \\ \gamma = 1, \\ \beta^2 \cdot \gamma^2 = k^2, \\ \alpha^2 - n^2 \cdot \gamma^2 = -l \cdot (l+1). \end{cases}$$

Funkcją sferyczną Bessela I rodzaju nazywamy funkcję postaci:

$$j_l(x) = \sqrt{\frac{\pi}{2x}} \cdot J_{l+\frac{1}{2}}(x). \tag{4.9}$$

Funkcją sferyczną Bessela II rodzaju nazywamy funkcję:

$$y_l(x) = \sqrt{\frac{\pi}{2x}} \cdot Y_{l+\frac{1}{2}}(x). \tag{4.10}$$

4.5.1 Zależności rekurencyjne dla sferycznych funkcji Bessela

Podobnie, jak dla zmodyfikowanych funkcji Bessela, również dla funkcji sferycznych zachodzą pewne zależności rekurencyjne. Te same własności są prawdziwe zarówno dla $j_n(x)$, jak i dla $y_n(x)$, dlatego zostaną uogólnione dla obu tych funkcji w poniższym twierdzeniu.

Twierdzenie 4.3. *[1] Jeżeli $f_n(x)$ jest jedną z funkcji: $j_n(x)$, bądź $y_n(x)$ oraz n jest dowolną liczbą całkowitą, to*

i) $\frac{d}{dx}\left(x^{n+1}\cdot f_n(x)\right) = x^{n+1}\cdot f_{n-1}(x)$,

ii) $\frac{d}{dx}\left(x^{-n}\cdot f_n(x)\right) = -x^{-n}\cdot f_{n+1}(x)$,

iii) $f_n^{'}(x) = f_{n-1}(x) - \frac{n+1}{x}\cdot f_n(x)$,

iv) $f_n^{'}(x) = \frac{n}{x}\cdot f_n(x) - f_{n+1}(x)$,

v) $(2n+1)\cdot f_n^{'}(x) = n\cdot f_{n-1}(x) - (n+1)\cdot f_{n+1}(x)$,

vi) $f_{n-1}(x) + f_{n+1}(x) = \frac{2n+1}{x}\cdot f_n(x)$.

4.5.2 Własności sferycznych funkcji Bessela

Twierdzenie 4.4. *[1] Dla $x \neq 0$ zachodzą następujące zależności:*

i) $j_0(x) = \frac{\sin x}{x}$,

ii) $y_0(x) = \frac{\cos x}{x}$.

Dowód. (i) Korzystając z definicji $j_n(x)$ oraz z równania (4.2):

$$j_0(x) = \sqrt{\frac{\pi}{2x}}\cdot J_{\frac{1}{2}}(x) = \sqrt{\frac{\pi}{2x}}\cdot\sum_{r=0}^{\infty}\frac{(-1)^r\cdot(\frac{x}{2})^{2r+\frac{1}{2}}}{r!\cdot\Gamma(\frac{1}{2}+r+1)}.$$

Opierając się na własności funkcji gamma dostajemy, że:

$$\Gamma\left(r+1+\frac{1}{2}\right) = \frac{(2r+2)!}{2^{2r+2}\cdot(r+1)!}\cdot\sqrt{\pi}.$$

Stąd:

$$\begin{aligned} j_0(x) &= \frac{\sqrt{\pi}}{2^{\frac{1}{2}}\cdot x^{\frac{1}{2}}}\cdot\sum_{r=0}^{\infty}(-1)^r\cdot\frac{2^{2r+2}\cdot(r+1)!}{r!\cdot(2r+2)!\cdot\sqrt{\pi}}\cdot\frac{x^{2r+\frac{1}{2}}}{2^{2r+\frac{1}{2}}} \\ &= \sum_{r=0}^{\infty}(-1)^r\cdot\frac{2\cdot(r+1)}{(2r+2)!}\cdot x^{2r} = \sum_{r=0}^{\infty}(-1)^r\frac{x^{2r}}{(2r+1)!} \\ &= \frac{1}{x}\cdot\sum_{r=0}^{\infty}(-1)^r\frac{x^{2r+1}}{(2r+1)!} = \frac{1}{x}\cdot\sin x. \end{aligned}$$

□

Dowód zależności (ii) przeprowadza się w sposób analogiczny, korzystając z rozwinięcia w szereg potęgowy funkcji $\cos x$.

Mając dane funkcje $j_0(x)$ oraz $y_0(x)$, możemy otrzymywać kolejne wyrażenia dla wyższych wartości wskaźnika. Własności te zostaną zaprezentowane w poniższym twierdzeniu, są one również znane pod nazwą wzorów Rayleigh'a.

Twierdzenie 4.5. *[1] Jeżeli n jest nieujemną liczbą całkowitą, to*

i) $j_n(x) = (-1)^n \cdot x^n \left(\frac{1}{x}\frac{d}{dx}\right)^n \left(\frac{\sin x}{x}\right),$

ii) $y_n(x) = -(-1)^n \cdot x^n \left(\frac{1}{x}\frac{d}{dx}\right)^n \left(\frac{\cos x}{x}\right).$

Powyższe twierdzenie umożliwia wyznaczenie funkcji sferycznych I oraz II rodzaju dla $n > 1$. Poniżej zostanie przedstawionych kilka wzorów kolejnych funkcji sferycznych dla początkowych wartości wskaźnika. Mianowicie

$$j_1(x) = \frac{\sin x}{x^2} - \frac{\cos x}{x},$$
$$j_2(x) = \left(\frac{3}{x^3} - \frac{1}{x}\right) \cdot \sin x - \frac{3}{x^2} \cdot \cos x,$$
$$j_3(x) = \left(\frac{15}{x^4} - \frac{6}{x^2}\right) \cdot \sin x - \left(\frac{15}{x^3} - \frac{1}{x}\right) \cdot \cos x.$$

Wzory te wyrażają sferyczne funkcje Bessela poprzez funkcje potęgowe (o ujemnych wykładnikach) i funkcje trygonometryczne. Oznacza to, że funkcje $j_n(x)$ oraz $y_n(x)$ są funkcjami elementarnymi [6].

4.5.3 Zastosowanie sferycznych i zmodyfikowanych funkcji Bessela

Zmodyfikowane i sferyczne funkcje Bessela mają zastosowanie w następujących dziedzinach:

- teoria liczb,

- astronomia (perturbacje ruchu ciał),
- mechanika (ruchy ciał w polach osiowych),
- termodynamika (rozpływ ciepła w przypadku przewodów o symetrii osiowej, stygnięcie walca kołowego),
- teoria promieniowania elektromagnetycznego układów o symetrii osiowej i dyfrakcji w takich układach.

4.6 Podsumowanie

Podsumowując, zmodyfikowane i sferyczne funkcje Bessela posiadają szereg własności różniczkowych i całkowych. Istnieje wiele twierdzeń pozwalających na dokładną analizę tych funkcji. Funkcje zmodyfikowane i sferyczne, jako jedne z podstawowych funkcji specjalnych cieszą się dużą popularnością wśród nauk ścisłych. Obecnie pojawia się coraz więcej zastosowań tych funkcji, nie tylko w matematyce, ale także w innych naukach technicznych.

Bibliografia

[1] W. W. Bell, *Special Functions for scientists and engineers*, D. Van Nostrand Company LTD, London, 1968, str. 92-153.

[2] J. Greń, D. Bobrowski, J. Browkin, *Poradnik inżyniera. Matematyka*, Wydawnictwa Naukowo - Techniczne, Warszawa, 1986, str. 658-674.

[3] L. Kunert, *Funkcje specjalne*, Środowiskowe Centrum Obliczeniowe CYFRONET, Kraków, 1986, str. 35-44.

[4] N. W. McLachlan, *Funkcje Bessela dla inżynierów*, Państwowe Wydawnictwo Naukowe, Warszawa, 1964.

[5] P. I. Romanowski, *Szeregi Fouriera. Teoria pola. Funkcje analityczne i specjalne. Przekształcenie Laplace'a*, Państwowe Wydawnictwo Naukowe, Warszawa, 1968, str. 234-255.

[6] G. N. Watson, *A treatise on the theory of Bessel Functions*, Cambridge University Press, Cambridge, 1966.

Uroki zupełności

Jędrzej Garnek
Uniwersytet im. Adama Mickiewicza w Poznaniu
Wydział Matematyki i Informatyki

5.1 Wstęp

Zupełność należy do własności, które kojarzą się raczej z topologią niż z algebrą. Jej defnicję poznajemy zazwyczaj na analizie, dowiadując się, dlaczego liczby rzeczywiste są „lepsze" od liczb wymiernych. Okazuje się jednak, że pierścienie zupełne pełnią ważną rolę także w algebrze. Pierścienie liczb p-adycznych należą do standardowego arsenału teorioliczbowców; w szczególności pojawiają się one w sformułowaniu tzw. zasady lokalno-globalnej Hassego. W geometrii algebraicznej uzupełnienie pozwala z kolei spojrzeć na obiekty geometryczne z analitycznego punktu widzenia. W niniejszym artykule postaramy się uzasadnić, czemu pierścienie zupełne są *zupełnie wyjątkowe*.

5.2 Dyskretne waluacje

Podrozdział ten zaczniemy od następującej definicji:

Definicja 5.1. (Dyskretną) waluacją na ciele K nazywamy dowolną funkcję $v : K^\times \to \mathbb{Z}$ spełniającą:

(i) $v(x \cdot y) = v(x) + v(y)$,

(ii) $v(x + y) \geqslant \min\{v(x), v(y)\}$,

(iii) istnieje $\pi \in K$ takie, że $v(\pi) = 1$.

Zwyczajowo przyjmuje się, że $v(0) = \infty$. Z warunków (i) oraz (iii) wynika, że waluacja musi być surjektywna. Dowolny element $\pi \in K$ spełniający warunek (iii) nazywamy **uniformizatorem**.

Definicja 5.2. Niech v będzie dyskretną waluacją na ciele K. Pierścień:

$$R_v := \{x \in K : v(x) \geqslant 0\}$$

nazywamy **pierścieniem waluacji** v. Jest to pierścień lokalny o ideale maksymalnym:

$$\mathfrak{m}_v := \{x \in R : v(x) > 0\}.$$

Ciało $k_v := R_v/\mathfrak{m}_v$ nazywamy **ciałem reszt waluacji** v.

Definicja 5.3. Niech R będzie dziedziną całkowitości o ciele ułamków K. Mówimy, że R jest **pierścieniem dyskretnej waluacji**, jeżeli $R = R_v$ dla pewnej waluacji v, określonej na ciele K.

Zaprezentujemy teraz trzy przykłady dyskretnych waluacji.

Przykład 5.4. *Ustalmy liczbę pierwszą p. Wtedy na ciele $\mathbb{Q}$ można określić waluację v_p wzorem:*

$$v_p\left(p^n \cdot \frac{a}{b}\right) = n, \qquad \textit{jeżeli } p \nmid a, b$$

– zauważmy, że uniformizatorem jest p. Pierścień waluacji dany jest jako:

$$\mathbb{Z}_{(p)} = \left\{\frac{a}{b} : p \nmid b\right\}.$$

Ciało reszt w tym przypadku to $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{F}_p$.

Przykład 5.5. *Ustalmy $a \in \mathbb{C}$. Wtedy na ciele $\mathbb{C}(z)$ można określić waluację:*

$$v_a\left((z-a)^n \cdot g(z)\right) = n, \qquad \textit{gdzie } g(a) \in \mathbb{C}^*$$

(rząd zera/bieguna w a). Uniformizatorem jest wtedy $(z-a)$. Pierścień waluacji dany jest jako:

$$\mathbb{C}(z)_{(z-a)} = \textit{funkcje wymierne dobrze określone w } a.$$

Ciało reszt dane jest jako:

$$\mathbb{C}(z)_{(z-a)}/(z-a) \cong \mathbb{C}.$$

Postaramy się teraz uogólnić poprzedni przykład.

Przykład 5.6. *Ustalmy następujące oznaczenia:*

- $C : f(x,y) = 0$ – *krzywa algebraiczna w* $\mathbb{A}^2_{\mathbb{C}}$,
- $A(C) := \mathbb{C}[x,y]/(f(x,y))$ – *pierścień funkcji regularnych na* C *(tzw.* ***pierścień współrzędnych*** C*)*,
- $P = (x_0, y_0) \in C(\mathbb{C})$ – *punkt na krzywej* C,
- $\mathfrak{m}_P = (x - x_0, y - y_0) \trianglelefteq A(C)$ – *ideał maksymalny odpowiadający punktowi* P.

Badanie pierścienia $\mathcal{O}_P$ pozwala na opis zachowania krzywej w otoczeniu punktu P. Okazuje się na przykład, że punkt P jest gładki wtw. gdy na pierścieniu:

$$\mathcal{O}_P := \textit{ funkcje regularne dobrze określone w } P \ = A(C)_{\mathfrak{m}_P}$$

można określić dyskretną waluację.

Waluację funkcji $f \in \mathcal{O}_P$ można wtedy interpretować jako krotność zerowania się w punkcie P. Uniformizatorem jest wówczas np. dowolna prosta przechodząca przez P i nie styczna do C (patrz [3, Theorem 3.2.1]).

5.3 Zupełność

Zauważmy, że na ciele K wraz z waluacją v można wprowadzić wartość bezwzględną wzorem:

$$\|x\|_v = e^{-v(x)},$$

co pozwala z kolei na wprowadzenie metryki na podanych powyżej pierścieniach. Metryka ta jest dość „zabawna" (przykładowo wszystkie trójkąty są w niej równoramienne), jednak problem sprawia nam co innego. Przypomnijmy definicję znaną wszystkim dobrze z analizy i topologii:

Definicja 5.7. Przestrzeń metryczną nazwiemy **zupełną**, jeżeli dowolny ciąg Cauchy'ego jest w niej zbieżny.

Zauważmy, że podane powyżej ciała nie są zupełne. Przykładowo przyjmując w przykładzie 5.5 $a = 0$ mamy: ciąg $(\sum_{k=0}^{n} \frac{x^n}{n!})_n$ nie jest zbieżny w $\mathbb{Q}(x)$, mimo iż jest ciągiem Cauchy'ego. Znana z analizy konstrukcja pozwala na ich uzupełnienie:

Definicja 5.8. Niech (X, d) będzie przestrzenią metryczną. **Uzupełnieniem** przestrzeni X nazywamy przestrzeń metryczną $(\widehat{X}, \widehat{d})$, gdzie:

- $\widehat{X} = \{(x_n)_n$ – ciąg Cauchy'ego o wyrazach w $X\} \Big/ \sim$,

  przy czym: $(x_n)_n \sim (y_n)_n \quad \overset{\text{def}}{\Leftrightarrow} \quad \lim\limits_{n\to\infty} d(x_n, y_n) = 0,$

- $\widehat{d}((x_n)_n, (y_n)_n) \overset{\text{def}}{=} \lim_{n\to\infty} d(x_n, y_n)$.

Przestrzeń X można zanurzyć w $\widehat{X}$, przypisując każdemu elementowi ciąg stały. Obraz tego zanurzenia jest wówczas gęsty w $\widehat{X}$.

Rozważmy teraz przypadek, gdy $X = K$ jest ciałem wraz z metryką, w której operacje dodawania, odejmowania i mnożenia są ciągłe. Jak łatwo zauważyć, $\widehat{K}$ ma również naturalną strukturę pierścienia. Ponadto, jeżeli metryka na K jest pochodzi od dyskretnej waluacji v, to waluację tą można w naturalny sposób przedłużyć do $\widehat{K}$. Istotnie, jeżeli $(x_n)_n$ jest ciągiem Cauchy'ego, to $(v(x_n))_n$ również. Ciąg Cauchy'ego złożony z liczb całkowitych musi być jednak stały od pewnego momentu – $v(x_n) = v_0$ dla $n > N_0$. Możemy zatem przyjąć $\widehat{v}((x_n)_n) := v_0$. Łatwo zauważyć, że ciało reszt nie zmienia się po uzupełnieniu; podobnie

za uniformizator możemy przyjąć ten sam element. Zobaczmy, co uzyskamy uzupełniając pierścienie i ciała z poprzednich przykładów:

Przykład 5.9. *Podstawiając w przykładzie 5.5 $a = 0$ oraz uzupełniając $\mathbb{C}(z)$ względem waluacji v_a dostajemy ciało szeregów Laurenta o współczynnikach wymiernych:*

$$\mathbb{C}((z)) = \left\{ \sum_{n \geqslant N} a_n z^n : N \in \mathbb{Z}, \quad a_n \in \mathbb{Q} \right\}$$

Pierścieniem waluacji jest wówczas $\mathbb{C}[[z]]$ – pierścień szeregów formalnych.

Przykład 5.10. *Uzupełniając $\mathbb{Q}$ względem waluacji v_p (zdefiniowanej w przykładzie 5.4) dostajemy tzw.* ***ciało liczb p-adycznych****:*

$$\mathbb{Q}_p = \left\{ \sum_{n \geqslant N} a_n p^n : a_n \in \{0, 1, \ldots, p-1\}, N \in \mathbb{Z} \right\}$$

(dodawanie następuje „z przenoszeniem" – tak jak w systemie dziesiętnym). Pierścień waluacji ma postać:

$$\mathbb{Z}_p = \left\{ \sum_{n \geqslant 0} a_n p^n : a_n \in \{0, 1, \ldots, p-1\} \right\}$$

(są to tzw. ***liczby całkowite p-adyczne****).*
Zauważmy, że każdy element $a = \sum_{n \geqslant 0} a_n p^n \in \mathbb{Z}_p$ jest wyznaczony przez „zgodny" ciąg elementów pierścieni $\mathbb{Z}/p^n$:

$$a_0 \in \mathbb{Z}/p, \quad a_0 + pa_1 \in \mathbb{Z}/p^2, \quad a_0 + pa_1 + p^2 a_2 \in \mathbb{Z}/p^3, \ldots.$$

Można zatem równoważnie zdefniować $\mathbb{Z}_p$ jako granicę odwrotną:

$$\varprojlim \mathbb{Z}/p^n. \tag{5.1}$$

Okazuje się, że uzupełnienie można zdefniować dla dowolnego pierścienia lokalnego, nie tylko dla pierścienia dyskretnej waluacji. Rozpatrzmy pierścień lokalny R o ideale maksymalnym $\mathfrak{m}$ wraz z bazą otoczeń zera zadaną przez ciąg zbiorów $(\mathfrak{m}^n)_n$. Uzupełnienie pierścienia R definiujemy w tym przypadku, uogólniając równość (5.1):

$$\widehat{R} = \varprojlim R/\mathfrak{m}^n.$$

Omówienie tej definicji można znaleźć np. w [4, Rozdział 10].

Przykład 5.11. *Zachowajmy oznaczenia z przykładu 5.6. Uzupełnienie pierścienia lokalnego $\widehat{\mathcal{O}}_P$ (zdefinowane jak powyżej) pozwala na bardziej „topologiczne" spojrzenie na krzywą. Niech P_1, P_2 będą punktami na krzywych C_1, C_2. Wtedy pierścienie $\widehat{\mathcal{O}}_{P_1}$ oraz $\widehat{\mathcal{O}}_{P_2}$ są izomorficzne (jako $\mathbb{C}$-algebry) wtedy i tylko wtedy, gdy pewne otoczenia punktów P_1, P_2 są „analitycznie izomorficzne", tzn. gdy istnieje izomorfizm zadany przez funkcje analityczne. Pozwala to np. na „zgrubną" klasyfikację typów osobliwości punktów na krzywej.*

W dalszym ciągu skupimy się na rozwiązywaniu równań wielomianowych pierścieniach zupełnych. W tym celu przyda nam się redukcja do R/π^n dana jako:

$$a_0 + a_1 \cdot \pi + \ldots \quad \mapsto \quad a_0 + a_1 \cdot \pi + \ldots + a_{n-1} \cdot \pi^{n-1} \pmod{\pi^n}$$

W szczególności będziemy redukowali elementy do **ciała reszt** $k := R/\mathfrak{m}$. Zastanówmy się, jak wyglądają nam znane liczby zapisane w postaci p-adycznej.

- Załóżmy, że $\frac{1}{2}$ jest postaci:

$$\frac{1}{2} = \sum_{n \geqslant 0} a_n 5^n.$$

  Redukując $\pmod 5$ dostajemy: $2a_0 \equiv 1 \pmod 5$, czyli $a_0 = 3$. Redukując $\pmod{5^2}$ mamy $2 \cdot (3 + a_1 \cdot 5) \equiv 1$

$(\mathrm{mod}\ 5^2)$, co daje $a_1 = 4$. Okazuje się, że rozumowanie to możemy iterować, dostając liczbę $a \in \mathbb{Z}_5$, spełniającą:

$$\forall_n \qquad \frac{1}{2} \equiv a \pmod{5^n},$$

czyli $a = \frac{1}{2}$ (waluacja $v(a - \frac{1}{2})$ musi być nieskończona).

- W $\mathbb{Q}_5$ zachodzi równość:

$$-1 = \sum_{n \geqslant 0} 4 \cdot 5^n$$

wynikająca ze wzoru na sumę szeregu geometrycznego.

- Zastanówmy się, czy $\sqrt{-1} \in \mathbb{Q}_5$, tzn. czy równanie $x^2+1 = 0$ ma rozwiązanie w $\mathbb{Q}_5$:

$$\sqrt{-1} = \sum_{n \geqslant 0} a_n 5^n \quad \Rightarrow \quad -1 \equiv a_0^2 \pmod{5}.$$

Ostatni warunek zachodzi dla $a_0 \equiv \pm 2 \pmod{5}$; bez straty ogólności załóżmy, że $a_0 = 2$. Stosując redukcję $\mathrm{mod}\ p^2$:

$$\begin{aligned} -1 &\equiv (2 + a_1 \cdot 5)^2 && (\mathrm{mod}\ 5^2) \\ 0 &\equiv 5 + 2 \cdot 5 \cdot a_1 && (\mathrm{mod}\ 5^2) \\ 0 &\equiv 1 + 2 \cdot a_1 && (\mathrm{mod}\ 5) \end{aligned}$$

– ostatnia kongruencja ma zaś dokładnie jedno rozwiązanie $\mathrm{mod}\ p$: $a_1 = 2$. Podobnie możemy zredukować kolejne równanie $\mathrm{mod}\ p^3$ i po drobnych przekształceniach uzyskać równanie liniowe w ciele $\mathbb{Z}/p$, mające dokładnie jedno rozwiązanie a_3. Za chwilę udowodnimy, że procedurę tą można zawsze kontynuować w nieskończoność.

Głównym powodem, dla którego ciała zupełne są tak ważne, jest to, że można w nich w prosty sposób konstruować elementy – zadając po prostu ciąg Cauchy'ego. Fakt ten wykorzystamy w następującym twierdzeniu, uogólniającym nasze poprzednie zmagania:

Lemat 5.12 (lemat Hensela)**.** *Załóżmy, że $(K, \|\cdot\|_v)$ jest przestrzenią zupełną. Niech $f \in R[x]$ i załóżmy, że $\widetilde{f} \in k[x]$ ma pierwiastek pojedynczy $a_0 \in k$ (tzn. $\widetilde{f}'(a_0) \neq 0$). Wtedy istnieje dokładnie jeden element $a \in R$ taki, że:*

$$a \equiv a_0 \pmod{\mathfrak{m}}, \qquad f(a) = 0$$

Dowód. Wystarczy pokazać indukcyjnie, że istnieje ciąg $a_n \in R$ taki, że element:

$$A_n := \sum_{0 \leqslant i \leqslant n} a_i \pi^i$$

spełnia $f(A_n) \equiv 0 \pmod{\pi^{n+1}}$ dla każdego n. Skonstruowany w ten sposób szereg jest zbieżny do pewnego elementu $a \in R$ (z zupełności R), który musi spełniać $f(a) = 0$.

Dla $n = 0$ wystarczy w dowolny sposób podnieść a_0 do R. Załóżmy, że mamy $a_0, \ldots, a_n$ takie, że zachodzi: $f(A_n) = \pi^{n+1} \cdot c$. Z rozwinięcia Taylora:

$$f(x + A_n) = f(A_n) + x \cdot f'(A_n) + x^2 \cdot g(x)$$

Podstawmy $x = \pi^{n+1} \cdot y$ i zredukujmy $\pmod{\pi^{n+2}}$:

$$f(\pi^{n+1} \cdot y + A_n) \equiv \pi^{n+1} \cdot c + \pi^{n+1} \cdot y \cdot f'(A_n) + 0 \pmod{\pi^{n+2}}$$

więc $f(\pi^{n+1} \cdot y + A_n) \equiv 0 \pmod{\pi^{n+2}}$ wtw. gdy:

$$c + y \cdot f'(A_n) \equiv 0 \pmod{\pi}$$

Zauważmy, że $f'(A_n) \equiv f'(a_0) \not\equiv 0 \pmod{\pi}$, więc powyższe równanie ma dokładnie jedno rozwiązanie $y \equiv (f'(A_n))^{-1} \cdot c \pmod{\pi}$. Wystarczy więc przyjąć $a_{n+1} := y$.

□

Lemat Hensela ma wiele uogólnień, przytoczmy niektóre z nich:

- jeżeli istnieje $a_0 \in R$ takie, że $v(f(a_0)) > 2 \cdot v(f'(a_0))$, to istnieje $a \in R$ spełniające $v(a - a_0) > v(f'(a_0)^2/f(a_0))$,

- jeżeli $\widetilde{f}(x) = g_0(x) \cdot h_0(x)$ dla pewnych $g_0, h_0 \in R[x]$, $NWD(g_0, h_0) = 1$, to istnieją wielomiany $g, h \in R[x]$, spełniające $\widetilde{g} = g_0$, $\widetilde{h} = h_0$, $f = g \cdot h$,

- wersja dla układu n równań z n niewiadomymi (zastępujemy pochodną przez jakobian).

Jako przykładowe zastosowania zauważmy jeszcze, że $\mu_{p-1} \subset \mathbb{Q}_p$ oraz $\sqrt{1+x} \in \mathbb{Q}((x))$.

5.4 Zasada lokalno-globalna

Z teorioliczbowego punktu widzenia, lemat Hensela pozwala nam na podnoszenie rozwiązań z ciał charakterystyki p do charakterystyki 0. Ciałem, które nas interesuje jest jednak $\mathbb{Q}$, a nie $\mathbb{Q}_p$! Czy można powiedzieć coś o wymiernych rozwiązaniach danego równania, wiedząc coś o rozwiązaniach p-adycznych? Jeżeli równanie nie ma rozwiązań p-adycznych, to nie ma też rozwiązań wymiernych – z zasady tej korzystamy często na elementarnej teorii liczb, stwierdzając, że równanie nie ma rozwiązań całkowitych/wymiernych, bo nie ma ich modulo np. 8, bądź też nie ma rozwiązań rzeczywistych. Czy jest możliwe odwrotne rozumowanie? Okazuje się, że w pewnych szczególnych przypadkach tak:

Twierdzenie 5.13 (zasada lokalno-globalna Hassego)**.** *Niech $q \in \mathbb{Q}[x_1, \ldots, x_n]$ będzie formą kwadratową n-zmiennych. Równanie $q(\boldsymbol{x}) = 0$ ma rozwiązanie w $\mathbb{Q}$ wtw. gdy ma rozwiązanie w dowolnym uzupełnieniu $\mathbb{Q}$, tzn. w $\mathbb{Q}_p$ dla każdego p oraz w $\mathbb{R}$.*

Zasada ta pozwala na uzyskanie efektywnych sposobów rozstrzygania, czy dana forma kwadratowa ma wymierne miejsca zerowe. Pokażemy przykładowo, w jaki sposób sprowadzić sprawdzenie rozwiązywalności równania $a_0x_0^2 + a_1x_1^2 + a_2x_2^2 = 0$ w liczbach wymiernych do prostych obliczeń. Przed sformułowaniem „efektywnej" wersji twierdzenia Hassego wprowadzimy pojęcie **reszty i niereszty kwadratowej** mod p. Przez zbiór reszt

kwadratowych $\mod p$ będziemy rozumieli:

$$K_p := \{x^2 : x \in \mathbb{F}_p^\times\}$$

(zauważmy, że jest to podgrupa indeksu 2 w $\mathbb{F}_p^\times$), zaś przez zbiór niereszt – $N_p := \mathbb{F}_p^\times \setminus K_p$.

Twierdzenie 5.14 (Legendre'a)**.** *Niech $a_0, a_1, a_2 \in \mathbb{Z}$, i załóżmy, że $a_0a_1a_2 \neq 0$ jest liczbą bezkwadratową. Wtedy równanie:*

$$a_0x_0^2 + a_1x_1^2 + a_2x_2^2 = 0$$

ma rozwiązanie $(x_0, x_1, x_2) \in \mathbb{Z}^3$, $(x_0, x_1, x_2) \neq (0, 0, 0)$, wtedy i tylko wtedy gdy:

(i) *a_0, a_1, a_2 nie są tego samego znaku,*

(ii) *dla dowolnej liczby pierwszej $p|a_i$:*

$$-a_ja_k^{-1} \in K_p,$$

gdzie $\{i, j, k\} = \{0, 1, 2\}$, zaś a^{-1} oznacza odwrotność a w grupie $\mathbb{F}_p^\times$.

Przed dowodem udowodnimy prosty lemat:

Lemat 5.15. *Ustalmy liczbę pierwszą p. Wówczas:*

(a) *istnieją dwie reszty kwadratowe, które sumują się do nieresztę kwadratową $\mod p$,*

(b) *istnieją dwie niereszty kwadratowe, które sumują się do resztę kwadratową $\mod p$.*

Dowód. (a) Niech $n \in \{0, \ldots, p-1\}$ będzie najmniejszą nieresztą kwadratową $\mod p$, wtedy $r := n - 1$ jest resztą kwadratową oraz $r + 1 = n$.

(b) Jeżeli n, r są zdefiniowane jak wyżej, to n, nr są nieresztami kwadratowymi, które sumują się do reszty kwadratowej n^2. □

Dowód Twierdzenia 5.14. Wykażemy, że dla $p \nmid 2a_0a_1a_2$ powyższe równanie ma rozwiązanie w $\mathbb{F}_p$, tzn. że

$$(a_0K_p + a_1K_p) \cap (-a_2K_p) \neq \varnothing.$$

Wśród liczb a_0, a_1, a_2 muszą znaleźć się przynajmniej dwie, które wyznaczają tą samą warstwę w $\mathbb{F}_p^\times/K_p$ (tzn. obie są resztami lub nieresztami kwadratowymi). Bez straty ogólności załóżmy, że $a_0, a_1 \in K_p$. Rozważmy dwa przypadki:

- $-a_2$ jest nieresztą kwadratową. Wtedy:

  $$(a_0K_p + a_1K_p) \cap (-a_2K_p) = (K_p + K_p) \cap N_p$$

  zaś ostatni zbiór jest niepusty na mocy lematu 5.15.

- $-a_2$ jest resztą kwadratową. Wtedy $-a_2 \cdot a_0^{-1}$ jest również resztą kwadratową (jako iloczyn reszt kwadratowych). Stąd: $-a_2 \cdot a_0^{-1} \equiv b^2 \pmod p$, co oznacza, że $(b, 0, -1)$ jest rozwiązaniem powyższego równania.

Korzystając z lematu Hensela możemy podnieść uzyskane rozwiązanie z ciała $\mathbb{F}_p$ do $\mathbb{Q}_p$. Warunek (ii) zapewnia zaś istnienie rozwiązania dla $p|abc$, $p \neq 2$. Rozważane równanie ma również rozwiązanie w $\mathbb{Q}_2$, co można zauważyć, korzystając z *prawa wzajemności Hilberta*. Stąd, z zasady lokalno globalnej, równanie to ma rozwiązanie wymierne. Dowód przeciwnej implikacji zostawiamy jako ćwiczenie. □

Dowód twierdzenia 5.14 nie korzystający z zasady Hassego można znaleźć np. w [1].
Okazuje się, że zasada Hassego nie zachodzi dla form wyższych stopni. Przykład stanowi równanie:

$$3x^3 + 4y^3 + 5z^3 = 0$$

które ma rozwiązanie w $\mathbb{R}$ oraz w dowolnym $\mathbb{Q}_p$, ale nie w $\mathbb{Q}$. Krzywe podobnej postaci są szczególnie przydatne przy obliczaniu rangi krzywej eliptycznej, tzn. rangi grupy $E(\mathbb{Q})$. Mamy ciąg dokładny:

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to Sel^{(2)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[2] \to 0$$

gdzie $Sel^{(2)}(E/\mathbb{Q})$ jest grupą 2-nakryć krzywej, zaś

$$Ш(E/\mathbb{Q}) = \ker\left(H^1(G_{\mathbb{Q}}, E) \to \prod_v H^1(G_{\mathbb{Q}_v}, E)\right)$$

jest grupą lokalnie trywialnych (mających punkt w dowolnym uzupełnieniu $\mathbb{Q}$) przestrzeni jednorodnych dla $E/\mathbb{Q}$. Grupa $Ш(E/\mathbb{Q})$ stanowi więc „przeszkodę do zachodzenia zasady Hassego". Jedyna nadzieja teorioliczbowców leży w tym, że jest ona skończona – pozwoliłoby to na sprytne ominięcie jej. Ale to już zupełnie inna historia...

Bibliografia

[1] Ireland K., Rosen M. *A classical introduction to modern number theory*, volume 84 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1990.

[2] Silverman Joseph. H., Tate J. T., *Rational Points on Elliptic Curves*, Springer, 1992.

[3] Fulton W., *Algebraic Curves: An Introduction to Algebraic Geometry*, The Benjamin/Cummings Publishing Co.; First edition (1969)

[4] Atiyah M. F., Macdonald I.G., *Wprowadzenie do algebry komutatywnej.* Wydawnictwo UJ, 2008.

Krótka historia paradoksu petersburskiego i jego wczesnych rozwiązań

Jakub Golik
Politechnika Gdańska

Początki teorii prawdopodobieństwa sięgają siedemnastego wieku, kiedy to we Francji hazard oraz gry losowe cieszyły się dużą popularnością, w szczególności wśród arystokracji. Pewien francuski pisarz, Antoine Gombaud, znany równiez jako Chavalier de Mere, miał znaczący wpływ na rozwój teorii prawdopodobieństwa. Poprosił on dwóch najbardziej znanych matematyków jego czasów tj. Pascala oraz Fermata o matematyczną pomoc przy grach hazardowych. Jego prośba zaowocowała późniejszą korespondencją pomiędzy dwoma wybitnymi matematykami dotyczącą problematyki gier. Co jest szczególnie interesujące, wyrażenie „prawdopodobieństwo" nigdy nie pojawiło się w ich korespondencji. Główną radą, jaką Pascal i Fermat dali Gombaud, było użycie wartości oczekiwanej wygranych. Była to bardzo ważna sugestia, ponieważ dała ona początek przekonaniu, że podejmowanie racjonalnych decyzji w warunkach ryzyka powinno opierać się właśnie na wartości oczekiwanej.

Korespondencja Pascala z Fermatem przyczyniła się do powstania późniejszych publikacji dotyczących prawdopodobieństwa. Christian Huygens odwiedzając Paryż w 1655 roku dowiedział się o niej i po powrocie do Holandii napisał bardzo ważny traktat o prawdopodobieństwie, który został później przetłumaczony na łacinę. Wersja łacińska została bardzo dobrze przyjęta przez matematyków tamtego okresu i została dalej przetłumaczo-

na na wiele innych języków. Praca Huygensa była przez prawie pół wieku jedyną szeroko dostepną pracą dotyczącą prawdopodobieństwa.

6.1 Zakład Pascala i geneza pojęcia „nieskończonego zysku"

Blaise Pascal po swoim drugim duchowym nawróceniu w listopadzie 1654 zaprzestał badań w dziedzinie matematyki oraz fizyki i skupił się na rozważaniach teologicznych oraz filozoficznych. Sformułował on w tamtym czasie niezwykle ciekawy i prowokujący argument mający potwierdzać istnienie Boga. W dzisiejszych czasach nazywany jest on zakładem Pascala i jest jednym z najbardziej znanych zagadnień teologii filozoficznej.

Zakład Pascala bazuje na założeniu, że albo ktoś wierzy w Boga albo nie wierzy, bez możliwości pośredniej. W związku z tym można na ten zakład spojrzeć jak na loterię prostą z dwoma „wyborami" oraz dwoma „przypadkami" o nieznanych prawdopodobieństwach. Niech E będzie przypadkiem reprezentującym istnienie Boga i p prawdopodobieństwem wystąpienia przypadku E (zakład Pascala przyjmuje, że p jest dodatnie - może być infinitezymalne, ale musi być różne od zera). Wtedy, niech nE oznacza przypadek nieistnienia Boga. Dwa wybory oznaczone są następująco: B - wierzyć; oraz nB - nie wierzyć. Poniższa tabela podsumowuje zakład wraz z jego potencjalnymi „użytecznościami" (w kontekście rezultatów i korzyści z nimi związanych), gdzie u_1, u_2, u_3 i u_4 oznaczają użyteczności dla każdego z czterech możliwych rezultatów.

Tabela 6.1: Zakład Pascala

	E	nE
B	∞	u_1
nB	u_2	u_3

Pascal argumentował, że jeżeli człowiek zaakceptuje istnienie

Boga i w niego uwierzy, może spodziewać się życia wiecznego. W związku z tym oczekiwana użyteczność takiego przypadku jest nieskończona. Z drugiej jednak strony, jeżeli człowiek odrzuci istnienie Boga i ostatecznie okaże się być w błędzie, wtedy traci szansę na życie wieczne. Bez względu na rozważany przypadek, można założyć, że każdy poziom użyteczności u_1, u_2 i u_3, poza przypadkiem istnienia Boga i wiary w niego, jest skończony. Na podstawie powyższych założeń, można łatwo wyznaczyć oczekiwane użyteczności dwóch wyborów: B - wiary w Boga; oraz nB – braku wiary.

$$E(B) = p \times \infty + (1-p) \times u_1 = \infty$$

$$E(nB) = p \times u_2 + (1-p) \times u_3 = u_4$$

Pomimo, że wartości numeryczne poziomów użyteczności u_1, u_2, u_3 i u_4 są nieznane i niemożliwe do obliczenia, pewne jest, że są skończone. W związku z tym:

$$u_4 \ll \infty \Leftrightarrow E(nB) \ll E(B)$$

Bazując tylko na obliczonych wartościach oczekiwanych, każdy racjonalny człowiek powienien wierzyć w Boga.

Pomimo, że zakład jest przede wszystkim zagadnieniem rozważanym przez filozofów i teologów, a nie matematyków, wskazuje on możliwość otrzymania nieskończonego zysku w grze losowej, co stanowi główne zagadnienie paradoksu petersburskiego.

6.2 Pięć problemów Nicolasa Bernoulliego

Paradoks petersburski został stworzony przez Nicolasa Bernoulliego (1687 - 1759), jednakże w innej formie niż ta znana dzisiaj. Nicolas był bratankiem znanego Jakuba Bernoulliego (1655 - 1705), twórcy traktatu o teorii prawdopodobieństwa uważanego

za krok milowy w tej dziedzinie. Pierwsza wersja paradoksu pojawiła się w liście Nicolasa do francuskiego matematyka Pierre'a de Montmort'a (1678 - 1719). Bernoulli, który od dłuższego czasu korespondował z de Montmort'em, wysłał mu w liście z dnia 9 września 1713 pięć problemów matematycznych, które później ukazały się w drugiej edycji znanej książki de Montmorta dotyczacej gier hazardowych.

Dwa ostatnie problemy (czwarty i piąty) są istotne z punktu widzenia paradoksu petersburskiego.

Czwarty problem

Gracz A obiecuje dać graczowi B koronę (monetę), jeżeli ten: wyrzuci sześć oczek zwyczajną kostką do gry w pierwszym rzucie, dwie korony, jeżeli wyrzuci szóstkę w drugim rzucie, trzy korony, jeżeli wyrzuci w trzecim rzucie, cztery, jeżeli w czwartym itd. Szukamy oczekiwań gracza B.

Rozwiązanie tego problemu można łatwo uzyskać za pomocą wartości oczekiwanej.

$$\frac{1}{6}\sum_{n=1}^{\infty} n\left(\frac{5}{6}\right)^{n-1} = \frac{1}{6}\frac{1}{\left(1-\frac{5}{6}\right)^2} = 6$$

Piąty problem

Analogicznie do poprzedniego problemu, rozważamy sytuację, gdy gracz A obieca dać graczowi B ilość koron określoną przez następujące ciągi:

a) 1, 2, 4, 8, 16, ... albo

b) 1, 3, 9, 27, ... albo

c) 1, 4, 9, 16, 25, ... albo

d) 1, 8, 27, 64, ...

zamiast 1, 2, 3, 4, 5, ... jak poprzednio.

Powyższe ciągi mogą być przedstawione analogicznie do czwartego problemu tj.

$$\text{(a)} \qquad a_n = 2^{n-1} \qquad \Longrightarrow \quad \frac{1}{6}\sum_{n=1}^{\infty} 2^{n-1}\left(\frac{5}{6}\right)^{n-1}$$

$$\text{(b)} \qquad a_n = 3^{n-1} \qquad \Longrightarrow \quad \frac{1}{6}\sum_{n=1}^{\infty} 3^{n-1}\left(\frac{5}{6}\right)^{n-1}$$

$$\text{(c)} \qquad a_n = n^2 \qquad \Longrightarrow \quad \frac{1}{6}\sum_{n=1}^{\infty} n^2\left(\frac{5}{6}\right)^{n-1}$$

$$\text{(d)} \qquad a_n = n^3 \qquad \Longrightarrow \quad \frac{1}{6}\sum_{n=1}^{\infty} n^3\left(\frac{5}{6}\right)^{n-1}$$

Rozwiązanie piątego problemu nie jest takie proste, ponieważ w przypadku (a) oraz (b) wartość oczekiwana nie istnieje (a przynajmniej nie jest skończona), jako że odpowiednie szeregi są rozbieżne. Z drugiej strony, szeregi z podpunktów (c) oraz (d) są zbieżne, możemy zatem obliczyć wartość oczekiwaną.

P. R. de Montmort nie zainteresował się problemami otrzymanymi od Bernoulliego i w odpowiedzi swierdził, że mogą one być rozwiązane poprzez zastosowanie metody sumowania szeregów opracowanej przez zmarłego wujka Nicolasa - Jakuba Bernoulliego. Dnia 20 lutego 1714 Nicolas wysłał kolejny list zawierający jego rozwiązania problemów. Dla czwartego problemu poprawnie zsumował zbieżny szereg otrzymując sumę równą 6. Jednakże, gdy próbował on zastosować tę metodę do pierwszego przypadku z piątego problemu, otrzymał wynik równy $-\frac{1}{4}$ w efekcie sumując szereg rozbieżny. Uznał to za sprzeczność, co poskutkowało błędnymi próbami rozwiązania problemu.

Pomimo nieskutecznych prób rozwiązania tej sprzeczności, wnioski wysnute przez Nicolasa były istotne z punktu widzenia dalszych rozważań nad problemem. Argumentował on, że uczciwa wartość oczekiwania nie musi być sumą składowych oczekiwań, ponieważ niektóre przypadki z bardzo małym prawdopo-

dobieństwem powinny zostac odrzucone i traktowane jako zero. Niemniej jednak, trzeba zdać sobie sprawę, że nieważne jak mało znaczące może wydawać się prawdopodobieństwo pewnych zdarzeń, wygrana z nimi związana może znacząco wpływać na końcowy wynik oczekiwań. Bernoulli i wielu jego następców uznawało paradoks za swoistą rozbieżność pomiędzy powszechnie akceptowanym użyciem wartości oczekiwanej do oceny gier losowych, a właściwym (życiowym) oczekiwaniem zwrotu w takich grach. W ostatniej odpowiedzi do Nicolasa, de Montmort zaakceptował jego rozumowanie, jednakże skłaniał się bardziej ku słuszności wartości oczekiwanej. Niemniej jednak, zasugerował w dyplomatyczny sposób, że jedyną kompetentną osobą do dalszych badań nad tym problemem jest właśnie sam Nicolas. Pomimo dalszych prób zainteresowania de Montmort'a tematem, nie wniósł on już nic znaczącego do rozważań przed swoją śmiercią w 1719.

Rozważmy teraz problem przedstawiony de Montmort'owi. Niech poszukiwana wartość oczekiwana będzie wyrażona poprzez użycie rozbieżnego nieskończonego szeregu skończonych oczekiwań:

$$\sum_{n=1}^{\infty} p(n)a(n) \tag{6.1}$$

Powyższe wyrażenie jest skonstruowane w taki sposób, że: $p(n)$ oznacza prawdopodobieństwo wygranej w n-tej próbie; $a(n)$ oznacza wygraną kwotę; przy czym $\{a(n)\}$ jest rosnącym ciągiem, a $\{p(n)\}$ malejącym.

Nicolas Bernoulli zasugerował zamianę ciągu $\{p(n)\}$ na inny ciąg $\{\bar{p}(n)\}$, taki, że nowo stworzony szereg:

$$\sum_{n=1}^{\infty} \bar{p}(n)a(n)$$

będzie zbieżny. Pomysł polegał na zastąpieniu bardzo małych prawdopodobieństw w ciągu $\{\bar{p}(n)\}$ zerem. Innymi słowy, polegało to na „ucięciu ogona" ciągu $\{p(n)\}$ dla n większych niż jakaś wartość m.

6.3 Wkład Gabriela Cramera

Forma, w jakiej znamy paradoks dzisiaj, została stworzona przez szwajcarskiego matematyka Gabriela Cramera, który miał największy wpływ na rozwój paradoksu petersburskiego w jego wczesnym etapie. W liście do Nicolasa Bernoulliego z 21 maja 1728 zasugerował on alternatywne rozwiązanie problemu opisanego równaniem 6.1. W przeciwieństwie do tego co zasugerował Nicolas, Cramer zaproponował analogiczne rozwiazanie polegające na zastąpieniu ciągu $\{a(n)\}$ innym ciągiem $\{\bar{a}(n)\}$, takim, że szereg

$$\sum_{n=1}^{\infty} p(n)\bar{a}(n) \tag{6.2}$$

będzie zbieżny. Jednakże, jednym z najważniejszych elementów listu było uproszczenie piątego problemu Nicolasa. Cramer zasugerował zastąpienie sześciennej kostki do gry dwustronną (zwyczajną/uczciwą) monetą oraz zamianę ról Gracza A oraz Gracza B. W rezultacie, jeżeli Gracz A wyrzuci pierwszą reszkę za n-tym razem, wyrzuciwszy wcześniej pod rząd $n-1$ orłów, dostanie on 2^{n-1} koron (monet) od Gracza B, gdzie $n = 1, 2, 3, \ldots$. Łatwo zauważyć, że oczekiwania Gracza A mogą zostać formalnie wyrażone przy pomocy szeregu 6.1.

Dzięki uproszczeniu Cramera możemy teraz sformułować współczesną wersję paradoksu petersburskiego opublikowaną później przez Daniela Bernoulliego:

Piotr rzuca monetą tak długo, aż wypadnie reszka. Zgadza się dać Pawłowi jednego dukata, jeżeli sam wyrzuci reszkę w pierwszym rzucie, dwa dukaty, jeżeli wyrzuci w drugim, cztery, jeżeli w trzecim, osiem, jeżeli w czwartym i tak dalej, w taki sposób, że z każdym następnym rzutem liczba wypłacanych dukatów jest podwajana. Załóżmy, że chcemy okreslić wartość oczekiwań Pawła.

Cramer uznał za paradoks fakt, że według obliczeń Gracz A powinien zapłacić Graczowi B nieskończoną sumę pieniędzy aby

wziąć udział w grze. Argumentował, iż jest to absurd, ponieważ żaden rozsądny człowiek nie zapłaciłby więcej niż 20 koron by wziąć udział w grze. Jego dalsze rozumowanie jest często cytowane w literaturze dotyczącej tego zagadnienia:

„Jaka jest przyczyna rozbieżności pomiędzy matematycznymi obliczeniami a zwyczajną oceną? Spowodowane jest to tym, że matematycy wartościują pieniądze w stosunku do ich ilości, a rozsądni ludzie wartościują je w stosunku do pożytku jaki mogą z nich uzyskać."

Podobne rozumowanie przedstawił Daniel Bernoulli w kontekście wyżej zacytowanej wersji paradoksu.

„. . . Pomimo, że standardowe obliczenia wskazują, że wartość oczekiwań Pawła jest nieskończenie wielka, musimy przyznać, że każdy w miarę rozsądny człowiek z wielką przyjemnością zapłaciłby za taką szansę dwadzieścia dukatów."

Inną uwagę, jednakże trochę ostrą, sforumował przyjaciel i korespondent Cramera - francuski naturalista G. L. L. Buffon (1707-1788).

„Skąpiec jest jak matematyk - obydwoje oceniają wartość pieniędzy po ich numerycznej ilości."

Cramer kontynuował swoje rozważania nad problemem wskazując na fakt, że to, co powoduje nieskończoną wartość oczekiwaną, to możliwość wygrania niewyobrażalnej kwoty pieniędzy, jeżeli gracz nie wyrzuci reszki do bardzo późnej próby np. do setnego lub tysięcznego rzutu. Co więcej, Cramer uważał, że dla rozsądnego człowieka nie powinno być warte mniej lub nieść za sobą mniej przyjemności, gdyby możliwa wygrana była ograniczona do 10 lub 20 milionów koron. Bazując na swoim założeniu, postanowił on policzyć oczekiwania zgodnie z szeregiem 6.2 dla ograniczonej ilości koron do $2^{24} = 16777216$. W związku z powyższym, suma szeregu 6.2 (który jest teraz skończony) jest

oczywiście skończona i równa 13. Cramer nazwał swój wynik „moralną wartością bogactwa", co współcześni ekonomiści nazwaliby użytecznością pieniądza.

Gabriel Cramer uznał osiągnięty wynik za zbyt wysoki i próbował go zmniejszyć poprzez wprowadzenie alternatywnego założenia. Zasugerował, że 100 milionów przynosi więcej przyjemności niż 10 milionów, ale na pewno nie 10 razy więcej. W związku z tym zasugerował, że moralna wartość bogactwa powinna zostać wyrażona poprzez pierwiastek kwadratowy wartości oczekiwanej.

6.4 Pochodzenie nazwy paradoksu i okoliczności jego pierwszej publikacji

Gdy Nicolas Bernoulli otrzymał od Gabriela Cramera uproszczoną wersję swojego problemu, postanowił przedstawić ją swojemu kuzynowi Danielowi Bernoulliemu, który był w tym czasie profesorem matematyki na uniwersytecie w Petersburgu. Dnia 27 października 1728 Nicolas wysłał swojemu kuzynowi czwarty i piąty problem w uproszczonej wersji Cramera. Z początku Daniel Bernoulli nie był nimi zainteresowany i uznał je za bardzo proste, choć trochę paradoksalne. W odpowiedzi do Nicolasa napisał, że prawdopodobieństwo, iż gra potrwa dłużej niż 20 lub 30 rzutów, jest niezmiernie małe. Nicolas odrzucił argumentację swojego kuzyna, co skłoniło Daniela do ponownego zastanowienia się nad problemami. Później Daniel Bernoulli wysłał do Nicolasa *memoir*, w którym rzucił nowe światło na problem. Zasugerował on, że początkowe bogactwo gracza również powinno być wzięte pod uwagę przy wyznaczaniu jego oczekiwań. W związku z sugestią Daniela, Nicolas uznał, że połączenie jego sugestii wraz z sugestią Gabriela Cramera może przyczynić się do dokładniejszego sposobu odrzucania małych prawdopodobieństw.

Paradoks petersburski zawdzięcza swoją nazwę miejscu jego pierwszej oficjalnej publikacji. Poza wzmianką o korespondencji z Nicolasem Bernoullim z 1713 w książce de Montmort'a, wszyst-

ko wskazuje na to, że problem nie został opublikowany przed rokiem 1738. W 1731 Daniel Bernoulli wysłał swój *memoir* do publikacji w czasopiśmie *Commentarii* Akademii Petersburskiej, który został oficjalnie opublikowany dopiero siedem lat później w 1738.

Daniel w swoim *memoir* wprowadził bardzo ważną hipotezę, która stanowi podstawę teorii marginalnej użyteczności szereko stosowanej we współczesnej ekonomii. Zasugerował, że aby określić wartość ryzyka dla konkretnej osoby, nie wystarczy zastosować wartości oczekiwanej. Co więcej, stwierdził, że w rzeczywistości możliwość wygrania danej sumy pieniędzy nie jest równie istotna dla różnych osób, ale jest raczej względna w stosunku do obecnego poziomu ich bogactwa (majątku). W związku z powyższym zdefiniował następującą hipotezę:

„Teraz jest wielce prawdopodobne, że jakikolwiek przyrost bogactwa, nieważne jak bardzo nieznaczący, będzie zawsze skutkował wzrostem użyteczności, która jest odwrotnie proporcjonalna do dóbr już posiadanych."

Powyższą hipotezę można zapisać w języku matematycznym za pomocą następującej pochodnej:

$$dy = k\frac{dx}{x}$$

gdzie dy oznacza przyrost użyteczności dla danej osoby, x oznacza jej obecne bogactwo oraz dx otrzymanie dodatkowej sumy pieniędzy, nastomiast $k > 0$ jest subiektywnym czynnikiem proporcjonalności ustalonym dla danej osoby. Aby wyznaczyć y musimy scałkować powyższy wzór w nastepujący sposób:

$$y = k\int_a^x \frac{dx}{x} = k\ln\frac{x}{a} \tag{6.3}$$

gdzie a (wymagamy, by $a > 0$) oznacza początkowe bogactwo. Następnie, niech a będzie oznaczać początkowe bogactwo osoby, która gra w grę w której kwota a_n może być wygrana z prawdopodobieństwem p_n dla $n = 1, 2, 3, \ldots$ oraz $\sum_{n=1}^{\infty} p_n = 1$. Jego war-

tość oczekiwana jest prosta do otrzymania i równa: $\sum_{n=1}^{\infty} p_n a_n$. Jednakże, według hipotezy Bernoulliego, którą nazwał „średnią użytecznością", jest ona równa:

$$k \sum_{n=1}^{\infty} p_n \ln \left[\frac{(a + a_n)}{a} \right]$$

pod warunkiem zbieżności szeregu.
„Średnia użyteczność" Bernoulliego została później nazwana „moralnym oczekiwaniem" przez Pierre'a Simon'a de Laplace'a (1749-1827).

Teoria Daniela została odrzucona przez Nicolasa, który upierał się, że stawka gry losowej musi być wyznaczona obiektywnie. Ponadto zauważył, iż gdyby teoria Daniela została wprowadzona do gry, każdy gracz musiałby zapłacić Piotrowi inną stawkę by wziąć w niej udział, podczas gdy potencjalne ryzyko Piotra pozostałoby takie samo.

6.5 Super-paradoks petersburski Mengera

Rozwiązanie Cramera-Bernoulliego nie przeszło próby czasu. Zostało ono obalone przez Carla Mengera (1840-1921) - austriackiego ekonomistę, który skonstruował kontrprzykład nazwany później przez innego ekonomistę Paula Anthony'ego Samuelson'a (1915-2009) super-paradoksem petersburskim. Menger pokazał, że zastosowanie „wystarczająco wklęsłego" przekształcenia wygranych jest zaledwie warunkiem koniecznym, ale nie wystarczającym by rozwiązać paradoks.

Pomysł Mengera polegał na zastąpieniu wypłaty $a(n) = 2^n$ przez $\hat{a}(n) = e^{2^n}$, która po zastosowaniu wklęsłego przekształcenia Bernoulliego $ln(\cdot)$ do $\hat{a}(n)$ przywracała paradoks. To samo mogło zostać zrobione w przypadku rozwiązania Cramera poprzez zastapienie $a(n) = 2^n$ wyrażeniem $\hat{a}(n) = (2^n)^2$. W ten sposób, stosując przekształcenie Cramera z użyciem pierwiastka kwadratowego $\sqrt{\hat{a}(n)}$, paradoks znów powraca. W ogólności,

kontrprzykłady Mengera pokazują, że dla każdej rosnącej i nieograniczonej funkcji użyteczności, można znaleźć takie rosnące przekształcenie, że przekształcone wygrane zbiegają szybciej do nieskończoności niż prawdopodobieństwa zbiegają do zera. Carl Menger był pierwszą osobą, która sformułowała i udowodniła warunek konieczny i wystarczający na uniknięcie wystąpienia paradoksu petersburskiego. Głównym wkładem Mengera do rozwiązania paradoksu petersburskiego było pokazanie, że warunkiem koniecznym jest ograniczoność funkcji użyteczności. Inymi słowy pokazał, że gra typu paradoks petersburski ma skończone rozwiązanie tylko wtedy, gdy funkcja użyteczności (wygranych) jest ograniczona. Wyżej wspomniany Paul Samuelson nazwał wkład Mengera „skokiem kwantowym" w analizie paradoksu petersburskiego.

Zadziwiający jest fakt, że paradoks petersburski musiał czekać tak długo na sformułowanie przez Mengera warunków koniecznych i wystarczających na jego uniknięcie. Według Christiana Seidl'a (Seidl, 2013) było to spowodowane pojmowaniem użyteczności i jej rozwojem na przestrzeni kilku wieków. Wielu naukowców tamtych czasów uważało użyteczność za coś *„zauważalnego, niezmiennego i interpersonalnie porównywalnego"* (Dutka, 1988). Dopiero w 1906 po raz pierwszy włoski ekonomista Vilfredo Pareto stwierdził, że użyteczność jest nieporównywalna interpersonalnie.

Bibliografia

[1] Dutka, J. (1988). *On the St. Petersburg paradox.* Archive for History of Exact Sciences, 39(1), 13-39

[2] Seidl, C. (2013). *The St. Petersburg Paradox at 300.* J Risk Uncertain, 46, 247-264

[3] Tabarrok, A. (2000). *BELIEVE IN PASCAL'S WAGER? HAVE I GOT A DEAL FOR YOU!.* Theory and Decision 48, 123-128

Twierdzenie Mihăilescu

Patryk Jaśniewski
Politechnika Gdańska

7.1 Hipoteza Catalana i dowód Mihăilescu (2003)

W 1844 roku Eugène Catalan postawił hipotezę, iż nie ma innych kolejnych potęg liczb całkowitych o wykładniku większym od 1 oprócz $8 = 2^3$ i $9 = 3^2$. Problem można sformułować następująco w postaci twierdzenia:

Twierdzenie 7.1 (Twierdzenie Mihăilescu)**.** *Niech $x, y \in \mathbb{Z}\setminus\{0\}$ oraz $p, q \in \mathbb{Z}$, $p, q > 1$. Równanie $x^p - y^q = 1$ ma następujące jedyne rozwiązania: $x = \pm 3, y = 2, p = 2, q = 3$.*

Problem przez ponad półtora wieku pozostawał nierozstrzygnięty. Jego rozwiązanie przedstawił w 2003 roku matematyk Preda Mihăilescu. Dowód tej hipotezy opiera się na dowiedzionych przez Mihăilescu trzech twierdzeniach. Ich uzasadnienie korzysta z teorii Galois i teorii ciał cyklotomicznych, których nie będę przedstawiał z powodów ograniczeń w objętości i wysokie skomplikowanie rozumowań przeprowadzonych w dowodach twierdzeń pomocniczych. Podamy jednakże ich sformułowanie:

Twierdzenie 7.2. *Niech $x, y \in \mathbb{Z} \setminus \{0\}$ oraz $p, q \in \mathbb{Z}$, $p, q > 1$ oraz dane jest równanie $x^p - y^q = 1$. Wtedy $p^{q-1} \equiv 1 \ (mod\ q^2)$ lub $q^{p-1} \equiv 1 \ (mod\ p^2)$.*

Twierdzenie 7.3. *Niech $x, y \in \mathbb{Z} \setminus \{0\}$ oraz $p, q \in \mathbb{Z}$, $p, q > 1$ oraz dane jest równanie $x^p - y^q = 1$. Wtedy $p \equiv 1 \pmod{q}$ lub $q \equiv 1 \pmod{p}$.*

Twierdzenie 7.4. *Niech $x, y \in \mathbb{Z} \setminus \{0\}$ oraz $p, q \in \mathbb{Z}$, $p, q > 1$ oraz dane jest równanie $x^p - y^q = 1$. Wtedy $p < 4q^2$ lub $q < 4p^2$.*

Zanim przejdziemy do dowodu twierdzenia Mihăilescu udowodnimy pewien prosty lemat.

Lemat 7.5. *Jeśli $x^{y-1} \equiv 1 \pmod{y^2}$ i $x \equiv 1 \pmod{y}$, to $x \equiv 1 \pmod{y^2}$.*

Dowód. Wiemy, że $x \equiv 1 \pmod{y}$, tzn. że istnieje $l \in \mathbb{Z}$, spełniające: $x = ly + 1$. Podnosząc to wyrażenie do potęgi $y - 1$ otrzymujemy, że:

$$\begin{aligned} x^{y-1} &= (ly+1)^{y-1} \\ &= (ly)^{y-1} + \binom{y-1}{1}(ly)^{y-2} + \ldots + \binom{y-1}{y-2}(ly) + 1 \\ &\equiv (y-1)(ly) + 1 \pmod{y^2}, \end{aligned}$$

czyli $x \equiv -ly + 1 \pmod{y^2}$. Wiemy, że $x^{y-1} \equiv 1 \pmod{y^2}$, a zatem $-ly \equiv 0 \pmod{y^2}$. Z tego wynika, że $y|l$, a zatem z równości $x = ly + 1$ otrzymujemy: $x \equiv 1 \pmod{y^2}$. □

Dowód twierdzenia Mihăilescu. Przypadek $q = 2$ został rozpatrzony w 1850 r. przez V. Lebesgue'a, zaś przypadek $p = 2$ - przez Ko Chao w 1965r.
Zauważmy, że wystarczy rozpatrzyć równanie tylko ze względu na p i q będące nieparzystymi liczbami pierwszymi. Istotnie, jeśli wykładniki są złożone, to zawsze można je rozłożyć tak, by czynnikiem była liczba pierwsza. Z własności działań na potęgach można zatem sprowadzić problem do rozpatrywania nieparzystych i pierwszych wykładników.
Równanie to jest symetryczne ze względu na p i q (układ (x, y, p, q) można zamienić na $(-y, -x, q, p)$). Wystarczy zatem bez straty

ogólności rozpatrywać jedną z możliwości podanych w tezach powyższych twierdzeń. Z twierdzeń 7.2, 7.3 oraz lematu 7.5 wynika, że $p \equiv 1 \pmod{y^2}$, czyli istnieje $k \in \mathbb{Z}_+$ takie, że $p = kq^2 + 1$. Z twierdzenia 7.4 mamy, że $p = kq^2 + 1 < 4q^2$. Z tego zaś wynika, że $k \in \{1, 2, 3\}$. Przypadek $k = 1$ oraz $k = 3$ należy odrzucić, ponieważ dla tych k liczba $p = kq^2 + 1$ jest parzysta, a to jest niemożliwe, bo q jest liczbą nieparzystą. Zatem $p = 2q^2 + 1$. Nietrudno zauważyć, że jeśli q nie dzieli się przez 3, to $2q^2 + 1 \equiv 0 \pmod 3$ i z tego, że p jest liczbą pierwszą, musiałoby zachodzić, że $p = 3$, co dawałoby, że $q = 1$ – sprzeczność. A zatem $3|q$, czyli $q = 3$ (bo q jest liczbą pierwszą). Wtedy $p = 2q^2 + 1 = 19$. Na mocy twierdzenia 7.2 mamy, że $3^{18} \equiv 1 \pmod{19^2}$, co jest nieprawdą (sprawdzenie zostawiam jako proste ćwiczenie). Owa sprzeczność kończy dowód twierdzenia. □

7.2 Przypadek q=2

Zajmiemy się teraz równaniem $x^p - y^2 = 1$, gdy $x, y \in \mathbb{Z}\setminus\{0\}$ oraz $p \in \mathbb{Z}$, $p > 1$. Wykażemy, że nie ma takich x, y, p, aby równanie było spełnione. Zanim przejdziemy do dowodu, pozostawię pięć prostych ćwiczeń dla Czytelnika, z których będziemy korzystać w dowodzie.

Ćwiczenie 7.6. *Pierścień $\mathbb{Z}[i]$ jest pierścieniem z jednoznacznością rozkładu.*

Ćwiczenie 7.7. *W pierścieniu $\mathbb{Z}[i]$ mamy, że $(1+i)|(a+bi) \iff a \equiv b \pmod 2$.*

Ćwiczenie 7.8. *Niech y będzie liczbą całkowitą parzystą. Wtedy elementy $1 + iy$ oraz $1 - iy$ są względnie pierwsze w pierścieniu $\mathbb{Z}[i]$.*

Ćwiczenie 7.9. *Niech x, y, z należą do pierścienia z jednoznacznością rozkładu, elementy y oraz z będą względnie pierwsze oraz $x^p = yz$. Wtedy $y = a^p$ oraz $z = b^p$ dla pewnych elementów względnie pierwszych a, b z tego pierścienia.*

Ćwiczenie 7.10. *Niech $v_p(n)$ oznacza wykładnik, z jakim liczba pierwsza p wchodzi w rozkładzie na czynniki pierwsze liczby n. Niech $x, y \in \mathbb{Z}$. Mamy, że $v_p(xy) = v_p(x)+v_p(y)$, a także $v_p(\frac{x}{y}) = v_p(x) - v_p(y)$ oraz, że $v_p(x) \geqslant 0$, jeśli $x \in \mathbb{Z}$.*

Twierdzenie 7.11. *Niech $x, y \in \mathbb{Z} \setminus \{0\}$ oraz $p \in \mathbb{Z}$, $p > 1$. Wtedy równanie $x^p - y^2 = 1$ nie ma rozwiązań.*

Dowód. Równanie dane w tezie zapiszmy w postaci następującej:

$$x^p = y^2 + 1.$$

Redukując je modulo 4 mamy, że x jest liczbą nieparzystą, a y parzystą. Rozpatrzymy je w pierścieniu $\mathbb{Z}[i]$. Mamy, że $x^p = (1+iy)(1-iy)$. Z powyższej obserwacji, ćwiczenia 7.8, ćwiczenia 7.6 i ćwiczenia 7.9 odpowiednio, wnosimy, że $1+iy = c^p$ i $1-iy = \overline{c}^p$. Dodając obie równości stronami mamy, że:

$$2 = (c + \overline{c})(c^{p-1} + \ldots + \overline{c}^{p-1}). \tag{7.1}$$

Wiadomo, że $c + \overline{c}$ jest liczbą całkowitą parzystą, albowiem rozważania prowadzimy w odniesieniu do $\mathbb{Z}[i]$. W związku z tym i z (7.1) mamy, że $c + \overline{c} = 2$, czyli $c = \pm(1 + bi)$. Z (7.1) widać, że $c = 1 + bi$, $b \in \mathbb{Z}$. Co więcej, z ćwiczenia 7.7 wiemy, że $1 + i$ nie dzieli $1+iy$, ponieważ y nie jest tej samej parzystości, co 1, czyli także $1+i$ nie dzieli $c = 1+bi$, zatem b nie jest tej samej parzystości co 1, tzn. b jest liczbą parzystą. Podstawiając $1+bi$ w miejsce c i $1 - bi$ w miejsce c otrzymujemy, że $(1 + bi)^p + (1 - bi)^p = 2$, równoważnie

$$\binom{p}{2}(bi)^2 + \binom{p}{4}(bi)^4 + \ldots + \binom{p}{p-1}(bi)^{p-1} = 0.$$

Pokażemy teraz, że $v_2(\binom{p}{k}(bi)^k) > v_2(\binom{p}{2}(bi)^2)$. Z ćwiczenia 7.10 wynika, że należy pokazać, iż:

$$v_2\left(\binom{p}{k}\binom{p}{2}^{-1}(bi)^{k-2}\right) > 0. \tag{7.2}$$

Nietrudno zauważyć, że:

$$v_2(2(bi)^{k-2}) \geqslant k-1 > \log_2 k \geqslant v_2(k) = v_2(k(k+1)) \qquad (7.3)$$

Zatem, z (7.3) i z własności podanych w ćwiczeniu 7.10, otrzymujemy:

$$v_2\left(\binom{p}{k}\binom{p}{2}^{-1}(bi)^{k-2}\right) = v_2\left(\binom{p-2}{k-2}\frac{2}{k(k+1)}(bi)^{k-2}\right) =$$
$$= v_2\left(\binom{p-2}{k-2}\right) + v_2(2(bi)^{k-2}) - v_2(k(k+1)) > 0,$$

a to należało pokazać. Jeśli $b \neq 0$, to z (7.2) otrzymujemy, że z jednej strony 2 znajduje się w rozkładzie na czynniki pierwsze lewej strony równości z dodatnim wykładnikiem, zaś po prawej stronie równości (7.2) mamy 0, co oznacza, że sytuacja jest niemożliwa. Zatem $b = 0$, z czego mamy, że $c = 1$, czyli $y = 0$, co prowadzi do sprzeczności, albowiem z założenia y jest niezerowe. □

7.3 Przypadek p=2

Zajmiemy się teraz równaniem $x^2 - y^q = 1$, gdy $x, y \in \mathbb{Z} \setminus \{0\}$ oraz $q \in \mathbb{Z}$, $q > 1$. Zanim przejdziemy do rozważań, pozostawię dla Czytelnika kilka ćwiczeń, z których będziemy korzystać w dowodzie.

Ćwiczenie 7.12. *Niech liczby całkowite x, y będą względnie pierwsze oraz niech q będzie liczbą pierwszą. Wtedy $NWD(x-y, \frac{x^q-y^q}{x-y})|q$.*

Ćwiczenie 7.13. *Niech q będzie liczbą pierwszą. Jeśli $x^q - y^q = 2$, to $x = 1, y = -1$.*

Lemat 7.14. *Niech $x, y \in \mathbb{Z} \setminus \{0\}$ oraz $q \in \mathbb{Z}$, $q \geqslant 3$. Dane jest równanie $x^2 - y^q = 1$. Wtedy istnieją $a, b \in \mathbb{Z}$ takie, że $NWD(2a, b) = 1$, $x - 1 = 2^{q-1}a^q$ oraz $x + 1 = 2b^q$.*

Dowód. Lemat wystarczy rozpatrywać dla pierwszych q, co wynika z działań na potęgach. Zapiszmy równanie w postaci $y^q = (x-1)(x+1)$. Nietrudno zauważyć, że $NWD(x-1, x+1) \in \{1, 2\}$, co pozostawiam jako proste ćwiczenie. Jeśli x jest liczbą parzystą, to wówczas $NWD(x-1, x+1) = 1$, a zatem z ćwiczenia 7.9 mamy, że $x - 1 = d^q$ oraz $x + 1 = e^q$ dla pewnych $d, e \in \mathbb{Z}$. Z ćwiczenia 7.13 wynika, że $x-1 = -1$ i $x+1 = 1$, czyli $x = 0$, równanie jednak rozpatrujemy dla niezerowych x. Z tego wynika, że x jest nieparzyste, a wówczas y jest parzyste. Z tego wynika, że $2^q | (x-1)(x+1)$, ale $NWD(x-1, x+1) = 2$, zatem, zmieniając znak x, gdy to potrzebne, możemy przyjąć, że $x \equiv 1 \pmod 4$ i wtedy $(\frac{x-1}{2^{q-1}})(\frac{x+1}{2}) = (\frac{y}{2})^q$. Na mocy powyższych rozważań liczby $\frac{x-1}{2^{q-1}}$ i $\frac{x+1}{2}$ są względnie pierwsze, a zatem, z ćwiczenia 7.9, istnieją liczby całkowite względnie pierwsze a, b takie, że $\frac{x-1}{2^{q-1}} = a^q$ oraz $\frac{x+1}{2} = b^q$. Zatem $x - 1 = 2^{q-1}a^q$ i $x + 1 = 2b^q$ dla pewnych a, b takich, że $NWD(2a, b) = 1$. □

Lemat 7.15. *Niech $x, y \in \mathbb{Z} \setminus \{0\}$ oraz $q \in \mathbb{Z}$, $q \geqslant 3$. Dane jest równanie $x^2 - y^q = 1$. Wtedy $x \equiv 0 \pmod q$.*

Dowód. Lemat wystarczy rozpatrywać dla pierwszych q, co wynika z działań na potęgach. Równanie zapiszmy w postaci $x^2 = y^q + 1 = (y+1)(\frac{y^q+1}{y+1})$. Przypuśćmy, że $NWD(y+1, \frac{y^q+1}{y+1}) = 1$. Wówczas z ćwiczenia 7.12 i ćwiczenia 7.9 mamy, że $y + 1 = u^2$. Widać, że y jest liczbą parzystą, zaś u nieparzystą, a także, że y i u są względnie pierwsze. Rozpatrzymy równanie Pella $X^2 - yY^2 = 1$. Równanie to spełniają pary liczb $(x, y^{\frac{q-1}{2}})$ oraz $(u, 1)$. Lewa strona równości jest normą dla pierścienia euklidesowego $\mathbb{Z}[\sqrt{y}]$. Można wykazać (co pozostawiam jako trudniejsze ćwiczenie), że generatorami jedności tego pierścienia są ± 1 oraz $u + \sqrt{y}$. Zatem:

$$x + y^{\frac{q-1}{2}} = (u + \sqrt{y})^m \tag{7.4}$$

dla pewnego $m \in \mathbb{Z}$. Elementem odwrotnym do $u + \sqrt{y}$ w tym pierścieniu jest $-(-u + \sqrt{y})$, z czego widać, że wystarczy rozpatrzyć jedynie nieujemne m. Dokonajmy redukcji równania (7.4)

modulo ideał $y\mathbb{Z}[\sqrt{y}]$. Otrzymamy, że

$$x \equiv u^m + mu^{m-1}\sqrt{y} \ (mod\ y\mathbb{Z}[\sqrt{y}]).$$

Z tego, że 1 i $\sqrt{y}$ tworzą $\mathbb{Z}$-bazę grupy addytywnej $\mathbb{Z}[\sqrt{y}]$ wynika, że $y|mu^{m-1}$. Z tego, że y jest parzyste, a u - nieparzyste dostajemy, że m jest parzyste. A zatem:

$$x + y^{\frac{q-1}{2}} = (u + \sqrt{y})^m = (u^2 + 2u\sqrt{y} + y)^{\frac{m}{2}} \tag{7.5}$$

Dokonajmy redukcji równania (7.5) modulo ideał $u\mathbb{Z}[\sqrt{y}]$. Otrzymamy, że $x + y^{\frac{q-1}{2}} \equiv y^{\frac{m}{2}}\ (mod\ u\mathbb{Z}[\sqrt{y}])$. Na podstawie analogicznych przesłanek jak wyżej wnosimy, że $u|y^{\frac{q-1}{2}}$. Z tego, że y i u są względnie pierwsze, to (z rozkładu kanonicznego y i u) wynika, że powyższa podzielność jest możliwa jedynie dla $u = 1$. Wtedy $y = 0$, co przeczy założeniu, iż y jest niezerowe. Zatem $NWD(y + 1, \frac{y^q+1}{y+1}) = q$, z czego wynika, że $q|x^2$ i także $q|x$, ponieważ q jest liczbą pierwszą. □

Lemat 7.16. *Niech $x, y \in \mathbb{Z} \setminus \{0\}$ oraz $q \in \mathbb{Z}$, $q \geqslant 3$. Dane jest równanie $x^2 - y^q = 1$. Wtedy $x \equiv 3\ (mod\ q)$.*

Dowód. Lemat wystarczy rozpatrywać dla pierwszych q, co wynika z działań na potęgach. Mając wynik lematu 7.15 wystarczy wykazać twierdzenie dla $q \geqslant 5$. Z lematu 7.14 mamy, że $x - 1 = 2^{q-1}a^q$ i $x + 1 = 2b^q$ dla pewnych a, b takich, że $NWD(2a, b) = 1$. Mamy, że

$$b^{2q} - (2a)^q = \frac{x+1}{2} - 2(x-1) = \left(\frac{x-3}{2}\right)^2$$

Rozkładając lewą stronę równości mamy: $(b^2 - 2a)(\frac{b^{2q}-(2a)^q}{b^2-2a}) = (\frac{x-3}{2})^2$. Przypuśćmy, że $NWD(b^2 - 2a, \frac{b^{2q}-(2a)^q}{b^2-2a}) = 1$. Wówczas $b^2 - 2a = c^2$. Z tego, że $|(b-1)^2 - b^2| \geqslant 2|b| - 1$ otrzymujemy $2|a| = |c^2 - b^2| \geqslant |(b-1)^2 - b^2| \geqslant 2|b| - 1$, zatem $|a| \geqslant |b|$. Z drugiej strony mamy jednak $|a|^q = \frac{|x-1|}{2^{q-1}} \leqslant \frac{|x-1|}{16} < \frac{|x+1|}{2} = |b|^q$. Powyższa sprzeczność ukazuje, że wg ćwiczenia 7.12,

$NWD(b^2-2a, \frac{b^{2q}-(2a)^q}{b^2-2a}) = q$ i dlatego $q|(\frac{x-3}{2})^2$, co implikuje, że $x \equiv 3 \ (mod\ q)$. □

Twierdzenie 7.17. *Niech $x, y \in \mathbb{Z} \setminus \{0\}$ oraz $q \in \mathbb{Z}$, $q > 1$. Dane jest równanie $x^2 - y^q = 1$. Wtedy $q = 3$.*

Dowód. Z lematu 7.15 i lematu 7.16 wprost wynika, że $q = 3$. □

7.4 Równanie $x^2 - y^3 = 1$

Twierdzenie 7.18. *Niech $x, y \in \mathbb{Z} \setminus \{0\}$. Rozwiązaniami równania $x^2 - y^3 = 1$ są pary liczb: $x = \pm 3, y = 2$.*

Dowód. Równanie napiszmy w postaci: $y^3 = x^2 - 1 = (x-1)(x+1)$. W jednym z dowodów powyżej zauważyliśmy, że $NWD(x-1, x+1) = 1$ lub $NWD(x-1, x+1) = 2$. Jeśli x jest liczbą parzystą, to wówczas $NWD(x-1, x+1) = 1$, a zatem z ćwiczenia 7.9 mamy, że $x - 1 = a^3$ i $x + 1 = b^3$. Wtedy $b^3 - a^3 = 2$, co na mocy ćwiczenia 7.13 oznacza, że $b = 1$ i $a = -1$, zatem $x = 0$, co przeczy temu, że x jest niezerowy.
Niech zatem x będzie nieparzysty i wówczas $NWD(x-1, x+1) = 2$. Z lematu 7.14 (zmieniając znak x, tak aby $x \equiv 1 \pmod 4$) mamy, że $x - 1 = 2^2 v^3$ i $x + 1 = 2u^3$. Odejmując pierwsze równanie od drugiego otrzymujemy, że $2u^3 - 4v^3 = 2 \iff u^3 - 2v^3 = 1$. Jako ćwiczenie z algebry abstrakcyjnej pozostawiam fakt, że wyrażenie $u^3 - 2v^3$ jest normą dla pierścienia euklidesowego $\mathbb{Z}[\sqrt[3]{2}]$. W tym przypadku rozpatrujemy zatem element odwracalny tego pierścienia $\epsilon = u - v\sqrt[3]{2} \in \mathbb{Z}[\sqrt[3]{2}]$. Można pokazać (co jest dość wymagające, ale elementarne), że generatorem grupy jedności $\mathbb{Z}[\sqrt[3]{2}]^\times$ jest element $\eta = \sqrt[3]{2} - 1$, którego norma jest równa 1. Zatem $\epsilon = \eta^n$ dla pewnego $n \in \mathbb{Z}$. Nietrudno zauważyć, że $n = 0$ lub $n = 1$, ponieważ element ϵ nie zawiera składnika, którego czynnikiem jest $\sqrt[3]{4}$.
Dla $n = 0$ mamy, że $u - v\sqrt[3]{2} = 1$, tzn. $u = 1 \ \wedge \ v = 0 \Rightarrow x = 1 \ \wedge \ y = 0$, co przeczy temu, że y jest niezerowy. Zatem $n = 1$ i wówczas $u - v\sqrt[3]{2} = \sqrt[3]{2} - 1$, tzn. $u = v = -1 \Rightarrow x = -3 \wedge y = 2$. W rozumowaniu (podobnie jak wcześniej) zmieniamy znak c, aby

$x \equiv 1 \pmod 4$, zatem także $x = 3 \wedge y = 2$.
Ostatecznie $x = \pm 3 \wedge y = 2$. □

Bibliografia

[1] René Schoof, *Catalan's Conjecture*, Springer 2008

[2] Chein E. Z., *A note on the equation* $x^2 = y^q + 1$, Proc. Amer. Math. Soc., 56 (1976)

[3] Daems J., *A cyclotomic proof of Catalan's conjecture*, Universiteit Leiden 2003

Wokół grup proskończonych

Aleksandra Kaim
Uniwersytet im. Adama Mickiewicza w Poznaniu
Wydział Matematyki i Informatyki

Grupy proskończone są podstawą w konstrukcji wielu obiektów istotnych m.in w teorii grup, teorii liczb i teorii ciał. Jednym z przykładów jest konstrukcja tzw. proskończonego uzupełnienia $\widehat{G}$ dla dowolnej grupy G oraz uzyskanie z niego pewnych informacji o wyjściowej grupie.

Celem tego artykułu jest wprowadzenie pojęcia grupy proskończonej, przedstawienie jej podstawowych własności (m.in. jako grupy topologicznej) oraz wskazanie pewnych związków z grupami skończonymi. W dalszej części zostanie przedstawione jedno z ważniejszych zastosowań tego obiektu - wyznaczanie grup Galois dla nieskończonych rozszerzeń ciał.

8.1 Wprowadzenie

Grupę proskończoną można zdefiniować w sposób dwojaki - jako granicę odwrotną systemu grup skończonych lub odwołując się do jej własności topologicznych (jako grupy topologicznej). Oba aspekty wymagają przypomnienia podstawowych definicji.

Definicja 8.1. Grupą topologiczną nazywamy grupę G, która jest jednocześnie przestrzenią topologiczną, a ponadto działania:

$$\begin{array}{rcccl} G \times G & \ni & (g,h) & \mapsto & g \cdot h \in G \\ G & \ni & g & \mapsto & g^{-1} \in G \end{array}$$

są ciągłe.

Przy badaniu grup topologicznych wymagamy również, aby homomorfizmy między nimi były ciągłe. W szczególności izomorfizm grup topologicznych to homomorfizm grup, który jest homeomorfizmem.

Zauważmy, że dowolna grupa rozważana wraz z topologią dyskretną jest grupą topologiczną.

Dalsze rozważania wymagają również przypomnienia pewnych pojęć teoriomnogościowych:

Definicja 8.2. Częściowo uporządkowany zbiór $(I, \leqslant)$ jest **skierowany**, jeżeli dla dowolnych $i, j \in I$ istnieje $k \in I$ takie, że $i \leqslant k$ oraz $j \leqslant k$.

Przykład 8.3. *Zbiór $\mathbb{Z}$ wraz z relacją:*

$$m \leqslant n \quad \overset{def}{\Leftrightarrow} \quad m|n$$

jest skierowany. Istotnie, dla dowolnych m, n mamy: $m, n \leqslant NWW(m, n)$.

Aby zdefiniować formalnie pojęcie grupy proskończonej konieczne jest również wprowadzenie technicznego pojęcia systemu odwrotnego oraz granicy odwrotnej.

Definicja 8.4. Niech $(I, \leqslant)$ będzie skierowanym zbiorem częściowo uporządkowanym. **Systemem odwrotnym** grup topologicznych nazywamy parę $(\{G_i : i \in I\}, \{f_i^j : i \leqslant j,\, i, j \in I\})$, gdzie:

(i) G_i są grupami topologicznymi,

(ii) dla dowolnych $i \leqslant j$ mamy dane ciągłe homomorfizmy grup:

$$f_i^j : G_j \to G_i$$

spełniające dla dowolnych $i \leqslant j \leqslant k$:

$$f_i^i = \mathrm{id}_{G_i}, \qquad f_i^k = f_i^j \circ f_j^k.$$

Warto w tym miejscu zilustrować to pojęcie na prostym przykładzie.
Jeśli:

(i) $I = \mathbb{N}$ wraz z relacją podzielności,

(ii) $G_n = \mathbb{Z}/n\mathbb{Z}$ z topologią dyskretną,

(iii) $f_n^m : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ - kanoniczne rzutowanie dla $m|n$,

to $(\{\mathbb{Z}/n\mathbb{Z}\}_{n\in\mathbb{N}}, \{f_n^m\}_{m\leqslant n})$ jest systemem odwrotnym skończonych grup topologicznych.

Definicja 8.5. Niech $(\{G_i\}_i, \{f_i^j\}_{i\leqslant j})$ będzie systemem odwrotnym grup topologicznych. **Granicą odwrotną** tego systemu nazywamy zbiór:

$$\varprojlim G_i := \left\{ (g_i) \in \prod_{i\in I} G_i : \quad f_i^j(g_j) = g_i \quad \forall_{i\leqslant j} \right\}$$

będący podgrupą w $\prod_{i\in I} G_i$.

Granica odwrotna $\varprojlim G_i$ dziedziczy strukturę grupy topologicznej jako podgrupa iloczynu kartezjańskiego $\prod_{i\in I} G_i$. Ponadto homomorfizmy $\varprojlim G_i \to G_j$ dla wszystkich $j \in I$ są homomorfizmami grup topologicznych, a granica odwrotna spełnia własność uniwersalną.

8.2 Grupa proskończona i jej własności

Posiadając przytoczone narzędzia możemy przejść do formalnego zdefiniowania grupy proskończonej.

Definicja 8.6. Grupą proskończoną nazywamy grupę topologiczną otrzymaną jako granicę odwrotną systemu grup skończonych rozważanych z topologią dyskretną.

Jak się okazuje, podgrupy grupy proskończonej G mają ciekawe własności związane z ich topologicznym charakterem:

- $H \subset G$ - domknięta $\Rightarrow$ H - proskończona,
- $N \subset G$ - domknięta podgrupa normalna $\Rightarrow$ G/N - proskończona z topologią ilorazową,
- $H \subset G$ - otwarta $\Leftrightarrow$ H jest domknięta i ma skończony indeks,
- H - normalna i domknięta $\Leftrightarrow$ jest przecięciem normalnych podgrup otwartych.

Wykorzystując podane zależności łatwo pokazać poniższe twierdzenie łączące techniczną konstrukcję z topologicznym charakterem grup proskończonych.

Twierdzenie 8.7. *Grupa topologiczna jest proskończona wtedy i tylko wtedy, gdy jest zwartą, całkowicie niespójną przestrzenią Hausdorffa.*

Zauważmy ponadto, że każda skończona grupa jest proskończona. Intensywnie badane są również pewne podklasy grup proskończonych. Na przykład - dla ustalonej liczby pierwszej p - pro-p grupy to granice odwrotne systemu p-grup skończonych. Ze względu na oczywisty związek grup skończonych z grupami proskończonymi pewne zagadnienia klasycznej teorii grup można w prosty sposób przenieść na grupy proskończone. Jednym z ciekawych przykładów są twierdzenia Sylowa sformułowane w języku pro-obiektów. Zainteresowanych czytelników odsyłam do książki Wilsona [1].

8.3 Teoria Galois

Głównym zadaniem teorii Galois jest przypisanie odpowiedniej grupy pewnemu rozszerzeniu ciał i odczytanie własności tego rozszerzenia z własności grupy. W tej pracy będziemy zajmować się tzw. rozszerzeniami Galois.

8.3.1 Klasyczna teoria Galois

Przypomnijmy niezbędne definicje:

Definicja 8.8. Stopniem rozszerzenia L/K nazywamy liczbę $[L : K] := \dim_K L$. Rozszerzenie L/K nazywamy **skończonym**, gdy $[L : K] < \infty$.

Algebraiczne rozszerzenie ciała $K \subset L$ jest:

- **normalne**, gdy wielomian minimalny każdego $\alpha \in L$ rozkłada się w $L[x]$ na czynniki liniowe,
- **rozdzielcze**, gdy dla dowolnego $\alpha \in L$ jego wielomian minimalny nad K ma różne pierwiastki w swoim ciele rozkładu.

Rozszerzenie L/K nazywamy **rozszerzeniem Galois** $\Leftrightarrow$ jest normalne i rozdzielcze. Klasycznie teoria Galois zajmuje się głównie skończonymi rozszerzeniami ciał.

Definicja 8.9. Niech L/K będzie rozszerzeniem Galois. **Grupą Galois** tego rozszerzenia nazywamy

$$G(L/K) := Aut_K(L) =$$

$$= \{\sigma : L \to L \quad | \quad \sigma\text{- automorfizm ciała } L \text{ oraz } \sigma|_K = \mathrm{id}_K\}.$$

Najważniejszym twierdzeniem łączącym podgrupy grupy Galois z podciałami badanego rozszerzenia jest Zasadnicze Twierdzenie Teorii Galois. Niech $H \subset Aut_K(L)$ oraz $L^H = \{x \in L \quad | \quad \forall_{\sigma \in H} \quad \sigma(x) = x\} \subset L$.

Twierdzenie 8.10 (Zasadnicze Twierdzenie Teorii Galois)**.** *Niech L/K będzie skończonym rozszerzeniem Galois oraz $G = G(L/K)$. Wtedy zachodzi wzajemnie jednoznaczna odpowiedniość:*

$$\begin{array}{ccc} \{E \text{ - ciało} \mid K \subset E \subset L\} & \leftrightarrow & \{H \leqslant G\} \\ E & \longrightarrow & G(L/E) \\ L^H & \longleftarrow & H \end{array}$$

8.3.2 Nieskończona teoria Galois

Powstaje pytanie, czy przytoczone wyniki można również zastosować dla nieskończonych rozszerzeń ciał. Okazuje się, że tak, a główną rolę grają tu grupy proskończone.

To podejście wymaga jednak zdefiniowania na grupie Galois $G = G(L/K)$ odpowiedniej topologii (zwanej topologią Krulla).

Rozważmy E/K - skończone rozszerzenie takie, że $L \supset E$. Wtedy definiujemy zbiór otwarty:

$$U_E(\sigma) = \{\tau \in G \quad | \quad \tau|_E = \sigma|_E\}.$$

Przebiegając po wszystkich takich E otrzymujemy bazę otoczeń σ.

Jeśli L/K jest rozszerzeniem skończonym, to topologia Krulla na $G(L/K)$ to topologia dyskretna.

Wówczas grupa Galois rozszerzenia L/K jest grupą proskończoną, przy czym:

- $G(L/K) = \lim\limits_{\leftarrow} G(E_i/K)$,
- $\forall_{i \in I} \quad E_i/K$ - skończone, Galois oraz $E_i \subset L$,
- $\forall_{E_i} \quad G(E_i/K)$ jest skończona,
- zbiór takich ciał E_i jest częściowo uporządkowany (przez relację zawierania) oraz skierowany,
- dla $E_1 \supset E_2$ rozważamy zawężenia $G(E_1/K) \to G(E_2/K)$,

W tej sytuacji możemy przenieść klasyczne Zasadnicze Twierdzenie Teorii Galois na przypadek rozszerzeń nieskończonych.

Twierdzenie 8.11. *Niech L/K będzie rozszerzeniem Galois oraz $G = G(L/K)$.*
Wtedy zachodzi wzajemnie jednoznaczna odpowiedniość:

$$\begin{array}{ccc} \{E \text{ - ciało } | K \subset E \subset L\} & \leftrightarrow & \{H \subset G \,|H \text{ jest podgrupą domkniętą }\} \\ E & \longmapsto & G(L/E) \\ L^H & \longleftarrow & H \end{array}$$

Dla grup proskończonych można również przytoczyć uogólnienie twierdzenia Cayley'a. Pozwala ono skonstuować rozszerzenie ciał, dla którego rozważana grupa jest grupą Galois.

Twierdzenie 8.12. *Każda grupa proskończona G jest izomorficzna (jako grupa topologiczna) z grupą Galois pewnego rozszerzenia ciał (skończonego lub nie).*

Dowód. (Szkic)
Niech:

- K – dowolne ciało,
- S – rozłączna suma zbiorów G/N, gdzie N – otwarta podgrupa normalna grupy G,
- $L = K(X_s|s \in S)$, gdzie X_s – elementy transcendentnie niezależne nad K.

Naturalne działanie grupy G na S indukuje homomorfizm θ z G do grupy automorfizmów ciała L. Jeśli $u \in L$, to
$u \in K(X_{s_1}, X_{s_2}, ..., X_{s_r})$ oraz jeśli $s_i = N_i g_i$ dla $i = 1, 2, \ldots, r$, to

$$Stab_G(u) \geqslant N_1 \cup N_2 \cup ... \cup N_r$$

jest zbiorem otwartym.
Niech L^G będzie ciałem stałym ze względu na działanie G.
Odwzorowanie $\theta : G \mapsto G(L/L^G)$ jest iniektywnym homomorfizmem. Jest również ciągłe i suriektywne.
Zatem θ jest izomorfizmem grup proskończonych. □

Bibliografia

[1] Wilson S.J., *Profinite Groups*, Clarendon Press, Oxford, 1998

[2] Ribes L., Zalesskii P., *Profinite Groups*, Springer, New York, 2000

[3] Lenstra H., *Profinite Groups*,
www.websites.math.leidenuniv.nl/algebra

[4] Osserman B., *Inverse Limits and Profinite Groups*,
www.math.ucdavis.edu/∼ osserman (notes)

[5] Milne J., *Fields and Galois Theory*, 2008,
www.jmilne.org/math/

Wykorzystanie teorii Galois w konstrukcjach geometrycznych

Andrzej Kokosza
Uniwersytet im. Adama Mickiewicza w Poznaniu
Wydział Matematyki i Informatyki

Konstrukcje geometryczne przy użyciu cyrkla i linijki były rozważane już przez matematyków w starożytnej Grecji. Celem artykułu jest pokazanie powiązania między konstrukcjami geometrycznymi a teorią Galois, która daje rozwiązanie trzech klasycznych problemów konstrukcji geometrycznych: podwojenie objętości sześcianu, trysekcji kąta i kwadratury koła.

9.1 Liczby konstruowalne

Zanim opiszemy konstrukcję geometryczne i udowodnimy twierdzenia z nimi związane, musimy zdefiniować czym jest konstrukcja geometryczna. Konstrukcję zaczynamy od znanych nam punktów. Na podstawie tych punktów konstruujemy linie i okręgi za pomocą cyrkla i linijki:

A1 Dla punktów $\alpha \neq \beta$ możemy narysować linię l, która przechodzi przez oba punkty.

A2 Dla punktów $\alpha \neq \beta$ i γ możemy narysować okrąg o środku w γ i promieniu równym odległości między α i β

Z przecięcia tych linii i okręgów otrzymujemy nowe punkty:

A3 Punkt przecięcia się różnych linii l_1 i l_2.

A4 Punkt przecięcia się linii l_1 i okręgu o_1.

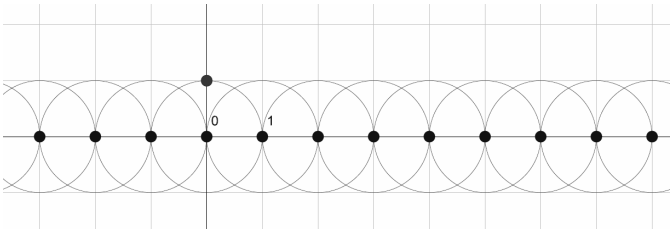
A5 Punkt przecięcia się różnych okręgów o_1 i o_2.

Nowo powstałe punkty możemy dołączyć do znanych punktów, a następnie zastosować na nich jedeną z konstrukcji A1, A2, A3, A4, A5. Proces ten powtarzamy skończoną liczbę razy.

Płaszczyznę będziemy utożsamiali ze zbiorem liczb zespolonych $\mathbb{C}$. Za zbiór punktów początkowych przyjmiemy $\{0, 1\}$. To prowadzi do następującej definicji:

Definicja 9.1. Liczbę zespoloną α nazywamy **konstruowalną**, jeżeli istnieje skończona sekwencja konstrukcji wykorzystujących A1, A2, A3, A4, A5, która zaczyna się od punktów 0 i 1, a kończy w α.

Przykład 9.2. ***Liczby całkowite są konstruowalne.*** *Istotnie, prowadźmy prostą przez punkty 0 i 1. Następnie narysujmy okrąg o promieniu długości 1 (odcinek miedzy 0 a 1) i środku 1. Punkt przecięcia prostej i okręgu daje nam 0 (które już mamy) i 2. Następnie taki sam okrąg o środku w 2 daje nam 3. Analogicznie możemy skonstruować każdą liczbę całkowitą.*



Twierdzenie 9.3. *Zbiór liczb konstruowalnych*

$$\mathcal{C} = \{\alpha \in \mathbb{C} \mid \alpha \text{ jest konstruowalne}\}$$

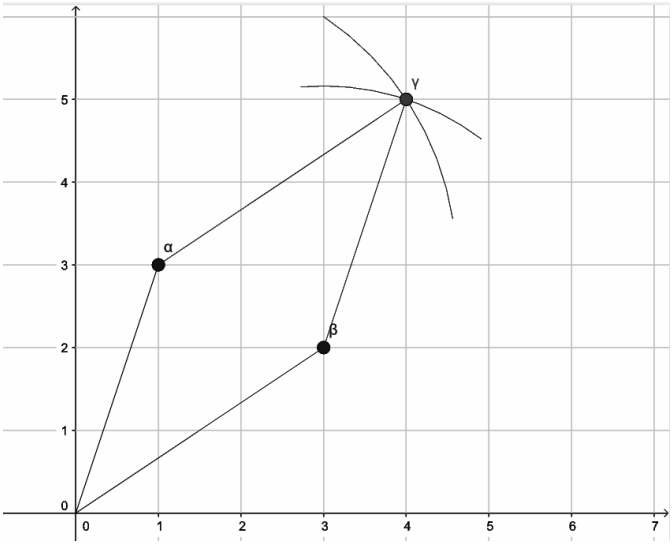
jest podciałem ciała $\mathbb{C}$. Ponadto:

1. *Niech $\alpha = a + ib$, gdzie $a, b \in \mathbb{R}$. Wówczas $\alpha \in \mathcal{C}$ wtedy i tylko wtedy, gdy $a, b \in \mathcal{C}$.*

2. Jeżeli $\alpha \in \mathcal{C}$, to $\sqrt{\alpha} \in \mathcal{C}$.

Dowód. Zakładamy, że znane nam są podstawowe konstrukcje, takie jak przenoszenie wektorów, odcinków, kątów, dodawanie kątów, bisekcja kąta czy prosta prostopadła, równoległa przechodząca przez dany punkt.

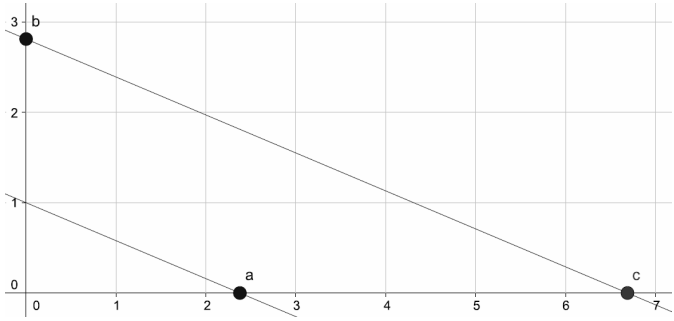
Niech $\alpha, \beta \in \mathcal{C}$. Skostruujemy $\alpha + \beta$. Jeżeli te punkty i 0 są współliniowe, wystarczy poprowadzić linię przez α i 0 oraz skonstuować okrąg o środku w α i długości $|\beta|$. Jeżeli nie są współliniowe, aby uzyskać punkt $\alpha + \beta$, skorzystamy z metody równoległoboku. Rysujemy okrąg o środku w punktcie α i długości $|\beta|$ oraz okrąg o środku w β i długości $|\alpha|$.



Konstrukcję elementu $-\alpha$ pozostawimy jako ćwiczenie.

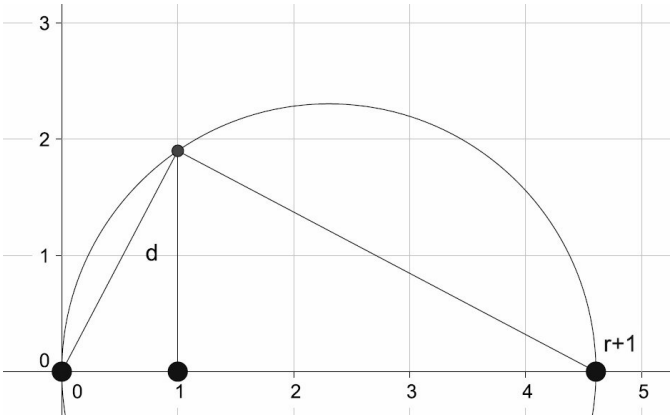
Żeby dowieść wewnętrzności mnożenia rozpatrzymy osobno moduł i argument. Niech $\alpha, \beta \in \mathcal{C}$. Zauważmy, że $Arg(\alpha\beta) = Arg(\alpha) + Arg(\beta)$ oraz $|\alpha\beta| = |\alpha||\beta|$. Zatem wystarczy wykonać sumę argumentów i iloczyn modułów, żeby otrzymać iloczyn. Sumę kątów umiemy wykonać, do wykonania iloczynu modułów

wykorzystamy twierdzenie Talesa. Oznaczmy na osi rzeczywistej taki punkt a, że $|0a| = |\alpha|$. Poprowadźmy prostą l_1 przechodzącą przez punkty a i i. Na osi urojonej oznaczmy taki punkt b, że $|0b| = |\beta|$. Prowadzimy prostą l_2 równoległą do prostej l_1 przechodzącą przez punkt b. Punkt przecięcia prostej l_2 i osi rzeczywistej oznaczamy przez c. Zachodzi wówczas równość $|0c| = |\alpha\beta|$.



Analogicznie postępujemy dla elementu odwrotnego – dzięki równości $Arg(\alpha^{-1}) = -Arg(\alpha)$ oraz $|\alpha^{-1}| = |\alpha|^{-1}$ wystarczy znaleźć odwrotność modułu. Podobnie z pierwiastkowaniem, rozdzielamy je na bisekcję kąta i pierwiastek z modułu. Konstrukcja bisekcji kąta jest znana ze szkoły.

Konstrukcję pierwiastka modułu obrazuje następujący rysunek:



Niech r oznacza moduł pierwiastkowanej liczby. Pokażemy, że odcinek d jest długości $\sqrt{r}$. Odcinek d dzieli trójkąt prostokątny na 2 trójkątny podobne. Stąd $\frac{1}{d} = \frac{d}{r}$, co jest równoważne z $r = d^2$. Zatem $d = \sqrt{r}$.

Pozostaje udowodnić punkt (1) twierdzenia. Niech $\alpha = a+bi$, by uzyskać a wystarczy poprowadzić prostą prostopadłą do osi rzeczywistej przechodzącą przez punkt α. Analogicznie dla b. W drugą stronę mamy dane $a, b \in \mathcal{C}$ rzeczywiste. Zaznaczmy element a oraz bi. Następnie poprowadzimy prostą prostopadłą do osi rzeczywistej przechodzącą przez a oraz prostą prostopadłą do osi urojonej przechodzącą przez bi. Punkt przecięcia tych prostych jest punktem $\alpha = a + bi$. □

Twierdzenie 9.4. *Niech α będzie liczbą zespoloną. To $\alpha \in \mathcal{C}$ wtedy i tylko wtedy, gdy taki istnieje ciąg podciał*

$$\mathbb{Q} = F_0 \subset F_1 \subset ...F_n \subset \mathcal{C}$$

że $\alpha \in F_n$ oraz $[F_i : F_{i-1}] = 2$ dla $i = 1, ..., n$

Przy założeniu, że $\alpha \in \mathcal{C}$ dowód sprowadza się do indukcji po liczbie operacji A3, A4, A5, jaka jest potrzebna do wykonania α.

W druga stronę wystarczy wykorzystać, że $F_{i+1} = F_i(\sqrt{\alpha_i})$, gdzie $\alpha_i \in F_i$ oraz fakt, że $\mathcal{C}$ jest zamknięte na operację pierwiastkowania.

Wniosek 9.5. *Ciało $\mathcal{C}$ jest najmniejszym podciałem ciała $\mathbb{C}$ zamkniętym na operację pierwiastkowania.*

Dowód. Niech F będzie dowolnym ciałem zamkniętym na operację pierwiastkowania. Niech α będzie dowolnym elementem ciała $\mathcal{C}$. Z twierdzenia 9.3 wynika, że istnieje ciąg ciał $\mathbb{Q} = F_0 \subset F_1 \subset ...F_n \subset \mathcal{C}$, $[F_i : F_{i-1}] = 2$ dla $1 = 1, ..., n$ i $\alpha \in F_n$. Wiemy, że $F_{i+1} = F_i(\sqrt{\alpha_i})$, gdzie $\alpha_i \in F_i$. Zauważmy, że $F_i \subset F$ dla $i = 1, ..., n$, gdyż F jest zamknięte na operację brania pierwiastka. Wiemy, że $\alpha \in F_n \subset F$. Zatem $\mathcal{C} \subset F$, więc $\mathcal{C}$ jest najmniejszym ciałem zamkniętym na pierwiastkowanie. □

Wniosek 9.6. *Jeżeli $\alpha \in \mathcal{C}$, to $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$ dla pewnego $m \geqslant 0$. Każda liczba konstruowalna jest zatem algebraiczna nad $\mathbb{Q}$, a stopień jej wielomianu minimalnego nad $\mathbb{Q}$ jest potęgą dwójki.*

Dowód. Niech $\alpha \in \mathcal{C}$. Z twierdzenia 9.4 wiemy, że istnieje ciąg ciał $\mathbb{Q} = F_0 \subset F_1 \subset ...F_n \subset \mathcal{C}$, $[F_i : F_{i-1}] = 2$ dla $1 = 1, ..., n$, $\alpha \in F_n$. Zatem

$$[F_n : \mathbb{Q}] = [F_n : F_{n-1}]...[F_1 : F_0] = 2^n.$$

Wiemy, że $\mathbb{Q}(\alpha) \subset F_n$, więc $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ dzieli $[F_n : \mathbb{Q}] = 2^n$. □

Wniosek 9.6 daje nam warunek konieczny na to, by dany element $\alpha \in \mathbb{C}$ był konstruowalny. Teraz skupimy się na trzech zagadnieniach, jakie rozważano w konstrukcjach geometrycznych od starożytnej Grecji.

Przykład 9.7. ***Trysekcja kąta.*** *Ze szkolnych lekcji wiemy, że możliwe jest skonstruowanie kąta $60°$ i $120°$. Jeżeli bylibyśmy w stanie wykonać trysekcję kąta, to moglibyśmy poprowadzić prostą przecinającą punkt 0 pod kątem $40°$ do osi OX. Po przecięciu z okręgiem o środku 0 i promieniem 1 otrzymamy punkt $\zeta_9 = e^{\frac{2\pi i}{9}}$, który byłby liczbą konstruowalną.*

Jednak wielomian minimalny ζ_9 jest równy x^6+x^3+1, zatem ζ_9 nie jest konstruowalne. Z tego wynika, że nie możemy dokonać trysekcji kąta $120°$, więc nie możemy podać metody trysekcji dowolnego kąta za pomocą cyrkla i linijki.

Przykład 9.8. ***Podwojenie objętości sześcianu.*** *Problem sprowadza się do rozwiązania równania $x^3 = 2n^3$, gdzie n jest długością boku wyjściowego sześcianu, a x – podwojonego. Dla $n = 1$ wynik wynosi $x = \sqrt[3]{2}$. Wielomian minimalny $\sqrt[3]{2}$ to x^3-2. Z wniosku 9.6 wynika, że $\sqrt[3]{2}$ nie jest konstruowalna, więc nie można podwoić objętości sześcianu za pomocą cyrkla i linijki.*

Przykład 9.9. ***Kwadratura koła.*** *Problem polega na skonstruowaniu kwadratu o polu danego koła. Weźmy koło o promieniu 1 – wtedy jego pole wynosi π. Zatem należy skonstruować kwadrat o boku $\sqrt{\pi}$. Jeżeli byłoby to możliwe, to π byłoby algebraiczne, ale w 1882 Lindemann udowodnił, że jest przestępne. Kwadratura koła jest zatem niemożliwa.*

Wniosek 9.6 pozwolił nam rozwiązać klasyczne problemy konstrukcji geometrycznych, ale można posunąć się dalej i spytać, czy ta implikacja zachodzi w drugą stronę. Innymi słowy, czy każda liczba $\alpha \in \mathbb{C}$, dla której stopień wielomianu minimalnego jest potęgą dwójki, musi być konstruowalna? Na to pytanie odpowiada następne twierdzenie.

Twierdzenie 9.10. *Niech $\alpha \in \mathcal{C}$ będzie elementem algebraicznym nad $\mathbb{Q}$. Niech L będzie ciałem rozkładu wielomianu minimalnego liczby α nad $\mathbb{Q}$. Element α jest konstruowalny wtedy i tylko wtedy, gdy $[L : \mathbb{Q}]$ jest potęgą dwójki.*

Dowód przy założeniu, że $[L : \mathbb{Q}] = 2^m$ polega na odpowiednim skorzystaniu z odpowiedniości Galois.Najpierw (korzystając z teorii grup) uzyskuje się wstępujący ciąg podgrup (G_i) dla grupy $Gal(L/\mathbb{Q})$, spełniający: $[G_{i+1} : G_i] = 2$ Ciągowi temu odpowiada ciąg podciał, co sprowadza się do twierdzenia 9.4.

W drugą stronę, niech $\alpha \in \mathbb{C}$. Najpierw należy udowodnić, że $\mathcal{C}$ jest rozszerzeniem normalnym. Następnie wystarczy zauważyć, że $[L : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ i wykorzystać wniosek 9.6.

9.2 Wielokąty foremne

W tym rozdziale wykorzystamy teorię z poprzedniego rozdziału, żeby pokazać jakie wielokąty foremne są konstruowalne. n-kąt foremny jest konstruowalny wtedy i tylko wtedy, gdy jesteśmy w stanie skonstruować kąt $\frac{2\pi}{n}$. Jak pokazaliśmy w przykładzie 9.7, jest to równoważne z konstrukcją n-tego pierwiastka z jedności $\zeta_n = e^{\frac{2\pi i}{n}}$. Zanim przejdziemy do twierdzenia przypomnijmy, że **liczbami pierwszymi Fermata** nazywamy liczby pierwsze postaci

$$p = 2^{2^m} + 1,$$

dla pewnego $m \geqslant 0$ całkowitego.

Twierdzenie 9.11. *Niech $n > 2$ będzie liczbą całkowitą. Wówczas n-kąt foremny jest konstuowalny wtedy i tylko wtedy, gdy*

$$n = 2^s \cdot p_1 \cdot \ldots \cdot p_m,$$

zaś $s \geqslant 0$ a $p_1, ..., p_m$ są różnymi liczbami pierwszymi Fermata.

Dowód. Zauważmy najpierw, że konstruowalność n-kąta foremnego jest równoważna konstruowalności liczby ζ_n. Wiemy, że rozszerzenie $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ jest Galois, więc ζ_n jest konstruowalne wtedy i tylko wtedy, gdy $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ jest potęgą dwójki. Jednocześnie $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$. Zatem ζ_n jest konstruowalne wtedy i tylko wtedy, gdy $\phi(n)$ jest potęgą dwójki. Załóżmy, że $n = 2^s p_1 ... p_m$ i $p_1, ..., p_m$ są różnymi liczbami pierwszymi Fermata.

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = \begin{cases} 2^{s-1}(p_1 - 1)(p_2 - 1)...(p_n - 1), & s > 0 \\ (p_1 - 1)(p_2 - 1)...(p_n - 1), & s = 0 \end{cases}$$

W obu przypadkach $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ jest potęgą dwójki.

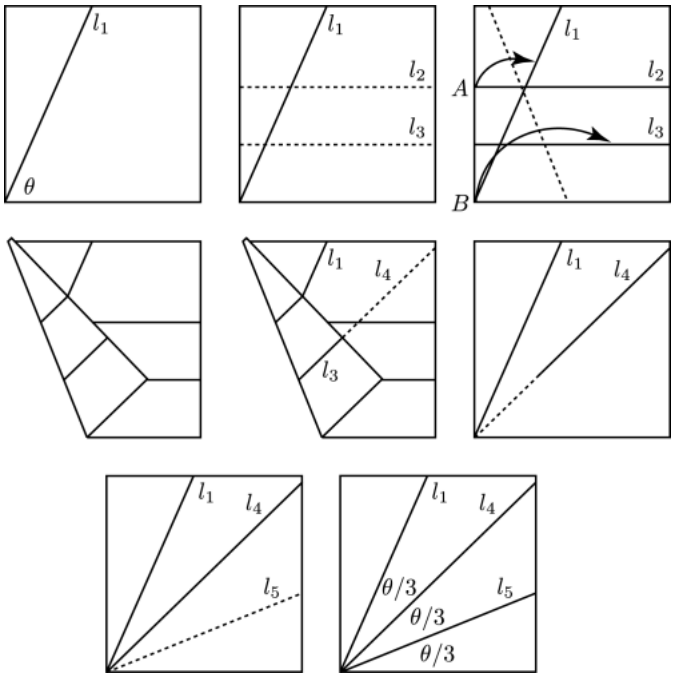
W drugą stronę, niech $n = 2^{s_0} q_1^{s_1}, ..., q_n^{s_n}$, gdzie $q_1, ..., q_n$ są nieparzystymi liczbami pierwszymi. Wówczas:

$$\phi(n) = n \prod_{q|n} \left(1 - \frac{1}{q}\right) = 2^{s_0 - 1} q_1^{s_1 - 1} \cdot (q_1 - 1) \cdot \ldots \cdot q_n^{s_n - 1} \cdot (q_n - 1).$$

Dlatego też musi zachodzić: $s_1 = \ldots = s_n = 1$, a ponadto wszystkie liczby $q_1, ..., q_n$ muszą być postaci $2^{k_i} + 1$. Wystarczy dowieść, że każda liczba pierwsza tej postaci jest liczbą Fermata. Pozostawiamy to czytelnikowi jako proste ćwiczenie z elementarnej teorii liczb. □

9.3 Liczby origami

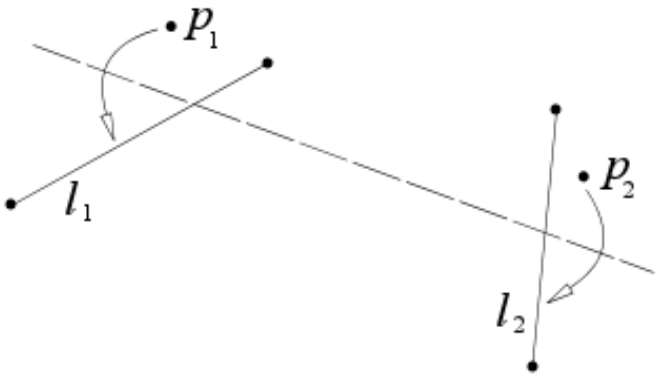
Rozpatrzmy konstrukcję za pomocą origami pokazaną na poniższym diagramie:



Prosta l_1 tworzy kąt θ z dolną krawędzią. Jest to dowolny kąt między $\frac{\pi}{2}$ a $\frac{\pi}{4}$. Zginamy kartkę tworząc prostą l_2, to jest dowolna prosta równoległa do dolnej krawędzi. Następnie przy-

kładamy dolną krawędź do l_2 tworząc l_3, która jest w połowie drogi między l_2 a dolną krawędzią. Potem przykładamy punkt przecięcia pionowej krawędzi i l_2 do l_1 oraz lewy dolny róg do l_3 i przedłużamy zgiętą część l_3. Otrzymaliśmy kąt $\frac{\theta}{3}$.

Udało się dokonać trysekcji kąta, która jest niewykonalna w klasycznych konstrukcjach. Wszystko dzięki przedostatniemu zgięciu, które przenosi 2 punkty na dwie różne proste. Pokażemy, że pozwala to rozwiązywać równania trzeciego stopnia.



Lemat 9.12. *Niech P_1 będzie punktem na płaszczyźnie nie leżącym na linii l_1. Linia l, o którą odbicie P_1 leży na prostej l_1, jest styczna z parabolą o ogniskowej w P_1 i kierownicy l_1.*

Z lematu wynika, że prosta, którą tworzymy zgięciem, jest styczną do dwóch paraboli o ogniskowych odpowiednio P_1, P_2 oraz kierownicach l_1 i l_2.

Przykład 9.13. *Pokażemy, jak za pomocą stycznej do dwóch paraboli policzyć pierwiastki wielomianu $x^3 + ax + c = 0$. W tym celu rozważmy parabole:*

$$\left(y - \frac{a}{2}\right)^2 = 2bx \text{ oraz } y = \frac{1}{2}x^2.$$

Niech l będzie prostą styczną do tych parabol w punktach (x_1, y_1) z pierwszą oraz (x_2, y_2) z drugą. Możemy wyliczyć współczynnik

nachylenia prostej korzystając z faktu, że jest ona styczna do pierwszej paraboli w punktcie (x_1, y_1)*:*

$$m = \frac{b}{y_1 - \frac{1}{2}a}$$

oraz $m \neq 0$ *i* $y_1 - \frac{1}{2}a = \frac{b}{m}$*. Z czego wynika, że:*

$$x_1 = \frac{(y_1 - \frac{1}{2}a)^2}{2b} = \frac{b}{2m^2}, \qquad y_1 = \frac{b}{m} + \frac{a}{2}.$$

Analogicznie dla drugiej paraboli dostajemy:

$$x_2 = m, \qquad y_2 = \frac{b}{m} + \frac{a}{2}.$$

Jeśli podstawimy pod $m = \frac{y_1 - y_2}{x_1 - x_2}$ *otrzymamy:*

$$m = \frac{y_1 - y_2}{x_1 - x_2} = \frac{\frac{m^2}{2} - (\frac{b}{m} + \frac{a}{2})}{m - \frac{2}{2m^2}} = \frac{m^4 - 2bm - am^2}{2m^3 - b}$$

Mamy $m \neq 0$*, zatem równanie sprowadza się do:*

$$m^3 + am + b = 0.$$

Analogicznie jak w przypadku konstrukcji klasycznych możemy opisać aksjomaty (znane jako aksjomaty Huzita-Hatori), określające zbiór liczb origami.

Twierdzenie 9.14. *Zbiór* $\mathcal{O} = \{\alpha\colon \alpha \text{ jest origami}\} \subset \mathbb{C}$ *jest podciałem ciała liczb zespolonych. Ponadto:*

1. *Niech* $\alpha = a + bi \in \mathbb{C}$*. Wówczas* $\alpha \in \mathcal{O}$ *wtedy i tylko wtedy, gdy* $a, b \in \mathcal{O}$*.*
2. *Jeżeli* $\alpha \in \mathcal{O}$*, to* $\sqrt{\alpha} \in \mathcal{O}$*.*
3. *Jeżeli* $\alpha \in \mathcal{O}$*, to* $\sqrt[3]{\alpha} \in \mathcal{O}$*.*

Dalsze rozumowanie przechodzi tak samo i sprowadza się do analogicznego twierdzenia:

Twierdzenie 9.15. *Niech* $\alpha \in \mathbb{C}$ *będzie elementem algebraicznym nad* $\mathbb{Q}$*. Niech* L *będzie ciałem rozkładu* α *nad* $\mathbb{Q}$*. Element* α *jest origami wtedy i tylko wtedy, gdy* $[L : \mathbb{Q}] = 2^n \cdot 3^m$*, dla* $m, n \geqslant 0$*.*

Bibliografia

[1] David A. Cox. *Galois Theory*. Wiley, 2012.

Zwarta grupa kwantowa $SU_q(2)$

Jacek Krajczok
Uniwersytet Warszawski
Wydział Fizyki

Teoria zwartych grup kwantowych jest częścią nieprzemiennej geometrii. Motywacją dla tego działu matematyki jest twierdzenie Gelfanda; mówi ono, że cała informacja o zwartej przestrzeni topologicznej Hausdorffa jest zawarta w przemiennej C^*-algebrze funkcji ciągłych na tej przestrzeni. Jeśli zdeformujemy tę algebrę tak, by nie była przemienna, otrzymujemy algebrę o której można myśleć jako o algebrze funkcji na „kwantowej przestrzeni". Podobnie, strukturę grupy możemy przenieść na poziom funkcji otrzymując po deformacji algebrę funkcji na „zwartej grupie kwantowej". W pracy wprowadzono formalną definicję zwartej grupy kwantowej. Następnie rozważono przykład zwartej grupy kwantowej $SU_q(2)$ będącej deformacją klasycznej grupy $SU(2)$. Udowodniono trywialność jej centrum, wierność jej funkcjonału Haara oraz przedstawiono nowy wzór na kojedynkę dowodzący jej ograniczoności.

10.1 Wprowadzenie

Zacznijmy od wprowadzenia kilku struktur algebraicznych.

Definicja 10.1. Algebra łączna nad $\mathbb{C}$ to przestrzeń wektorowa nad $\mathbb{C}$, A, wraz z dwuliniowym odwzorowaniem (zwanym mnożeniem) $\cdot\colon A \times A \to A$, $(a,b) \mapsto a \cdot b \equiv ab$ spełniającym warunek łączności: $\forall_{a,b,c\in A}\ a(bc) = (ab)c$.
Jeśli dodatkowo wyposażymy A w odwzorowanie $*\colon A \to A$, $a \mapsto a^*$, które jest:

- antyliniowe:

$$\forall_{\alpha,\beta\in\mathbb{C}} \quad \forall_{a,b\in A} \qquad (\alpha a + \beta b)^* = \overline{\alpha} a^* + \overline{\beta} b^*,$$

- antymultiplikatywne: $\forall_{a,b\in A} \qquad (ab)^* = b^* a^*$,

- inwolucją: $\forall_{a\in A} \qquad (a^*)^* = a$,

to otrzymaną strukturę nazywamy **$*$-algebrą**.

Przykład 10.2. *Niech X będzie zwartą przestrzenią topologiczną, która spełnia warunek Hausdorffa. Oznaczmy przez $C(X)$ zbiór funkcji ciągłych $X \to \mathbb{C}$ (na $\mathbb{C}$ wprowadzamy topologię indukowaną przez metrykę moduł). Zadajmy na $C(X)$ strukturę przestrzeni wektorowej nad $\mathbb{C}$ poprzez działania punktowe, tzn. $(f + \widetilde{f})(x) := f(x) + \widetilde{f}(x)$, $(\alpha f)(x) := \alpha f(x)$ dla $\alpha \in \mathbb{C}$, $f, \widetilde{f} \in C(X)$, $x \in X$. $C(X)$ stanie się algebrą łączną nad $\mathbb{C}$, jeśli zdefiniujemy mnożenie wzorem $(f\widetilde{f})(x) := f(x)\widetilde{f}(x)$, natomiast $*$-algebrą jeśli dodatkowo zdefiniujemy inwolucję $*$ poprzez $f^*(x) := \overline{f(x)}$ $\big(f, \widetilde{f} \in C(X),\ x \in X\big)$.*

Wprowadźmy jeszcze dwie definicje, które będą nam potrzebne w dalszej części:

Definicja 10.3. **$*$-algebra Banacha** to $*$-algebra A, która jest przestrzenią Banacha i prawdziwe w niej są następujące relacje: $\forall_{a,b\in A}\ \|ab\| \leqslant \|a\|\|b\|$, $\|a^*\| = \|a\|$. Jeśli dodatkowo zachodzi tzw. C^*-tożsamość: $\forall_{a\in A}\ \|a^*a\| = \|a\|^2$ to mówimy że A jest **C^*-algebrą**. W takiej sytuacji warunek izometryczności inwolucji $*$ jest zbędny.

Przykład 10.4.

- *Niech $\mathcal{H}$ będzie przestrzenią Hilberta, $B(\mathcal{H})$ zbiorem operatorów ograniczonych. Wraz ze standardową strukturą liniową, mnożeniem zadanym przez składanie operatorów, inwolucją $*$ - sprzężeniem hermitowskim i normą operatorową, $B(\mathcal{H})$ staje się C^*-algebrą. Ogólniej, dowolna normowo domknięta $*$-podalgebra $B(\mathcal{H})$ jest C^*-algebrą.*

- *Niech X będzie przestrzenią topologiczną taką, jak we wcześniejszym przykładzie. $C(X)$ staje się C^*-algebrą jeśli zadamy normę wzorem:*

$$\|\cdot\|\colon C(X) \to \mathbb{R}_{\geqslant 0}, \qquad f \mapsto \|f\| := \sup_{x\in X} |f(x)|.$$

Ta C^*-algebra posiada jedynkę, t.j. element neutralny względem mnożenia: jest to funkcja $\mathbb{1}\colon X \to \mathbb{C}\colon x \mapsto 1$. Skoro mnożenie skalarów w $\mathbb{C}$ jest przemienne to i mnożenie w $C(X)$ jest przemienne. Okazuje się, że wszystkie przemienne C^*-algebry z jedynką są tej postaci.

Twierdzenie 10.5 (**Gelfand**). *Niech A będzie przemienną C^*-algebrą z jedynką. Istnieje zwarta przestrzeń topologiczna Hausdorffa X, taka że A jest izometrycznie izomorficzna $C(X)$. Przestrzeń X jest wyznaczona jednoznacznie z dokładnością do homeomorfizmu.*

Przestrzeń X z twierdzenia Gelfanda posiada prostą charakteryzację: zdefiniujmy (jako zbiór) $X := \mathrm{Hom}(A, \mathbb{C}) \subset A^*$, czyli zbiór odwzorowań $\phi\colon A \to \mathbb{C}$, które są liniowe, ograniczone i $*$-multiplikatywne. Wprowadźmy na A^* topologię słabą*. Jest to topologia zadana przez rodzinę półnorm

$$p_a\colon A^* \to \mathbb{R}_{\geqslant 0}, \qquad \chi \mapsto |\chi(a)| \quad (a \in A).$$

W terminach zbieżności ciągów uogólnionych jest to topologia zbieżności punktowej: ciąg uogólniony $(\chi_\lambda)_{\lambda\in\Lambda}$ zbiega w tej topologii do $\chi \in A^*$ wtedy i tylko wtedy, gdy $(\chi_\lambda(a))_{\lambda\in\Lambda}$ zbiega do $\chi(a)$ w $\mathbb{C}$ dla każdego $a \in A$. Twierdzenie Banacha-Alaoglu mówi, że domknięta kula jednostkowa w A^* jest zwarta w topologii słabej*. Łatwo się przekonać, że X jest domkniętym jej podzbiorem, jest to więc podzbiór zwarty. Jeśli więc na X zadamy topologię podprzestrzeni, dostaniemy przestrzeń zwartą.
Spójrzmy na konkretny przykład: niech X będzie zwartą przestrzenią Hausdorffa, $A = C(X)$. Wtedy:

$$\mathrm{Hom}(C(X), \mathbb{C}) = \{\delta_x \mid x \in X\},$$

gdzie δ_x jest funkcjonałem ewaluacji w x. Widoczna jest więc bijekcja między X a $\mathrm{Hom}(C(X), \mathbb{C})$, nietrudno się przekonać, iż jest to w istocie homeomorfizm.

Twierdzenie Gelfanda mówi nam, że cała informacja o zwartej przestrzeni topologicznej jest zakodowana w algebrze funkcji ciągłych na niej. Algebra ta jest przemienną C^*-algebrą z jedynką. O ogólnej C^*-algebrze z jedynką możemy myśleć zatem jako o „algebrze funkcji ciągłych na zwartej nieprzemiennej/kwantowej przestrzeni". Chcielibyśmy do tego obrazka dołączyć strukturę grupową. Spójrzmy więc najpierw na przypadek klasyczny. Ustalmy G, zwartą grupę topologiczną Hausdorffa. Działanie grupowe to ciągłe odwzorowanie $\cdot\colon G \times G \to G$, możemy je przenieść na poziom funkcji poprzez tzw. komnożenie Δ. Jest to odwzorowanie zadane jako:

$$\begin{aligned} \Delta\colon C(G) &\to C(G) \otimes C(G) \backsimeq C(G \times G) \\ \Delta(f)(x,y) &= f(x \cdot y), \end{aligned}$$

gdzie $f \in C(G)$, $x, y \in G$, zaś przez $\otimes$ oznaczamy minimalny iloczyn tensorowy. Łączność działania grupowego wyraża się w tzw. kołączności: $(\Delta \otimes \mathrm{id})\Delta = (\mathrm{id} \otimes \Delta)\Delta$. Można się o tym łatwo przekonać, korzystając z tego, że funkcje postaci $\sum_{i=1}^{n} f_i \otimes f_i'$ tworzą podprzestrzeń gęstą w $C(G \times G)$.

Jak dotąd korzystaliśmy jedynie z własności półgrupy, musimy jeszcze wyrazić istnienie elementu neutralnego i odwrotności na poziomie $C(G)$. Okazuje się, że bezpośrednie zdefiniowanie kojedynki i koodwrotności nie jest dobrym pomysłem. Takie odwzorowania będą istnieć, jednak w ogólności będą zdefiniowane jedynie na gęstej $*$-podalgebrze. Skorzystamy z alternatywnej charakteryzacji zwartych grup wśród zwartych półgrup.

Twierdzenie 10.6. *[2] Niech G będzie zwartą półgrupą. G jest zwartą grupą wtedy i tylko wtedy, gdy zbiory $\Delta(C(G))(\mathbb{1} \otimes C(G))$ i $\Delta(C(G))(C(G) \otimes \mathbb{1})$ rozpinają podprzestrzenie gęste w $C(G) \otimes C(G)$.*

Dyskusja ta powinna uzasadnić następującą definicję zwartej grupy kwantowej:

Definicja 10.7. Zwarta grupa kwantowa to para (A, Δ), gdzie A to C^*-algebra z jedynką, natomiast Δ to $*$-homomorfizm (zwany komnożeniem) $\Delta\colon A \to A \otimes A$, taki że:

- $(\Delta \otimes \mathrm{id})\Delta = (\mathrm{id} \otimes \Delta)\Delta$,
- $\Delta(A)(\mathbb{1} \otimes A)$ i $\Delta(A)(A \otimes \mathbb{1})$ rozpinają podprzestrzenie gęste w $A \otimes A$.

10.2 Zwarta grupa kwantowa $SU_q(2)$

10.2.1

W tej części będziemy chcieli zdefiniować „kwantową deformację" grupy $SU(2)$. Rozważmy najpierw przypadek klasyczny. Jako zbiór $SU(2)$ składa się z macierzy kwadratowych 2×2 o wyrazach zespolonych, które są unitarne i mają wyznacznik 1:

$$\begin{aligned} SU(2) &= \{A \in \mathrm{Mat}(2, \mathbb{C}) \mid A^*A = \mathbb{1} \wedge \det A = 1\} \\ &= \left\{ \begin{bmatrix} \alpha & -\overline{\gamma} \\ \gamma & \overline{\alpha} \end{bmatrix} \;\middle|\; \alpha, \gamma \in \mathbb{C} :\ |\alpha|^2 + |\gamma|^2 = 1 \right\}. \end{aligned}$$

Wraz z topologią indukowaną z $\mathrm{Mat}(2, \mathbb{C}) \simeq \mathbb{R}^8$ i mnożeniem macierzowym jako działaniem grupowym, $SU(2)$ staje się zwartą grupą Hausdorffa. Mamy dwie naturalnie zdefiniowane funkcje „współrzędnościowe": $\boldsymbol{\alpha}, \boldsymbol{\gamma} \in C(SU(2))$. Funkcje te rozdzielają punkty, możemy więc skorzystać z twierdzenia Stone'a-Weierstrassa. Pozwala ono na stwierdzenie, że $*$-algebra generowana przez te dwie funkcje jest gęsta w $C(SU(2))$ (jest to $*$-podalgebra z jedynką, bo $\boldsymbol{\alpha}^*\boldsymbol{\alpha} + \boldsymbol{\gamma}\boldsymbol{\gamma}^* = \mathbb{1}$). W $C(SU(2))$ mamy określone zdefiniowane wcześniej komnożenie

$$\Delta\colon C(SU(2)) \to C(SU(2)) \otimes C(SU(2)),$$

działa ono na $\boldsymbol{\alpha}, \boldsymbol{\gamma}$ w następujący sposób:

$$\begin{aligned} \Delta(\boldsymbol{\alpha}) &= \boldsymbol{\alpha} \otimes \boldsymbol{\alpha} - \boldsymbol{\gamma}^* \otimes \boldsymbol{\gamma}, \\ \Delta(\boldsymbol{\gamma}) &= \boldsymbol{\gamma} \otimes \boldsymbol{\alpha} + \boldsymbol{\alpha}^* \otimes \boldsymbol{\gamma}. \end{aligned}$$

10.2.2

Aby uzyskać kwantową wersję grupy $SU(2)$, zdeformujmy gęstą $*$-podalgebrę funkcji rozpinaną przez $\boldsymbol{\alpha}, \boldsymbol{\gamma}$, wprowadzając parametr $q \in]0, 1]$.

Definicja 10.8. Oznaczmy przez $\mathscr{A}$ $*$-algebrę z jedynką generowaną przez dwa elementy α, γ, spełniające następujące relacje:

$$\begin{aligned} \alpha^*\alpha + \gamma\gamma^* &= \mathbb{1}, & \gamma^*\gamma &= \gamma\gamma^*, \\ \alpha\alpha^* + q^2\gamma\gamma^* &= \mathbb{1}, & \alpha\gamma &= q\gamma\alpha, \\ \alpha\gamma^* &= q\gamma^*\alpha. \end{aligned}$$

Algebra funkcji na kwantowej grupie $SU_q(2)$, $C(SU_q(2))$, to C^*-algebra zdefiniowana jako uzupełnienie $\mathscr{A}$ w maksymalnej C^*-normie:

$$\|a\| := \sup\{\|\pi(a)\| \mid \pi\colon \mathscr{A} \to B(\mathcal{H}) \text{ jest reprezentacją } \mathscr{A}\} \quad (a \in \mathscr{A}).$$

Komnożenie $\Delta\colon C(SU_q(2)) \to C(SU_q(2)) \otimes C(SU_q(2))$ zadane jest na generatorach poprzez:

$$\begin{aligned} \Delta(\alpha) &= \alpha \otimes \alpha - q\gamma^* \otimes \gamma, \\ \Delta(\gamma) &= \gamma \otimes \alpha + \alpha^* \otimes \gamma. \end{aligned}$$

Uzyskana w ten sposób para $(C(SU_q(2)), \Delta)$ jest nazywana **zwartą kwantową grupą** $SU_q(2)$. W przypadku $q = 1$ odzyskujemy grupę $SU(2)$. Szczegóły (oraz uzasadnienie poprawności) konstrukcji można znaleźć w [4].

10.2.3

Oznaczmy przez Λ zbiór $\Lambda := \mathbb{Z}_+ \times \mathbb{Z}$. W [4] wprowadzono reprezentację $C(SU_q(2))$, t.j. $*$-homomorfizm $\pi\colon C(SU_q(2)) \to$

$B(\ell^2(\Lambda))$. Spełnia on

$$\begin{aligned}\pi(\alpha)\phi_{n,k} =& \begin{cases}\sqrt{1-q^{2n}}\phi_{n-1,k} & n \geqslant 1\\ 0 & n=0\end{cases},\\ \pi(\alpha^*)\phi_{n,k} =& \sqrt{1-q^{2(n+1)}}\phi_{n+1,k},\\ \pi(\gamma)\phi_{n,k} =& q^n\phi_{n,k+1},\\ \pi(\gamma^*)\phi_{n,k} =& q^n\phi_{n,k-1},\end{aligned} \tag{10.1}$$

gdzie $\{\phi_{n,k}\}_{(n,k)\in\Lambda}$ jest standardową bazą ortonormalną $\ell^2(\Lambda)$. Wprowadźmy oznaczenie $\widetilde{A} := \overline{\pi(\mathscr{A})}^{\|\cdot\|}$ - jest to C^*-algebra z jedynką. Na $\widetilde{A}$ można wprowadzić strukturę zwartej grupy kwantowej.

Twierdzenie 10.9. *Istnieje $*$-homomorfizm $\widetilde{\Delta}\colon \widetilde{A} \to \widetilde{A}\otimes\widetilde{A}$ spełniający*

$$\begin{aligned}\widetilde{\Delta}(\pi(\alpha)) &= \pi(\alpha)\otimes\pi(\alpha) - q\pi(\gamma)^*\otimes\pi(\gamma),\\ \widetilde{\Delta}(\pi(\gamma)) &= \pi(\gamma)\otimes\pi(\alpha) + \pi(\alpha)^*\otimes\pi(\gamma),\end{aligned}$$

taki że $\left(\widetilde{A},\widetilde{\Delta}\right)$ jest zwartą grupą kwantową. Dodatkowo, $\pi|_{\mathscr{A}}\colon \mathscr{A}\to\pi(\mathscr{A})$ jest izomorfizmem $*$-algebr z jedynką zachowującym komnożenie.

Okazuje się, że zwarte grupy kwantowe $(C(SU_q(2)),\Delta)$ i $(\widetilde{A},\widetilde{\Delta})$ są izomorficzne - wrócimy jeszcze do tego problemu.

Twierdzenie 10.10. *Centrum $\widetilde{A} = \overline{\pi(\mathscr{A})}^{\|\cdot\|}$ jest trywialne, tzn.*

$$\mathcal{Z}(\widetilde{A}) := \left\{T\in\widetilde{A} \mid TS = ST \quad \forall_{S\in\widetilde{A}}\right\} = \{z\mathbb{1} \mid z\in\mathbb{C}\}.$$

Dowód. Ustalmy dowolny element $T\in\mathcal{Z}(\widetilde{A})$ i oznaczmy jego elementy elementy macierzowe przez $T^{n,k}_{n',k'}$:

$$T\phi_{n,k} = \sum_{(n',k')\in\Lambda} T^{n,k}_{n',k'}\phi_{n',k'}. \tag{10.2}$$

Możemy skorzystać z tego, że T komutuje z $\pi(\gamma)$:

$$\begin{aligned} T\pi(\gamma)\phi_{n,k} = Tq^n\phi_{n,k+1} &= \sum_{(n',k')\in\Lambda} T^{n,k+1}_{n',k'} q^n \phi_{n',k'} = \\ &= \sum_{(n',k')\in\Lambda} T^{n,k+1}_{n',k'+1} q^n \phi_{n',k'+1} = \pi(\gamma) T\phi_{n,k} = \\ &= \pi(\gamma) \sum_{(n',k')\in\Lambda} T^{n,k}_{n',k'} \phi_{n'k'} = \sum_{(n',k')\in\Lambda} T^{n,k}_{n',k'} q^{n'} \phi_{n',k'+1}, \end{aligned}$$

gdzie korzystamy z wzorów (10.1) i (10.2). Dostajemy w ten sposób następujące ograniczenie na elementy macierzowe:

$$\forall_{(n,k),(n',k')\in\Lambda}\ T^{n,k+1}_{n',k'+1} q^n = T^{n,k}_{n',k'} q^{n'}. \tag{10.3}$$

Możemy również skorzystać z tego, że T komutuje z $\pi(\gamma)^*$, otrzymamy wtedy:

$$\forall_{(n,k),(n',k')\in\Lambda}\ T^{n,k-1}_{n',k'-1} q^n = T^{n,k}_{n',k'} q^{n'}. \tag{10.4}$$

Ustalmy $(n,k),(n',k')\in\Lambda$ i połączmy równania (10.3) i (10.4):

$$T^{n,k}_{n',k'} \overset{(10.3)}{=} q^{n-n'} T^{n,k+1}_{n',k'+1} \overset{(10.4)}{=} q^{2(n-n')} T^{n,k}_{n',k'}.$$

To implikuje następujące stwierdzenie:

$$\forall_{(n,k),(n',k')\in\Lambda:\ n\neq n'} \quad T^{n,k}_{n',k'} = 0. \tag{10.5}$$

Wiemy również, że T komutuje z $\pi(\alpha)^*$, możemy z tego skorzystać by otrzymać kolejny warunek na elementy macierzowe:

$$\forall_{n\in\mathbb{N}}\forall_{k,k'\in\mathbb{Z}} \qquad T^{n,k}_{n,k'} = T^{n-1,k}_{n-1,k'}. \tag{10.6}$$

Po połączeniu równań (10.4) i (10.6) otrzymamy:

$$\forall_{n\in\mathbb{Z}_+}\forall_{k,k'\in\mathbb{Z}} \qquad T^{n,k}_{n,k'} = T^{0,k-k'}_{0,0}. \tag{10.7}$$

Żeby uzyskać pożądany wynik musimy jeszcze skorzystać z tego, że T jest operatorem należącym do $\widetilde{A} = \overline{\pi(\mathscr{A})}^{\|\cdot\|}$. Przestrzeń

$\pi(\mathscr{A})$ posiada bazę (patrz [4]), składa się ona z operatorów postaci $\pi\left(a^{k,m,n}\right)$, gdzie:

$$\pi(a^{k,m,n}) := \begin{cases} \pi\left(\alpha^k \gamma^m \gamma^{*n}\right) & k \geqslant 0 \\ \pi\left(\alpha^{*|k|} \gamma^m \gamma^{*n}\right) & k < 0 \end{cases} \quad ((k,m,n) \in \mathbb{Z} \times \mathbb{Z}_+ \times \mathbb{Z}_+) \,.$$

Zapiszmy T jako granicę (normową) operatorów z $\pi(\mathscr{A})$,

$$T = \lim_{\lambda \to \infty} \sum_{(k,m,n) \in \mathbb{Z} \times \mathbb{Z}_+ \times \mathbb{Z}_+} C^{\lambda}_{k,m,n} \pi\left(a^{k,m,n}\right),$$

i wybierzmy dowolnie $\varepsilon > 0$. Możemy znaleźć takie $\lambda \in \mathbb{N}$ by:

$$\left\| T - \sum_{(k,m,n) \in \mathbb{Z} \times \mathbb{Z}_+ \times \mathbb{Z}_+} C^{\lambda}_{k,m,n} \pi\left(a^{k,m,n}\right) \right\| \leqslant \frac{\varepsilon}{2}.$$

Ustalmy dowolnie $l \in \mathbb{Z}_+$. Korzystając z definicji normy operatorowej oraz równań (10.1), (10.5), (10.7) możemy napisać:

$$\begin{aligned} \left(\frac{\varepsilon}{2}\right)^2 &\geqslant \left\| \left(\sum_{(k,m,n) \in \mathbb{Z} \times \mathbb{Z}_+ \times \mathbb{Z}_+} C^{\lambda}_{k,m,n} \pi(a^{k,m,n}) - T \right) \phi_{l,0} \right\|^2 = \\ &= \Bigg\| \sum_{\substack{k \in \{1,\ldots,l\} \\ s \in \mathbb{Z}}} \left(\sum_{\substack{m,n \in \mathbb{Z}_+ \\ m-n=s}} C^{\lambda}_{k,m,n} q^{l(m+n)} \prod_{i=0}^{k-1} \sqrt{1 - q^{2(l-i)}} \right) \phi_{l-k,s} + \\ &+ \sum_{\substack{k \in -\mathbb{N} \\ s \in \mathbb{Z}}} \left(\sum_{\substack{m,n \in \mathbb{Z}_+ \\ m-n=s}} C^{\lambda}_{k,m,n} q^{l(m+n)} \prod_{i=0}^{|k|-1} \sqrt{1 - q^{2(l+1+i)}} \right) \phi_{l+|k|,s} + \\ &+ \sum_{s \in \mathbb{Z}} \left(\sum_{\substack{m,n \in \mathbb{Z}_+ \\ m-n=s}} C^{\lambda}_{0,m,n} q^{l(m+n)} - T^{0,-s}_{0,0} \right) \phi_{l,s} \Bigg\|^2 \geqslant \\ &\geqslant \sum_{s \in \mathbb{Z}} \left| \sum_{\substack{m,n \in \mathbb{Z}_+ \\ m-n=s}} C^{\lambda}_{0,m,n} q^{l(m+n)} - T^{0,-s}_{0,0} \right|^2 . \end{aligned}$$

Dostajemy następujące zdania:

$$\forall_{\varepsilon>0}\ \exists_{\lambda\in\mathbb{N}}\ \forall_{l\in\mathbb{Z}_+}\ \forall_{s\in\mathbb{Z}}\quad \left|\sum_{\substack{m,n\in\mathbb{Z}_+\\ m-n=s}} C^{\lambda}_{0,m,n}q^{l(m+n)} - T^{0,-s}_{0,0}\right| \leqslant \frac{\varepsilon}{2},$$

$$\forall_{\varepsilon>0}\ \forall_{s\in\mathbb{Z}}\ \exists_{\lambda\in\mathbb{N}}\ \forall_{l\in\mathbb{Z}_+}\quad \left|\sum_{\substack{m,n\in\mathbb{Z}_+\\ m-n=s}} C^{\lambda}_{0,m,n}q^{l(m+n)} - T^{0,-s}_{0,0}\right| \leqslant \frac{\varepsilon}{2}. \tag{10.8}$$

Wybierzmy dowolnie $\varepsilon > 0$, $s \in \mathbb{Z}\backslash\{0\}$ i odpowiadające im $\lambda \in \mathbb{N}$ z (10.8). Skoro:

$$\lim_{l\to\infty}\left|\sum_{\substack{m,n\in\mathbb{Z}_+\\ m-n=s}} C^{\lambda}_{0,m,n}q^{l(m+n)}\right| = 0,$$

to możemy znaleźć $l \in \mathbb{Z}_+$ takie by:

$$\left|\sum_{\substack{m,n\in\mathbb{Z}_+\\ m-n=s}} C^{\lambda}_{0,m,n}q^{l(m+n)}\right| \leqslant \frac{\varepsilon}{2}. \tag{10.9}$$

Korzystamy tu z tego że tylko skończona ilość współczynników $C^{\lambda}_{0,m,n}$ jest różna od zera, możemy więc wejść z granicą pod sumę. Po połączeniu (10.8) i (10.9) otrzymujemy:

$$\begin{aligned}\left|T^{0,-s}_{0,0}\right| &\leqslant \left|T^{0,-s}_{0,0} - \sum_{\substack{m,n\in\mathbb{Z}_+\\ m-n=s}} C^{\lambda}_{0,m,n} q^{l(m+n)}\right| \\ &+ \left|\sum_{\substack{m,n\in\mathbb{Z}_+\\ m-n=s}} C^{\lambda}_{0,m,n} q^{l(m+n)}\right| \leqslant \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,\end{aligned}$$

co pokazuje że $T^{0,-s}_{0,0} = 0$ dla $s \in \mathbb{Z}\setminus\{0\}$. Ostatecznie otrzymujemy pożądany rezultat, $T = T^{0,0}_{0,0}\mathbb{1}$. Druga inkluzja jest trywialna, co kończy dowód. □

10.3 Funkcjonał Haara i kojedynka

Aby uzasadnić izomorficzność zwartych grup kwantowych $(C(SU_q(2)), \Delta)$ oraz $(\widetilde{A}, \widetilde{\Delta})$ wprowadzimy dwa pojęcia - funkcjonału Haara oraz kojedynki.

Definicja 10.11. Niech (A, Δ) będzie zwartą grupą kwantową. **Funkcjonał Haara dla** (A, Δ) to stan (dodatni funkcjonał o normie 1) $h \in A^*$ spełniający

$$(h \otimes \mathrm{id})\Delta = (\mathrm{id} \otimes h)\Delta = h(\cdot)\mathbb{1}. \tag{10.10}$$

Twierdzenie 10.12. *Niech (A, Δ) będzie zwartą grupą kwantową. Istnieje dokładnie jeden funkcjonał Haara dla (A, Δ).*

Nazwę funkcjonału Haara tłumaczy następujący przykład:

Przykład 10.13. *Niech $(C(G), \Delta)$ będzie zwartą grupą kwantową odpowiadającą zwartej grupie Hausdorffa G. Funkcjonał Haara jest dany przez $h(f) := \int_G f\,d\mu \quad (f \in C(G))$, gdzie μ jest znormalizowaną miarą Haara dla G. Równanie* (10.10) *wyraża lewą i prawą niezmienniczość miary Haara.*

Przykład 10.14. *Funkcjonał Haara h dla $(C(SU_q(2)), \Delta)$ dany jest przez:*

$$h(a) = (1-q^2)\sum_{n=0}^{\infty} q^{2n}\,(\phi_{n,0}|\pi(a)\phi_{n,0}) \quad (a \in C(SU_q(2)))$$

(patrz [4]). Łatwo więc sprawdzić że funkcjonał Haara dla $(\widetilde{A}, \widetilde{\Delta})$ dany jest przez

$$\widetilde{h}(T) = (1-q^2)\sum_{n=0}^{\infty} q^{2n}\,(\phi_{n,0}|T\phi_{n,0}) \quad (T \in \widetilde{A}).$$

Lemat 10.15. *Funkcjonał Haara $\widetilde{h}$ dla $(\widetilde{A}, \widetilde{\Delta})$ jest wierny, tzn. $\widetilde{h}(T^*T) = 0$ dla $T \in \widetilde{A}$ implikuje $T = 0$.*

Dowód. Zdefiniujmy operator

$$\text{phase } \pi(\gamma)\colon \ell^2(\Lambda) \ni \phi_{n,k} \mapsto \phi_{n,k+1} \in \ell^2(\Lambda).$$

Jest to operator unitarny (jego nazwę uzasadnia fakt, że jest on jednym z operatorów występujących w rozkładzie biegunowym operatora $\pi(\gamma)$). Łatwo się przekonać, że operator ten komutuje ze wszystkimi operatorami z $\widetilde{A}$ - wynika to bezpośrednio z równań (10.1).
Weźmy $T \in \widetilde{A}$ takie, że $\widetilde{h}(T^*T) = 0$. Z definicji $\widetilde{h}$ wynika, że $T\phi_{n,0} = 0$ dla każdego $n \in \mathbb{Z}_+$. Ustalmy dowolnie $(n,k) \in \Lambda$. Wówczas:

$$\begin{aligned}\|T\phi_{n,k}\|^2 &= (\phi_{n,k}|T^*T\phi_{n,k}) = \\ &= \Big(\phi_{n,0}\Big|\,(\text{phase }\pi(\gamma))^{-k}\,T^*T(\text{phase }\pi(\gamma))^k\phi_{n,0}\Big) = \\ &= \big(\phi_{n,0}\big|T^*T\phi_{n,0}\big) = \|T\phi_{n,0}\|^2 = 0.\end{aligned}$$

Skoro $\{\phi_{n,k}\}_{(n,k)\in\Lambda}$ jest bazą $\ell^2(\Lambda)$, to powyższy rezultat dowodzi tego, że $T = 0$. □

Kolejnym pojęciem, które wprowadzimy, jest pojęcie kojedynki.

Definicja 10.16. Kojedynka dla $(\widetilde{A}, \widetilde{\Delta})$ to $*$-homomorfizm $\widetilde{\varepsilon}\colon \pi(\mathscr{A}) \to \mathbb{C}$ spełniający

$$(\widetilde{\varepsilon} \otimes \mathrm{id})\Delta(T) = (\mathrm{id} \otimes \widetilde{\varepsilon})\Delta(T) = T \quad (T \in \pi(\mathscr{A})). \tag{10.11}$$

Zadany jest on przez

$$\widetilde{\varepsilon}(\pi(\alpha)) = 1, \quad \widetilde{\varepsilon}(\pi(\gamma)) = 0.$$

Kojedynkę można zdefiniować dla ogólnej zwartej grupy kwantowej - jest to $*$-homomorfizm z pewnej gęstej $*$-podalgebry w $\mathbb{C}$ spełniający równanie (10.11). Podalgebra ta jest rozpinana przez elementy macierzowe skończeniowymiarowych unitarnych koreprezentacji (patrz [2]). Dla $(\widetilde{A}, \widetilde{\Delta})$ tą $*$-podalgebrą jest właśnie $\pi(\mathscr{A})$.

Twierdzenie 10.17. *Kojedynka dla* $(\widetilde{A}, \widetilde{\Delta})$*,* $\widetilde{\varepsilon}$*, jest odwzorowaniem ograniczonym, rozszerza się więc do* $*$*-homomorfizmu* $\widetilde{A} \to \mathbb{C}$*.*

Dowód. Ograniczoność $\widetilde{\varepsilon}$ pokażemy znajdując funkcjonał $\omega \in \left(\widetilde{A}\right)^*$, który pokrywa się z $\widetilde{\varepsilon}$ na $\pi(\mathscr{A})$. Rozważmy rodzinę funkcjonałów ograniczonych $\omega_L \in \left(\widetilde{A}\right)^*$ $(L \in \mathbb{N})$ zadanych wzorem:

$$\omega_L\colon \widetilde{A} \ni T \mapsto \frac{1}{L}\left(\sum_{l=0}^{L} \phi_{l,0}\middle| T \sum_{l=0}^{L} \phi_{l,0}\right) \in \mathbb{C}.$$

Rachunek

$$\begin{aligned} \|\omega_L\| &= \sup_{T \in \widetilde{A}:\|T\|=1} \frac{1}{L}\left|\left(\sum_{l=0}^{L} \phi_{l,0}\middle| T \sum_{l'=0}^{L} \phi_{l',0}\right)\right| \\ &\leqslant \frac{1}{L}\left\|\sum_{l=0}^{L} \phi_{l,0}\right\|^2 = \frac{L+1}{L} \leqslant 2 \end{aligned}$$

pokazuje, że $\{\omega_L\}_{L \in \mathbb{N}}$ jest podzbiorem kuli domkniętej o promieniu 2. Wnioskiem z twierdzenia Banacha-Alaoglu jest zwartość

takiej kuli w topologii słabej*. Wiemy więc, że istnieje pewien podciąg zbieżny, $(\omega_{L_p})_{p\in\mathbb{N}}$. Oznaczmy jego granicę przez ω:

$$\omega := \mathrm{w}^*\text{-}\lim_{p\to\infty} \omega_{L_p} \in \left(\widetilde{A}\right)^*.$$

Korzystamy tutaj również z tego że w świetle ośrodkowości $\widetilde{A}$ topologia słaba* jest metryzowalna na domkniętej kuli o promieniu 2 (patrz [3, tw. 3.16]). Bezpośredni rachunek pokazuje, że istotnie: $\omega(T) = \widetilde{\varepsilon}(T)$ dla $T \in \pi(\mathscr{A})$. □

Izomorficzność $(C(SU_q(2)), \Delta)$ i $(\widetilde{A}, \widetilde{\Delta})$ pokazują połączone twierdzenia (2.2) i (3.9) z pracy [1]. Przystosowane do naszej sytuacji brzmią następująco:

Twierdzenie 10.18. *Jeśli funkcjonał Haara $\widetilde{h}$ jest wierny, a kojedynka $\widetilde{\varepsilon}$ jest ograniczona, to $\pi(\mathscr{A})$ posiada tylko jedno (z dokładnością do izomorfizmu) uzupełnienie do zwartej grupy kwantowej. W szczególności zwarte grupy kwantowe $(C(SU_q(2)), \Delta)$ i $(\widetilde{A}, \widetilde{\Delta})$ są izomorficzne.*

Bibliografia

[1] E. Bédos, G.J. Murphy, L. Tuset, *Co-Amenability of Compact Quantum Groups*, Int. J. Math. Math. Sci. 31 (2002), 577-601.

[2] A. Maes, A. Van Daele, *Notes on Compact Quantum Groups* Nieuw Arch. Wisk. (4) 16 (1998), 73-112.

[3] W. Rudin, *Functional Analysis*, 2nd ed., McGraw Hill, 1991.

[4] S.L. Woronowicz, *Twisted SU(2) Group. An Example of a Non-commutative Differential Calculus*, Publications of the Research Institute for Mathematical Sciences, 23 (1987), 117-181.

Uzwarcenie Wallmana

Mateusz Krukowski
Politechnika Łódzka
Instytut Matematyki

Z dedykacją dla Magdaleny, za wszystko.

11.1 Wstęp

W poniższej pracy zaprezentujemy podejście Wallmana do uzwarcenia przestrzeni topologicznej (T, τ_T). Przez uzwarcenie przestrzeni T rozumiemy parę (X, e), gdzie X jest zwartą przestrzenią Hausdorffa, natomiast $e : T \to X$ jest homeomorfizmem o gęstym obrazie. Widać tym samym, że aby móc rozważać uzwarcenie przestrzeni T, musi być ona *przestrzenią Tichonowa* ([5], strona 211), tzn. spełniać aksjomat oddzielania T_1 oraz oddzielać punkty od zbiorów domkniętych za pomocą funkcji ciągłych.

W pracy dużo uwagi poświęcone jest przestrzeniom funkcji ciągłych oraz funkcji ciągłych i ograniczonych, oznaczanych odpowiednio przez $C(T)$ oraz $C^b(T)$. Zakładamy, że funkcje z tych przestrzeni przyjmują wartości zespolone. W pierwszej kolejności, staramy się przedstawić Czytelnikowi zbiory zerowe (i kozerowe), które będą stanowiły podstawowy budulec dalszych konstrukcji. Po krótkim zapoznaniu się z tymi obiektami, przechodzimy do badania ultrafiltrów Wallmana, z których będzie składało się docelowe uzwarcenie.

Punktem kulminacyjnym pracy jest wprowadzenie topologii Wallmana i wykazanie, że uzwarcenie Wallmana jest w istocie

uzwarceniem Čecha-Stone'a. W tym celu wykorzystujemy tzw. własność uniwersalną. W epilogu wspominamy o możliwości dalszego wykorzystania uzwarcenia Wallmana w kontekście twierdzenia Arzelà-Ascoli.

11.2 Zbiory zerowe

Zdefiniujmy rodzinę

$$\mathcal{Z}(T) := \left\{ f^{-1}(0) \ : \ f \in C(T) \right\},$$

której elementy będziemy nazywać *zbiorami zerowymi* ([2], strona 14). Zauważmy, że zamiast rodziny $C(T)$ moglibyśmy równoważnie użyć $C^b(T)$ (dlaczego?). Rodzinę dopełnień zbiorów zerowych oznaczamy przez $\mathcal{Z}^c(T)$, a jej elementy nazywamy *zbiorami kozerowymi*.

Zauważmy, że rodzina $\mathcal{Z}(T)$ jest zamknięta na skończone przecięcia: jeżeli $A = f_1^{-1}(0) \cap \ldots \cap f_n^{-1}(0)$ to kładąc

$$\forall_{t \in T} \ f(t) := |f_1(t)| + \ldots + |f_n(t)|$$

otrzymujemy $A = f^{-1}(0)$. Czytelnik z łatwością sprawdzi, że analogiczna uwaga dotyczy skończonych sum zbiorów zerowych.

Naturalnie, każdy zbiór zerowy jest zbiorem domkniętym. Interesującym pytaniem jest:

Kiedy dowolnym zbiór domknięty przestrzeni topologicznej jest zbiorem zerowym?

Aby odpowiedzieć na tak postawione pytanie, oznaczmy przez $\Pi_1^0(T)$ rodzinę wszystkich zbiorów domkniętych przestrzeni topologicznej T. Okazuje się, że wystarczająco wysoki aksjomat oddzielania (dokładnie T_6, por. [6] strona 16) jest warunkiem koniecznym i dostatecznym, co pokazuje następujące twierdzenie.

Twierdzenie 11.1. *Równość $\Pi_1^0(T) = \mathcal{Z}(T)$ zachodzi wtedy i tylko wtedy, gdy przestrzeń T jest doskonale normalna.*

Dowód. '$\Longleftarrow$'

Niech $A \in \Pi^0_1(T)$. Jeśli $A = T$, to oczywiście $A \in \mathcal{Z}(T)$. W przeciwnym wypadku, ustalmy $t_* \in T \backslash A$. Z doskonałej normalności istnieje funkcja $f \in C(T)$ taka, że $A = f^{-1}(0)$ oraz, co mniej nas interesuje, $\{t_*\} = f^{-1}(1)$. Tym samym $A \in \mathcal{Z}(T)$.
'$\Longrightarrow$'

Niech $A, B \in \Pi^0_1(T)$ będą zbiorami rozłącznymi. Z założenia wiemy, że $A = f_A^{-1}(0)$ oraz $B = f_B^{-1}(0)$ dla pewnych funkcji $f_A, f_B \in C(T)$. Zdefiniujmy $f \in C(T)$ wzorem

$$\forall_{t \in T}\ f(t) := \frac{|f_A(t)|}{|f_A(t)| + |f_B(t)|}. \tag{11.1}$$

Jest to funkcja ciągła, gdyż mianownik nie może się równać 0 (z rozłączności A i B). W oczywisty sposób $A = f^{-1}(0)$ oraz $B = f^{-1}(1)$, co kończy dowód. □

Widać zatem, że w dowolnej przestrzeni, która nie jest doskonale normalna, np. na *płaszczyźnie Sorgenfreya* ([6], strona 103), istnieją zbiory domknięte, które nie są zerowe. Powodem, dla którego zbiory zerowe są dla nas szczególnie ważne, jest kolejny lemat. Mówi on o tym, że $\mathcal{Z}(T)$ nadaje przestrzeni namiastkę normalności.

Lemat 11.2. *Dla dowolnych $A, B \in \mathcal{Z}(T)$ takich, że $A \cap B = \emptyset$ istnieją $U, V \in \mathcal{Z}^c(T)$ takie, że $A \subset U,\ B \subset V$ oraz $U \cap V = \emptyset$.*

Dowód. Niech $A = f_A^{-1}(0),\ B = f_B^{-1}(0)$ dla pewnych $f_A, f_B \in C(T)$. Definiujemy $f \in C^b(T)$ jak w (11.1). Zauważmy, że:

$$\left\{ t \in T\ :\ |f(t)| < \frac{1}{2} \right\} \supset f^{-1}(0)$$

oraz

$$\left\{ t \in T\ :\ |f(t)| > \frac{1}{2} \right\} \supset f^{-1}(1).$$

Ponadto mamy:

$$\begin{aligned}\left\{t \in T \ : \ |f(t)| < \frac{1}{2}\right\} &= T \backslash \left\{t \in T \ : \ |f(t)| \geqslant \frac{1}{2}\right\} \\ &= T \backslash f^{-1}\left(\mathbb{C} \backslash B\left(0, \frac{1}{2}\right)\right) \\ &= T \backslash (\varphi \circ f)^{-1}(0),\end{aligned}$$

gdzie $\varphi : \mathbb{C} \to \mathbb{C}$ jest dowolną funkcją ciągłą taką, że $\mathbb{C} \backslash B(0, \frac{1}{2}) = \varphi^{-1}(0)$. Rozumowanie to pokazuje, że zbiór

$$\left\{t \in T \ : \ |f(t)| < \frac{1}{2}\right\}$$

jest kozerowy. Analogiczna argumentacja działa dla

$$\left\{t \in T \ : \ |f(t)| > \frac{1}{2}\right\},$$

co kończy dowód. □

11.3 Konstrukcja Wallmana

Omówiliśmy już w skrócie zbiory zerowe (i kozerowe). Jak się okazuje, stanowią one podstawowy budulec *ultrafiltrów Wallmana*, które definiujemy poniżej.

Definicja 11.3. (ultrafiltr Wallmana / ω-ultrafiltr)
Rodzinę $\mathcal{U} \subset \mathcal{Z}(T)$ nazywamy ultrafiltrem Wallmana lub ω-ultrafiltrem, jeśli:

- **(ω1)** $\mathcal{U}$ testuje zwartość przestrzeni T, czyli dowolne skończone przecięcie elementów z $\mathcal{U}$ jest niepuste,
- **(ω2)** rodzina $\mathcal{U}$ jest maksymalna (nie można jej rozszerzyć przy zachowaniu własności ***(ω1)***).

Zbiór wszystkich ω-ultrafiltrów na T oznaczamy przez $\mathrm{Wall}(T)$.

O ultrafiltrach Wallmana można myśleć jako o maksymalnych rodzinach testujących zwartość przestrzeni (por. [5], strona 169). Maksymalność ta przejawia się w następującym fakcie, który pozostawiamy jako proste ćwiczenie.

Problem 11.4. *Niech $\mathcal{U} \in Wall(T)$. Dla $A, B \in \mathcal{Z}(T)$ spełniających $A \subset B$ oraz $A \in \mathcal{U}$ pokazać, że zachodzi $B \in \mathcal{U}$.*

Każdy punkt $t \in T$ wyznacza tzw. *ω-ultrafiltr główny*

$$\mathcal{P}_t := \Big\{ A \in \mathcal{Z}(T) \ : \ t \in A \Big\}.$$

Funkcję $\wp : T \to \mathrm{Wall}(T)$ daną wzorem

$$\forall_{t \in T} \ \wp(t) := \mathcal{P}_t$$

nazywamy *funkcją główną*.

Kolejnym naturalnym pytaniem, które samo narzuca się po definicji ultrafiltrów Wallmana, jest:

Czy każdą rodzinę, składającą się ze zbiorów zerowych i testującą zwartość można rozszerzyć do ultrafiltru Wallmana?

Intuicja podpowiada odpowiedź pozytywną, jednak formalizm matematyczny domaga się (mniej lub bardziej) rygorystycznego dowodu. Okazuje się, że możliwość takiego rozszerzenia jest konsekwencją aksjomatu wyboru. Bardziej precyzyjnie, w dowodzie wykorzystamy lemat Tukeya, który można odnaleźć w [3] na stronie 10.

Lemat 11.5. *Każda rodzina $\mathcal{T} \subset \mathcal{Z}(T)$ testująca zwartość przestrzeni jest zawarta w pewnym ultrafiltrze Wallmana.*

Dowód. Niech $\mathbb{T}$ oznacza rodzinę rodzin testujących zwartość, w której rozważamy częściowy porządek zadany przez zawieranie. Czytelnik łatwo sprawdzi, że $\mathbb{T}$ jest rodziną skończonego charakteru ([3], strona 9). W konsekwencji, z lematu Tukey'a, dla każdej rodziny testującej zwartość $\mathcal{T} \in \mathbb{T}$ istnieje element maksymalny $\mathcal{U} \in \mathbb{T}$ taki, że $\mathcal{U} \supset \mathcal{T}$, co należało pokazać. □

Kolejne twierdzenie charakteryzuje ultrafiltry Wallmana. Charakteryzacja ta przydaje się w wielu technicznych rachunkach.

Twierdzenie 11.6. *(charakteryzacja ultrafiltrów Wallmana) Rodzina $\mathcal{U} \subset \mathcal{Z}(T)\backslash\{\emptyset\}$ jest ω-ultrafiltrem wtedy i tylko wtedy, gdy:*

(Char1) $\forall_{A_1,\ldots,A_n \in \mathcal{U}} \bigcap_{i=1}^{n} A_i \in \mathcal{U}$,

(Char2) *dla dowolnego $A \in \mathcal{Z}(T)$ zachodzi implikacja:*

$$\left(\forall_{B\in\mathcal{U}}\ A \cap B \neq \emptyset\right) \implies A \in \mathcal{U}.$$

Dowód. '$\Longrightarrow$'

Jeśli dla pewnych $A_1, \ldots, A_n \in \mathcal{U}$ warunek **(Char1)** nie jest spełniony to kładziemy $A = \bigcap_{i=1}^{n} A_i \notin \mathcal{U}$. Z **($\omega$1)** wiemy, że $A \neq \emptyset$. Rozszerzmy $\mathcal{U}$ o element A. Pojawia się pytanie, czy ta rozszerzona rodzina testuje zwartość? Odpowiedź jest pozytywna, ponieważ przecięcie A ze skończoną liczbą zbiorów z $\mathcal{U}$ także jest takiej postaci jak w **(ω1)**. Tym samym rozszerzyliśmy ultrafiltr $\mathcal{U}$, co przeczy maksymalności (warunek **(ω2)**).

Przy wykazywaniu warunku **(ω2)**, analogicznie jak poprzednio zakładamy, że istnieje $A \in \mathcal{Z}(T)$ takie, że $A \notin \mathcal{U}$, a mimo to dla każdego $B \in \mathcal{U}$ zachodzi $A \cap B \neq \emptyset$. Otrzymujemy ponownie sprzeczność z maksymalnością (rozważając rozszerzenie o A).

'$\Longleftarrow$'

Warunek **(ω1)** jest oczywiście spełniony. Załóżmy zatem, że $\mathcal{U} \in \mathrm{Wall}(T)$ można rozszerzyć o $A \in \mathcal{Z}(T)$ przy zachowaniu **(ω1)**. Wtedy dla każdego $B \in \mathcal{U}$ mamy $A \cap B \neq \emptyset$, więc z **(Char2)** mamy $A \in \mathcal{U}$. Otrzymana sprzeczność kończy dowód. □

Wyżej przytoczona charakteryzacja przydaje się do sprawdzania, kiedy dwa ultrafiltry Wallmana są tożsame. Proste rozumowanie podsumowuje następujący wniosek:

Wniosek 11.7. *(równość ω-ultrafiltrów) Ultrafiltry $\mathcal{U}, \mathcal{V} \in \mathit{Wall}(T)$ są tożsame wtedy i tylko wtedy, gdy dla dowolnych $A \in \mathcal{U}$ oraz $B \in \mathcal{V}$ zachodzi $A \cap B \neq \emptyset$.*

Dowód. Jedynie implikacja '$\Longleftarrow$' wymaga komentarza. Załóżmy, że $\mathcal{U} \neq \mathcal{V}$, tzn. istnieje $A \in \mathcal{Z}(T)$ takie, że $A \in \mathcal{U}$ i $A \notin \mathcal{V}$. Z prawa kontrapozycji oraz **(Char2)** otrzymujemy implikację

$$A \notin \mathcal{V} \implies \exists_{B \in \mathcal{V}}\ A \cap B = \emptyset$$

co daje sprzeczność z założeniem. □

Następna definicja jest pierwszym krokiem w kierunku wprowadzenia topologii na rodzinie wszystkich ultrafiltrów Wallmana, czyli Wall(T). Jak się okaże, zbiory U^*, które teraz wprowadzimy, będą stanowiły bazę topologii.

Definicja 11.8. (odwzorowanie $*$)
Odwzorowanie $* : \mathcal{Z}^c(T) \to 2^{\mathrm{Wall}(T)}$ zdefiniowane jest wzorem:

$$\forall_{U \in \mathcal{Z}^c(T)}\ U^* := \Big\{ \mathcal{U} \in \mathrm{Wall}(T)\ :\ T \backslash U \notin \mathcal{U} \Big\}.$$

Autor postanowił zebrać podstawowe własności odwzorowania $*$ w postaci serii problemów. Ich rozwiązania, będące w istocie prostymi przeliczeniami, pozostawiamy w gestii zainteresowanego Czytelnika.

Problem 11.9. *Pokazać, że dla dowolnego $U \in \mathcal{Z}^c(T)$ zachodzi*

$$u \in U \iff \wp(u) \in U^*. \tag{11.2}$$

Kolejne zadanie pokazuje, że odwzorowanie $*$ jest rosnące względem zawierania.

Problem 11.10. *Dla zbiorów $U, V \in \mathcal{Z}^c(T)$ takich, że $U \subset V$ pokazać, że $U^* \subset V^*$.*

W następnym ćwiczeniu podajemy dwie dodatkowe charakteryzacje zbioru U^* - są to własności **($\mathbf{W}^*$1)** i **($\mathbf{W}^*$2)**. Ponadto, zastanawiamy się jak odwzorowanie $*$ współgra ze skończonymi sumami i przecięciami zbiorów (własności **($\mathbf{W}^*$3)** i **($\mathbf{W}^*$4)**).

Problem 11.11. *Niech $U, V \in \mathcal{Z}^c(T)$. Pokazać, że zachodzą własności*

(W*1) $U^* = \left\{\mathcal{U} \in \mathit{Wall}(T) \ : \ \exists_{A\in\mathcal{U}}\ A \subset U\right\}$

(W*2) $U^* = \left\{\mathcal{U} \in \mathit{Wall}(T) \ : \ \forall_{A\in\mathcal{U}}\ A \cap U \neq \emptyset\right\}$

(W*3) $(U \cup V)^* = U^* \cup V^*$

(W*4) $(U \cap V)^* = U^* \cap V^*$

Dzięki własności **(W*4)** widać, że rodzina $(U^*)_{U\in\mathcal{Z}^c(T)}$ może posłużyć za bazę topologii, którą nazywamy *topologią Wallmana* i oznaczamy przez τ^*. Jesteśmy w tym momencie w stanie naszkicować dowód faktu, że przestrzeń Wallmana (czyli $\mathrm{Wall}(T)$ z właśnie wprowadzoną topologią τ^*) jest w istocie uzwarceniem Čecha-Stone'a.

Twierdzenie 11.12. *Para* $(\mathit{Wall}(T), \wp)$ *jest uzwarceniem Čecha-Stone'a.*

Dowód. W pierwszej kolejności sprawdzamy, że $(\mathrm{Wall}(T), \tau^*)$ jest przestrzenią Hausdorffa. Z lematu 11.7 wiemy, że ω-ultrafiltry $\mathcal{U},\ \mathcal{V} \in \mathrm{Wall}(T)$ są różne wtedy i tylko wtedy, gdy istnieją $A \in \mathcal{U}$ oraz $B \in \mathcal{V}$ takie, że $A \cap B = \emptyset$. Z lematu 11.2 znajdujemy $U, V \in \mathcal{Z}^c(T)$ takie, że $U \supset A,\ V \supset B$ oraz $U \cap V = \emptyset$. Zatem z **(W*1)** otrzymujemy $\mathcal{U} \in U^*$ oraz $\mathcal{V} \in V^*$. Rozłączność U^* i V^* wynika z **(W*4)**.

Kolejną rzeczą, która wymaga sprawdzenia to fakt, że $(\mathrm{Wall}(T), \tau^*)$ jest przestrzenią zwartą. Niech $\mathcal{F} \subset C(T)$ będzie taką rodziną, że

$$\mathrm{Wall}(T) = \bigcup_{f\in\mathcal{F}} \left(T\backslash f^{-1}(0)\right)^* \tag{11.3}$$

Pomysłem jest rozważenie rodziny

$$\mathcal{R} := \left(f^{-1}(0)\right)_{f\in\mathcal{F}} \subset \mathcal{Z}(T)$$

Pokażemy, że rodzina $\mathcal{R}$ nie testuje zwartości. Jeśli byłoby inaczej, to z lematu 11.5 istniałby ω-ultrafiltr $\mathcal{U} \in \mathrm{Wall}(T)$ taki, że $\mathcal{U} \supset \mathcal{R}$. Z drugiej strony, (11.3) implikowałoby istnienie funkcji $f \in \mathcal{F}$ takiej, że $\mathcal{U} \in \left(T \backslash f^{-1}(0)\right)^*$. Otrzymalibyśmy, że $f^{-1}(0) \notin \mathcal{U}$ co jest sprzecznością z $\mathcal{U} \supset \mathcal{R}$.

Pokazaliśmy, że istnieje $n \in \mathbb{N}$ oraz funkcje $(f_i)_{i=1}^n \subset \mathcal{F}$ takie, że $\bigcap_{i=1}^n f_i^{-1}(0) = \emptyset$. Kładąc $U_i = T \backslash f_i^{-1}(0)$ dla $i \leqslant n$ otrzymujemy

$$\bigcup_{i=1}^n U_i = T \implies \left(\bigcup_{i=1}^n U_i\right)^* = T^* \overset{\mathbf{(W^*3)}}{\implies} \bigcup_{i=1}^n U_i^* = \mathrm{Wall}(T)$$

co dowodzi zwartości $(\mathrm{Wall}(T), \tau^*)$.

Aby wykazać, że $(\mathrm{Wall}(T), \wp)$ jest uzwarceniem należy dowieść, że funkcja główna $\wp : T \to \mathrm{Wall}(T)$ jest homeomorfizmem na swój obraz, który jest gęsty w $\mathrm{Wall}(T)$. Aby wykazać różnowartościowość $\wp$ przypuśmy, że $x \neq y$. Skoro zbiory $\{x\}$ oraz $\{y\}$ są domknięte, więc istnieje funkcja $f \in C(T)$ taka, że $f(x) = 0$ oraz $f(y) = 1$. Tym samym, $x \in f^{-1}(0)$ oraz $y \notin f^{-1}(0)$, czyli $f^{-1}(0) \in \wp(x)$ oraz $f^{-1}(0) \notin \wp(y)$. Otrzymaliśmy, że $\wp(x) \neq \wp(y)$ co oznacza różnowartościowość funkcji.

Aby sprawdzić ciągłość i otwartość funkcji $\wp$ ustalmy $U \in \mathcal{Z}^c(T)$. Wtedy U^* jest elementem bazowym w τ^* i wyznacza zbiór bazowy $U^* \cap \wp(T)$ w topologii indukowanej na $\wp(T)$. Przeliczenie

$$t \in \wp^{-1}(U^* \cap \wp(T)) \iff \wp(t) \in U^* \overset{(11.2)}{\iff} t \in U$$

dowodzi ciągłości $\wp$. Ponadto, przeliczenie

$$\begin{aligned} \wp(U) &= \left\{\wp(u) \in \mathrm{Wall}(T) \ : \ u \in U\right\} \\ &\overset{(11.2)}{=} \left\{\wp(u) \in \mathrm{Wall}(T) \ : \ \wp(u) \in U^*\right\} = U^* \cap \wp(T) \end{aligned}$$

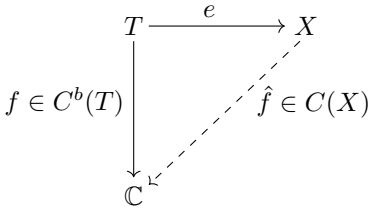
dowodzi otwartości $\wp$.

W celu pokazania, że $\wp(T)$ jest gęsty w $\mathrm{Wall}(T)$ musimy dla każdego $U^* \in \mathrm{Wall}(T)$ znaleźć $t \in T$ takie, że $\wp(t) \in U^*$. Nietrudno jest to zrobić, ponieważ $\wp(u) \in U^*$ dla każdego $u \in U$.

Ostatecznie należy sprawdzić, że $(\mathrm{Wall}(T), \wp)$ jest w istocie uzwarceniem Čecha-Stone'a. Jest to najtrudniejsza część dowodu, którą tutaj jedynie zarysujemy. Korzystamy z faktu, że uzwarcenie Čecha-Stone'a ma następującą charakteryzację:

Uzwarcenie (X, e) przestrzeni topologicznej T jest uzwarceniem Čecha-Stone'a wtedy i tylko wtedy, gdy dowolną funkcję $f \in C^b(T)$ można rozszerzyć do funkcji $\hat{f} \in C(\mathit{Wall}(T))$ w sensie $\hat{f} \circ e = f$, gdzie $e : T \to X$ jest homeomorfizmem o gęstym obrazie.

Graficznie sytuację tą przedstawia następujący diagram:



Opisaną powyżej własność nazywamy *własnością uniwersalną*. Aby wykazać, że $(\mathrm{Wall}(T), \wp)$ posiada własność uniwersalną ustalmy $\mathcal{U} \in \mathrm{Wall}(T)$ oraz $f \in C^b(T)$. W dużym uproszczeniu, ideą jest rozpatrzenie rodziny

$$\mathcal{U}_f := \left\{ A \subset \overline{\mathrm{Im}(f)} \ : \ f^{-1}(A) \in \mathcal{U} \right\},$$

której przecięcie okazuje się być niepuste. Co więcej, można pokazać, że jest ono jednopunktowe. Możemy zatem zdefiniować $\hat{f}(\mathcal{U})$ jako właśnie ten punkt znajdujący się w $\bigcap \mathcal{U}_f$. Pozostaje sprawdzić, że jest to funkcja ciągła, spełniająca $\hat{f} \circ \wp = f$. To kończy dowód. □

11.4 Epilog

Podczas konferencji $\theta\beta\ell\iota c\mathbb{Z}\varepsilon$ 2016 (Poznań, dnia 15.05.2016) miałem przyjemność przedstawić referat pt. 'Twierdzenie Arzelà-Ascoli i uzwarcenie Wallmana'. Starałem się w nim opowiedzieć, jak opisana wyżej machineria ultrafiltrów Wallmana pozwala scharakteryzować zbiory zwarte w przestrzeni $C^b(T)$. Zainteresowanego Czytelnika zachęcam do zapoznania się z artykułem [4], który obecnie znajduje się w recenzji do czasopisma Fundementa Mathematicae.

Bibliografia

[1] Frink O. : *Compactifications and semi-normal spaces*, The American Journal of Mathematics 86, p. 602-607 (1964),

[2] Gillman L., Jerison M. : *Rings of Continuous Functions*, D.Van Nostrand Company (1960)

[3] Jech T. : *The axiom of choice*, North-Hollan Publishing Company, 1973

[4] Krukowski M. : *Arzelà-Ascoli theorem via Wallman compactification*, arXiv: 1602.05691, praca wysłana do Fundamenta Mathematicae (2016)

[5] Munkres J. : *Topology*, Prentice Hall, Inc., 2000

[6] Seebach J.A., Steen L.A. : *Counterexamples in topology*, Dover Publications, New York, 1978

[7] Simmons G.F. : *Introduction to topology and modern analysis*, Robert E. Krieger Publishing Company, 1963

[8] Steiner E.F. : *Wallman spaces and compactifications*, Fundamenta Mathematicae 61, p. 295-304 (1967/68)

[9] Walker R.C. : *The Stone-Čech Compactification*, Springer-Verlag, 1974

[10] Wallman H. : *Lattices and topological space*, Annals of Mathematics, 39, 112-126 (1938)

[11] Willard S. : *General Topology*, Addison-Wesley Publishing Company, 1970

Trudne proste problemy matematyczne

Małgorzata Lebiedź
Uniwersytet Gdański

12.1 Wstęp

Istnieje wiele problemów matematycznych, których sformułowanie jest proste, a które od lat, czasem nawet wieków, opierają się próbom dowodu. Celem tego artykułu jest przedstawienie dwóch takich problemów: problemu Collatza i problemu wyznaczania liczb Ramseya.

12.2 Problem Collatza

12.2.1 Definicja problemu

Problem Collatza (problem $3x+1$) został po raz pierwszy zdefiniowany przez niemieckiego matematyka Lothara Collatza w latach trzydziestych XX wieku.

Definicja 12.1. Weźmy dowolną liczbę naturalną dodatnią c_0. Tworzymy ciąg (c_n) zadany wzorem rekurencyjnym

$$c_{n+1} = \begin{cases} \frac{1}{2}c_n & \text{gdy } c_n \text{ jest parzyste} \\ 3c_n + 1 & \text{gdy } c_n \text{ jest nieparzyste} \end{cases}$$

Hipoteza: istnieje $n \in \mathbb{N}$ takie, że $c_n = 1$.

Zauważmy, że:

- Wystarczy rozpatrywać tylko c_0 nieparzyste, ponieważ przy c_0 parzystym dzielimy przez 2 tyle razy, aż otrzymamy liczbę nieparzystą.
- Dla c_n nieparzystego c_{n+1} zawsze jest parzyste.
- Dla c_n=1 mamy $c_{n+1} = 4, c_{n+2} = 2, c_{n+3} = 1, \ldots$, czyli ciąg (c_n) wpada w cykl $(1, 4, 2)$. Oznacza to, że powyższa hipoteza jest równoważna hipotezie: ciąg (c_n) zawsze wpada w cykl $(1, 4, 2)$.
- Jeżeli pewien z wyrazów ciągu c_n jest potęgą liczy 2, to zgodnie z definicją ciągu dzielimy przez 2, aż otrzymamy 1, czyli taki ciąg wpada w cykl $(1, 4, 2)$.

Przykład 12.2. *Przedstawimy kilka przykładów dojścia do cyklu* $(1, 4, 2)$ *w zależności od* c_0.
Dla $c_0 = 3$ *otrzymujemy ciąg:*

$$(3, 10, 5, 16, 8, 4, 2, 1, 4, 2, 1, \ldots).$$

Dla $c_0 = 9$ *otrzymujemy ciąg:*

$$(9, 28, 14, 7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, 4, 2, 1, \ldots).$$

Dla $c_0 = 27$ *otrzymujemy ciąg:*

$$(27, 82, 41, 124, 62, 31, 94, 47, 142, 71, 214, 107, 322, 161, 484,$$
$$242, 121, 364, 182, 91, 274, 137, 412, 206, 103, 310, 155, 466, 233,$$
$$700, 350, 175, 526, 263, 790, 395, 1186, 593, 1780, 890, 445, 1336,$$
$$668, 334, 167, 502, 251, 754, 377, 1132, 566, 283, 850, 425, 1276,$$
$$638, 319, 958, 479, 1438, 719, 2158, 1079, 3238, 1619, 4858, 2429,$$
$$7288, 3644, 1822, 911, 2734, 1367, 4102, 2051, 6154, 3077, \mathbf{9232},$$
$$4616, 2308, 1154, 577, 1732, 866, 433, 1300, 650, 325, 976, 488,$$
$$244, 122, 61, 184, 92, 46, 23, 70, 35, 106, 53, 160, 80, 40, 20,$$
$$10, 5, 16, 8, 4, 2, 1, 4, 2, 1, \ldots)$$

Dla $c_0 = 27$ *dojście do 1 zajmuje* ***111*** *kroków, a największą wartością jest* ***9232****.*

12.2.2 Próby obalenia hipotezy

Większość matematyków skłania się ku temu, że hipoteza Collatza jest prawdziwa. Jednakże istnieje wiele projektów, których celem jest zaprzeczenie tej hipotezie. Korzystając z komputerów dużej mocy naukowcy próbują znaleźć taką wartość początkową ciągu, która wpadnie w cykl inny niż (1, 4, 2). Tomás Oliveira e Silva (Universidade de Aveiro, Portugalia) zweryfikował doświadczalnie hipotezę dla wszystkich dodatnich liczb naturalnych mniejszych od $20 \cdot 2^{58} = 5764607523034234880 > 5,764 \cdot 10^{18}$ (patrz [1]).

12.2.3 Analityczna próba rozwiązania problemu

Rozpatrzmy jak wyglądają ewentualne cykle. Załóżmy, że nieparzysta liczba dodatnia x jest elementem takiego cyklu. Przyjmijmy, że $c_0 = x$. Załóżmy, że w tym cyklu występuje k liczb nieparzystych. Liczbę dzieleń przez 2 po wystąpieniu i-tej liczby nieparzystej oznaczmy jako l_i, $i = 1, \ldots, k$. Wtedy liczbami nieparzystymi są:

$$\begin{aligned}
c_0 &= x \\
c_{l_1+1} &= \frac{3x}{2^{l_1}} + \frac{1}{2^{l_1}} \\
c_{l_1+l_2+2} &= \frac{3^2 x}{2^{l_1+l_2}} + \frac{2^{l_1}+3}{2^{l_1+l_2}} \\
c_{l_1+l_2+l_3+3} &= \frac{3^3 x}{2^{l_1+l_2+l_3}} + \frac{2^{l_1+l_2}+3\cdot 2^{l_1}+3^2}{2^{l_1+l_2+l_3}}
\end{aligned}$$

$$
\begin{aligned}
c_{l_1+l_2+l_3+l_4+4} &= \frac{3^4 x}{2^{l_1+l_2+l_3+l_4}} + \frac{2^{l_1+l_2+l_3} + 3 \cdot 2^{l_1+l_2} + 3^2 \cdot 2^{l_1} + 3^3}{2^{l_1+l_2+l_3+l_4}} \\
&\vdots \\
c_{l_1+l_2+\cdots+l_k+k} &= \frac{3^k x}{2^{l_1+l_2+\cdots+l_k}} + \frac{1}{2^{l_1+l_2+\cdots+l_k}} \Big(2^{l_1+l_2+\cdots+l_{k-1}} \\
&+ 3 \cdot 2^{l_1+l_2+\cdots+l_{k-2}} + 3^2 \cdot 2^{l_1+l_2+\cdots+l_{k-3}} + \ldots \\
&+ 3^{k-3} \cdot 2^{l_1+l_2} + 3^{k-2} \cdot 2^{l_1} + 3^{k-1} \Big)
\end{aligned}
$$

Otrzymujemy:

$$
\begin{aligned}
x &= \frac{3^k x}{2^{l_1+l_2+\cdots+l_k}} + \frac{1}{2^{l_1+l_2+\cdots+l_{k-1}}} \Big(3 \cdot 2^{l_1+l_2+\cdots+l_{k-2}} \\
&+ 3^2 \cdot 2^{l_1+l_2+\cdots+l_{k-3}} + \cdots + 3^{k-3} \cdot 2^{l_1+l_2} + 3^{k-2} \cdot 2^{l_1} + 3^{k-1} \Big)
\end{aligned}
$$

Oznaczmy: $l = l_1 + l_2 + \cdots + l_k$. Wtedy:

$$
\begin{aligned}
x &= \frac{3^k x}{2^l} + \frac{1}{2^l} \Big(2^{l_1+l_2+\cdots+l_{k-1}} + 3 \cdot 2^{l_1+l_2+\cdots+l_{k-2}} + \\
&+ 3^2 \cdot 2^{l_1+l_2+\cdots+l_{k-3}} + \cdots + 3^{k-3} \cdot 2^{l_1+l_2} + 3^{k-2} \cdot 2^{l_1} + 3^{k-1} \Big)
\end{aligned}
$$

co po prostych przekształceniach algebraicznych daje:

$$
\begin{aligned}
x &= \frac{1}{2^l - 3^k} \Big(2^{l_1+l_2+\cdots+l_{k-1}} + 3 \cdot 2^{l_1+l_2+\cdots+l_{k-2}} \\
&+ 3^2 \cdot 2^{l_1+l_2+\cdots+l_{k-3}} + \cdots + 3^{k-3} \cdot 2^{l_1+l_2} + 3^{k-2} \cdot 2^{l_1} + 3^{k-1} \Big)
\end{aligned}
$$

Spostrzeżenia:

- $2^l - 3^k$ musi być dodatnie, gdyź x jest dodatnie;
- licznik musi być podzielny przez mianownik, gdyż x jest liczbą naturalną.

Najprostszym przypadkiem jest, gdy $2^l - 3^k = 1$. Zauważmy, że $l, k > 0$. Ponadto $k > 0$ oznacza, że $l > 1$.
Dla $l = 2$ mamy $4 - 3^k = 1$, czyli $k = 1$. Wtedy $x = 1$ i otrzymujemy znany cykl $(1, 4, 2)$. Dla $l \geqslant 3$ mamy, że 2^l jest podzielne przez 8. Stąd $3^k + 1$ jest podzielne przez 8, czyli $3^k + 1 \equiv 0 \bmod 8$. Stąd $3^k \equiv 7 \bmod 8$. Ale:

$$3^k \equiv \begin{cases} 3, & 2 \nmid k \\ 1, & 2 | k \end{cases} \pmod 8,$$

więc nie istnieje takie k naturalne dodatnie, że $3^k \equiv 7 \bmod 8$. Stąd jedynym rozwiązaniem równania $2^l - 3^k = 1$ jest $(k, l) = (1, 2)$.
Gdyby udało się udowodnić, że w rozpatrywanym wzorze licznik jest podzielny przez mianownik tylko dla mianownika równego 1, hipoteza Collatza byłaby udowodniona.

12.2.4 Analiza długości możliwych cykli

Lynn E. Garner w 1981 roku badał długość możliwych cykli. Zauważył, że zachowanie ciągu Collatza jest silnie związane z potęgami dwójki i trójki. Udowodnił, że potęgi dwójki są oddzielone od potęg trójki i ta odległość rośnie prawie tak samo szybko jak rosną potęgi trójki. Udało mu się powiązać najmniejszą możliwą długość cyklu niezawierającego 1 z najmiejszą liczbą występującą w cyklu. Dla najmniejszej występującej w cyklu liczby równej $2 \cdot 10^9$ długość odpowiadajacego jej cyklu musi być większa lub równa 105 000.
Wniosek: jedynym „krótkim” cyklem jest cykl $(1, 4, 2)$.

12.2.5 Argument probabilistyczny

Argument opiera się na założeniu, że dla danej liczby naturalnej nieparzystej n liczba $\frac{3n+1}{2}$ jest parzysta z prawdopodobieństwem $\frac{1}{2}$ oraz nieparzysta z prawdopodobieństwem $\frac{1}{2}$.
Rozważmy trajektorię od jednej liczby nieparzystej do innej nieparzystej. Załóżmy, że pomiędzy nimi jest $N - 1$ nieparzystych

liczb. Wtedy mamy N przejść od jednej liczby nieparzystej do następnej. Dla każdego z przejść prawdopodobieństwo, że dzielimy dokładnie raz przez 2 wynosi $\frac{1}{2}$. Prawdopodobieństwo, że dzielimy dokładnie dwa razy przez 2 wynosi $\frac{1}{2^2}$, że dokładnie trzy razy – $\frac{1}{2^3}$ itd. Oczekujemy więc, że dzielimy dokładnie przez 2 w $\frac{N}{2}$ wszystkich przejść, dokładnie przez 2^2 w $\frac{N}{2^2}$ wszystkich przejść, dokładnie przez 2^3 w $\frac{N}{2^3}$ wszystkich przejść itd. Wobec tego średni wzrost ciągu rozpatrywanych liczb nieparzystych wynosi:

$$\frac{3^N}{2^{\frac{N}{2}} \cdot (2^2)^{\frac{N}{2^2}} \cdot (2^3)^{\frac{N}{2^3}} \cdot \ldots} = \frac{3^N}{2^{N(\frac{1}{2}+\frac{2}{4}+\frac{3}{8}+\frac{4}{16}+\ldots)}} = \frac{3^N}{2^{2N}} = \left(\frac{3}{4}\right)^N$$

Średni wzrost pomiędzy dwoma kolejnymi liczbami nieparzystymi z ciągu Collatza ($N = 1$) wynosi $\frac{3}{4}$. Jako że $\frac{3}{4} < 1$, to kolejne liczby nieparzyste z ciągu Collatza średnio zmniejszają się, co przemawia za prawdziwością hipotezy Collatza.

Nie jest to bynajmniej dowód hipotezy. Problemem jest, czy założenie, że dla danej liczby naturalnej nieparzystej n liczba $\frac{3n+1}{2}$ jest z prawdopodobieństwem $\frac{1}{2}$ parzysta i z prawdopodobieństwem $\frac{1}{2}$ nieparzysta, jest prawdziwe.

12.2.6 Różne podejścia do problemu Collatza

Do problemu Collatza można podejść na różne sposoby: można badać trajektorie, długości trajektorii, największy wyraz występujący w danej trajektorii czy tzw. czas stopu (dla danego c_0 najmniejsza liczba naturalna k, taka, że $c_k < c_0$). Używa się także metod spoza teorii liczb.
Wielu matematyków zajmuje się problemem Collatza. W 2011 roku Gerhard Opfer z uniwersytetu w Hamburgu (Niemcy) opublikował artykuł z dowodem hipotezy znanej jako problem Collatza. Jednakże niektóre stwierdzenia użyte w tej pracy nie były wystarczająco ścisłe i po konstruktywnej krytyce sam przyznał:

„It is true that (in the very end) some arguments are missing".

Wobec tego problem Collatza na dzień dzisiejszy pozostaje problemem otwartym.

12.2.7 Problemy podobne do problemu Collatza

Rozpatrzmy, co się dzieje, gdy w problemie $3x+1$ zdefiniujemy c_0 jako liczbę całkowitą ujemną. Wtedy okazuje się, że znanych jest kilka cykli. Są to:

- $(-1, -2)$,
- $(-5, -14, -7, -20, -10)$,
- $(-68, -34, -17, -50, -25, -74, -37, -110,$

  $-55, -164, -82, -41, -122, -61, -182, -91, -272, -136)$.

Jak dotąd nie wykryto innych cykli. Tak zdefiniowany problem jest odpowiednikiem problemu dla ciągu określonego dla liczb naturalnych dodatnich, gdzie zamiast $3x+1$ mamy $3x-1$. Wtedy znanymi pętlami są:

$$(1, 2), (5, 14, 7, 20, 10), (-5, -14, -7, -20, -10),$$

$$(68, 34, 17, 50, 25, 74, 37, 110, 55, 164, 82, 41, 122, 61, 182, 91, 272, 136).$$

Oprócz problemu $3x+1$ można także rozpatrywać inne problemy, takie jak problem $5x+1$, $7x+1$ i ogólnie $px+q$, gdzie p, q są nieparzyste i p jest liczbą pierwszą. W wielu przypadkach istnieją cykle niezawierające 1.

12.3 Liczby Ramseya

12.3.1 Wyznaczanie liczb Ramseya

Definicja 12.3. Grafem nazywamy parę $G = (V, E)$, gdzie V jest niepustym zbiorem punktów (wierzchołków), a E to zbiór dwuelementowych podzbiorów zbioru V (krawędzi).

Moc zbioru V nazywamy rzędem grafu, a moc zbioru E rozmiarem grafu.

Definicja 12.4. Grafem pełnym nazywamy graf, w którym każde dwa wierzchołki połączone są krawędzią. Graf pełny o n wierzchołkach oznaczamy przez K_n.

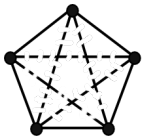
Definicja 12.5. Liczbą Ramseya $R(k, l)$ nazywamy najmniejszy rząd grafu pełnego takiego, że przy dowolnym pokolorowaniu jego krawędzi dwoma kolorami, istnieje podgraf K_k w pierwszym kolorze lub podgraf K_l w drugim kolorze. Jeżeli $k = l$, to piszemy $R(k)$ i mówimy, że jest to k-ta liczba Ramseya.

k \ l	3	4	5	6	7	8	9	10	11	12	13	14	15
3	6	9	14	18	23	28	36	40 42	47 50	52 59	59 68	66 77	73 87
4		18	25	36 41	49 61	58 84	73 115	92 149	98 191	128 238	133 291	141 349	153 417
5			43 49	58 87	80 143	101 216	126 316	144 442	171 633	191 848	213 1138	239 1461	265 1878
6				102 165	113 298	132 495	169 780	179 1171	253 1804	263 2566	317 3703	5033	401 6911
7					205 540	217 1031	241 1713	289 2826	405 4553	417 6954	511 10578	15263	22112
8						282 1870	317 3583	6090	10630	16944	817 27485	41525	861 63609
9							565 6588	581 12677	22325	38832	64864		
10								798 23556	45881	81123			1265

Rysunek 12.1: Znane wartości liczb Ramseya lub ograniczenia dolne i górne.[7]

Jak widać, ustalono jedynie dokładne wartości trzeciej i czwartej liczby Ramseya. Dokładna wartość piątej liczby Ramseya jak dotąd pozostaje nieznana.
Przesledźmy, co oznacza, że trzecia liczba Ramseya $R(3)$ wynosi 6.
$R(3) = 6$, czyli przy kolorowaniu krawędzi grafu dwoma kolorami dla grafu K_5 znajdziemy takie pokolorowanie, które nie zawiera pografu pełnego K_3 w jednym kolorze. Natomiast dla grafu K_6

przy każdym pokolorowaniu krawędzi dwoma kolorami otrzymujemy jednokolorowy (monochromatyczny) podgraf K_3.



Rysunek 12.2: Pokolorowanie grafu K_5 dwoma kolorami, przy którym nie istnieje monochromatyczny podgraf K_3

Uzasadnienie, że przy dowolnym pokolorowaniu dwoma kolorami grafu K_6 zawsze istnieje podgraf monochromatyczny K_3: Graf K_6 ma 6 wierzchołków, więc każdy wierzchołek połączony jest krawędzią z dokładnie 5 innymi wierzchołkami. To oznacza, że (przy kolorowaniu dwoma kolorami) co najmniej 3 z tych krawędzi są w jednym kolorze. Przyjmijmy, że krawędzie v_1v_2, v_1v_3, v_1v_4 sa w kolorze czerwonym, a v_1v_5 i v_1v_6 w kolorze niebieskim. Rozpatrzmy krawędzie v_2v_3, v_2v_4, v_3v_4. Jeżeli wszystkie są w kolorze niebieskim, to mamy trójkąt (graf K_3) w kolorze niebieskim. Natomiast jeżeli któraś z nich jest w kolorze czerwonym, to istnije trójkąt (graf K_3) w kolorze czerwonym (np. jeżeli v_2v_3 jest czerwona, to istnieje trójkąt o wierzchołkach v_1, v_2, v_3 w kolorze czerwonym). Stąd K_6 jest najmniejszym grafem pełnym, w którym przy dowolnym pokolorowaniu krawędzi dwoma kolorami istnieje monochromatyczny podgraf pełny K_3. Stąd $R(3) = 6$.

W przypadku liczb Ramseya problemem jest oczywiście wyznaczanie ich wartości. Istnieją analitycznie oszacowane ograniczenia dolne i górne dla wielu liczb Ramseya, ale dokładne wartości często nie są znane. Zwykle dokładne wartości wyznaczane są za pomocą komputerów poprzez sprawdzenie warunku istnienia odpowiedniego podgrafu pełnego we wszystkich możliwych pokolorowaniach grafu. Zauważmy, że graf pełny o n wierzchołkach ma $\binom{n}{2} = \frac{n!}{(n-2)!2!} = \frac{(n-1)n}{2}$ krawędzi, z których każda może

być pokolorowana na 2 sposoby, co daje $2^{\frac{(n-1)n}{2}}$ różnych pokolorowań grafu. Oznacza to, że mamy do czynienia ze wzrostem wykładniczym i nawet najlepsze superkomputery nie są w stanie sprawdzić wszystkich możliwości w rozsądnym czasie.

12.3.2 Niektóre oszacowania

Fakt 12.6. $R(n,m) \leqslant R(n-1,m) + R(n,m-1)$

Dowód. Rozważmy graf pełny o $R(n-1,m)+R(n,m-1)$ wierzchołkach, którego krawędzie są pokolorowane dwoma kolorami. Wybierzmy wierzchołek v z tego grafu i rozdzielmy pozostałe wierzchołki na dwa zbiory V_1 i V_2 tak, że dla każdego wierzchołka w zachodzi $w \in V_1$, jeżeli krawędź vw jest niebieska i $w \in V_2$ jeżeli krawędź vw jest czerwona. Graf ma $R(n-1,m)+R(n,m-1) = |V_1| + |V_2| + 1$ wierzchołków, więc albo $|V_1| \geqslant R(n-1,m)$, albo $|V_2| \geqslant R(n,m-1)$.
Dla $|V_1| \geqslant R(n-1,m)$, jeżeli w V_1 jest czerwony K_m, to jest też w rozpatrywanym grafie. Jeżeli w V_1 nie ma czerwonego K_m, to jest niebieski K_{n-1}, więc w $V_1 \cup \{v\}$ jest niebieski K_n.
Dla $|V_2| \geqslant R(n,m-1)$, jeżeli w V_2 jest niebieski K_n, to jest też w rozpatrywanym grafie. Jeżeli w V_2 nie ma niebieskiego K_n, to jest czerwony K_{m-1}, więc w $V_2 \cup \{v\}$ jest czerwony K_m.
Zatem w rozpatrywanym grafie zawsze jest albo niebieski K_n, albo czerwony K_m, czyli $R(n,m) \leqslant R(n-1,m)+R(n,m-1)$. □

Fakt 12.7. $R(n,m) \leqslant \binom{n+m-2}{m-1}$

Dowód przeprowadza się indukcyjnie korzystając z ostatniej nierówności.

Fakt 12.8. $R(n) \geqslant n 2^{\frac{n}{2}} 2^{-\frac{1}{2}} e^{-1}$

Liczby Ramseya mogą być zdefiniowane także dla większej liczby kolorów. Np. liczba $R(n,m,k)$ oznacza najmniejszy rząd grafu pełnego, w którym przy dowolnym pokolorowaniu krawędzi istnieje czerwony podgraf pełny K_n lub niebieski podgraf pełny K_m, lub zielony podgraf pełny K_k.

12.4 Podsumowanie

Opis każdego z powyższych problemów wraz ze wszystkim, co do tej pory zostało zrobione przy próbach ich rozwiązania mógłby zostać wydany w postaci całkiem grubej książki. Ponadto problem Collatza i trudności związane ze znajdowaniem liczb Ramseya to tylko dwa z licznych przykładów ciągle nierozwiązanych problemów matematycznych o bardzo prostym sformułowaniu. Artykuł miał na celu zapoznanie czytelników z przedstawionymi zagadnieniami i zainteresowanie poszukiwaniem rozwiązań.

Bibliografia

[1] Tomás Oliveira e Silva, *Empirical Verification of the 3x + 1 and Related Conjectures.* in The Ultimate Challenge: The 3x + 1 Problem, pp. 189-207, American Mathematical Society, 2010.

[2] Lynn E. Garner, *On the Collatz 3n + 1 algorithm*, Proceedings of American Mathematical Society, vol. 82, number 1, 1981.

[3] Jean Paul Van Bendegem, *The Collatz Conjecture. A Case Study in Mathematical Problem Solving*, Logic and Logical Philosophy, vol. 14, pp. 7-23, 2005.

[4] John L. Simons, *Exotic Collatz cycles*, Acta Arithmetica 134(3), 2007.

[5] Gerhard Opfer, *An Analytic Approach to the Collatz 3n + 1 Problem*, Hamburger Beiträge zur Angewandten Mathematik, Nr. 2011-09, May 2011.

[6] Benne de Weger, *Comments on Opfer's alleged proof of the 3n + 1 Conjecture*, June 2011.

[7] Stanisław P. Radziszkowski, *Small Ramsey Numbers*, The Electronic Journal of Combinatorics, 1994, revision: 2014.

Matematyczny język piękna

Ewa Michalska
Uniwersytet im. Adama Mickiewicza w Poznaniu
Wydział Matematyki i Informatyki

13.1 Wstęp

Mówiąc o pięknie słyszymy hasła, takie jak: złota proporcja, boska proporcja, złoty stosunek, itp. Otaczające nas piękno w przyrodzie, muzyce, malarstwie, architekturze często kryje się za pewną niewielką matematyczną wartością, a mianowicie liczbą $\frac{1+\sqrt{5}}{2}$, która posiada nieskończone rozwinięcie, dające liczbę $1,6180339887\ldots$. Liczę tę oznaczamy grecką dużą literą fi- ϕ (czasem również oznacza się małą literą φ, jednak my w naszych obliczeniach stosować będziemy konwencję z dużym fi). Została ona odkryta przez starożytnych Greków, a jej pierwsze udokumentowanie możemy znaleźć w *Elementach* Euklidesa, których napisanie datuje się na około 300 roku p.n.e. Był to pierwszy podręcznik matematyki. Pełnił funkcję tzw. encyklopedii matematycznej, zbierając wszystkie matematyczne odkrycia epoki. *Elementy* składają się z XIII ksiąg, a każda z nich zawiera metodologię dowodzenia twierdzeń i nową teorię opartą na aksjomatach i prawach wnioskowania.

W VI księdze znajdujemy tekst dotyczący złotej proporcji:

„Powiedzmy, że linia prosta została podzielona harmonicznie, gdy większy odcinek ma się tak do mniejszego, jak całość do większego".

Zakładamy, że cały odcinek jest równy x, większy jest równy 1, a mniejszy $x-1$. Podstawiając, jak w powyższym tekście,

otrzymujemy równanie:

$$\frac{x}{1} = \frac{1}{x-1}.$$

Wykonując obliczenia mamy:

$$x(x-1) = 1 \cdot 1,$$

$$x^2 - x - 1 = 0,$$

co po obliczeniu i wzięciu pod uwagę tylko dodatniego rozwiązania daje wynik:

$$x = \frac{1+\sqrt{5}}{2},$$

jest to dokładnie nasza liczba ϕ.

Zauważmy pewne własności tej liczby:

$$\phi = \frac{1}{\phi} + 1,$$

mnożąc razy ϕ otrzymujemy kolejno:

$$\phi^2 = \phi + 1,$$

$$\phi^3 = \phi^2 + \phi = 2\phi + 1,$$

$$\phi^4 = \phi^3 + \phi^2 = 3\phi + 2,$$

$$\phi^5 = \phi^4 + \phi^3 = 5\phi + 3,$$

$$\phi^6 = \phi^5 + \phi^4 = 8\phi + 5,$$

$$\vdots$$

Możemy zaobserwować pewną zależność dotyczącą współczynników liczby ϕ, a także tą samą, lecz przesuniętą zależność w wyrazach wolnych. Zależnością tą jest ciąg Fibonacciego.

13.2 Ciąg Fibonacciego

Leonardo z Pizy, potocznie zwany Fibonaccim, co prawdopodobnie oznaczało syn Bonacciego, żył w latach 1170-1250. Drogę do matematyki otworzyła mu księgowość. Jego ojciec był włoskim kupcem z międzynarodowymi powiązaniami handlowymi. Fibonacci wiele z nim podróżował, poznając dzięki temu różne kultury. Nauczył się matematyki arabskiej od muzułmańskich mistrzów. Jako pierwszy wprowadził do Europy system arabski zamiast abaku. Jednak jego największym osiągnięciem, które nosi jego imię, było odkrycie, dotyczące ciągu Fibonacciego. Odkrycie to opierało się na rozwiązaniu zadania:

„Ile par królików będziemy mieli na końcu roku, jeśli zaczniemy w styczniu z jedną parą królików, to w każdym miesiącu, poczynając od marca, wyda na świat kolejną parę królików i z każdej pary urodzą się kolejne pary po 2 miesiącach od narodzin".

Oryginalny tekst rozwiązania Fibonacciego znajdziemy m.in. w książce *Złota proporcja. Matematyczny język piękna. Wyd. RBA, strona 152.* My natomiast omówimy rozwiązanie w skrócie. Otóż, mając na początku parę królików, kiedy urodzi ona w pierwszym miesiącu będziemy mieli 2 pary. Jedna z nich, która już była parą w kolejnym miesiącu urodzi jedną parę, zatem dodając 2 poprzednie pary uzyskamy 3 pary. W trzecim miesiącu 2 z nich zajdą w ciążę, zatem urodzą się kolejne 2 pary, do których dodając pozostałe 3 uzyskamy łącznie 5 par itd., aż do dwunastego miesiąca gdzie będziemy mieli łącznie 377 par.

Ciąg Fibonacciego to zatem ciąg zaczynający się od dwóch jedynek, w którym kolejne wyrazy powstają przez sumę 2 poprzednich wyrazów. Przedstawimy więc ciąg dwunastu pierwszych wyrazów, który możemy generować w nieskończoność:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \ldots$$

Nasz ciąg ma wiele interesujących własności. Jedną z nich jest fakt, że dzieląc wyraz a_{n+1}, przez wyraz a_n przesuwając się do coraz dalszych wyrazów uzyskujemy coraz lepsze przybliżenie liczby ϕ, a co za tym idzie zbieżność ilorazu do tej liczby. Pokażemy kilka takich ilorazów, mianowicie:

- $\frac{1}{1} = 1$, co jest przybliżeniem liczby ϕ z niedomiarem równym około 0,618033,
- $\frac{2}{1} = 2$, co jest przybliżeniem liczby ϕ z nadmiarem równym około 0,381966,
- $\frac{3}{2} = 1,5$, co jest przybliżeniem liczby ϕ z niedomiarem równym około 0,118033,
- $\frac{5}{3} = 1,(6)$, co jest przybliżeniem liczby ϕ z nadmiarem równym około 0,04863,
- $\vdots$
- $\frac{55}{34} = 1,61764\cdots$ co jest przybliżeniem liczby ϕ z niedomiarem równym około 0,0003869,
- $\frac{89}{55} = 1,6(18)$ co jest przybliżeniem liczby ϕ z nadmiarem równym około 0,0001478,itd.

Inna własność, to taka, że suma 10 kolejnych wyrazów ciągu Fibonacciego jest wielokrotnością liczby 11 pomnożonej przez 4 wyraz od końca wykorzystanego w tej sumie ciągu liczb, np.:

$$1+1+2+3+5+8+13+21+34+55=$$
$$=143=11\cdot 13,$$
$$21+34+55+89+144+233+377+610+987+1597=$$
$$=4147=11\cdot 377.$$

Kolejną cechą naszego ciągu jest fakt, że biorąc 4 jego kolejne liczby i stosując na nich odpowiednie działania otrzymamy trójkę Pitagorejską. Własności te przedstawimy na przykładzie.

Weźmy 4 kolejne liczby ciągu Fibonacciego, np. 2,3,5,8. Pierwszą liczbę pitagorejską otrzymamy przez pomnożenie przez siebie skrajnych liczb: $2 \cdot 8 = 16$. Kolejną liczbę uzyskamy poprzez podwojenie iloczynu liczb środkowych, mianowicie $2 \cdot (3 \cdot 5) = 30$. Ostatnia liczba powstaje poprzez zsumowanie kwadratów środkowych wyrazów naszego ciągu, a zatem mamy $3^2 + 5^2 = 34$.

Sprawdzamy, czy faktycznie otrzymane przez nas liczby spełniają twierdzenie Pitagorasa

$$34^2 = 30^2 + 16^2$$

$$1156 = 256 + 900,$$

zatem fatycznie uzyskaliśmy trójkę Piagorejską.

Inną własnością jest wzór:

$$a_n^2 - a_{n-1} \cdot a_{n+1} = (-1)^{n-1},$$

który prowadzi do wzoru ogólnego wyprowadzonego przez Jaques'a Binet'a w 1843 roku o postaci:

$$a_n = \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n] =$$

$$= \frac{1}{\sqrt{5}}[\phi^n + \frac{(-1)^{n+1}}{\phi^n}].$$

Zauważamy w nim zależność tego ciągu od naszej złotej proporcji.

Harmonię i piękno matematyczne możemy również zaobserwować w muzyce. Częstotliwości oraz nuty układają się kolejno w ciąg Fibonacciego. Przykładem jego zastosowania jest np. *V Symfonia Beethovena*.

Także w przyrodzie obserwujemy występowanie zależności. Ziarna słonecznika układają się w spirale skręcone zarówno w kierunku ruchu wskazówek zegara, jak i przeciwnym. Gdy policzymy jedne i drugie otrzymamy takie pary liczb, jak: (21,34), (34,55),(55,89), czy (89,144). W innych kwiatkach liczba ich płatków stanowi wyrazy ciągu Fibinacciego i tak: liczba płatków bzu jest równa z reguły 3, jaskrów 5, ostronóżek 8, nagietków 13, astrów 21, stokrotek 21,34,55,89, w zależności od rodzaju.

Nasuwa się zatem pytanie, czy zakochany matematyk recytując znaną wyliczankę „*kocha, nie kocha* ...” potrafi z góry oszacować jej wynik? Otóż odpowiedź brzmi nie. Po pierwsze przyroda lubi płatać figle, a po drugie w ciągu Fibonacciego występują zarówno liczby parzyste jak i nieparzyste.

Ciąg Fibonacciego znajdujemy także w ludzkim ciele, a mianowicie w długości paliczków palców i dłoni. Zaczynając od czubka palca obserwujemy wzrost długości każdej z kości w stosunku 2,3,5,8. Ponadto znany jest wzór na idealne wymiary człowieka:

wzrost(całkowita wysokość)=zasięg rąk(odległość między palcami rozciągniętych rąk)=8 dłoni= 6 stóp= 8 twarzy = 1,618 razy wysokość pępka (liczona od podłogi).

Nie załamujmy się jednak, kiedy po zmierzeniu i podstawieniu do wzoru nasze wymiary staną się odległe od ideału. Jak wykazał belgijski matematyk Lambert Adolphe Quetelet (1796-1874)- postać ludzka jest idealna tylko jako średnia. Wykazał to poprzez badania w 1871 roku badając proporcje europejskich mężczyzn. Badania te przeniosły się w kolejnych latach również na wymiary kobiet oraz ludzi zamieszkujących inne kontynety.

13.3 Złoty prostokąt

Przechodząc do geometrycznych zastosowań, złoty prostokąt to figura, w której jeden z boków, jest równy długości drugiego boku przemnożonemu przez liczbę ϕ. Przykładem jego zastosowania są m.in. karty kredytowe. Złote prostokąty możemy znaleźć w sztuce, np. w obrazie *Mona Lisa*, *Ostatnia wieczerza*, czy też w ateńskim partenonie, choć wymiary tego ostatniego wykazują niewielkie odchylenia od tych idealnych, być może jednak powodem tego stał się upływ czasu. Również w naturze ukazuje się taka proporcja, choćby w ułożeniu pierwszego i drugiego zęba w szczęce człowieka.

13.4 Spirala logarytmiczna

Jacob Bernoulli (1654-1705), znany szwajcarski matematyk, przez całe swoje życie był wielkim fascynatem i odkrywcą nowych zagadnień związanych ze spiralą logarytmiczną. W związku ze swoja miłością do niej pragnął, aby po śmierci na jego grobie wyryto napis „*Eadem mutato resurso*" (co w tłumaczeniu z łac. ozna-

cza „Choć przekształcana, odradzam się niezmieniona"). Słowa te oddają jej własności, do których należy fakt, że jej kształt nie zmienia się przy powiększaniu, ani zmniejszaniu, co nosi nazwę samopodobieństwa, a ponadto jest ona równokątna. Ponadto pragnieniem Benroulliego, było aby obok wspomnianego napisu pojawiła się ikona spirali logarytmicznej. Niestety jej twórca nie znał się dostatecznie na matematyce lub też zabrakło mu zdolności, ponieważ spirala na nagrobku powstała, jednak niestety wiele brakuje jej do umiłowanej przez naszego matematyka spirali logarytmicznej.

Wiele przykładów takich spirali możemy odnaleźć w naturze, jak choćby w szyszce pinii, gdzie pojawia się kilka spirali w każdym kierunku obrotu, naszej galaktyce, czy turbulencjach obrotowych z rosnącą prędkością rozszerzania, jakie można zaobserwować w wirach rzecznych lub podczas spuszczania wody z wanny. Innym ciekawym przykładem jest nautilus, mięczak z rodziny łodzików. Wewnętrzna struktura jego muszli powstaje przez narastanie za każdym razem coraz większej komory, przy czym ogólny kształt zostaje zachowany, a nowa komora, nadbudowana nad poprzednią ma dokładnie taki sam kształt, choć większe rozmiary.

13.5 Podsumowanie

Jak widzimy, wiele elementów ze świata natury, ale również i sztuki związanych jest z matematycznymi pojęciami takimi jak złoty stosunek, liczba ϕ, ciąg Fibonacciego, czy też spirala logarytmiczna. Są to tylko niektóre, wybrane z ogromu innych równie ciekawych zagadnień. Dla chętnych ich rozszerzenia polecam książkę *Złota proporcja. Matematyczny język piękna. Wyd. RBA*, która była mi bardzo pomocna przy układaniu tego referatu.

Od grup ilorazowych do teorii modeli

Paweł Płaczek
Uniwersytet im. Adama Mickiewicza w Poznaniu
Wydział Matematyki i Informatyki

W algebrze abstrakcyjnej rozważa się struktury ilorazowe, w szczególności grupy ilorazowe, pierścienie, przestrzenie liniowe czy moduły. Przypomnijmy dla przykładu konstrukcję grupy ilorazowej.

Niech $(G, +)$ będzie dowolną grupą. Niech $H \subset G$. Zbiór H nazywamy podgrupą G wtedy i tylko wtedy, gdy dla dowolnych elementów $a, b \in H$ zachodzi $a - b \in H$. Oznacza to, że działanie $+$ oraz branie odwrotności na elementach H nie wyprowadza nas poza H.

Niech $g \in G$ będzie dowolne. Poprzez $g+H$ oznaczamy $\{g+h : h \in H\}$, analogicznie $H + g = \{h + g : h \in H\}$. Nazywamy je odpowiednio warstwą lewostronną i prawostronną. Jeżeli dla dowolnego $g \in G$ zachodzi $g + H = H + g$, to H nazywamy dzielnikiem normalnym.

Definiujemy grupę $({}^{G}/_{H}, \oplus)$ w sposób następujący:

$$ {}^{G}/_{H} = \{g + H : g \in G\}$$
$$\forall_{g_1, g_2 \in G} (g_1 + H) \oplus (g_2 + H) = (g_1 + g_2) + H$$

Grupę tę nazywamy grupą ilorazową.

Przypomnijmy też pierwsze twierdzenie o izomorfizmie. Niech $(G, \star)$ i $(H, \diamond)$ będą dowolnymi grupami. Przekształcenie $f : G \to H$ nazywamy homomorfizmem, gdy $f(a \star b) = f(a) \diamond f(b)$. Mówimy, że homomorfizm zachowuje działania. Homomorfizm, który jest bijekcją nazywamy izomorfizmem.

Jądrem homomorfizmu f nazywamy zbiór $\ker f = \{g \in G : f(g) = 0_H\}$.

Twierdzenie 14.1 (Pierwsze twierdzenie o izomorfizmie grup)**.** *Niech $f : G \to H$ będzie homomorfizmem suriektywnym (epimorfizmem), wtedy* $\ker f$ *jest dzielnikiem normalnym, ${}^{G}/_{\ker f} \cong H$ oraz istnieje dokładnie jeden izomorfizm f^* taki, że $f = f^* \circ \kappa$, gdzie κ jest odwzorowaniem kanonicznym.*

Definicja 14.2. Językiem L nazywamy język rachunku predykatów ograniczony do symboli stałych $Const_L = \{c_i : i \in I\}$, symboli funkcyjnych $Fun_L = \{f_f : f \in F\}$ oraz predykatów $Rel_L = \{R_k : k \in K\}$, gdzie I, J, K są zbiorami wskaźników. Piszemy wtedy $L = Const_L \cup Fun_L \cup Rel_L$.

Definicja 14.3. Niech L będzie językiem bez predykatów ($Rel_L = \emptyset$). Strukturą algebraiczną języka L nazywamy $\mathcal{A} = (A, \{c^{\mathcal{A}} : c \in Const_L\}, \{f^{\mathcal{A}} : f \in Fun_L\})$, gdzie $c^{\mathcal{M}}$ jest pewnym elementem zbioru A (nazywany interpretacją symbolu stałej c), a $f^{\mathcal{M}}$ jest funkcją $A^n \to A$, gdzie n jest argumentowością symbolu funkcyjnego f ($f^{\mathcal{A}}$ nazywamy interpretacją symbolu funkcyjnego f).

Jak wiadomo, każda klasa struktur podobnych (struktur tego samego języka) ma własny odpowiednik homomorfizmu. Rozważmy klasę najprostszych struktur - zbiorów. Homomorfizmem między dowolnymi zbiorami będzie dowolne odwzorowanie między nimi. Jak się można łatwo domyślić izomorfizmami będą tutaj bijekcje. Nasze rozważania toczą się wokół struktur ilorazowych. Jak można zdefiniować zbiór ilorazowy?

Przypomnijmy, że na każdym zbiorze A można określić szereg relacji równoważności. Relacje te dzielą cały zbiór A na rozłączne i niepuste klasy abstrakcji. Niech $\equiv$ będzie taką relacją. Zbiór klas abstrakcji często oznacza się ${}^{A}/_{\equiv}$ i oznaczenie to nie jest przypadkowe. Zbiór klas abstrakcji jest odpowiednikiem grupy ilorazowej. Żeby się o tym przekonać przepiszmy pierwsze twierdzenie o izomorfizmie.

Twierdzenie 14.4 (Pierwsze twierdzenie o izomorfizmie zbiorów)**.** *Niech A i B będą dowolnymi zbiorami. Niech $f : A \to B$*

będzie suriekcją (epimorfizmem). Określamy relację $(a_1, a_2) \in \ker f \iff f(a_1) = f(a_2)$*, która jest relacją równoważności. Wtedy* ${}^{A}/_{\ker f} \cong B$ *oraz istnieje dokładnie jedna bijekcja (izomorfizm)* f^* *taki, że* $f = f^* \circ \kappa$*, gdzie* $\kappa(a) = {}^{a}/_{\ker f}$*.*

Dowód. Relacja $\ker f$ jest relacją równoważności, ponieważ relacja równości nią jest. Określamy f^* następująco:

$$f^*({}^{a}/_{\ker f}) = f(a).$$

Z definicji relacji widać, że przekształcenie jest dobrze określone. Widać także, że $f^* \circ \kappa = f$. Niech $f^*({}^{a_1}/_{\ker f}) = f^*({}^{a_2}/_{\ker f})$, wtedy $f(a_1) = f(a_2)$, czyli ${}^{a_1}/_{\ker f} = {}^{a_2}/_{\ker f}$. Łatwo zauważyć, że f^* jest suriekcją. Wynika to z suriektywności f i podziału A na klasy abstrakcji. Zatem f^* jest bijekcją.

Niech teraz g^* będzie inną bijekcją taką, że $f = g^* \circ \kappa$. Przypuśćmy, że $f^*({}^{a}/_{\ker f}) \neq g^*({}^{a}/_{\ker f})$ dla pewnej klasy ${}^{a}/_{\ker f}$. Ale to jest równoważne: $f^* \circ \kappa(a) \neq g^* \circ \kappa(a)$, czyli $f(a) \neq f(a)$. Doszliśmy do sprzeczności, zatem $f^* = g^*$. □

Odejdźmy trochę na bok i przypomnijmy sobie własności pierścieni względem ich grup. Jak wiadomo, każdy pierścień jest też grupą ze względu na działanie addytywne. Zauważmy, że homomorfizm pierścieni jest również homomorfizmem ich grup addytywnych. Zależność ta jednak nie daje się odwrócić, gdyż nie każdy homomorfizm grup jest homomorfizmem pierścieni. Podobnie ma się rzecz z pierścieniami z jedynką. Nie każdy homomorfizm pierścieni jest homomorfizmem pierścieni z jedynką. Jeżeli zatem zapiszemy pierścień z jedynką w postaci $(R, 0, 1, +, -, \cdot)$, to widzimy, że obcięcie tej struktury o pewne operacje i stałe, to homomorficzność przekształceń zostaje zachowana.

Podobnie ma się rzecz z ilorazami. Jeżeli weźmiemy pierścień ilorazowy i obetniemy go ze względu na mnożenie, to uzyskujemy poprawnie zdefiniowaną grupę ilorazową.

Zatem obcinając dalej dochodzimy do „gołej" struktury samego zbioru. W takim przypadku grupę ilorazową powinniśmy również móc przedstawić jako zbiór ilorazowy bez działań.

W teorii grup mówi się o przystawaniu modulo podgrupa. To jest doskonały kandydat na relację równoważności, której szukamy. Przypomnijmy definicję.

Definicja 14.5. Niech G będzie grupą, a H jej dzielnikiem normalnym. Mówimy, że $g_1, g_2 \in G$ przystają do siebie modulo H wtedy i tylko wtedy, gdy $g_1 + H = g_2 + H$. Piszemy wtedy $g_1 \equiv_H g_2$.

Uwaga 14.6. *Relacja $\equiv_H$ jest relacją równoważności.*

Dowód tego faktu polega na bezpośrednim sprawdzeniu definicji relacji równoważności.

Zauważmy, że kongruencja modulo H daje taki sam podział na klasy abstrakcji jak w ${}^{G}/_{H}$. Z definicji warstwy $g + H$ mamy, że $g' \in (g + H)$ wtedy i tylko wtedy, gdy $g' = g + h$ dla pewnego $h \in H$, więc $g' - h = g$, co jest równoważne na mocy definicji podgrupy $g \in (g' + H)$. Oczywiście zachodzi także $g \in (g + H)$ oraz $g' \in (g' + H)$, dzięki czemu mamy $g + H = g' + H$ i to spełnia nam definicję klasy abstrakcji.

Nasuwa się następujące pytanie: Skoro każdy dzielnik normalny wyznacza relację równoważności, to czy każda relacja równoważności wyznacza jakiś dzielnik normalny? Odpowiedź jest niestety negatywna, co można łatwo sprawdzić na grupie $\mathbb{Z}_4$ przy podziale na klasy abstrakcji: $\{0, 1\}, \{2, 3\}$.

Co zatem musi spełniać relacja równoważności, aby wyznaczała grupę ilorazową? Spójrzmy ponownie na konstrukcję podgrupy. Jak wcześniej zauważyliśmy, podgrupa jest zamknięta na działanie, operację odwrotności, a także zawiera zero. Nie każda relacja równoważności nam to zapewnia, musimy zatem dołożyć dodatkowe warunki.

Definicja 14.7. Niech $(G, +, 0, -)$ będzie grupą. Kongruencją na grupie G nazywać będziemy dowolną relację równoważności $\equiv$ taką, że:

$$g_1 \equiv g_2 \implies -g_1 \equiv -g_2$$
$$g_1 \equiv g_2 \wedge g_1' \equiv g_2' \implies g_1 + g_1' \equiv g_2 + g_2'$$

Pokażemy teraz, że ta relacja wyznacza nam stosowny podział na warstwy, tworząc grupę ilorazową. Naszym dzielnikiem normalnym będzie $H = \{g \in G : g \equiv 0\}$. Niech $g_1, g_2 \in H$, wtedy $g_1 \equiv 0$ i $g_2 \equiv 0$, czyli $-g_2 \equiv 0$, zatem $g_1 - g_2 \equiv 0$ i ostatecznie $g_1 - g_2 \in H$. Zatem H jest podgrupą. Warstwa $g' + H$ ma postać $\{g \in G : g \equiv g'\}$. Istotnie: $g' + H = \{g \in G : g = g' + h \wedge h \in H\}$, czyli $h \equiv 0$ i $g' \equiv g'$, czyli $g' + h \equiv g'$. Identycznie definiuje się warstwę prawostronną, a dowód przebiega analogicznie. Zatem H jest dzielnikiem normalnym.

Widzimy zatem, że dzielniki normalne i kongruencje na grupie są sobie równoważne.

W przypadku pierścieni wszystko przebiega bardzo podobnie. Ideały generują nam relacje równoważności. Natomiast kongruencje na pierścieniach indukują ideały. Przy czym kongruencja na pierścieniu ma definicję taką, jak na grupie z dodanym warunkiem:

$$g_1 \equiv g_2 \wedge g_1' \equiv g_2' \implies g_1 g_1' \equiv g_2 g_2'$$

Przyglądając się innym znanym strukturom ilorazowym możemy wyszczególnić podobne definicje kongruencji i zauważamy te same zależności. Można podejrzewać, że jest możliwe uogólnienie tego rozumowania na dowolną strukturę algebraiczną.

Możemy teraz zdefiniować kongruencję na strukturze algebraicznej.

Definicja 14.8. Niech L będzie językiem, takim że $Rel_L = \emptyset$. Oznaczmy $\sigma(f)$ jako argumentowość symbolu funkcyjnego f. Niech $\mathcal{A}$ będzie strukturą języka L. Kongruencją nazywamy relację równoważności $\equiv$, taką że:

$$\forall_{f \in Fun_L} \quad \left\{ \begin{array}{l} a_1 \equiv a_1' \\ a_2 \equiv a_2' \\ ... \\ a_{\sigma(f)} \equiv a_{\sigma(f)}' \end{array} \right\} \implies$$

$$f^{\mathcal{A}}(a_1, a_2, ..., a_{\sigma(f)}) \equiv f^{\mathcal{A}}(a_1', a_2', ..., a_{\sigma(f)}')$$

Łatwo możemy sprawdzić, że dla wspominanych struktur de-

finicja kongruencji jest taka sama jak powyższa. Podobnie definiuje się homomorfizm.

Definicja 14.9. Niech $\mathcal{A}, \mathcal{B}$ będą strukturami podobnymi. Homomorfizmem $\phi : A \to B$ nazywamy funkcję, taką, że:

$$\forall_{c \in Const_L} \quad \phi(c^{\mathcal{A}}) = c^{\mathcal{B}}$$
$$\forall_{f \in Fun_L} \quad \phi(f^{\mathcal{A}}(x_1, x_2, ..., x_{\sigma(f)})) = f^{\mathcal{B}}(\phi(x_1), \phi(x_2), ..., \phi(x_{\sigma(f)}))$$

Ponownie widzimy analogię między definicją homomorfizmu grup a powyższą. Izomorfizm jest to bijektywny homomorfizm. Podajmy wreszcie definicję struktury ilorazowej.

Definicja 14.10. Niech $\mathcal{A}$ będzie dowolną strukturą algebraiczną, a $\equiv$ kongruencją na niej. Strukturą ilorazową ${}^{\mathcal{A}}/_{\equiv}$ nazywamy układ $({}^{A}/_{\equiv}, \{c^{{}^{\mathcal{A}}/_{\equiv}} : c \in Const_L\}, \{f^{{}^{\mathcal{A}}/_{\equiv}} : f \in Fun_L\})$, gdzie $c^{{}^{\mathcal{A}}/_{\equiv}} = {}^{c^{\mathcal{A}}}/_{\equiv}$ oraz $f^{{}^{\mathcal{A}}/_{\equiv}}({}^{x_1}/_{\equiv}, {}^{x_2}/_{\equiv}, ..., {}^{x_{n_j}}/_{\equiv}) = {}^{f^{\mathcal{A}}(x_1, x_2, ..., x_{n_j})}/_{\equiv}$.

Poprawność tej definicji można łatwo sprawdzić z definicji kongruencji. Możemy teraz sformułować pierwsze twierdzenie o izomorfizmie dla dowolnych struktur.

Twierdzenie 14.11 (Pierwsze twierdzenie o izomorfizmie dla struktur algebraicznych)**.** *Niech L będzie językiem bez predykatów ($Rel_L = \emptyset$). Niech $\mathcal{A}, \mathcal{B}$ będą strukturami podobnymi. Niech $\phi : \mathcal{A} \to \mathcal{B}$ będzie homomorfizmem suriektywnym. Niech $\ker \phi$ będzie relacją taką, że $(a_1, a_2) \in \ker \phi \iff \phi(a_1) = \phi(a_2)$. Relacja $\ker \phi$ jest kongruencją na $\mathcal{A}$. Wtedy ${}^{\mathcal{A}}/_{\ker \phi} \cong \mathcal{B}$. Ponadto istnieje dokładnie jeden izomorfizm ϕ^* taki, że $\phi = \phi^* \circ \kappa$.*

Dowód. Relacja $\ker \phi$ jest relacją równoważności. Pokażemy, że jest to kongruencja. Niech $f \in Fun_L$ będzie dowolne. Niech

$$(a_1, a_1') \in \ker \phi, (a_2, a_2') \in \ker \phi, ..., (a_{\sigma(f)}, a_{\sigma(f)}') \in \ker \phi$$

Wtedy

$$\phi(f^{\mathcal{A}}(a_1, a_2, ..., a_{\sigma(f)})) = f^{\mathcal{B}}(\phi(a_1), \phi(a_2), ..., \phi(a_{\sigma(f)}))) =$$
$$= f^{\mathcal{B}}(\phi(a_1'), \phi(a_2'), ..., \phi(a_{\sigma(f)}'))) = \phi(f^{\mathcal{A}}(a_1', a_2', ..., a_{n_j}')),$$

czyli $(f^{\mathcal{A}}(a_1, a_2, ..., a_{\sigma(f)}), f^{\mathcal{A}}(a'_1, a'_2, ..., a'_{\sigma(f)})) \in \ker\phi$. Zatem $\ker\phi$ jest kongruencją.

Definiujemy przekształcenie $\phi^* : {}^{A}/_{\ker\phi} \to B$ wzorem:

$$\phi^*({}^{a}/_{\ker\phi}) = \phi(a).$$

Pokazywaliśmy już, że jest to bijekcja i że jest ona wyznaczona jednoznacznie przy założeniu $\phi = \phi^* \circ \kappa$. Wystarczy pokazać, że ϕ^* jest homomorfizmem. Warunek dla stałych wynika wprost z faktu, że ϕ jest homomorfizmem. Niech $f \in Fun_L$ będzie dowolne, wówczas:

$$\begin{aligned}
\phi^* \quad & \left(f^{\mathcal{A}/_{\ker\phi}}({}^{x_1}/_{\ker\phi}, {}^{x_2}/_{\ker\phi}, ..., {}^{x_{\sigma(f)}}/_{\ker\phi}) \right) = \\
= \quad & \phi^* \left({}^{f^{\mathcal{A}}(x_1, x_2, ..., x_{\sigma(f)})}/_{\ker\phi} \right) = \phi(f^{\mathcal{A}}(x_1, x_2, ..., x_{\sigma(f)})) = \\
= \quad & f^{\mathcal{B}}(\phi(x_1), \phi(x_2), ..., \phi(x_{\sigma(f)})) = \\
= \quad & f^{\mathcal{B}}(\phi^*({}^{x_1}/_{\ker\phi}), \phi^*({}^{x_2}/_{\ker\phi}), \ldots, \phi^*({}^{x_{\sigma(f)}}/_{\ker\phi}))
\end{aligned}$$

□

Zdefiniowaliśmy zatem ilorazy dowolnych struktur algebraicznych. Zachowują się one zgodnie z naszą intuicją, dzięki czemu prawdziwe jest pierwsze twierdzenie o izomorfizmie i wszystkie jego konsekwencje. Pozostaje zatem problem ostatniego uogólnienia. Czy możemy zdefiniować ilorazy dla dowolnych modeli, niekoniecznie czysto algebraicznych?

Intuicyjnie musimy nałożyć pewne warunki na kongruencję, żeby działała również dla relacji. Przypomnijmy definicję modelu:

Definicja 14.12. Niech L będzie dowolnym językiem. Modelem (strukturą relacyjną) języka L nazywamy $\mathcal{M} = (M, \{c^{\mathcal{M}} : c \in Const_L\}, \{f^{\mathcal{M}} : f \in Fun_L\}, \{R^{\mathcal{M}} : R \in Rel_L\})$, gdzie $c^{\mathcal{M}}, f^{\mathcal{M}}$ są jak w definicji stuktury algebraicznej, a $R^{\mathcal{M}} \subset M^{\sigma(R)}$ ($\sigma(R)$ - argumentowość predykatu).

Spróbujmy zatem zdefiniować kongruencję na modelu zgodnie z intuicją.

Definicja 14.13. Niech $\mathcal{M}$ będzie dowolnym modelem języka L. Niech $\equiv$ będzie relacją równoważności taką, która zachowuje operacje (jak w poprzedniej definicji) i niech dodatkowo spełnia:

$$\forall_{R\in Rel_L} \begin{Bmatrix} a_1 \equiv a'_1 \\ a_2 \equiv a'_2 \\ ... \\ a_{m_k} \equiv a'_{m_k} \end{Bmatrix} \wedge (a_1, a_2, ..., a_{m_k}) \in R^{\mathcal{M}} \implies$$

$$\implies (a'_1, a'_2, ..., a'_{m_k}) \in R^{\mathcal{M}}$$

tj. kongruencja zachowuje relacje. Zdefiniujmy wtedy model ilorazowy

$$\mathcal{M}/_{\equiv} = \Big({}^{M}/_{\equiv}, \{c^{\mathcal{M}/_{\equiv}} : c \in Const_L\}, \{f^{\mathcal{M}/_{\equiv}} : f \in Fun_L\},$$

$$\{R^{\mathcal{M}/_{\equiv}} : R \in Rel_F\}\Big),$$

gdzie $c^{\mathcal{M}/_{\equiv}}, f^{\mathcal{M}/_{\equiv}}$ są jak w poprzedniej definicji oraz

$$({}^{a_1}/_{\equiv}, {}^{a_2}/_{\equiv}, ..., {}^{a_{\sigma(R)}}/_{\equiv}) \in R^{\mathcal{M}/_{\equiv}} \iff (a_1, a_2, ..., a_{\sigma(R)}) \in R^{\mathcal{M}}.$$

Definicja intuicyjnie wydaje się poprawna. Wzmocniliśmy kongruencje o zachowywanie relacji i podaliśmy relacje w modelu ilorazowym. Napotykamy się jednak na pewien istotny problem.

Niech $\phi : M \to N$ będzie epimorfizmem modelu $\mathcal{M}$ na $\mathcal{N}$. Niech $(a_1, a_2) \in \ker\phi \iff \phi(a_1) = \phi(a_2)$. Przypuśćmy, że $\ker\phi$ jest kongruencją w modelu $\mathcal{M}$. Jednakże zakłada to wtedy, że jeśli $\phi(a_1) = \phi(a_2)$, to $(a_1, *, ..., *) \in R^{\mathcal{M}} \iff (a_2, *, ..., *) \in R^{\mathcal{M}}$ dla dowolnej relacji R. Łatwo skonstruować odpowiedni kontrprzykład:

$$\phi : (\mathbb{Z}, +, \leqslant) \to (\{0\}, +, \leqslant)$$

Przekształcenie ϕ daje nam relację totalną i tym samym relacja $\leqslant$ musiałaby być totalna. Widzimy zatem, że nie jest to kongruencja w modelu relacyjnym. W takim przypadku pierwsze

twierdzenie o izomorfizmie nie jest prawdziwe, czyli nasz model ilorazowy nie zachowuje się zgodnie z oczekiwaniami.

Matematykiem jest, kto umie znajdować analogie między twierdzeniami, lepszym - kto widzi analogie między dowodami, jeszcze lepszym - kto dostrzega analogie miedzy teoriami, a można wyobrazić sobie i takiego, co widzi analogie między analogiami. Stefan Banach.

Dotychczas tworzyliśmy definicje poprzez analogie. Następnie w sposób analogiczny formułowaliśmy pierwsze twierdzenie o izomorfizmie, a na koniec w sposób analogiczny go dowodziliśmy. Niestety, nasza intuicja zawiodła nas w ostatnim kroku. Problem wynika z faktu, że nie dostrzegliśmy analogii między analogiami, która to pozwoliłaby nam poprawnie sformułować definicję kongruencji w dowolnych modelach.

Musimy zatem przyjrzeć się temu zagadnieniu od innej strony. Spróbujmy innymi drogami dojść do definicji kongruencji.

Na początku wykonamy następujące kroki: znajdziemy minimalny zestaw warunków, który definiuje kongruencję na strukturach algebraicznych, a następnie spróbujemy je zastosować do kongruencji na dowolnych strukturach.

Niech L będzie dowolnym językiem. Niech $\mathcal{M}$ będzie dowolnym modelem tego języka, a $\equiv$ relacją równoważności określoną na uniwersum tego modelu. Niech $\mathcal{N}$ będzie L-strukturą, której uniwersum jest zbiór ${}^{M}/_{\equiv}$.

Niech $f \in Fun_L$ będzie dowolnym symbolem funkcyjnym o n argumentach. Wybierzmy $a_1, a_2, ..., a_n \in M$. Wtedy:

$$f^{\mathcal{N}}({}^{a_1}/_{\equiv}, {}^{a_2}/_{\equiv}, ..., {}^{a_n}/_{\equiv}) = {}^{a}/_{\equiv}$$

dla pewnego $a \in M$. Weźmy $a'_1 \equiv a_1, a'_2 \equiv a_2, ..., a'_n \equiv a_n$. Wtedy:

$$f^{\mathcal{N}}({}^{a'_1}/_{\equiv}, {}^{a'_2}/_{\equiv}, ..., {}^{a'_n}/_{\equiv}) = {}^{a}/_{\equiv}$$

Widzimy zatem, że:

$$\forall_{f\in Fun_L} \left\{ \begin{array}{l} a_1 \equiv a_1' \\ a_2 \equiv a_2' \\ ... \\ a_n \equiv a_n' \end{array} \right\} \Longrightarrow$$
$$\Longrightarrow f^{\mathcal{N}}({}^{a_1}/_{\equiv}, {}^{a_2}/_{\equiv}, ..., {}^{a_n}/_{\equiv}) = f^{\mathcal{N}}({}^{a_1'}/_{\equiv}, {}^{a_2'}/_{\equiv}, ..., {}^{a_n'}/_{\equiv})$$

UWAGA! Warunek ten, choć bardzo podobny, nie jest równoważny z warunkiem kongruencji, ponieważ nie wynika z niego, że $f^{\mathcal{M}}(a_1, a_2, ..., a_n) \equiv a$. Wystarczy intuicyjne założenie, że przekształcenie kanoniczne jest homomorfizmem. Istotnie:

$$\kappa(f^{\mathcal{M}}(a_1, a_2, ..., a_n)) = f^{\mathcal{N}}(\kappa(a_1), \kappa(a_2), ..., \kappa(a_n)) =$$
$$= f^{\mathcal{N}}({}^{a_1}/_{\equiv}, {}^{a_2}/_{\equiv}, ..., {}^{a_n}/_{\equiv}) = {}^{a}/_{\equiv}$$

Widzimy więc, że założenie o homomorficzności κ wymusza na relacji $\equiv$ zachowywanie operacji.

Założyliśmy zatem następujące rzeczy: $\equiv$ jest relacją równoważności, uniwersum struktury ilorazowej jest zbiorem klas abstrakcji $\equiv$ oraz κ jest homomorfizmem. Te trzy warunki wystarczyły, by definicja kongruencji wyłoniła się w tej samej formie. Co więcej, możemy nawet nie definiować struktury ilorazowej explicite, lecz napisać twierdzenie jako:

Twierdzenie 14.14 (Pierwsze twierdzenie o izomorfizmie struktur algebraicznych)**.** *Niech L będzie dowolnym językiem, takim że $Rel_L = \emptyset$. Niech $\mathcal{A}, \mathcal{B}$ będą L-strukturami. Niech $\phi : A \to B$ będzie homomorfizmem suriektywnym. Wtedy* $\ker \phi = \{(a_1, a_2) \in A^2 : \phi(a_1) = \phi(a_2)\}$ *jest relacją równoważności na A oraz istnieje dokładnie jedna L-struktura $\mathcal{A}'$, taka że jej uniwersum stanowi zbiór klas abstrakcji relacji* $\ker \phi$*, przekształcenie $\kappa : a \mapsto {}^{a}/_{\equiv}$ jest homomorfizmem oraz $\mathcal{A}' \cong \mathcal{B}$. Ponadto istnieje dokładnie jedna funkcja ϕ^*, taka że $\phi = \phi^* \circ \kappa$.*

Przyjmując te same założenia, rozważmy teraz zachowanie relacji w modelu ilorazowym. Niech $R \in Rel_L$ będzie dowolnym

predykatem n-członowym. Wybierzmy $a_1, a_2, ..., a_n \in M$, takie że $({}^{a_1}/_{\equiv}, {}^{a_2}/_{\equiv}, ..., {}^{a_n}/_{\equiv}) \in R^{\mathcal{N}}$. Podobnie jak wcześniej weźmy $a'_1 \equiv a_1, a'_2 \equiv a_2, ..., a'_n \equiv a_n$, wtedy $({}^{a'_1}/_{\equiv}, {}^{a'_2}/_{\equiv}, ..., {}^{a'_n}/_{\equiv}) \in R^{\mathcal{N}}$. Uzyskujemy zatem:

$$\forall_{R \in Rel_L} \left\{ \begin{array}{l} a_1 \equiv a'_1 \\ a_2 \equiv a'_2 \\ ... \\ a_n \equiv a'_n \end{array} \right\} \Longrightarrow$$

$$\left(({}^{a_1}/_{\equiv}, {}^{a_2}/_{\equiv}, ..., {}^{a_n}/_{\equiv}) \in R^{\mathcal{N}} \iff ({}^{a'_1}/_{\equiv}, {}^{a'_2}/_{\equiv}, ..., {}^{a'_n}/_{\equiv}) \in R^{\mathcal{N}} \right)$$

Ponownie mamy słabszy warunek niż w kongruencji. Skorzystajmy teraz z homomorficzności κ.

$$(a_1, a_2, ..., a_n) \in R^{\mathcal{M}} \implies ({}^{a_1}/_{\equiv}, {}^{a_2}/_{\equiv}, ..., {}^{a_n}/_{\equiv}) \in R^{\mathcal{N}}$$

Widzimy zatem, że gdyby przepisać powyższe twierdzenie, dopuszczając predykaty w języku, uzyskamy inne twierdzenie niż pierwotnie formułowane, ponieważ nasze założenia są słabsze.

Twierdzenie 14.15 (Pierwsze twierdzenie o izomorfizmie modeli)**.** *Niech L będzie dowolnym językiem. Niech $\mathcal{M}, \mathcal{N}$ będą modelami tego języka. Niech $\phi : M \to N$ będzie homomorfizmem suriektywnym. Wtedy* $\ker \phi = \{(a_1, a_2) \in M^2 : \phi(a_1) = \phi(a_2)\}$ *jest relacją równoważności na M oraz istnieje dokładnie jedna L-struktura $\mathcal{M}'$, taka że jej uniwersum stanowi zbiór klas abstrakcji relacji* $\ker \phi$*, przekształcenie $\kappa : a \mapsto {}^{a}/_{\equiv}$ jest homomorfizmem oraz $\mathcal{M}' \cong \mathcal{N}$. Ponadto istnieje dokładnie jedna funkcja ϕ^*, taka że $\phi = \phi^* \circ \kappa$.*

Dowód. $\ker \phi$ jest relacją równoważności, ponieważ relacja równości nią jest. Definiujemy

$$\mathcal{M}' = \Big({}^{M}/_{\ker \phi}, \{c^{\mathcal{M}'} : c \in Const_L\}, \{f^{\mathcal{M}'} : f \in Fun_L\}, \{R^{\mathcal{M}'} : R \in Rel_L\} \Big)$$

w sposób następujący:

$$c^{\mathcal{M}'} = {}^{c^{\mathcal{M}}}/_{\ker\phi}$$
$$f^{\mathcal{M}'}({}^{x_1}/_{\ker\phi}, {}^{x_2}/_{\ker\phi}, ..., {}^{x_{\sigma(f)}}/_{\ker\phi}) = {}^{f^{\mathcal{M}}(x_1,x_2,...,x_{\sigma(f)})}/_{\ker\phi}$$

oraz $({}^{x_1}/_{\ker\phi}, {}^{x_2}/_{\ker\phi}, ..., {}^{x_{\sigma(R)}}/_{\ker\phi}) \in R^{\mathcal{M}'}$ wtedy i tylko wtedy, gdy:

$$(\phi(x_1), \phi(x_2), ..., \phi(x_{\sigma(R)})) \in R^{\mathcal{N}}.$$

Definicja stałych nie budzi wątpliwości co do poprawności, gdyż relacja równoważności wyznacza klasy abstrakcji jednoznacznie. Definicja operacji jest poprawna na mocy własności homomorfizmu ϕ. Istotnie, niech $(x_1, x_1') \in \ker\phi$, $(x_2, x_2') \in \ker\phi$, ..., $(x_{\sigma(f)}, x'_{\sigma(f)}) \in \ker\phi$.

$$\phi(f^{\mathcal{M}}(x_1, x_2, ..., x_{\sigma(f)})) = f^{\mathcal{N}}(\phi(x_1), \phi(x_2), ..., \phi(x_{\sigma(f)}))) =$$
$$= f^{\mathcal{N}}(\phi(x_1'), \phi(x_2'), ..., \phi(x'_{\sigma(f)}))) = \phi(f^{\mathcal{M}}(x_1', x_2', ..., x'_{\sigma(f)}))$$

Pozostaje przyjrzeć się definicji relacji, ale jest ona jednoznaczna z definicji $\ker\phi$.

Zdefiniowaliśmy poprawną L-strukturę. Pokażemy, że κ jest homomorfizmem. Udowodnimy ten fakt tylko dla relacji, gdyż stałe i operacje są tak samo zdefiniowane jak w twierdzeniu dla struktur algebraicznych. Weźmy:

$$(x_1, x_2, ..., x_{\sigma(R)}) \in R^{\mathcal{M}} \implies$$
$$(\phi(x_1), \phi(x_2), ..., \phi(x_{\sigma(R)})) \in R^{\mathcal{N}} \implies$$
$$({}^{x_1}/_{\ker\phi}, {}^{x_2}/_{\ker\phi}, ..., {}^{x_{\sigma(R)}}/_{\ker\phi}) \in R^{\mathcal{M}'}.$$

Niech $\phi^* : {}^{a}/_{\ker\phi} \mapsto \phi(a)$. Przekształcenie jest poprawnie określone na mocy definicji relacji. Jest to bijekcja, ponieważ każdy element N wyznacza dokładnie jedną klasę abstrakcji (korzystamy z suriektywności ϕ). Jest to również homomorfizm struktur algebraicznych na mocy poprzedniego twierdzenia. Wystarczy pokazać, iż jest to mocny homomorfizm ze względu na relacje. Homomorficzność wynika z samej definicji relacji. Niech

$(y_1, y_2, ..., y_{\sigma(R)}) \in R^{\mathcal{N}}$). Przekształcenie ϕ jest suriekcją, zatem mamy $y_1 = \phi(x_1), y_2 = \phi(x_2), ..., y_{\sigma(R)} = \phi(x_{\sigma(R)})$. Wystarczy wziąć klasy abstrakcji elementów $x_1, x_2, ..., x_{\sigma(R)}$.

Pokazaliśmy zatem, że jest to izomorfizm. Jednoznaczność pokazywaliśmy w wersji twierdzenia dla zbiorów. □

Podajmy zatem ostateczną definicję modelu ilorazowego.

Definicja 14.16. Niech L będzie dowolnym językiem, a $\mathcal{M}$ jego modelem. Niech ϕ będzie dowolnym homomorfizmem modelu $\mathcal{M}$. Modelem ilorazowym $\mathcal{M}/_{\phi}$ nazywamy L-strukturę, której uniwersum jest zbiór klas abstrakcji jądra tego homomorfizmu oraz przekształcenie $\kappa : m \mapsto m/_{\ker \phi}$ jest homomorfizmem.

Bibliografia

[1] Gorbunov V., *Algebraic Theory Of Quasivarieties*, Consultants Bureau, 1998

Funkcje Morse'a a rozkład rozmaitości na rączki

Marcin Sroka
Uniwersytet Jagielloński w Krakowie
Wydział Matematyki i Informatyki

W artykule przedstawimy ideę rozkładu gładkiej rozmaitości różniczkowej na tzw. „rączki" będące cegiełkami z których, jak się okazuje, można zbudować dowolną rozmaitość zamkniętą. Narzędziem, przy pomocy którego otrzymuje się wspomniany rozkład jest teoria funkcji Morse'a. Ukazuje ona związek między szczególnymi gładkimi funkcjami na rozmaitości a jej topologią. Przedstawioną w sposób skrócony i skondensowany teorię zobrazujemy dokładnie przeanalizowanym przykładem oraz licznymi ilustracjami.

15.1 Teoria funkcji Morse'a

Ten krótki paragraf stanowi niezbędne minimum dające aparat techniczny, który pozwoli nam w następnym paragrafie dokonać rozkładu rozmaitości na rączki. Rozpoczniemy, od podania definicji punktu krytycznego.

Definicja 15.1 (Punkt krytyczny i wartość krytyczna)**.** Dla gładkiej rozmaitości różniczkowej M wymiaru m (rozmaitość M w obrębie całego artykułu jest zamknięta tzn. zwarta i bez brzegu) oraz gładkiej (w obrębie całego artykułu gładki oznacza klasy C^∞) funkcji $f \in C^\infty(M)$, punkt $p \in M$ nazywamy *krytycznym* jeśli różniczka $d_p f : T_pM \to T_{f(p)}\mathbb{R} \cong \mathbb{R}$ wynosi 0. Natomiast

liczbę $a \in \mathbb{R}$ nazywamy *wartością krytyczną* (dla f) jeśli istnieje punkt krytyczny $p \in M$ taki, że $f(p) = a$.

Dla osób wolących pracowac w lokalnym układzie współrzędnych oznacza to, że w dowolnej mapie $\phi : U \to \mathbb{R}^m$ takiej, że $p \in U$ zachodzi:

$$\frac{\partial f}{\partial \phi_1}(p) = 0, \ ..., \ \frac{\partial f}{\partial \phi_m}(p) = 0.$$

Jak się okaże w niedalekiej przyszłości, funkcje Morse'a to takie o szczególnych punktach krytycznych. Aby być w stanie wysłowić jakie mają być te punkty krytyczne potrzebujemy pojęcia Hessianu.

Definicja 15.2 (Hessian w punkcie krytycznym)**.** Dla gładkiej funkcji $f \in C^\infty(M)$ (na gładkiej rozmaitości M wymiaru m), jej punktu krytycznego $p \in M$ i mapy $\phi : p \in U \to \mathbb{R}^m$ definiujemy Hessian:

$$\mathcal{H}_f^\phi(p) = [\frac{\partial^2 f}{\partial \phi_i \partial \phi_j}(p)]_{i,j \in \{1, ..., m\}}$$

Jako proste ćwiczenie pozostawiamy wykazanie, że Hessian w punkcie p zależy od wybranej mapy oraz że zależność ta jest następująca.

Wniosek 15.3. *Dla dwóch map jak w ostatniej definicji - ϕ i ψ zachodzi:*

$$\mathcal{H}_f^\phi(p) = J_{\psi \circ \phi^{-1}}(\phi(p))^T \mathcal{H}_f^\psi(p) J_{\psi \circ \phi^{-1}}(\phi(p)),$$

gdzie $J_{\psi \circ \phi^{-1}}(\phi(p))$ jest macierzą Jacobiego odwzorowania przejścia od ϕ do ψ w punkcie $\phi(p)$.

Dzięki temu, że jakobian odwzorowania przejścia jest niezerowy, poprzednia uwaga pozwala nam wprowadzić definicję niezdegenerowanego punktu krytycznego bez obaw o jej zależność od wybranej mapy.

Definicja 15.4 (Niezdegenerowany punkt krytyczny)**.** Niech M będzie gładką rozmaitością wymiaru m, zaś $f \in C^\infty(M)$ – funkcją gładką. Jej punkt krytyczny $p \in M$ nazwiemy *niezdegenerowanym* jeśli

$$\det \mathcal{H}_f^\phi(p) \neq 0$$

dla jakiejś (równoważnie każdej) mapy $\phi : p \in U \to \mathbb{R}^m$.

Przyszedł moment aby wysłowić zapowiedzianą definicję funkcji Morse'a.

Definicja 15.5 (Funkcja Morse'a)**.** Gładką funkcję $f \in C^\infty(M)$ (na gładkiej rozmaitości M) nazywamy *funkcją Morse'a*, jeśli każdy jej punkt krytyczny jest niezdegenerowany.

Na pierwszy rzut oka nie widać celu badania właśnie takich funkcji. Aby stał się on jasny musimy poczekać do paragrafu 2, gdzie przedstawiona zostanie procedura odtwarzania rozmaitości przy pomocy punktów krytycznych funkcji Morse'a. Chwilowo musimy natomiast zadowolić się następującym lematem, pokazującym jak szczególną lokalną postać musi przyjmować dowolna funkcja Morse'a.

Twierdzenie 15.6 (Lemat Morse'a)**.** *Niech $f \in C^\infty(M)$ będzie gładką funkcją na rozmaitości M wymiaru m, zaś $p \in M$ będzie jej niezdegenerowanym punktem krytycznym. Wówczas istnieje mapa ϕ taka, że $\phi(p) = 0$ oraz:*

$$\left(f \circ \phi^{-1}\right)(x) = -x_1^2 - ... - x_\lambda^2 + x_{\lambda+1}^2 + ... + x_m^2 + f(p).$$

Czytelnika ciekawego dowodu odsyłamy po elementarny acz technicznie uciążliwy dowód do [1, 2]. Okazuje się, że liczba minusów w kanonicznej postaci z poprzedniego lematu jest równa indeksowi (liczbie minusów na przekątej po diagonalizacji) Hessianu, apriori w zalezności od wybranej mapy. Dzięki 15.3 wybór mapy nie wpływa na jednak otrzymany wynik, a to pozwala nam sformułować kolejną definicję.

Definicja 15.7 (Indeks niezdegenerowanego punktu krytycznego)**.** W sytuacji z poprzedniego lematu λ (niezalezna od rozważanej mapy) jest nazywana *indeksem* punktu p.

Łatwo otrzymujemy nastepujący wniosek z 15.6 (prawdziwy nawet dla niezwartej rozmaitości).

Wniosek 15.8. *Niezdegenerowane punkty krytyczne gładkiej funkcji $f \in C^\infty(M)$ na rozmaitości M są izolowane.*

Wynika z tego, że w dziedzinie mapy jak w 15.6 nie ma innych punktów krytycznych niezdegenerowanych. Jeśli natomiast będziemy zakładać zwartość M, to z poprzedniej uwagi łatwo wywnioskować następujący wniosek:

Wniosek 15.9. *Gładka funkcja $f \in C^\infty(M)$ na zwartej rozmaitości M ma skończenie wiele niezdegenerowanych punktów krytycznych.*

Dotychczas wyliczyliśmy wiele własności funkcji Morse'a. W szczególności wydawać by się mogło, że skoro spełniają one 15.6, to kwestia ich istnienia może byc sprawa kłopotliwą. Nic bardziej mylnego. Okazuje się bowiem, że wystepują one na każdej rozmaitości tak gęsto, jak tylko można sobie tego życzyć.

Twierdzenie 15.10 (Aproksymacja funkcjami Morse'a)**.** *Niech M będzie zamkniętą rozmaitością wymiaru m, zaś $g \in C^\infty(M)$ funkcja gładką. Wówczas dla każdego $\epsilon > 0$ istnieje funkcja Morse'a ϵ-blisko funkcji g.*

Oczywiście wymagałoby wyjaśnienia co oznacza sformułowanie ϵ-blisko użyte w wypowiedzi ostatniego twierdzenia. Nie będzie to jednak istotne w naszych rozważaniach i spokojnie można uważać, że oznacza ono ϵ-blisko w normie supremum (w pewnym sensie tak musi być). Po tym, jak zagwarantowaliśmy sobie istnienie interesujących nas obiektów, przytoczymy jeszcze jedno twierdzenie na temat „poprawiania" funkcji Morse'a.

Twierdzenie 15.11. *Niech M będzie gładką rozmaitością wymiaru m, zaś $f \in C^\infty(M)$ funkcją Morse'a której wszystkimi punktami krytycznymi są: p_0, ..., p_n. Wówczas istnieje funkcja Morse'a g, której wszystkimi punktami krytycznymi są: p_0, ..., p_n oraz*

$$g(x_i) \neq g(x_j), \quad i \neq j.$$

W powyższym twierdzeniu (podobnie jak poprzednio) można dodatkowo zarządać, aby uzyskana funkcja g spełniała tezę i była dowolnie blisko funkcji f.

15.2 Rozkład rozmaitości na rączki

Zajmiemy się teraz zapowiedzianym w poprzednim paragrafie odtwarzaniem rozmaitości ze zdefiniowanej na niej funkcji Morse'a. Pomocna w ścisłym zrozumieniu niektórych rozumowań będzie wiedza z zakresu rozmaitości z brzegiem, po którą odsyłamy do [4]. Przypomnijmy, że interesować nas będą rozmaitości zamknięte M tzn. zwarte i bez brzegu. Ustalmy funkcję Morse'a $f : M \to \mathbb{R}$ jak w 15.11 (tzn. taką, która różnym punktom krytycznym przypisuje różne wartości). Oznaczmy:

$$M_t = \{p \in M \mid f(p) \leqslant t\}.$$

Naszym zasadniczmym celem jest zbadanie, jak zmienia się M_t wraz z t. Pierwszym wynikiem z tego zakresu jest nastepujące twierdzenie.

Twierdzenie 15.12. *Jeśli f nie ma wartości krytycznych w $[a, b]$ dla $a, b \in \mathbb{R}$ takich, że $a < b$, to rozmaitości (z brzegiem) M_a i M_b są dyfeomorficzne.*

Jeśli czytelnik uwierzy (lub sprawdzi), że funkcja wysokości (rzutowanie na oś z) na sferze dwuwymiarowej S^2 zanurzonej w $\mathbb{R}^3$ jest funkcją Morse'a, to według ostaniego twierdzenia wszystkie S^2 po usunięciu „czapeczki" są dyfeomorficzne, niezaleznie od tego jak wysoką „czapeczkę" weźmiemy. Ostatnie twierdzenie mówi nam także, że zmiana w kształcie M_t nastepuje tylko podczas przechodzenia przez wartość krytyczną. Zbadamy teraz, jak dokładnie ta zmiana wygląda. Załóżmy, że f jest funkcją Morse'a o punktach krytycznych:

$$p_0, \ ..., \ p_n,$$

które spełniają ponadto:

$$f(p_0) < \ ... < \ f(p_n).$$

Natychmiast widzimy, że $f(p_0)$ musi być minimum funkcji f, gdyż jako funkcja ciągła takowe osiąga na zwartym M. Ponadto (wobec tego, że funkcja jest gładka) jej lokalne minima muszą być punktami krytycznymi. Zupełnie analogiczne rozumowanie pokazuje, że $f(p_n)$ jest najwiekszą wartością f.

Wiadomo, że dla każdego $t < f(p_0)$ mamy $M_t = \emptyset$. Wybierzmy mapę ϕ dla f i p_0, jak w 15.6. Indeks p_0 musi wynosić 0, inaczej nie byłby lokalnym minimum, co wynika z tego jaką postać ma f w tej mapie (patrz 15.6). Wówczas:

$$\left(f \circ \phi^{-1}\right)(x) = x_1^2 + ... + x_m^2 + f(p_0),$$

a zatem:

$$\phi(M_{f(p_0)+\epsilon}) = D^m(0, \epsilon)$$

(jako że mapy są zawsze dyfeomorfizmami, $M_{f(p_0)+\epsilon}$ jest dyfeomorficzne z m-wymiarowym dyskiem $D^m(0, \epsilon)$) dla ϵ tak małego, aby $D^m(0, \epsilon)$ był zawarty w obrazie mapy. W przypadku dowolnego punktu krytycznego p_i o indeksie 0 pojawia się wówczas m-wymiarowy dysk, zaś $\boldsymbol{M_{f(p_i)+\epsilon}}$ **jest dyfeomorficzne z** $\boldsymbol{M_{f(p_i)-\epsilon} \sqcup D^m(0,1)}$.

Dysk m-wymiarowy nazywamy w tym kontekście *0-rączką*. Przechodząc do rozważań drugiego ekstremum, dla $t > f(p_n)$ mamy oczywiście $M = M_t$. W mapie ψ ponownie wybranej jak w 15.6 dla punktu p_n mamy:

$$f \circ \psi(x) = -x_1^2 - ... - x_m^2 + f(p_n).$$

$M = M_{f(p_n)+\epsilon}$ otrzymuje się zatem z $M_{f(p_n)-\epsilon}$ poprzez nakrycie obiektem dyfeomorficznym z $D^m(0, \epsilon)$, doklejonym wzdłuż brzegu $M_{f(p_n)-\epsilon}$ (brzeg ten jest dyfeomorficzny z $S^{m-1}(0, \epsilon)$). W tym przypadku m-wymiarowy dysk nazywamy *m-rączką*. *0-rączka* i *m-rączka* są tym samym obiektem tzn. m wymiarowym dyskiem $D^m(0, 1)$, różnią się jednak zasadniczo sposobem doklejania. Pierwsza z nich jest zawsze dostawiana obok rozmaitości, druga pełni rolę „czapeczki" zakrywającej dziurę.

Bez wdawania się w dalsze szczegóły (o których można przeczytać w [1]), m-wymiarową *λ-rączką* nazywamy zbiór

$D^\lambda(0,1) \times D^{m-\lambda}(0,1)$ doklejany zawsze wzdłuż $S^{\lambda-1}(0,1) \times D^{m-\lambda}(0,1)$. Prawdziwe jest także nastepujące twierdzenie, dające pełny obraz tego, jak zmienia się M_t, podczas gdy t przechodzi przez wartość krytyczną.

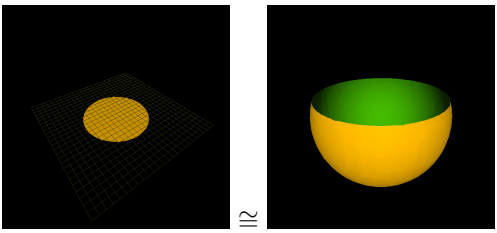
Twierdzenie 15.13. *Jeśli p_i jest punktem krytycznym o indeksie λ, to*

$$\boldsymbol{M_{f(p_i)+\epsilon} \text{ jest dyfeomorficzne z } M_{f(p_i)-\epsilon} \uplus D^\lambda(0,1) \times D^{m-\lambda}(0,1),}$$

gdzie symbol $\uplus$ oznacza doklejanie λ-rączki do brzegu $M_{f(p_i)-\epsilon}$.

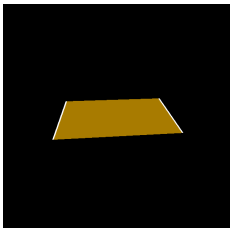
Dla zobrazowania dotychczasowych rozważań prześledzimy, jak przedstawiona procedura działa w przypadku dwuwymiarowego torusa T^2. Jako że jest to rozmaitość dwuwymiarowa, to musimy zdać sobie sprawę, jak wyglądają rączki w drugim wymiarze. Poniżej przedstawiamy ilustracje 0-rączki, 1-rączki i 2-rączki.

0-rączka



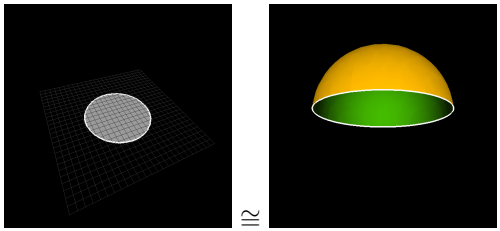
Rysunek 15.1: Najlepiej wyobrażać sobie *0-rączkę* jako „miskę" w $\mathbb{R}^3$.

1-rączka



Rysunek 15.2: *1-rączka* czyli $D^1(0,1) \times D^1(0,1)$ jest dyfeomorficzna z prostokątem. Doklejamy ją zawsze wzdłuż zaznaczonych na rysunku na biało dwóch z jej czterech boków.

2-rączka



Rysunek 15.3: *2-rączkę*, czyli $D^2 \times D^0$, utożsamiamy z „czapeczką" zanurzoną w $\mathbb{R}^3$. Zaznaczony biały okrąg $S^1 \times D^0$ służy do jej doklejania

Wracając do torusa T^2 załóżmy, że jego równanie w $\mathbb{R}^3$ to:

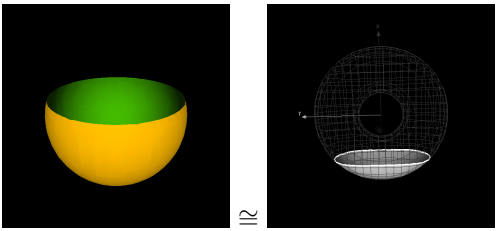
$$\left((x^2+y^2)^{\frac{1}{2}} - 2\right)^2 + z^2 = 1 \text{ (torus leży)}.$$

Funkcją Morse'a jest w tym przypadku projekcja na oś x tzn. odwzorowanie

$$f : T^2 \ni (x,y,z) \mapsto x \in \mathbb{R}$$

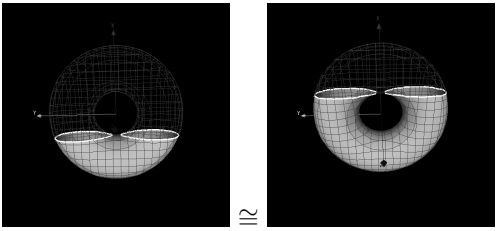
(udowodnienie tego faktu zostawiamy jako ćwiczenie). Posiada ona cztery punkty krytyczne $p = (-3,0,0)$, $q = (-1,0,0)$, $r =$

$(1,0,0)$, $s = (3,0,0)$. Punkt p jest punktem, w którym funkcja osiąga minimum, zatem ma on indeks 0.



Rysunek 15.4: Przechodząc przez wartość $f(p)$ dodajemy do zbioru pustego 0-rączkę, czyli tworzymy sumę rozłączną zbioru pustego z „miską".

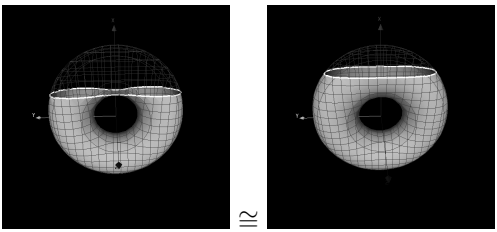
Przechodząc przez wartość dla q (którego indeks wynosi 1) zmuszeni jesteśmy dokleić 1-rączkę do zaznaczonego na poprzednim rysunku białym kolorem okręgu, w taki sposób by utworzyć „koszyczek".



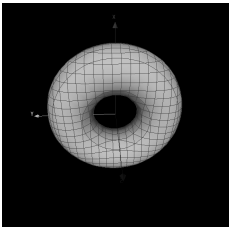
Rysunek 15.5: Rysunek po lewej to właśnie „koszyczek" z dość spłaszczoną rączką. Jest on oczywiście dyfeomorficzny z częścią torusa pokazaną po prawej.

Punkt r także jest indeksu 1, więc ponownie zmuszeni jesteśmy dokleić 1-rączkę. Brzeg 1-rączki, czyli dwa odcinki trzeba dokleić do brzegu z ostatniego rysunku, czyli dwóch okręgów.

Na koniec, przechodząc przez maksimum funkcji f (czyli $f(r)$) doklejamy 2-rączkę.



Rysunek 15.6: Doklejanie 1-rączki można porównać do budowy mostu między dwoma ramionami fragmentu torusa, który zbudowaliśmy dotychczas.



Rysunek 15.7: Doklejanie 2-rączki polega na zaklejeniu dziury w torusie z ostatniego kroku „czapeczką" wzdłuż zaznaczonego na biało okręgu.

Wróćmy na chwilę do ogólnej procedury odtwarzania rozmaitości z funkcji Morse'a. Łatwo zauważyć, że zachodzi następujące twierdzenie:

Twierdzenie 15.14 (Rozkład rozmaitości na rączki)**.** *Funkcja Morse'a f pozwala utworzyć rozmaitość poprzez doklejania kolejnych rączek, która jest dyfeomorficzna z wyjściową M.*

15.3 Twierdzenie Reeba

Proces odtwarzania rozmaitości z funkcji Morse'a jest pomocny w dowodzie nastepującego faktu:

Twierdzenie 15.15 (Reeb)**.** *Niech M będzie zamkniętą rozmaitością wymiaru m, zaś $f \in C^\infty(M)$ – funkcją Morse'a. Jeśli f ma dokładnie dwa punkty krytyczne, to M jest homeomorficzna z S^m.*

Polecamy spróbować udowodnić powyższy fakt przy pomocy 15.12 oraz faktu, że homeomorfizm między sferami można zawsze rozszerzyć do homeomorfizmu między dyskami, które te sfery ograniczają. Po narzuceniu pewnego ograniczenia na wymiar, można udowodnić nawet więcej.

Twierdzenie 15.16. *Niech M będzie zamkniętą rozmaitością wymiaru $m \leqslant 6$, zaś $f \in C^\infty(M)$ – funkcją Morse'a z dokładnie dwoma punktami krytycznymi. Wówczas M jest dyfeomorficzna z S^m.*

Dowód jest identyczny jak poprzednio, z tą różnicą że w wymiarach nie większych od 6 także dyfeomorfizm między sferami można rozszerzyć do dyfeomorfizmu między dyskami. Jak wykazał J. Milnor w swej słynnej pracy [3], w ogólności twierdzenie to jest nieprawdziwe. Uczynił on to, konstruując rozmaitość homeomorficzną, ale nie dyfeomorficzną z S^7, na której istnieje funkcja Morse'a z dokładnie dwoma punktami krytycznymi.

Bibliografia

[1] Y. Matsumoto, *An Introduction to Morse Theory*, Providence: Rhode Island, AMS, 2002.

[2] J. Milnor, *Morse Theory*, Princeton University Press, 1969.

[3] J. Milnor, *On manifolds homeomorphic to the 7-sphere*, Ann. of Math., 64, 399-405, 1956.

[4] L. W. Tu, *An Introduction to Manifolds*, New York, Springer, 2013.

Nieuczesane myśli topologa

Agnieszka Stelmaszyk
Uniwersytet im. Adama Mickiewicza w Poznaniu
Wydział Matematyki i Informatyki

16.1 Wstęp

W salonie fryzjerskim siedzi matematyk, obok połyskująca para nożyczek, mnóstwo szczotek i innych sprzętów. Nerwowo wierci się w fotelu – przecież nie od dziś wie, że sfery zaczesać się nie da. Fryzjer intuicyjnie sięga po nożyczki, szalejące nad czołem rozmaitości nie rokują zbyt dobrze. Niechętny rozspójnieniu klient wpada na pomysł – warkocz będzie idealny!

U progu XX wieku Artin wprowadził do topologii kolejną dziedzinę (pozornie) blisko związaną z codziennością. Teoria warkoczy znajduje szerokie zastosowania między innymi w biologii i kryptografii, a także w teorii węzłów. Niniejszy artykuł stanowi elementarne zaproszenie do rozważań tego zagadnienia przedstawiając niezbędne definicje i fakty odnośnie struktury grup warkoczy oraz klasyczne algorytmy czesania.

Zachęcam do aktywnego czytania - większość przekształceń można zbadać empirycznie, wystarczą cztery kawałki sznurka.

16.2 Warkocz matematyczny

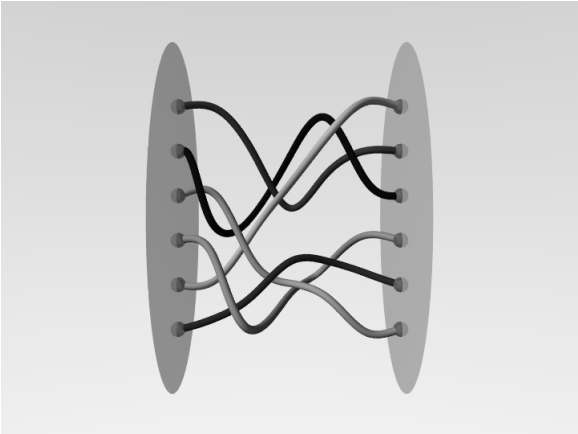
Rozpatrzmy dysk i wybierzmy na nim n punktów $p_1, p_2, \ldots, p_n \in \mathbb{D}$.

Definicja 16.1. Warkoczem geometrycznym β o n pasmach nazywamy układ

$$\beta = (b_1, b_2, \ldots, b_n)$$

n ścieżek $b_i : \mathbb{I} \longrightarrow \mathbb{I} \times \mathbb{D}$ spełniających warunki:

- $b_i(0) = (0, p_i) \quad \forall i \in \{1, 2, \ldots, n\}$,
- $\exists$ permutacja $\sigma \in S_n$ taka, że $b_i(1) = (1, p_{\sigma(i)})$, nazywamy ją **permutacją indukowaną** przez warkocz β,
- $b_i(t) \in \{t\} \times \mathbb{D} \quad \forall t \in \mathbb{I}$.



Rysunek 16.1: Zanurzenie warkocza w walcu.

Nie ma potrzeby rozróżniać układu ścieżek od ich obrazów zanurzonych w walcu $\mathbb{D} \times \mathbb{I}$, zatem jako warkocz możemy traktować układ:

$$\beta = (b_1(\mathbb{I}), b_2(\mathbb{I}), \ldots, b_n(\mathbb{I})).$$

Wobec tego pierwsze dwa warunki gwarantują, że początki i końce ścieżek znajdują się na podstawach, trzeci natomiast, że w trakcie „splatania" ścieżki nie opuszczą walca.

Wprowadzimy teraz w zbiorze warkoczy relację równoważności opisaną przy pomocy izotopii, czyli homotopii złożonej z zanurzeń.

Definicja 16.2. Izotopią pomiędzy warkoczami geometrycznymi β i γ o n włóknach (pasmach) nazywamy układ

$$\mathbf{F} = (F_1, F_2, \ldots, F_n)$$

n ciągłych odwzorowań $F_i : \mathbb{I} \times \mathbb{I} \to \mathbb{I} \times \mathbb{D}$ o własnościach:

- $\forall t \in \mathbb{I} \quad \{F_i(\{t\} \times \mathbb{I})\}_{i=1,2,\ldots,n}$ jest geometrycznym warkoczem o n pasmach,
- $\{F_i(\{0\} \times \mathbb{I})\}_{i=1,2,\ldots,n} = \beta$,
- $\{F_i(\{1\} \times \mathbb{I})\}_{i=1,2,\ldots,n} = \gamma$.

Wobec tego dwa warkocze uznamy za równoważne, jeśli jeden powstaje z drugiego poprzez powyginanie pasm. Końce pozostają nieruszone, więc permutacja indukowana jest niezmiennikiem warkoczy. Klasy abstrakcji w tej relacji nazywamy **warkoczami** lub **n-warkoczami**.

16.3 Struktura grupy

W zbiorze warkoczy na określonej liczbie pasm wprowadzamy działanie odpowiadające złożeniu warkoczy. Intuicyjnie można je rozumieć jako przedłużenie jednego warkocza drugim poprzez związanie pasm.

Niech β i γ będą warkoczami geometrycznymi o n pasmach z permutacjami σ i τ odpowiednio.

Definicja 16.3. Złożeniem (związaniem) β i γ nazywamy n-warkocz $\delta = \beta * \gamma$

$$\delta = (d_1, d_2, \ldots, d_n),$$

gdzie

$$d_i(t) = \begin{cases} b_i(2t) & t \in [0, \frac{1}{2}] \\ c_{\sigma(i)}(2t-1) & t \in [\frac{1}{2}, 1] \end{cases}$$

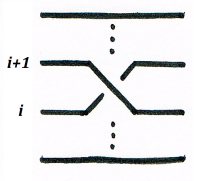
Permutacją indukowaną przez γ jest złożenie permutacji $\tau \cdot \sigma$.

Nietrudno sprawdzić, że tak określone składanie warkoczy jest dobrze określone i spełnia aksjomaty grupy (istnienie elementu neutralnego i elementów przeciwnych oraz łączność) – wynika to wprost z definicji, ponieważ jest to tradycyjne określenie mnożenia dróg zaczerpnięte z teorii homotopii.

Twierdzenie 16.4. *Zbiór warkoczy na n-pasmach wraz z działaniem składania tworzy grupę B_n. Nie jest to grupa abelowa.*

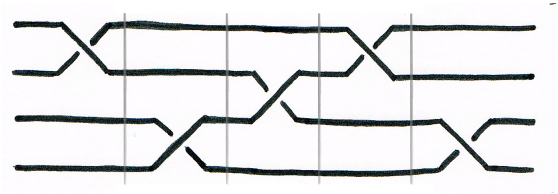
Aby usystematyzować opis warkoczy, wprowadza się tak zwane warkocze elementarne.

Definicja 16.5. Warkoczem elementarnym σ_i nazywamy warkocz, w którym $(i+1)$-sze pasmo przecina i-te ponad nim, a pozostałe pasma są proste.



Rysunek 16.2: Warkocz elementarny

Odpowiednio „rozluźniając" sploty, możemy każdy warkocz przedstawić w postaci słów odpowiadających złożeniom warkoczy elementarnych.



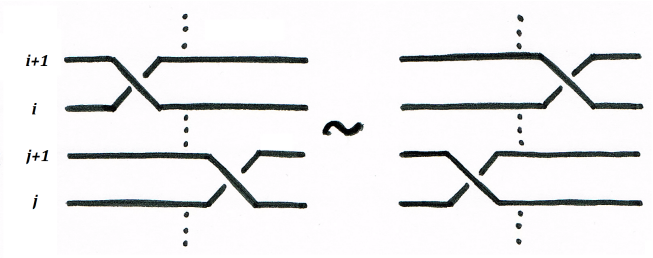
Rysunek 16.3: Przedstawienie warkocza za pomocą słów; na rysunku warkocz. $\sigma_3\sigma_1^{-1}\sigma_2^{-1}\sigma_3\sigma_1$

Twierdzenie 16.6. *(Artin, Magnus) Warkocze elementarne*

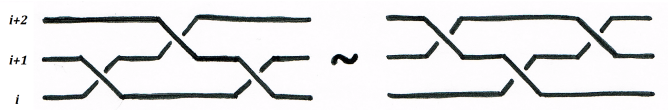
$$\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$$

tworzą zbiór generatorów grupy B_n. Zupełny zbiór relacji jest dany przez:

- $\sigma_i\sigma_j = \sigma_j\sigma_i$, *gdzie* $|i-j| > 1$



- $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$, *gdzie* $1 \leqslant 1 \leqslant n-2$



Co ciekawe taka reprezentacja, z pozoru wygodniejsza, nastręcza pewnych trudności. Mając dwa słowa możemy rozstrzy-

gnąć, czy reprezentują ten sam warkocz, niestety powyższe twierdzenie jest niekonstruktywne, więc nie wyjaśnia w jaki sposób takie słowa uzyskać.

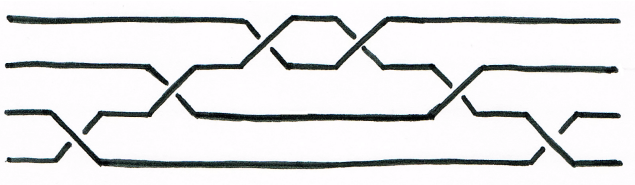
16.4 Problem słów - algorytmy

Problem słów w kombinatorycznej teorii grup jest zagadnieniem polegającym na rozstrzygnięciu, czy dany element jest równoważny elementowi neutralnemu. W dalszej części przyjrzymy się metodom rozstrzygającym go. Przedstawione algorytmy mają wysoką złożoność i w praktyce raczej ustępują miejsca innym.

Definicja 16.7. Warkocz nazywamy **czystym**, gdy indukuje trywialną permutację. Innymi słowy warkocze czyste są jądrem homomorfizmu $B_n \longrightarrow S_n$ i tę podgrupę oznaczamy przez P_n.

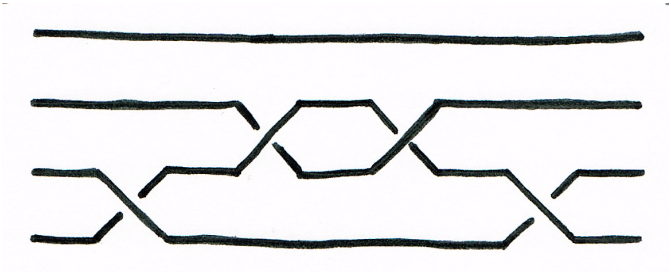
16.4.1 Grzebień Artina

W 1926 roku ukazał się artykuł autorstwa Artina *„Theorie der Zöpfe”*, w którym przedstawił algorytm „czesania” warkoczy. Weźmy n-warkocz czysty β (innych nie ma sensu rozpatrywać - nie mogą być równoważne warkoczowi trywialnemu) i rozczeszmy go:



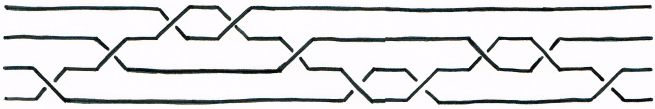
Rysunek 16.4: Warkocz β.

KROK 1: Tworzymy kopię warkocza β i usuwamy z niej pierwsze pasmo zastępując je prostym, otrzymany w ten sposób warkocz nazywamy γ_1.

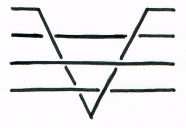


Rysunek 16.5: γ_1

KROK 2: Składamy $\beta\gamma_1^{-1} = \alpha_1$ i redukujemy zgodnie ze zbiorem relacji. Nasz wyjściowy warkocz możemy zapisać jako $\beta = \alpha_1\gamma_1$, napinamy wszystkie pasma poza pierwszym, wówczas pierwsza część warkocza jest „wyczesana".



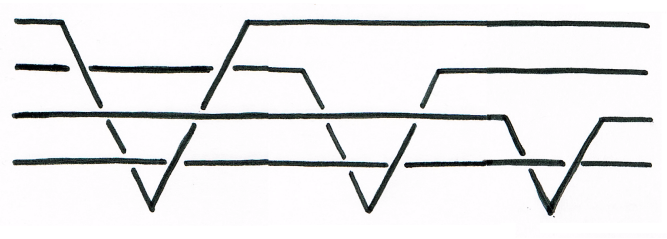
Rysunek 16.6: $\alpha_1 = \beta\gamma_1^{-1}$



Rysunek 16.7: Warkocz α_1 po naciągnięciu pasm.

KROK 3: Procedurę opisaną w krokach 1 i 2 powtarzamy dla warkocza γ_1.

KROK 4: Po odpowiedniej liczbie powtórzeń otrzymujemy rozkład $\beta = \alpha_1 \dots \alpha_{n-1}$, w którym każdy z segmentów α_i jest „wyczesany"



Twierdzenie 16.8 (Artin)**.** *Niech A_k oznacza zbiór uczesanych k-warkoczy, takich, że usunięcie ostatniego pasma utworzy warkocz trywialny na $(k-1)$ pasmach. Dla każdego $k > 0$ A_k jest wolną grupą o zbiorze generatorów danym przez elementy*

$$a_i = (\sigma_{k-1}\sigma_{k-2}\dots\sigma_{i+1})\sigma_i^2(\sigma_{i+1}^{-1}\sigma_{i+2}^{-1}\dots\sigma_{k-1}^{-1}) \quad 1 \leqslant i \leqslant k-1$$

Twierdzenie 16.9. *(Artin) Warkocz $\beta = \alpha_1\alpha_2\dots\alpha_n$, gdzie warkocze α_i otrzymane są w sposób zaprezentowany wcześniej jest trywialny wtedy i tylko wtedy, gdy każdy α_i jest trywialny.*

Definicja 16.10. Postacią normalną nazywamy „wyczesaną" formę warkocza. Dla każdego warkocza istnieje dokładnie jeden „wyczesany" warkocz, w którym wszystkie α_i są zredukowane zgodnie z relacjami.

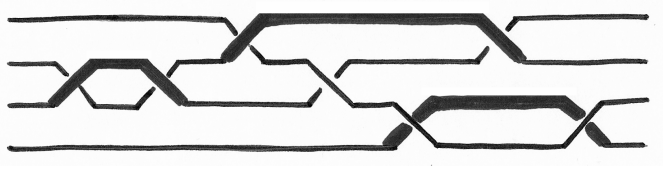
16.4.2 Redukcja rączek

Przyjrzymy się teraz drugiej metodzie rozstrzygania problemu słów zaproponowanej przez Dehornoy'a w 1997 roku. Redukcja rączek polega na wskazaniu podwarkoczy określonego typu - rączek, które stopniowo opuszczane za pomocą pewnego homomorfizmu rozplatają warkocz, a tym samym pozwalają na sprawdzenie jego trywialności. Podobnie jak poprzednio rozpatrywać będziemy warkocze czyste.

Definicja 16.11. Rączką nazywamy podwarkocz (podsłowo) postaci

$$\sigma_i^e x \sigma_i^{-e}$$

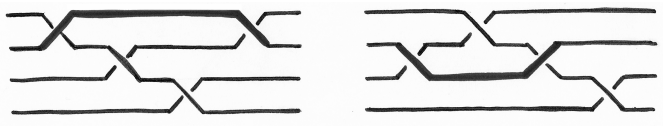
gdzie $e = \pm 1$, a x złożony jest tylko z generatorów $\sigma_j^{\pm 1}$ przy $j < i$.



Rysunek 16.8: Rączki.

Dla dowolnego $1 \leqslant i \leqslant n$ określamy homomorfizm $\phi_i : B_n \to B_n$ w następujący sposób:

- $\sigma_i^{\pm 1} \mapsto 1$
- $\sigma_{i-1}^{\pm 1} \mapsto \sigma_{i-1}^{-e} \sigma_i^{\pm 1} \sigma_{i-1}^{e}$
- $\sigma_j \mapsto \sigma_j \quad j \neq i-1, i$



Rysunek 16.9: Rączka przed i po redukcji.

Twierdzenie 16.12. *(Dehornoy) Redukcja rączek przekształca słowo warkocza w słowo równoważne. Jeśli słowo warkocza nie zawiera rączek, to albo jest puste, albo nie jest równoważne z identycznością.*

Twierdzenie 16.13. *(Dehornoy) Algorytm redukcji rączek zawsze się kończy.*

Bibliografia

[1] Artin E., *Theory of braids*, Annals of Mathematics (1947), 2nd Ser., 48 (1): 101–126

[2] Dalvit E., *New proposals for the popularization of braid theory*, praca magisterska, dostępna na `http://science.unitn.it/ dalvit/ docs/PopularizationBraids.pdf`

[3] Pawałowski K., *Wielomiany Jonesa węzłów i splotów*, Uniwersytet im. Adama Mickiewicza, 2013.

[4] Smeltzer R., *Linear Representations of Braid Groups*, praca magisterska, dostępna na `http://ms.mcmaster.ca/ boden/students/Smeltzer-MSc.pdf`

[5] `http://matematita.science.unitn.it/braids/index.html`

[6] `http://www.math.unicaen.fr/tressapp/`

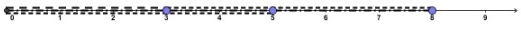
Krótka wycieczka od 2+2 do ciał wirtualnych

Tomasz Stroiński
Uniwersytet im. Adama Mickiewicza w Poznaniu
Wydział Matematyki i Informatyki

Poniższy artykuł ma na celu krótkie wprowadzenie do tematyki ciał wirtualnych, które są klasami abstrakcji pewnej relacji określonej na przestrzeni składającej się z par podzbiorów wypukłych, domkniętych, ograniczonych i niepustych przestrzeni liczb rzeczywistych. Jeżeli w poniższym artykule nie zostanie wspomniane inaczej przestrzeń X jest przestrzenią $\mathbb{R}^2$. W większości przypadków można przestrzeń tę uogólnić, lecz może to powodować pewne problemy i uniemożliwić intuicyjne pojmowanie nowych pojęć.

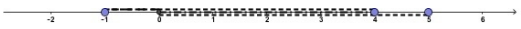
Naszą wycieczkę zaczynamy od $2 + 2$, czyli dodawania liczb naturalnych. Jest ono zgodnie z nazwą najbardziej naturalnym działaniem, którego uczymy się już na samym początku naszej przygody z matematyką. Każdą z liczb naturalnych możemy zamienić na odpowiednio wiele obiektów, a wynikiem dodawania tych liczb będzie wspólna liczebność wszystkich obiektów. Weźmy na przykład $3 + 5$, możemy to rozumieć jako standardowe zadanie ze szkoły podstawowej – „Jaś ma 3 jabłka, Małgosia ma 5 jabłek, ile jabłek mają razem?" Oczywiście, gdy najpierw wspomnimy ile jabłek ma Małgosia, a dopiero potem ile jabłek ma Jaś, to razem będą mieli tyle samo, ale adekwatnym zapisem liczbowym tej sytuacji będzie $5 + 3$.

Dodawanie liczb naturalnych możemy wizualnie przedstawić także w inny sposób, rzec by można – bardziej profesjonalnie. Weźmy więc oś liczbową, zaznaczmy na niej zero i jeden. Następnie zaznaczając taką samą odległość jak od zera do jedynki, zaznaczmy od jedynki w drugą stronę, w ten sposób zaznaczymy dwójkę. Postępując tak dalej jesteśmy w stanie wskazać każdą liczbę naturalną. Jeżeli teraz wybraną liczbę utożsamimy z odcinkiem łączącym ten punkt na osi liczbowej z zerem, to możemy odpowiednio przedstawić dodawanie liczb naturalnych, jako przesunięcie jednego z odcinków tak, aby jego lewy koniec pokrywał się z prawym końcem drugiego. Wynikiem takiego dodawania będzie prawy koniec otrzymanego w ten sposób odcinka. Przykładowo $3 + 5$ jest przesunięciem odcinka $[0, 5]$, na koniec odcinka $[0, 3]$. Otrzymamy w ten sposób odcinek $[0, 3+5]$, a więc rzeczywiście prawy koniec jest sumą tych dwóch liczb.



Rysunek 17.1: $3 + 5$ jako suma odcinków

Podobnie jak działanie dodawania na liczbach naturalnych, tak samo na liczbach całkowitych dodawanie możemy traktować jako przesunięcie odpowiednich odcinków na osi liczbowej. Tym razem jednak należy zwrócić szczególną uwagę na odpowiednie położenie tych odcinków względem siebie, gdyż dopuszczamy teraz również wartości ujemne.



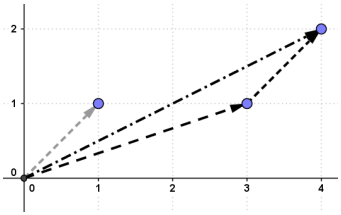
Rysunek 17.2: $-1 + 5$ jako suma odcinków

Skoro jesteśmy na wycieczce, to przydałaby się jakaś mapa. Gdy weźmiemy takową do ręki – niech to będzie na przykład mapa fizyczna Polski – wówczas zauważymy pewną siatkę nałożoną na mapę, która pozwala za pomocą dwóch liczb określić dokładnie, o którym miejscu w Polsce wspominamy. Jest to tzw.

siatka współrzędnych geograficznych. W podobny sposób możemy mówić o parach liczb całkowitych.

Stwórzmy kartezjański układ współrzędnych ustawiając prostopadle do siebie dwie osi liczbowe, tak aby przecinały się w zerze na obu osiach. Wówczas rysując proste równoległe do osi, tak aby przecinały one drugą z osi w wartościach całkowitych uzyskamy podobną siatkę jak na mapie. Przecięcia tak stworzonych linii utożsamiać możemy z parami liczb całkowitych. Załóżmy, że przy zapisie (a, b) wartość a odpowiada liczbie całkowitej z poziomej osi, natomiast wartość b odpowiada liczbie całkowitej z pionowej osi. Wówczas para (a, b) odpowiada punktowi, który jest przecięciem wyżej wspomnianych prostych przechodzących przez liczby a i b.

Oczywiście pary liczb całkowitych możemy dodawać, wykonując działanie po współrzędnych, tzn. $(a, b) + (c, d) = (a + c, b + d)$. Możemy jednak traktować pary liczb całkowitych jako punkty na płaszczyźnie, wówczas dodanie dwóch takich punktów możemy utożsamiać z dodawaniem odpowiednich wektorów zaczepionych w punkcie $(0, 0)$, a kończących się w punktach będącymi składnikami sumy. Dodanie tych wektorów przebiega analogicznie jak w przypadku dodawania odcinków w poprzednich sytuacjach – początek jednego z wektorów przesuwamy na koniec drugiego. Wówczas koniec tego przesuwanego odpowiada wartości sumy. Jako przykład dodajmy do siebie $(3, 1) + (1, 1)$.



Rysunek 17.3: $(3, 1) + (1, 1)$ jako suma wektorów

Oczywiście, w tym miejscu moglibyśmy podążyć dalej, zastanawiając się nad dodawaniem par liczb wymiernych, czy rzeczywistych. Sądzę, że takie przeformułowanie powyższych rozumowań jest warte polecenia, jeżeli rozważamy samodzielne wędrówki. Jednak czymże byłaby dobra wycieczka, jeżeli przeszlibyśmy tylko po trasie, która jest wszystkim doskonale znana i wielokrotnie przemierzona? Spróbujmy zejść z tej poznanej trasy i wyruszmy w obszary, które być może są niektórym znane, ale zapewne większość z osób w pewnym momencie skręciła w inne rejony matematyki.
Załóżmy, że zamiast dodawać do siebie pary liczb całkowitych dodajemy zbiory jednoelementowe składające się z par liczb całkowitych. Chcielibyśmy, aby takie działanie w wyniku również dawało nam zbiór jednoelementowy składający się z pary liczb całkowitych, która będzie sumą wcześniej wspomnianych par. Oczywiście suma mnogościowa $A \cup B$ nie spełnia naszych wymagań, bo $\{(a,b)\} \cup \{(c,d)\} = \{(a,b),(c,d)\} \neq \{(a+c,b+d)\}$, gdy $(a,b) \neq (c,d) \neq (0,0)$.

Spójrzmy na drogowskaz, na nim bowiem spisana jest pewna definicja:

Definicja 17.1. Niech X będzie przestrzenią liniową nad $\mathbb{R}$ oraz $A, B \subset X$. Wówczas działanie dodawania Minkowskiego definiujemy wzorem

$$A + B = \{a + b : a \in A, b \in B\}.$$

Sprawdźmy, czy dodawanie Minkowskiego spełnia nasze wymagania wobec działania na zbiorach. Rozpatrzmy przykład, który jest przeformułowaniem rozpatrywanych już punktów. Niech $A = \{(3,2)\}, B = \{(1,1)\}$. Stosując definicję mamy $A + B = \{(3,2) + (1,1)\} = \{(4,3)\}$. Zatem otrzymaliśmy oczekiwany wynik. Zauważmy, że żaden dodatkowy element nie może powstać, ponieważ nie ma więcej elementów w zbiorach A i B. Mamy więc działanie, które możemy rozpatrywać jako uogólnienie zwykłego dodawania par liczb całkowitych. Rozpatrzmy, jak będzie zachowywać się suma Minkowskiego, gdy składnikami nie będą

wyłącznie zbiory jednoelementowe. Jednak zanim do tego przejdziemy, zauważmy, że możemy traktować $A+B$ jako przesunięcie zbioru A o wektor utożsamiany z parą liczb całkowitych $(1,1)$ i analogicznie jako przesunięcie zbioru B o wektor utożsamiany z parą liczb całkowitych $(3,2)$. Możemy zatem wyciągnąć pewien wniosek, który jest pierwszą własnością przedstawionego działania

Wniosek 17.2. *Jeżeli jeden z elementów sumy Minkowskiego jest zbiorem jednoelementowym, to $A+B$ możemy obliczyć przesuwając o wektor utożsamiany z elementem zbioru jednoelementowego drugi zbiór, tzn.*

$A + \{(a,b)\}$ *jest zbiorem A przesuniętym o wektor* $[(0,0),(a,b)]$

Powracając do wspomnianej idei – należałoby rozszerzyć jeden ze zbiorów do przynajmniej dwóch elementów. Niech zatem zbiór A będzie zbiorem składającym się z dwóch elementów, a zbiór B zbiorem jednoelementowym. Korzystając z pierwszej własności możemy utożsamić $A+B$ z przesunięciem zbioru A o odpowiedni wektor odpowiadający elementowi ze zbioru B.
Jednak popatrzmy na zbiór dwuelementowy jako zbiór, który posiada dwa wektory. Zatem chcąc dodać taki zbiór powinniśmy postępować następująco – wziąć drugi zbiór, najpierw przesunąć go o jeden z wektorów odpowiadający pierwszemu elementowi ze zbioru dwuelementowego, a następnie o drugi wektor. Jako sumę Minkowskiego rozpatrzyć sumę mnogościową tak powstałych zbiorów. Otrzymujemy w ten sposób prosty wniosek – jeżeli zbiory są przeliczalne, to schematem postępowania jest przesunięcie drugiego zbioru o wszystkie wektory odpowiadające elementom z pierwszego zbioru, a następnie skorzystać z sumy mnogościowej, aby uzyskać ostateczny wynik.

$$A + B = \bigcup_{b \in B} A + \{b\}$$

Pozostaje więc zastanowić się, co stanie się, gdy zbiory będą nieprzeliczalne. W skrócie poniżej będziemy mówić o zbiorach nieskończonych, mając na myśli zbiory nieprzeliczalne.

Załóżmy, że zbiór A jest nieskończony, zaś B – jednoelementowy. Wówczas chcąc obliczyć sumę $A + B$ z definicji, otrzymamy zbiór złożony z nieskończonej liczby sum. Oczywiście liczenie wszystkich sum jest nieefektywne, zatem powinniśmy znaleźć sposób, aby uzyskać odpowiedni wynik w skończonej liczbie kroków. W tym celu warto poznać takie pojęcia jak zbiór wypukły, powłoka wypukła, czy też punkty ekstremalne. Jednak wrócimy do tego za chwilę, ponieważ problem dodawania zbioru nieskończonego i jednoelementowego staje się łatwy do rozwiązania, gdy skorzystamy z własności przesunięcia zbioru, gdy dodajemy do niego zbiór jednoelementowy. Wówczas fakt, że zbiór A jest nieskończony nie wpływa na nasz sposób postępowania. Zatem jeden ze sposobów obliczenia takiej sumy znamy. Przygotujmy się do poznania innego.

Definicja 17.3. Zbiór A nazywamy **zbiorem wypukłym**, jeżeli spełniony jest warunek:

$$\forall_{\alpha\in[0,1]}\ \alpha A + (1-\alpha)A = A$$

Równoważnie, jeżeli dla dowolnych $a, b \in A$ odcinek $[a, b] = \{\alpha a + (1-\alpha)b : \alpha \in [0, 1]\}$ jest zawarty w zbiorze A.

Powłoką wypukłą zbioru A nazywamy zbiór:

$$\operatorname{conv}(A) = \{\sum_{i=1}^{n} \alpha_i a_i :\ \alpha_i \in \mathbb{R}_+,\ a_i \in A,\ \sum_{i=1}^{n} \alpha_i = 1,\ n \in \mathbb{N}\}.$$

Definicja 17.4. Niech $B \subset A$. Podzbiór ten nazywamy **ekstremalnym**, jeżeli z warunku, że dla dowolnego $a, b \in A$ i pewnego $t \in (0, 1)$ zachodzi $ta + (1-t)b \in B$ wynika fakt, że $a, b \in B$. Jeżeli $\{x\}$ jest podzbiorem ekstremalnym dla pewnego $x \in A$, to punkt x nazywamy **punktem ekstremalnym** zbioru A. Zdefiniujmy zbiór

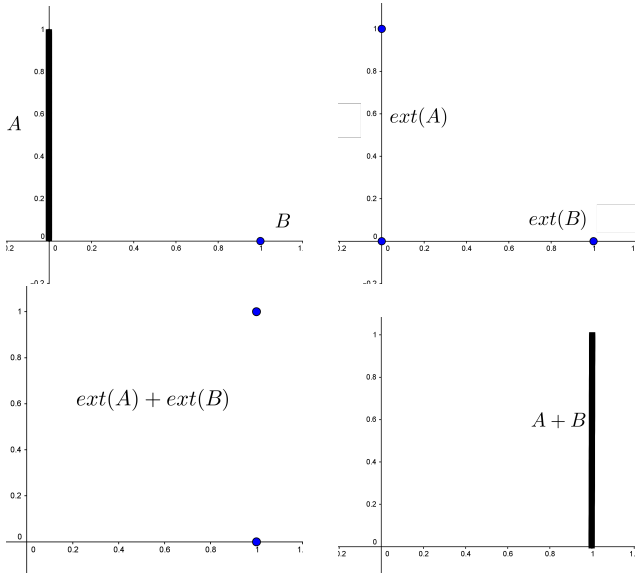
$$\operatorname{ext}(A) = \{a \in A : a - \text{punkt ekstremalny zbioru } A\ \}$$

(tzw. **zbiór punktów ekstremalnych** zbioru A).

Powróćmy teraz do naszego zagadnienia. Zbiór A jest nieskończony, a zbiór B jest jednoelementowy. Możemy użyć pewnej własności sumy Minkowskiego dotyczącej zbiorów wypukłych, domkniętych, ograniczonych i zwartych:

$$A + B = \text{conv}(\text{ext}(A) + \text{ext}(B)). \tag{17.1}$$

Aby dobrze zobrazować wzór 17.1 na przykładzie, niech $A = [(0,0),(0,1)], B = \{(1,0)\}$. Wówczas jeżeli A jest odcinkiem, a B punktem, to $\text{ext}(A)$ jest zbiorem dwuelementowym, do którego dodajemy zbiór jednoelementowy. Otrzymaną w ten sposób sumę uwypuklamy uzyskując sumę, którą pierwotnie chcieliśmy obliczyć. Spójrzmy na rysunek 17.4.



Rysunek 17.4: Zastosowanie wzoru 17.1.

Niech teraz zbiory A i B będą zbiorami nieskończonymi. Możemy uzyskać ich sumę, wykorzystując zbiory ekstremalne, zsumować je, a następnie policzyć z nich powłokę wypukłą. Zastanówmy się jednak, co uzyskalibyśmy, jeżeli znajdujemy się na płaszczyźnie i gdybyśmy chcieli skorzystać w tym przypadku z własności przesuwania zbioru. Niech zbiorami A i B są prostopadłe odcinki o długości jeden, mające jeden punkt wspólny – środek układu współrzędnych. Wówczas przesuwamy jeden z odcinków o wektory odpowiadające każdemu z tych wektorów, które odpowiadają punktom z drugiego odcinka. Rysując kolejne takie przesunięcia zauważyć możemy, że tak właściwie takie dodawanie odcinków utożsamiane jest z przesunięciem jednego odcinka po drugim.

Jednak w powyższym przykładzie ukryta jest pewna bardzo ważna informacja, która być może nie jest widoczna na pierwszy rzut oka. $(0,0) \in A, B$ co powoduje, że rzeczywiście możemy w ten sposób przesuwać. Jeżeli zbiory A i B są odcinkami, które nie zawierają punktu $(0,0)$, to ich dodawanie do siebie również jest pewnym przesuwaniem, lecz nie jednego odcinka po drugim, ponieważ należy przesuwać o odpowiednie wektory, które w tym przypadku odsuwają sumę od składników. Jeżeli jednak rozpatrzymy na moment zbiór A jako odcinek A z dodanym punktem $(0,0)$, wówczas możemy cały ten zbiór przesuwać (zachowując odpowiednie odległości) po zbiorze B, chwytając za punkt $(0,0)$ i to właśnie nim przesuwać się po zbiorze B. Wówczas ślad jaki zakreśli zbiór A jest sumą $A + B$. Nie jest to łatwo sobie wyobrazić, jednak jak dowiemy się później – nie jest to konieczne z praktycznego punktu widzenia, lecz warto o tym pamiętać.

Zanim przejdziemy do własności sumy Minkowskiego podsumujmy jakie omówiliśmy dwie najprostsze metody (poza definicją) na obliczanie sumy Minkowskiego dwóch zbiorów.

- Możemy zastosować wzór $A + B = \mathrm{conv}(\mathrm{ext}(A) + \mathrm{ext}(B))$, co w przypadku wielokątów sprawi, że dodawać będziemy

dwa przeliczalne zbiory punktów, co umiemy wykonać poprzez odpowiednie przesuwanie jednego ze zbiorów o wektory odpowiadające elementom drugiego zbioru.

- Możemy odpowiednio „chwycić" jeden ze zbiorów w punkcie $(0,0)$ (nawet, gdy nie należy on do zbioru) i przesunąć go w każdy punkt drugiego zbioru.

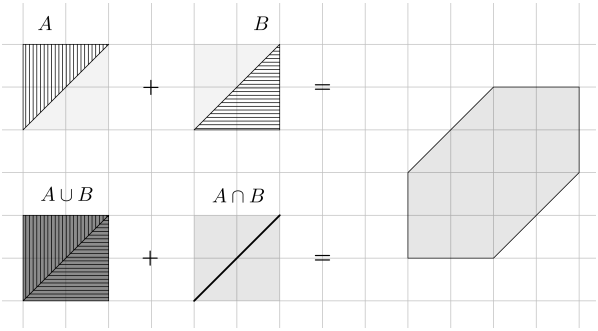
Druga z metod byłaby użyteczniejsza, gdybyśmy mogli „chwycić" jeden ze zbiorów w dowolnym jego punkcie. Zajmiemy się tym zagadnieniem, jednak wcześniej przypomnijmy poznane już nieoczywiste własności sumy Minkowskiego, gdy A i B są wypukłe, domknięte, ograniczone i zwarte:

- $A + \{a\}$ jest zbiorem A przesuniętym o wektor odpowiadający a,
- $A + B = \mathrm{conv}(\mathrm{ext}(A) + \mathrm{ext}(B))$.

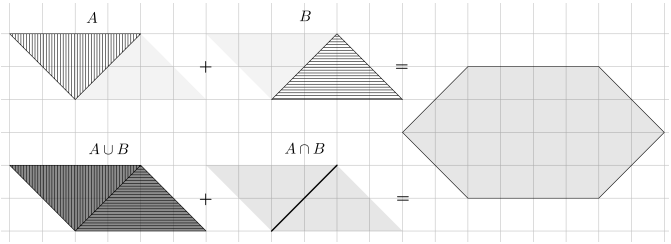
Zauważyć powinniśmy, że suma Minkowskiego dla dowolnego zbioru i zbioru jednoelementowego to nic innego jak translacja tego zbioru o odpowiedni wektor. Jeżeli więc dodajemy zbiór jednoelementowy, który zawiera tylko element neutralny dla zwykłego dodawania elementów, wówczas taki zbiór jest także elementem neutralnym dla dodawania Minkowskiego. Zatem dwa zbiory jednoelementowe, których suma Minkowskiego jest elementem neutralnym mogą być dodawane w dowolnym momencie do każdej sumy. Zauważmy, że gdy oznaczymy sobie te zbiory jako A_1 i A_{-1} możemy zapisać $A + B = A + B + A_1 + A_{-1} = A + A_1 + B + A_{-1} = ((A + A_1) + B) + A_{-1}$, ponieważ suma Minkowskiego jest przemienna i łączna. Oznacza to, że jeden ze składników sumy możemy dowolnie przesunąć, o ile obliczoną sumę również przesuniemy, ale o wektor przeciwny. Pozwala nam to na stwierdzenie, że dla dodawania Minkowskiego położenie składników nie jest czynnikiem, który wpływa na kształt sumy. Możemy zatem przesunąć jeden ze zbiorów tak, aby zawierał punkt $(0,0)$, jeżeli sumę przesuniemy o wektor przeciwny. Rozwiązaliśmy zatem problem „chwytania" zbioru w punkcie $(0,0)$.

Przejdźmy do kolejnej własności, a zarazem metody obliczania sumy Minkowskiego. Rozpatrywaliśmy już, że suma Minkowskiego i suma mnogościowa tych samych zbiorów różnią się między sobą. Jeżeli przyjrzymy się dokładnie poniższemu rysunkowi 17.5 zauważymy, że istnieje pewna zależność między sumą Minkowskiego, a sumą mnogościową, którą, o ile $A \cup B, A \cap B, A$ i B są zbiorami wypukłymi, możemy zapisać następująco:

$$A \cup B + A \cap B = A + B.$$



(a) Dwa trójkąty tworzą kwadrat, a jego przekątna jest przekrojem.



(b) Dwa trójkąty tworzą równoległobok.

Rysunek 17.5: Zastosowanie wzoru $A \cup B + A \cap B = A + B$

Przypomnijmy sobie jednak, jaki jest cel naszej wycieczki – ciała wirtualne. Należałoby zatem wkroczyć na ścieżkę, która doprowadzi nas do nich. Przygotujmy się do tej wyprawy należycie wyposażając się w odpowiednie oznaczenia.

Definiujemy następujące rodziny zbiorów:

$$\begin{aligned} B(X) &= \{A \subset X : A - \text{ wypukły, domknięty, ograniczony, niepusty }\} \\ K(X) &= \{A \in B(X) : A - \text{ zwarty }\}. \end{aligned}$$

Oczywiście dla $X = \mathbb{R}^n$ zachodzi $B(X) = K(X)$, co wynika z twierdzenia Heinego-Borela.

Niech $A \subset X$, jeżeli zbiór $A = \text{conv}(\{x_1, \ldots, x_n\})$ dla pewnych $x_1, \ldots, x_n \in X$, to zbiór A nazywamy wielościanem wypukłym.

Definiujemy następującą rodzinę zbiorów

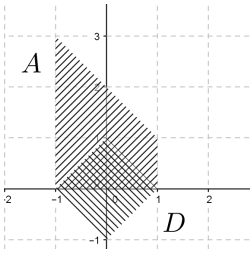
$$P(\mathbb{R}^n) = \{A \in K(\mathbb{R}^n) : A - \text{ wielościan wypukły }\}.$$

Nie bez powodu na wstępie zaczynaliśmy od liczb całkowitych, a później przechodziliśmy do par liczb całkowitych. Teraz będziemy chcieli wykonać podobny manewr przy użyciu zbiorów z $B(\mathbb{R}^n)$. Czyli rozpatrywać będziemy pary zbiorów postaci (A, B), gdzie $A, B \in B(\mathbb{R}^n)$.

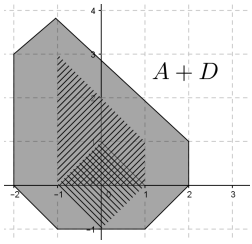
Mając tak przygotowane pary zbiorów ustalmy, że

$$(A, B) \sim (C, D) \Leftrightarrow A + D = B + C.$$

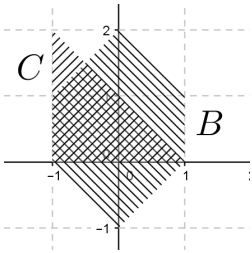
Jest to relacja równoważności, wobec czego otrzymujemy pewne klasy abstrakcji. Zauważyć możemy pewną analogię do ułamków, bo przecież $\frac{a}{b} = \frac{c}{d} \Leftrightarrow a \cdot d = b \cdot c$. Spójrzmy na przykładzie (rysunek 17.6) jak działa powyższa relacja.



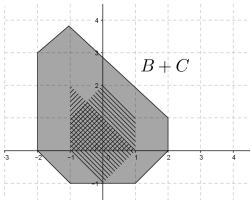
(a) Zbiory A i D



(b) Zbiór $A + D$



(c) Zbiory B i C



(d) Zbiór $B + C$

Rysunek 17.6: Relacja równoważności $(A, B) \sim (C, D)$.

Gdy droga stawała się coraz cięższa, gdy zaczynało brakować prowiantu, a i zapasy wody zaczynały się kończyć, wydawało się, że wyprawa musi skończyć się niepowodzeniem. Lecz choć nie było to oczywiste, to cel znajdował się tuż za rogiem. Taki tekst moglibyśmy usłyszeć z ust barda, który chciałby opisać naszą wycieczkę, bowiem mamy już wszystko co nam potrzebne, aby móc ją zakończyć sukcesem.

Definicja 17.5. Element $[A, B]_\sim$ przestrzeni wektorowej $B^2(\mathbb{R}^n)/_\sim$ nazywamy **ciałem wirtualnym**.
Element $[A, B]_\sim$ przestrzeni wektorowej $P^2(\mathbb{R}^n)/_\sim$ nazywamy **wielościanem wirtualnym**.

To już koniec wędrówki, mogę jedynie z tego miejsca polecić piękne ścieżki, których początek jest w miejscu, w którym stoimy. Jednak to jest temat na zupełnie inną historię.

Kongruencje na liczbach harmonicznych i ich uogólnienia

Marcin Szweda
Politechnika Śląska

Przedstawiona będzie historia tematu (sięgająca XIX wieku), współczesne wyniki i kierunki badań. Naświetlony będzie wkład własny, uwzględniający kongruencje na klasycznych, a nade wszystko uogólnionych liczbach harmonicznych. Omówione będą pewne aspekty zastosowań. Na zakończenie, przypomnijmy, że jak udowodnił J. C. Lagarias, hipoteza Riemanna jest równoważna pewnej nierówności na liczbach harmonicznych. Z kolei z asymptotyką liczb harmonicznych związana jest stała Eulera!

18.1 Liczby harmoniczne – definicje i klasyczne wyniki

Definicja 18.1. n-tą (uogólnioną) liczbą harmoniczną rzędu α nazywamy sumę

$$H_n^{(\alpha)} = \sum_{k=1}^{n} \frac{1}{k^\alpha}.$$

W szczególności jeśli $\alpha = 1$, to liczbę $\sum_{k=1}^{n} \frac{1}{k}$ nazywamy **n-tą liczbą harmoniczną** i oznaczamy H_n.

Na początek przypomnę kilka klasycznych wyników:

1. Leonhard Euler podał następujący wzór:

$$H_n = \int_0^1 \frac{1-x^n}{1-x} dx,$$

który wynika łatwo z tożsamości $\frac{1-x^n}{1-x} = 1+x+\ldots+x^{n-1}$.

2. Liczba $\gamma = \lim\limits_{n\to\infty} (H_n - \ln n) \approx 0.5772$ oznacza stałą Eulera-Mascheroniego. Do dzisiaj nie wiemy, czy liczba ta jest wymierna.

3. W 2010 roku Polak – Stefan Czekalski – przedstawił nieoczekiwany wzór, w którym liczba γ jest sumą szeregu o składnikach wymiernych:

$$1-\gamma = \frac{1}{4} + \sum_{n=2}^{\infty} \frac{1}{n(n+1)} \begin{vmatrix} 1 & \frac{1}{2} & \frac{1}{3} & \ldots & \frac{1}{n} \\ 0 & 1 & \frac{1}{2} & \ldots & \frac{1}{n-1} \\ 0 & 0 & 1 & \ldots & \frac{1}{n-2} \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & \ldots & \frac{1}{2} \\ \frac{1}{2} & \frac{2}{3} & \frac{3}{4} & \ldots & \frac{n}{n+1} \end{vmatrix}.$$

4. Tożsamość:

$$H_n = \psi(n+1) + \gamma$$

pozwala uogólnić liczby harmoniczne na indeksy zespolone, gdyż funkcja psi $\psi(x) = \frac{\Gamma'(x)}{\Gamma(x)}$ (zwana też digammą) określona jest dla $x \in \mathcal{C} \setminus \{0, -1, -2, \ldots\}$.

5. Zachodzi następująca zależność: $\sum\limits_{k=1}^{n} H_k = (n+1)H_{n+1} - (n+1)$,

6. Liczby harmoniczne związane są również z liczbami Stir-

linga[1] pierwszego rodzaju poprzez następujące tożsamości:

$$H_n = \frac{1}{n!}\begin{bmatrix} n+1 \\ 2 \end{bmatrix}, \quad \begin{bmatrix} n+1 \\ 3 \end{bmatrix} = \frac{n!}{2}(H_n^2 - H_n^{(2)}),$$

$$\begin{bmatrix} n+1 \\ 4 \end{bmatrix} = \frac{n!}{6}(H_n^3 - 3H_n H_n^{(2)} + 2H_n^{(3)}), \text{ itd.}$$

Dowód. W książce Donalda Knutha [6] można znaleźć dowód analityczny zależności: $H_n = \frac{1}{n!}\left[\begin{smallmatrix} n+1 \\ 2 \end{smallmatrix}\right]$. Można ją jednak łatwo wykazać w sposób kombinatoryczny:

$$\begin{aligned}\begin{bmatrix} n+1 \\ 2 \end{bmatrix} &= \frac{1}{2}\sum_{k=1}^{n}\binom{n+1}{k}\begin{bmatrix} k \\ 1 \end{bmatrix}\begin{bmatrix} n+1-k \\ 1 \end{bmatrix} = \\ &= \frac{1}{2}\sum_{k=1}^{n}\frac{(n+1)!}{k!(n+1-k)!}\cdot(k-1)!\cdot(n-k)! = \\ &= \frac{n!}{2}\sum_{k=1}^{n}\frac{n+1}{k(n+1-k)} = \frac{n!}{2}\sum_{k=1}^{n}\left(\frac{1}{k}+\frac{1}{n+1-k}\right) = n!H_n.\end{aligned}$$

W podobny sposób można udowodnić tożsamość $\left[\begin{smallmatrix} n+1 \\ 3 \end{smallmatrix}\right] = \frac{n!}{2}(H_n^2 - H_n^{(2)})$:

$$\begin{aligned}\begin{bmatrix} n+1 \\ 3 \end{bmatrix} &= \frac{1}{3}\sum_{k=1}^{n-1}\binom{n+1}{k}\begin{bmatrix} k \\ 1 \end{bmatrix}\begin{bmatrix} n+1-k \\ 2 \end{bmatrix} = \\ &= \frac{1}{3}\sum_{k=1}^{n-1}\frac{(n+1)!}{k!(n+1-k)!}\cdot(k-1)!\cdot(n-k)!H_{n-k} = \\ &= \frac{n!}{3}\sum_{k=1}^{n-1}\frac{n+1}{k(n+1-k)}H_{n-k} = \\ &= \frac{n!}{3}\sum_{k=1}^{n-1}\left(\frac{1}{k}+\frac{1}{n+1-k}\right)H_{n-k}.\end{aligned}$$

[1]Liczby Stirlinga pierwszego rodzaju opisują liczbę tych permutacji na n elementach, które rozkładają się dokładnie na k rozłącznych cykli. Oznacza się je symbolem $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]$.

Zauważmy, że zachodzi równość:

$$\sum_{k=1}^{n-1} \frac{1}{n+1-k} H_{n-k} = \sum_{1 \leqslant i < j \leqslant n} \frac{1}{ij} = \frac{1}{2}\left(H_n^2 - H_n^{(2)}\right).$$

Indukcyjnie można pokazać, że prawdziwa jest zależność:

$$\sum_{k=1}^{n-1} \frac{H_{n-k}}{k} = H_n^2 - H_n^{(2)}.$$

Z powyższych równości otrzymujemy tezę:

$$\begin{bmatrix} n+1 \\ 3 \end{bmatrix} = \frac{n!}{2}\left(H_n^2 - H_n^{(2)}\right).$$

□

7. Istnieje wiele zależności wiążących liczbę π z liczbami harmonicznymi, np.:

$$\sum_{n=1}^{\infty} \frac{H_n}{n \cdot 2^n} = \frac{\pi^2}{12}, \qquad \sum_{n=1}^{\infty} \frac{H_n}{n^3} = \frac{5}{4}\zeta(4) = \frac{\pi^4}{72}.$$

18.2 Kongruencje na liczbach harmonicznych

Poniższa definicja stanowi rozszerzenie na liczby wymierne pojęcia kongruencji dla liczb naturalnych.

Definicja 18.2. Niech $x, y \in \mathbb{Q}$ oraz $m \in \mathbb{N}$. Powiemy, że x przystaje do y modulo m, jeśli różnica tych liczb wyrażona jako ułamek nieskracalny jest postaci: $\frac{mp}{q}$, czyli $\gcd(q, mp) = 1$.

Powyższą definicję możemy zapisać symbolicznie w postaci:

$$x \equiv y \pmod{m} \;\Leftrightarrow\; \exists p, q \in \mathbb{N}\colon\ \gcd(q, mp) = 1 \text{ i } |x - y| = m \cdot \frac{p}{q}.$$

Będziemy też używali oznaczenia $x \equiv_m y$, które jest równoważne zapisowi $x \equiv y \pmod{m}$.

Przykład 18.3. *Powyższą definicję zilustrujemy następującymi przykładami:*

$$\begin{aligned}
\frac{1}{2} &\equiv_7 4, \quad bo \quad \left|\frac{1}{2}-4\right| = \frac{7}{2},\\
\frac{1}{4} &\equiv_7 2, \quad bo \quad \left|\frac{1}{4}-2\right| = \frac{7}{4},\\
\frac{1}{3} &\equiv_8 3, \quad bo \quad \left|\frac{1}{3}-3\right| = \frac{8}{3}.
\end{aligned}$$

18.2.1 Twierdzenie Wolstenholme'a

Joseph Wolstenholme[2] w pracy: *On certain properties of prime numbers* z 1862 roku, udowodnił następujące twierdzenie:

Twierdzenie 18.4. *Niech $\mathbb{P}$ oznacza zbiór liczb pierwszych. Dla $p \in \mathbb{P}$, $p \geqslant 5$ zachodzą następujące kongruencje:*

$$H_{p-1} \equiv 0 \pmod{p^2}, \quad H_{p-1}^{(2)} \equiv 0 \pmod{p}.$$

W dalszej części tej pracy będziemy korzystać wielokrotnie z powyższego rezultatu. Stanowi on też punkt wyjścia do prezentowanych poniżej wyników własnych.

Przykładowo dla $p = 7$ mamy:

$$H_6 = \frac{7^2}{20} \equiv 0 \pmod{7^2}, \qquad H_6^{(2)} = \frac{7 \cdot 13 \cdot 59}{3600} \equiv 0 \pmod{7}.$$

Pytanie 1. *Czy istnieją liczby pierwsze p, dla których mamy:*

$$H_{p-1} \equiv 0 \pmod{p^3}.$$

Okazuje się, że pierwszą liczbą $p \in \mathbb{P}$, dla której powyższa kongruencja jest prawdziwa jest $p = 16\,843$ i jest to 1944 liczba pierwsza!

[2] Joseph Wolstenholme (30.09.1829 – 18.11.1891) – matematyk angielski.

Pytanie 2. *Podobnie możemy zapytać, czy istnieją liczby pierwsze p, dla których mamy:*

$$H_{p-1}^{(2)} \equiv 0 \pmod{p^2}.$$

Okazuje się, że pierwszą liczbą $p \in \mathbb{P}$, która spełnia powyższą kongruencję znów jest $p = 16\,843$.

18.2.2 Odkryte tożsamości

1. Dla $p \in \mathbb{P}$, $p \geqslant 5$, mamy $\displaystyle\sum_{k=1}^{p-1} \frac{H_k}{k} \equiv 0 \pmod{p}$,

   Dowód. Zauważmy, że zachodzi równość:

   $$\sum_{k=1}^{p-1} \left(H_k - \frac{1}{k}\right)^2 - \sum_{k=1}^{p-1} H_k^2 - \sum_{k=1}^{p-1} \frac{1}{k^2} = -2\sum_{k=1}^{p-1} \frac{H_k}{k}.$$

   Istotnie, ponieważ $H_k - \frac{1}{k} = H_{k-1}$ oraz $H_{p-1}^{(2)} = \sum\limits_{k=1}^{p-1} \frac{1}{k^2}$, więc mamy:

   $$\sum_{k=1}^{p-2} H_k^2 - \sum_{k=1}^{p-1} H_k^2 - H_{p-1}^{(2)} = -2\sum_{k=1}^{p-1} \frac{H_k}{k}.$$

   Stąd otrzymujemy: $H_{p-1}^2 + H_{p-1}^{(2)} = 2\sum\limits_{k=1}^{p-1} \frac{H_k}{k}$. Z twierdzenia Wolstenholme'a wynika teza. □

2. Dla $p \in \mathbb{P}$, $p \geqslant 3$, mamy $\displaystyle\sum_{k=1}^{p-1} H_k \equiv 1 \pmod{p}$,

Dowód. Obliczamy:

$$\sum_{k=1}^{p-1} H_k = \sum_{k=1}^{p-1}\sum_{n=1}^{k} \frac{1}{n} = \sum_{n=1}^{p-1}\sum_{k=n}^{p-1} \frac{1}{n} = \sum_{n=1}^{p-1} \frac{p-n}{n}$$
$$= \sum_{n=1}^{p-1} \left(\frac{p}{n} - 1\right) = \left(\sum_{n=1}^{p-1} \frac{p}{n}\right) - (p-1) \equiv_p 1.$$

□

3. Dla $p \in \mathbb{P}$, $p \geqslant 3$, mamy $\displaystyle\sum_{k=1}^{p-1} H_k^2 \equiv p-2 \pmod{p}$.

Dowód. Wykonujemy następujące przekształcenia:

$$\sum_{k=1}^{p-1} H_k^2 = \sum_{k=1}^{p-1} \left(\sum_{n=1}^{k} \frac{1}{n}\right)^2 = \sum_{k=1}^{p-1}\sum_{n=1}^{k} \frac{1}{n^2} + \sum_{k=1}^{p-1} \sum_{1 \leqslant n < m \leqslant k} \frac{2}{mn} =$$
$$= \sum_{n=1}^{p-1}\sum_{k=n}^{p-1} \frac{1}{n^2} + \sum_{k=1}^{p-1}\sum_{n=1}^{k}\sum_{m=n+1}^{k} \frac{2}{mn}$$
$$= \sum_{n=1}^{p-1} \frac{p-n}{n^2} + \sum_{n=1}^{p-1}\sum_{k=n}^{p-1}\sum_{m=n+1}^{k} \frac{2}{mn}$$
$$\equiv_p -\sum_{n=1}^{p-1} \frac{1}{n} + \sum_{n=1}^{p-1}\sum_{m=n+1}^{p-1} \frac{2(p-m)}{mn} \equiv_p$$
$$\equiv_p \sum_{n=1}^{p-1}\sum_{m=n+1}^{p-1} \frac{-2}{n} \equiv_p \sum_{n=1}^{p-1} \frac{-2(p-1-n)}{n} \equiv_p$$
$$\equiv_p \sum_{n=1}^{p-1} \left(\frac{2}{n} + 2\right)$$
$$\equiv_p 2H_{p-1} + 2(p-1) \equiv_p -2 \equiv_p p-2.$$

□

Wniosek 18.5. *Niech $\{p_n\}_{n\in\mathbb{N}}$ będzie ciągiem kolejnych liczb pierwszych oraz niech $S_n \in \{0, 1, \ldots, p_n - 1\}$ będzie resztą z dzielenia liczby $\sum_{k=1}^{p_n-1} H_k^2$ przez p_n w sensie wprowadzonej definicji relacji modulo dla liczb wymiernych. Wtedy prawdziwa jest zależność:*

$$S_n - S_{n-1} = p_n - p_{n-1}, \qquad \text{dla } n \in \mathbb{N}, n \geqslant 3.$$

Dowody poniższych relacji przebiegają podobnie jak wcześniejsze, lecz wymagają większej ilości obliczeń. Dlatego przedstawię tylko końcowe wyniki:

1. Dla $p \in \mathbb{P}$, $p \geqslant 5$, mamy $\displaystyle\sum_{k=1}^{p-1} H_k^2 \equiv 2(p-1) \pmod{p^2}$,

2. Dla $p \in \mathbb{P}$, $p \geqslant 3$, mamy $\displaystyle\sum_{k=1}^{p-1} H_k^3 \equiv \begin{cases} 1 \pmod{p} & \text{dla } p \in \{3, 5\}, \\ 6 \pmod{p} & \text{dla } p \geqslant 7. \end{cases}$

Oczywiście podobnych relacji można zauważyć znacznie więcej. Oto niektóre z nich (nie wszystkie potrafimy zweryfikować bezpośrednio, ale w tych sytuacjach zweryfikowaliśmy prawdziwość kongruencji dla 200 początkowych liczb pierwszych z użyciem programu Mathematica).

1. Dla $p \in \mathbb{P}$, $p \geqslant 7$, mamy $\displaystyle\sum_{k=1}^{p-1} \frac{H_k^2}{k^2} \equiv 0 \pmod{p}$,

2. Dla $p \in \mathbb{P}$, $p \geqslant 5$, mamy $\displaystyle\sum_{k=1}^{p-1} \frac{H_k^3}{k} \equiv 0 \pmod{p}$,

3. Dla $p \in \mathbb{P}$, $p \geqslant 7$, mamy $\displaystyle\sum_{k=1}^{p-1} \frac{H_k}{k^3} \equiv 0 \pmod{p}$,

4. Dla $p \in \mathbb{P}$, $p \geqslant 3$, mamy $\displaystyle\sum_{k=1}^{p-1} \frac{H_k}{k(k+1)} \equiv 0 \pmod{p}$,

5. Dla $p \in \mathbb{P}$, $p \geqslant 5$, mamy $\displaystyle\sum_{k=1}^{p-1} \frac{H_k^3}{k(k+1)} \equiv 0 \pmod{p}$,

6. Dla $p \in \mathbb{P}$, $p \geqslant 7$, mamy

$$\sum_{k=1}^{p-1} \frac{H_k - H_k^{(2)}}{k^2} \equiv -\sum_{k=1}^{p-1} \frac{H_k^{(2)}}{k} \equiv \sum_{k=1}^{p-2} \frac{H_k}{(k+1)^2} \pmod{p}.$$

18.3 Ciekawostki

18.3.1 Hipoteza Riemanna $\Leftrightarrow$ nierówność Lagariasa

Z tematyką liczb harmonicznych wiąże się pewna „elementarna" nierówność odkryta w 2002 roku przez znanego amerykańskiego matematyka Jeffrey'a Lagariasa. Do dzisiaj pozostaje ona tylko hipotezą.

Hipoteza 3 (Nierówność Lagariasa)**.** *Dla dowolnego $n \in \mathbb{N}_+$ zachodzi nierówność:*

$$\sigma(n) \leqslant H_n + e^{H_n} \ln H_n,$$

gdzie $\sigma\colon \mathbb{N}_+ \to \mathbb{N}_+$ przyporządkowuje liczbie naturalnej n sumę jej wszystkich dodatnich dzielników, czyli σ wyraża się wzorem $\sigma(n) = \displaystyle\sum_{\substack{d \mid n \\ d \geqslant 1}} d$.

Definicja 18.6 (Funkcja zeta Riemanna)**.** Dla liczb zespolonych s spełniających warunek $\operatorname{Re} s > 1$ funkcja zeta określona jest wzorem $\zeta(s) = \displaystyle\sum_{n=1}^{\infty} \frac{1}{n^s}$.

Funkcja ta daje się jednoznacznie przedłużyć analitycznie dla $s \in \mathcal{C} \setminus \{1\}$. Co można przedstawić następującymi wzorami:

$$\zeta(s) = \frac{1}{s-1} \sum_{n=0}^{\infty} \frac{1}{n+1} \sum_{k=0}^{n} (-1)^k \binom{n}{k} (k+1)^{1-s}, \quad s \in \mathcal{C} \setminus \{1\},$$

$$\zeta(s) = \frac{1}{1-2^{1-s}} \sum_{n=0}^{\infty} \frac{1}{2^{n+1}} \sum_{k=0}^{n} (-1)^k \binom{n}{k} (k+1)^{-s}, \quad s \in \mathcal{C} \setminus \{1\}.$$

Analityczne przedłużenie funkcji zeta Riemanna ma tzw. trywialne miejsca zerowe w punktach $s = -2, -4, -6, \ldots$

Hipoteza 4 (Hipoteza Riemanna)**.** *Wszystkie nietrywialne miejsca zerowe analitycznego rozszerzenia funkcji zeta Riemanna znajdują się na prostej* $\operatorname{Re} s = \frac{1}{2}$*, zwanej prostą krytyczną.*

Okazuje się, że nierówność Lagariasa, pozornie tak prosta i elementarna, jest równoważna hipotezie Riemanna. Spośród wielu równoważnych sformułowań hipotezy Riemanna, to jest o tyle szczególne, że nie zawiera przejść granicznych, stałych typu γ Eulera, nie jest kwantyfikowane po nieprzeliczalnym zbiorze, oraz obie strony nierówności są zdefiniowane konstruktywnie.

18.3.2 Wybrane tożsamości

W trakcie badań nad kongruencjami dla liczb harmonicznych odkryliśmy następującą zależność wiążącą wartości funkcji zeta dla argumentów parzystych i nieparzystych (przypomnijmy, że $\frac{\zeta(2k)}{\pi^{2k}} \in \mathbb{Q}$ dla każdego $k \in \mathbb{N}_+$):

$$\begin{aligned}
&\sum_{n=1}^{\infty} \frac{H_n}{(n+x)^2} = 2\zeta(\mathbf{3}) + \sum_{k=1}^{\infty} \sum_{n=1}^{\infty} \frac{(-1)^k (k+1) H_n}{(n+x)^{k+2}} x^k = \\
&= 2\zeta(\mathbf{3}) - \frac{\pi^4 x}{36} + \left(-\frac{1}{2}\pi^2 \zeta(\mathbf{3}) + 9\zeta(\mathbf{5}) \right) x^2 + \\
&+ \left(-\frac{\pi^6}{135} + 2\zeta(\mathbf{3})^2 \right) x^3 + \left(-\frac{1}{18}\pi^4 \zeta(\mathbf{3}) - \frac{5}{6}\pi^2 \zeta(\mathbf{5}) + 20\zeta(\mathbf{7}) \right) x^4 + \\
&+ \left(-\frac{\pi^8}{700} + 6\zeta(\mathbf{3})\zeta(\mathbf{5}) \right) x^5 + \\
&+ \left(-\frac{1}{270}\pi^2 \left(2\pi^4 \zeta(\mathbf{3}) + 21\pi^2 \zeta(\mathbf{5}) + 315\zeta(\mathbf{7}) \right) + 35\zeta(\mathbf{9}) \right) x^6 + \ldots
\end{aligned}$$

Z powyższej tożsamości wynikają między innymi poniższe zależności:

$$\sum_{n=1}^{\infty} \frac{H_n}{n^4} = 3\zeta(5) - \zeta(2)\zeta(3), \quad 4\sum_{n=1}^{\infty} \frac{H_n}{n^5} = 7\zeta(6) - 2(\zeta(3))^2,$$

$$4\sum_{n=1}^{\infty} \frac{H_n}{n^7} = 9\zeta(8) - 4\zeta(3)\zeta(5).$$

Ciekawostka. *Nadal nie wiadomo, czy wszyskie liczby* $\zeta(2n-1)$ *dla* $n \in \mathbb{N}_+$ *są niewymierne. Na pewno wiadomo, że liczba* $\zeta(3)$ *jest niewymierna (Roger Apéry) oraz że nieskończenie wiele liczb postaci* $\zeta(2n-1)$ *dla* $n \in \mathbb{N}_+$ *jest niewymiernych.*

Podziękowania

W tym miejscu chciałbym podziękować dr. hab. Romanowi Witule za pomoc i opiekę merytoryczną w przygotowaniu wystąpienia na konferencji Oblicze 2016, jak również za współpracę naukową w trakcie całego przebiegu studiów.

Bibliografia

[1] A. Basu, *A new method in the study of Euler sums*, Ramanujan Journal **16** (2008), 7-24.

[2] J.M. Borwein, D.M. Bradley, *Thirty-two Goldbach variations*, International Journal of Number Theory **2** (2006), 65-103.

[3] S. Czekalski, *The continued fraction expansion of Euler's constant*, Tamkang J. Math., **41**(4) (2010), 313-316.

[4] A. Dil, V. Kurt, *Polynomials related to harmonic numbers and evaluation of harmonic number series I*, arXiv: http://arxiv.org/pdf/0912.1834.pdf.

[5] A. Dil, V. Kurt, *Polynomials related to harmonic numbers and evaluation of harmonic number series II*, Appl. Anal. Discrete Math. **5** (2011), 212-229.

[6] R.L. Graham, D.E. Knuth, O. Patashnik, *Matematyka konkretna*, PWN, 2002.

[7] C. Helou, G. Terjanian, *On Wolstenholme's theorem and its converse*, J. Number Theory **128** (2008), 475-499.

[8] J.C. Lagarias, *An elementary problem equivalent to the Riemann hypothesis*, Amer. Math. Monthly **109** (2002), 534–543.

[9] Sz. Rabsztyn, D. Słota, R. Wituła, *Funkcje gamma i beta*, Wydawnictwo Politechniki Śląskiej, Gliwice 2012.

[10] A. Sofo, H.M. Srivastava, *A family of shifted harmonic sums*, Ramanujan Journal **37** (2015), 89-108.

[11] A. Sofo, *Computational Techniques for the Summation of Series*, Kluwer Academic/Plenum Publisher, New York 2003.

[12] A. Sofo, D. Cvijovic, *Extensions of Euler Harmonic Sums*, Appl. Anal. Discrete Math. **6** (2012), 317-328.

[13] A. Sofo, *Shifted harmonic sums of order two*, Commun. Korean Math. Soc. **29** (2014), 239-255.

[14] A. Sofo, *Summation formula involving harmonic numbers*, Anal. Math. **37** (2011), 51-64.

[15] M.D. Schmidt, *Generalized j-Factorial Functions, Polynomials, and Applications*, Journal of Integer Sequences **13** (2010).

[16] H.M. Srivastava, *Certain classes of series associated with the Zeta and relates functions*, Appl. Math. Comp. **141** (2003), 13-49.

[17] R. Wituła, E. Hetmaniok, D. Słota, *Generalized Gregory's series*, Appl. Math. Comput. **237** (2014), 203-216.

[18] R. Wituła, *O pewnych zastosowaniach wzorów na sumę unimodularnych liczb zespolonych*, Pracowania Komputerowa Jacka Skalmierskiego, Gliwice 2011.

[19] R. Wituła, N. Gawrońska, D. Słota, A. Zielonka, *Some generalizations of Gregory's power series and their applications*, J. Appl. Math. Comp. Mech. **12** (2013), 79-91.

[20] J. Wolstenholme, *On certain properties of prime numbers*, Journal of Pure and Applied Mathematics **5** (1862), 35–39.

[21] D.Y. Zheng *Further summation formulae related to generalized harmonic numbers*, J. Math. Anal. Appl. **335** (2007), 692-706.

Centralne konfiguracje w zagadnieniu n ciał

Sabina Szymczak
Politechnika Gdańska

Centralne konfiguracje są pewnym podzagadnieniem problemu n ciał spełniającym dodatkowe warunki. Ruch ciał niebieskich był od zawsze przedmiotem zainteresowania uczonych, natomiast zagadnienie n ciał zostało sformułowane w XVII w., kiedy to okazało się, że rozwiązanie mające określić ruch planety podane przez Newtona nie daje prawidłowych wyników. Spostrzeżenie to doprowadziło Newtona do sformułowania prawa powszechnego ciążenia, jednak wyjściowy problem pozostał nierozwiązany. Zbadanie zagadnienia centralnych konfiguracji jest istotne jako próba zbliżenia się do poznania ogólniejszego problemu zachowania układu n ciał, a także z punktu widzenia zastosowań. Centralne konfiguracje mają swój udział m. in. w badaniu kolizji i ekspansji układów mas. Celem niniejszego artykułu jest przedstawienie znanych rozwiązań problemu centralnych konfiguracji dla $n = 3$ oraz metod użytych przy numerycznym wyznaczaniu współliniowych konfiguracji 4 ciał w programie stworzonym do symulacji zachowań wymieniowych układów.

19.1 Zagadnienie n ciał

Zagadnienie to polega na określeniu zachowania układu n ciał o znanych masach $m_1, ..., m_n$ oraz położeniach i prędkościach początkowych odpowiednio $q_1, ..., q_n$ i $\dot{q}_1, ..., \dot{q}_n$. Przyjmujemy, że

układ jest inercjalny i termodynamicznie izolowany, tzn. nie występuje wymiana energii lub materii z otoczeniem. Korzystając z prawa powszechnego ciążenia oraz II zasady dynamiki Newtona otrzymujemy następujące równania opisujące problem:

$$m_i\ddot{q}_i = \sum_{j\neq i} \frac{m_i m_j}{\|q_j - q_i\|^2} \cdot \frac{q_j - q_i}{\|q_j - q_i\|}, \qquad i = 1, ..., n \tag{19.1}$$

$q_i \in \mathbb{R}^d$, gdzie d jest wymiarem przestrzeni (w ogólności $q_i \in \mathbb{R}^3$, w zagadnieniach planarnych $q_i \in \mathbb{R}^2$, współliniowych - $q_i \in \mathbb{R}$). *Wektorem konfiguracji* będziemy nazywać wektor $q = (q_1, ..., q_n) \in \mathbb{R}^{dn}$.
Wprowadzając potencjał grawitacyjny:

$$U(q) = \sum_{i<j} \frac{m_i m_j}{\|q_i - q_j\|}$$

określony poza zbiorem zderzeń ciał, siłę wypadkową działającą na i-te ciało można zapisać w postaci

$$F_i = \nabla_i U. \tag{19.2}$$

Tym samym równania (19.1) przyjmują postać

$$m_i\ddot{q}_i = \nabla_i U.$$

Ponieważ potencjał U nie jest określony, gdy $q_i = q_j$ dla pewnych $i \neq j$, ograniczymy q do zbioru $\mathbb{R}^{nd} \setminus \Delta$, gdzie

$$\Delta = \{q : q_i = q_j,\ i \neq j\}$$

jest zbiorem kolizji. Zbiór $\mathbb{R}^{nd} \setminus \Delta$ nazywamy *przestrzenią konfiguracji*.

Do zdefiniowania centralnych konfiguracji potrzebujemy jeszcze wprowadzić pojęcie środka masy układu:

$$\mathbb{R}^d \ni c = \frac{1}{\mathcal{M}} \sum_{i=1}^{n} m_i q_i,$$

gdzie $\mathcal{M} = m_1 + ... + m_n$ oznacza całkowitą masę układu.
Centralną konfiguracją ciał o danych masach $m_1, ..., m_n$ nazywamy układ spełniający równanie (19.1), w którym wektor przyspieszenia każdego z ciał jest zwrócony w kierunku środka masy układu, a jego długość jest proporcjonalna do odległości ciała od środka masy z pewną stałą dodatnią wspólną dla wszystkich ciał.
Powyższą definicję można zapisać wzorem

$$\ddot{q}_i = -\lambda(q_i - c), \qquad i = 1, ..., n \tag{19.3}$$

dla pewnej $\lambda \in \mathbb{R}_+$, jednak bardziej powszechny jest zapis

$$\nabla_i U = -\lambda m_i(q_i - c), \qquad i = 1, ..., n. \tag{19.4}$$

Poszukiwanie centralnych konfiguracji sprowadza się właściwie do poszukiwania ich klas równoważności względem transformacji takich jak przesunięcia, obroty, odbicia i jednokładność. Dwie konfiguracje uważa się za równoważne, jeżeli jedną można otrzymać z drugiej przy pomocy wymienionych operacji.
Inna, często pojawiająca się interpretacja warunku na centralną konfigurację, to przedstawienie centralnych konfiguracji jako pewnych punktów krytycznych. Z uwagi na niezmienniczość równań względem translacji dowolną konfigurację można rozpatrywać jako równoważną jej konfigurację przesuniętą tak, aby środek masy znajdował się w początku uładu współrzędnych ($c = 0$). Wtedy moment bezwładności układu wyraża się wzorem:

$$I = \sum_{i=1}^{n} m_i q_i^2. \tag{19.5}$$

Ponieważ:

$$\nabla_i I = 2m_i q_i, \tag{19.6}$$

warunki 19.4 dla układu z $c = 0$ można przedstawić jako:

$$\nabla_i U + \frac{\lambda}{2}\nabla_i I = 0, \qquad i = 1, ..., n \tag{19.7}$$

Łatwo zauważyć, że każdy układ dwóch ciał będzie centralną konfiguracją.

19.2 Centralne konfiguracje dla 3 ciał

Dla konfiguracji 3 ciał można rozważać 2 przypadki, w zależności od tego, czy ciała leżą na jednej prostej (konfiguracja współliniowa) czy nie (konfiguracja planarna). Historycznie pierwsze pojawiło się rozwiązanie problemu współliniowych centralnych konfiguracji 3 ciał. W 1767 r. Euler wykazał, że dla każdego uporządkowania mas m_1, m_2, m_3 na prostej istnieje dokładnie jedna klasa centralnych konfiguracji. Ogólnie, możliwości ustawienia 3 mas jest $3! = 6$, jednak każda z nich ma swój symetryczny odpowiednik, zatem istotnie różnych ustawień mamy dokładnie 3. Rozważymy zatem przypadek $n = 3$, $d = 1$. Przyjmujemy kolejność mas m_1, m_2, m_3 zgodnie z indeksami. Bez straty ogólności można przyjąć $q_1 = 0$, $q_2 = 1$, wtedy $q_3 = 1 + r$, gdzie $r > 0$. Wówcza środek masy $c = \frac{m_2+m_3(1+r)}{m_1+m_2+m_3}$. Równania (19.4) są postaci

$$\begin{aligned} m_1 m_2 + \frac{m_1 m_3}{(1+r)^2} &= \lambda m_1 c \\ -m_1 m_2 + \frac{m_2 m_3}{r^2} &= -\lambda m_2 (1-c) \\ -\frac{m_1 m_3}{(1+r)^2} - \frac{m_2 m_3}{r^2} &= -\lambda m_3 (1+r-c), \end{aligned}$$

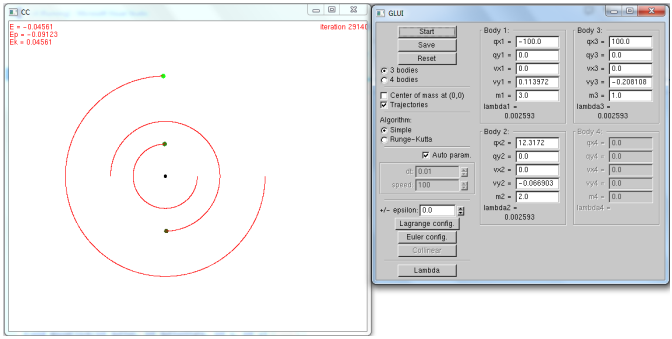
przy czym tylko dwa z nich są niezależne. Zawsze mając n równań tej postaci tylko $n-1$ z nich jest niezależnych, co wynika z faktu, że po zsumowaniu powyższych równań stronami po lewej stronie zawsze otrzymujemy 0. Mamy zatem 2 równania, gdzie niewiadomymi są λ i r. Pozbywając się λ dostajemy równanie wielomianowe z niewiadomą r:

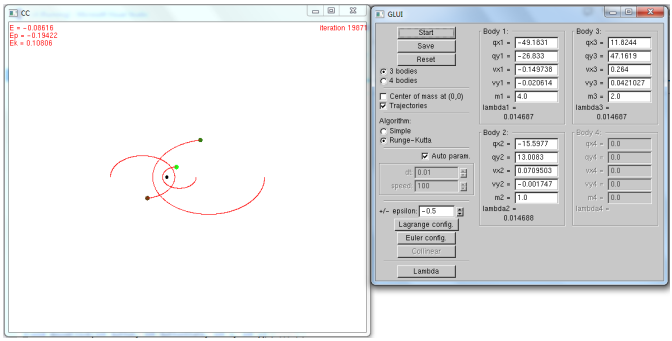
$$\begin{aligned} &(m_1+m_2)r^5 + (3m_1+2m_2)r^4 + (3m_1+m_2)r^3 \\ &-(m_2+3m_3)r^2 - (2m_2+3m_3)r - (m_2+m_3) = 0. \end{aligned} \tag{19.8}$$

Ze względu na postać współczynników wielomianu łatwo określić ich znaki. Z pomocą przychodzi reguła znaków Kartezjusza, która mówi, że dla wielomianu o współczynnikach rzeczywistych, uporządkowanego od najwyższej potęgi, ilość jego pierwiastków

dodatnich jest nie większa niż liczba zmian znaków jego współczynników i może się różnić od niej o liczbę parzystą. W wielomianie (19.8) znak zmienia się tylko raz - między współczynnikami przy r^3 a r^2, zatem wielomian ten ma dokładnie 1 pierwiastek dodatni, wyjściowy problem ma zatem dokładnie jedno rozwiązanie. Wynik Eulera został uogólniony przez Moultona na przypadek n ciał w 1910 r. - dla każdego uporządkowania n mas na prostej istnieje dokładnie jedno rozwiązanie problemu centralnych konfiguracji.

Poniżej znajdują się przykłady symulacji - konfiguracje centralne Eulera dla różnych mas i prędkości początkowych. Czarny punkt prezentuje położenie środka masy. Wyświetlane dane dotyczące współrzędnych i prędkości są wartościami początkowymi.





Drugi przypadek, czyli $n = 3$, $d = 2$, został rozwiązany

w 1772 r. przez Lagrange'a. Zamiast współrzędnych q_1, q_2, q_3 wygodnie będzie użyć wzajemnych odległości między ciałami. Oznaczmy je przez r_{12}, r_{23}, r_{31}. Takie współrzędne również jednoznacznie wyznaczają pewną klasę konfiguracji. Potencjał i moment bezwładności będą w tych zmiennych postaci:

$$\begin{aligned} U &= \frac{m_1 m_2}{r_{12}} + \frac{m_1 m_3}{r_{31}} + \frac{m_2 m_3}{r_{23}}, \\ I &= \frac{1}{\mathcal{M}}(m_1 m_2 r_{12}^2 + m_1 m_3 r_{31}^2 + m_2 m_3 r_{23}^2) \end{aligned}$$

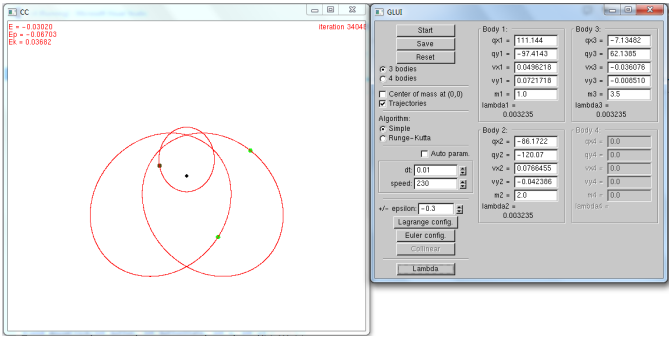
Warunki (19.7) w wersji dla współrzędnych r_{12}, r_{23}, r_{31} przestawiają się jako

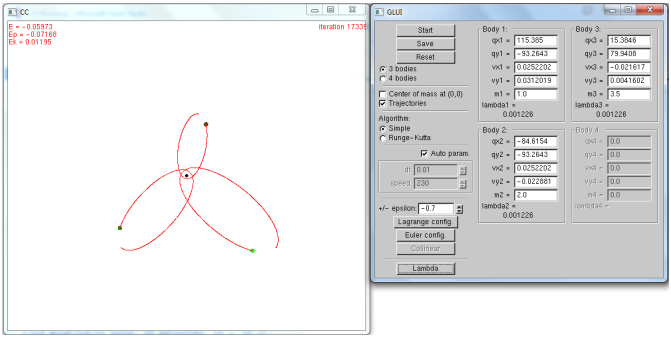
$$\frac{\partial U}{\partial r_{ij}} + \frac{\lambda}{2}\frac{\partial I}{\partial r_{ij}} = 0, \quad i, j = 1, 2, 3,\ i \neq j,$$

i sprowadzają do

$$r_{ij}^3 = \frac{\mathcal{M}}{\lambda}.$$

Widzimy, że aby układ był centralną konfiguracją, odległości między poszczególnymi ciałami muszą być sobie równe, czyli ciała muszą być rozmieszczone w wierzchołkach trójkąta równobocznego. Ciekawym wnioskiem z ostatniego równania jest to, że taki układ ciał będzie centralną konfiguracją niezależnie od doboru mas.



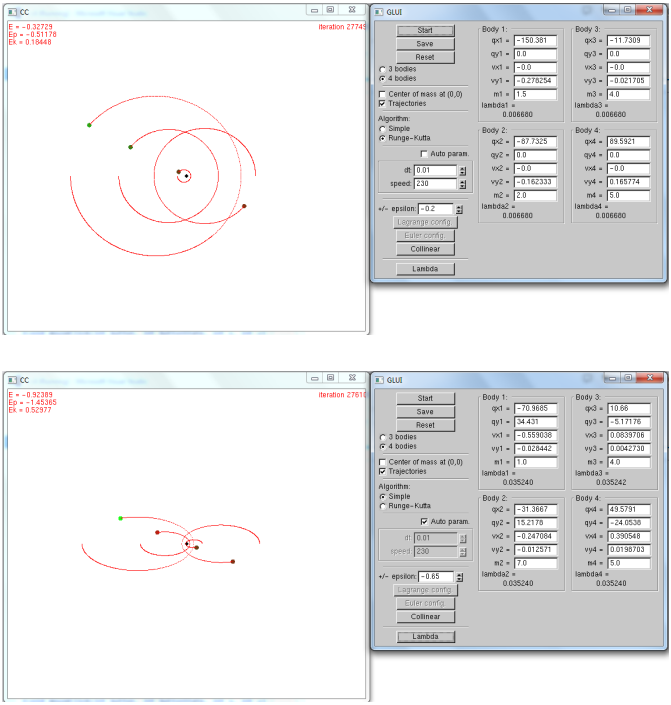


19.3 Współliniowe konfiguracje centralne 4 ciał

Planarne konfiguracje centralne 4 ciał są ciągle problemem otwartym poza pewnymi szczególnymi przypadkami, jak na przykład konfiguracja 3 ciał Lagrange'a z dodaną czwartą masą umieszczoną w środku masy układu. Dla problemu współliniowych konfiguracji, dzieki twierdzeniu Moultona, znamy przynajmniej liczbę rozwiązań zagadnienia, natomiast wyznaczenie wektora konfiguracji w tym przypadku nie jest już tak proste jak dla $n = 3$. W programie symulacyjnym wykorzystane są transformacje układu opisane w pracach E. Pina, tu przedstawione tylko pokrótce, ze względu na obszerność rozumowania. Konfigurację rozmieszczoną początkowo w wierzchołkach czworościanu ortocentrycznego poddajemy skalowaniu i obrotom, co ostatecznie pozwala zdefiniowac ją przy pomocy dwóch współrzędnych sferycznych ϕ i θ zamiast klasycznych współrzędnych kartezjańskich. W transformacji wykorzystywane są własności geometryczne czworościanu ortocentrycznego oraz układu głównych osi bezwładności. Dzięki takiemu podejściu poszukiwanie centralnych konfiguracji danych mas sprowadza się do znalezienia dwóch wartości ϕ i θ, które będą jednoznacznie wyznaczały wektor konfiguracji dla tego przypadku. Ustalając kolejność mas na prostej, można łatwo ograniczyć zakres poszukiwań do przedziału długości $\pi/2$ dla θ

i π dla ϕ, co bardzo ułatwia użycie metod numerycznych. Algorytm zastosowany w programie bada próbne wartości kątów z przedziału poszukiwań, porównując rozbieżności między wartościami współczynników λ (19.4) dla konfiguracji wyznaczonych przez te kąty. Warunkiem na centralną konfigurację jest równość tych współczynników dla wszystkich ciał, zatem wokół pary (θ, ϕ), dla której wartość ta jest najbliższa zeru, budowana jest nowa, drobniejsza siatka punktów, które znowu są poddawane testowi na różnicę lambd. W ten sposób procedura jest powtarzana aż do uzyskania pary (θ, ϕ) generującej konfigurację, dla której błąd jest akceptowalnie mały.

Poniżej przykłady współliniowych centralnych konfiguracji 4 ciał dla różnych mas i prędkości początkowych, wygenerowanych za pomocą powyższego algorytmu.



Bibliografia

[1] R. Moeckel, *"Lectures on central configurations"*, notatki do wykładów przeprowadzonych w Centre de Recerca Matematica w Barcelonie w styczniu 2014r.

[2] R. Moeckel, *Central configurations* - artykuł ze *Scholarpedia*

[3] E. Piña, *New coordinates for the Four-Body problem*, 2009.

[4] E. Piña, *Computing collinear 4-Body Problem central configurations with given masses*, 2011.