Działania i ich własności. Ciała

Ostatnia aktualizacja: 27.10.2021 r.

Na ostatnim wykładzie rozważaliśmy układy równań liniowych o współczynnikach rzeczywistych. Są to ciągi równań postaci

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b,$$

gdzie $a_1, a_2, \ldots, a_n, b \in \mathbb{R}$. Sprawdzenie, że $(s_1, \ldots, s_n)$ jest rozwiązaniem równania wyżej dokonywaliśmy przez wykonanie **działań** dodawania i mnożenia w $\mathbb{R}$ postaci:

$$a_1 \cdot s_1 + a_2 \cdot s_2 + \ldots + a_n \cdot s_n,$$

żądając, by wynikiem było b. Czy zamiast zbioru $\mathbb{R}$ z działaniami $+$ oraz $\cdot$ można rozważać układy równań liniowych, gdzie współczynnikami są **inne zbiory** X z **innymi działaniami** dodawania i mnożenia $\boxplus, \boxtimes$? Na pewno nie mamy tu pełnej dowolności. Przecież choćby równanie liniowe $4x = 2$ nie ma rozwiązania w zbiorze liczb całkowitych, a wykonywanie na nim operacji opisanych na poprzednim wykładzie jak najbardziej ma sens. Aby rozpocząć dyskusję na ten temat sprecyzujmy najpierw definicję działania.

Definicja 1. *Niech X będzie zbiorem niepustym. Przez X^n rozumieć będziemy zbiór ciągów postaci $(x_1, x_2, \ldots, x_n)$, gdzie $x_i \in X$, dla $1 \leqslant i \leqslant n$. **Działaniem n-argumentowym** na zbiorze X nazywamy każdą funkcję $\omega : X^n \to X$.*

Najczęściej rozważanymi działaniami są działania dwuargumentowe. Oto ich przykłady.

zbiór X	działanie ω
liczby rzeczywiste/wymierne/całkowite/naturalne	dodawanie/mnożenie
liczby rzeczywiste	$a \boxplus b = a + b + ab$
zbiór podzbiorów danego zbioru	suma/część wspólna
zbiór funkcji ze zbioru X na zbiór X	złożenie

Kluczowym elementem definicji działania jest żądanie, by nie wyprowadzało ono poza zbiór, na którym jest określone. A więc na przykład odejmowanie nie jest działaniem w zbiorze liczb całkowitych dodatnich, bo $1 - 3 \notin \mathbb{Z}_+$. Jakie są przykłady działań o innej liczbie argumentów, niż 2?

Działanie 1-argumentowe, to na przykład branie liczby przeciwnej w zbiorze liczb całkowitych lub przypisanie liczbie jej kwadratu. Mówi się też o działach 0-argumentowych, które polegają na wyróżnieniu elementu w danym zbiorze, np. zera. A co z działaniami o liczbie argumentów wyższej niż 2? Oczywiście nie jest trudno podać rozmaite przykłady[1], ale istnieją dość głębokie twierdzenia mówiące, że działania te pochodzą w istocie od działań dwuargumentowych[2]. Wszystkie te działania wyróżniamy po to, by określać tzw. **struktury algebraiczne**. Nie potrzebujemy tu ścisłych definicji. Strukturą jest ciąg: $(X, \omega_1, \omega_2, \ldots)$, gdzie X jest zbiorem, zaś $\omega_1, \omega_2, \ldots$ są różnymi działaniami na X.

Działania dwuargumentowe dodawania i mnożenia w zbiorze $\mathbb{R}$ mają pewne szczególnie istotne własności.

Definicja 2. *Niech $* : X^2 \to X$ będzie działaniem dwuargumentowym na zbiorze X. Mówimy, że $*$ jest:*

- ***łączne**, jeśli dla każdych $a, b, c \in X$ mamy $(a * b) * c = a * (b * c)$,*
- ***przemienne**, jeśli dla każdych $a, b \in X$ mamy $a * b = b * a$.*

Przyjrzyjmy się ponownie kilku przykładom.

- działanie $a \boxplus b = a^2 + b^2$ na zbiorze $\mathbb{R}$ nie jest łączne, bo: $(1 \boxplus 2) \boxplus 3 = 34$, zaś $1 \boxplus (2 \boxplus 3) = 170$.
- działanie $a \boxplus b = a + b + ab$ na zbiorze $\mathbb{R}$ jest łączne i przemienne,
- działanie $a \boxtimes b = a^b$ na zbiorze $\mathbb{R}_+ = \{x \in \mathbb{R} : x > 0\}$ nie jest przemienne,
- złożenie w zbiorze bijekcji (czyli odwzorowań 1-1 i „na") zbioru $\mathbb{R}$ nie jest przemienne.

[1] Wikipedia podaje przykład 3-argumentowego działania polegającego na wyznaczaniu sprzężenia harmonicznego punktu względem pary punktów (układ ten tworzy na prostej czwórkę o dwustosunku równym -1), patrz hasło: *Ternary operation*.

[2] Jest to wynik W. Sierpińskiego z pracy *Sur les fonctions de plusieurs variables*, Fund. Math. 33 (1945), 169-173. Patrz też: https://math.stackexchange.com/questions/116771/are-all-n-ary-operators-simply-compositions-of-binary-operators.

Definicja 3. ***Ciałem*** *nazywamy piątkę* $(K, \boxplus, \boxtimes, 0, 1)$*, gdzie* K *jest zbiorem przynajmniej dwuelementowym z wyróżnionymi elementami* $0 \neq 1$*, zwanymi* ***zerem*** *i* ***jedynką****, zaś* $\boxplus$*,* $\boxtimes$ *są dwuargumentowymi działaniami zwanymi dodawaniem i mnożeniem, spełniającymi następujące* ***aksjomaty ciała****:*

1)	$(a \boxplus b) \boxplus c = a \boxplus (b \boxplus c)$	$\forall_{a,b,c \in K}$	*łączność dodawania*
2)	$a \boxplus b = b \boxplus a$	$\forall_{a,b \in K}$	*przemienność dodawania*
3)	$a \boxplus 0 = a = 0 \boxplus a$	$\forall_{a \in K}$	*własność elementu 0*
4)	$a \boxplus b = 0 = b \boxplus a$	$\forall_{a \in K} \exists_{b \in K}$	*element przeciwny*
5)	$(a \boxtimes b) \boxtimes c = a \boxtimes (b \boxtimes c)$	$\forall_{a,b,c \in K}$	*łączność mnożenia*
6)	$a \boxtimes b = b \boxtimes a$	$\forall_{a,b \in K}$	*przemienność mnożenia*
7)	$a \boxtimes 1 = 1 \boxtimes a = a$	$\forall_{a \in K}$	*własność elementu 1*
8)	$a \boxtimes b = b \boxtimes a = 1$	$\forall_{a \in K \setminus \{0\}} \exists_{b \in K}$	*odwrotność dla* $a \neq 0$
9)	$a \boxtimes (b \boxplus c) = (a \boxtimes b) \boxplus (a \boxtimes c)$	$\forall_{a,b,c \in K}$	*rozdzielność* $\boxtimes$ *wzgl.* $\boxplus$

Teoria ciał jest bardzo szeroką dziedziną algebry abstrakcyjnej i w trakcie studiów będziecie Państwo poznawać różne nowe jej aspekty. W ramach naszego wykładu skupimy się na najbardziej podstawowych przykładach i własnościach. Zacznijmy od kilku intuicyjnych przykładów.

- piątka $(\mathbb{R}, +, \cdot, 0, 1)$, jest ciałem, gdzie $+, \cdot$ – standardowe dodawanie i mnożenie liczb rzeczywistych,
- piątka $(\mathbb{Q}, +, \cdot, 0, 1)$ jest ciałem, gdzie $+, \cdot$ – standardowe dodawanie i mnożenie liczb wymiernych,
- piątka $(\mathbb{Z}, +, \cdot, 0, 1)$ nie jest ciałem, bo 2 nie ma elementu odwrotnego. Warto odnotować, że wszystkie inne aksjomaty poza (8) są spełnione!

Z aksjomatów ciała wyprowadzać można rozmaite ich własności. W tym miejscu przedstawimy jedną z nich, potrzebną do ustalenia notacji. Inne wspomnimy na końcu i w dodatkach.

Obserwacja 1. *Niech* K *będzie ciałem. Dla każdego elementu* $a \in K$ *istnieje dokładnie jeden element przeciwny do* a*. Dla każdego niezerowego elementu* $b \in K$ *istnieje dokładnie jeden element odwrotny do* b*.*

Dowód. Wykażemy jedynie jednoznaczność elementu przeciwnego. Druga część dowodzi się analogicznie. Załóżmy, że dla pewnych elementów x, x' ciała K mamy $a \boxplus x = 0 = a \boxplus x'$. Korzystamy dalej z aksjomatów ciała i powyższej równości:

$$\begin{aligned}
x &= x \boxplus 0 && \text{(aksjomat 3 - wł. elementu 0)} \\
&= x \boxplus (a \boxplus x') && \text{(równość wyżej)} \\
&= (x \boxplus a) \boxplus x' && \text{(aksjomat 1 - łączność } \boxplus\text{)} \\
&= x' \boxplus (a \boxplus x) && \text{(aksjomat 2 - przemienność } \boxplus\text{)} \\
&= x' \boxplus 0 && \text{(równość wyżej)} \\
&= x'. && \text{(aksjomat 3 - wł. elementu 0)}
\end{aligned}$$

□

W dalszym ciągu, o ile nie prowadzi to do nieporozumień, wprowadzamy następujące umowy: dodawanie i mnożenie w ciele K oznaczamy odpowiednio jako $+$ oraz $\cdot$, przy czym znak mnożenia może być pomijany. Przez a^n rozumiemy wynik n-krotnego przemnożenia przez siebie elementu a. Przyjmujemy też:

oznaczenie	definicja
$-a$	element odwrotny do a ze względu na $+$
a^{-1}	element odwrotny do a ze względu na $\cdot$
$a - b$	element postaci $a + (-b)$
$\frac{a}{b}$	element postaci $a \cdot (b^{-1})$

Wszystkie pojęcia zdefiniowane na poprzednim wykładzie dla układów równań o współczynnikach w $\mathbb{R}$ (równanie liniowe, układy równoważne, rozwiązania ogólne, macierz układu, operacje elementarne na wierszach, macierze w postaci schodkowej i zredukowanej) przenoszą się na układy o współczynnikach w dowolnym ciele K. Podobnie, opisana na poprzednim wykładzie metoda eliminacji Gaussa stosuje się do układów równań liniowych o współczynnikach w dowolnym ciele K. Mianowicie zachodzi twierdzenie:

Twierdzenie 1. *Niech* K *będzie ciałem. Każdą macierz* $A = M_{m \times n}(K)$ *można za pomocą operacji elementarnych (1)-(2) na wierszach doprowadzić do postaci schodkowej. Każdą macierz* $A = M_{m \times n}(K)$ *można za pomocą operacji elementarnych (1)-(3) na wierszach doprowadzić do postaci zredukowanej. Każdy niesprzeczny układ równań liniowych o współczynnikach w* K *ma rozwiązanie ogólne. Aby je znaleźć wystarczy sprowadzić macierz tego układu do postaci schodkowej zredukowanej elementarnymi operacjami na wierszach, a następnie z otrzymanej macierzy otrzymać rozwiązanie ogólne.*

To twierdzenie jest jednym z niewielu, których nie udowodnimy, ale uznamy za prawdziwe – po prostu stwierdzając, że dowód jest nietrudnym powtórzeniem znanych argumentów. Zachęcamy Państwa do prześledzenia dowodów z poprzedniego wykładu i zastanowienia się w jaki sposób własności liczb rzeczywistych można w nich zastąpić przez kolejne aksjomaty ciała. Kluczowym elementem, który się wyłoni jest kwestia istnienia elementu przeciwnego oraz odwrotnego, które są niezbędne do wykonania eliminacji Gaussa. Aby zobaczyć jak istotne są te aksjomaty, rozważymy następujący, egzotyczny przykład struktury algebraicznej z działaniami dodawania i mnożenia. Będą to... zbiory słów, czyli w skrócie: słowniki.

Aby mieć słownik, trzeba mieć najpierw słowa. Niech $\Sigma_{a,b}$ będzie zbiorem złożonym ze wszystkich słów złożonych z liter a, b, np. $a, aaa, abaa, bbba$ oraz słowa pustego ϵ. W $\Sigma_{a,b}$ wprowadzamy działanie dwuargumentowe, tzw. **konkatenację**, $\cdot$ postaci $w_1 \cdot w_2 = w_1 w_2$, np.

$$aba \cdot bb = ababb, \qquad \epsilon \cdot abb = abb.$$

Rozważamy zbiór $X = P(\Sigma_{a,b})$ złożony z podzbiorów (także nieskończonych!) zbioru $\Sigma_{a,b}$, np.

$$\{\epsilon, a, ab\}, \quad \{a, aa, aaa, aaaa, \ldots\}, \quad , \{ab, abab, ababab, \ldots\}.$$

Elementy zbioru X nazywać będziemy słownikami. W $P(\Sigma_{a,b})$ wprowadzamy działania dwuargumentowe:

- $+$ oznaczające sumę mnogościową zbiorów, np. $\{aba, bb, ab\} + \{a, aa, bb\} = \{aba, bb, ab, a, aa\}$,
- $\cdot$ oznaczające zbiór powstający przez konkatenację wszystkich wyrazów z pierwszego zbioru ze wszystkimi elementami z drugiego. Innymi słowy, dla dowolnych słowników A, B, zbiór $A \cdot B$ złożony jest ze słów postaci $a \cdot b$, gdzie $a \in A, b \in B$. Np.

$$\{aba, bb, ab\} \cdot \{a, aa, bb\} = \{abaa, abaaa, ababb, bba, bbaa, bbbb, aba, abbb\}$$

Rozważamy równania liniowe o współczynnikach w $P(\Sigma_{a,b})$, np. równanie o zmiennych x_1, x_2:

$$\{a, aa\} \cdot x_1 + \{bb\} \cdot x_2 = \{ab, aab, bbb, aaab\},$$

którego **rozwiązaniem są pary elementów $P(\Sigma_{a,b})$**. W tym przypadku: $x_1 = \{b, ab\}$, $x_2 = \{b\}$.

Widzimy, że od strony formalnej cała opisana konstrukcja mieści się w definicji równania liniowego i jego rozwiązania. Równania liniowe , między innymi takie, jak wyżej, nazywa się **równaniami językowymi**[3]. Rozwiązywanie tych równań w niczym nie przypomina znanych nam metod. Dlaczego?

- Pierwszy problem to konieczność określenia strony, z której piszemy współczynniki. Równania:

  $$\{a\} \cdot x_1 = \{abaa\}, \quad x_1 \cdot \{a\} = \{abaa\}$$

  mają różne rozwiązania! Przyczyna – nieprzemienność działania $\cdot$.

- Zauważmy, że w zbiorze słowników $P(\Sigma_{a,b})$ nie ma elementów *przeciwnych* i *odwrotnych*. Mając układ:

  $$\begin{cases} \{a\} \cdot x_1 = \{abaa\} \\ \{a\} \cdot x_1 = \{aba\}. \end{cases}$$

  nie sprowadzimy jego *macierzy* do postaci schodkowej lub zredukowanej, co utrudnia sprawdzanie kiedy jest on sprzeczny!

- Układy jednorodne nie mają sensu, bo $\{\epsilon\} \cup \{w\} = \{w\}$, ale $\{\epsilon\} \cdot \{w\} \neq \{\epsilon\}$.

- Trudno kontrolować zbiory rozwiązań. Rozwiązanie równania wyżej było proste, bo współczynnikami były skończone słowniki. Proszę jednak pomyśleć na przykład o równaniu postaci:

  $$X = \{a^n b^n \mid n \geqslant 1\} \cdot X \cdot \{b^n a^n \mid n \geqslant 1\} \cup \{\epsilon\},$$

  gdzie ϵ jest słowem pustym.

[3] W ramach tego wykładu nie musicie Państwo nic wiedzieć o równaniach językowych. Na potrzeby ilustracji problemów z nieprzemiennością i brakiem odwrotności operacji mnożenia (a to nie jedyne problemy, jak widać wyżej) dokonuję tu i tak dużego uproszczenia tego tematu. Czytelnik zainteresowany szczegółami może zapoznać się z prezentacją Michala Kunca pt. Language Equations (dostępna online) lub z monografią *Language Equations* autorstwa Ernsta Leissa (biblioteka IMPAN). Wcześniej jednak warto przejść/przeczytać wykład kursowy z Języków, automatów i obliczeń.

Celem tego wykładu nie jest systematyczny wykład teorii ciał (dotkniemy tego zagadnienia w dodatkach) ale omówienie najważniejszych przykładów ciał. Szczególnie dużo miejsca poświęcimy dwóm: ciału $\mathbb{Z}_p$ reszt z dzielenia przez liczbę pierwszą p oraz ciału $\mathbb{C}$ liczb zespolonych. Na końcu wykładu powiemy o wzajemnych związkach pomiędzy ciałami, pozwalającymi na budowanie większej liczby przykładów.

Twierdzenie 2. *Niech $n > 1$ będzie liczbą całkowitą. Rozważmy zbiór reszt z dzielenia przez n:*

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

*Określamy działania $+_n$, tzw. **dodawanie modulo n**, oraz $\cdot_n$, tzw. **mnożenie modulo n**, w zbiorze $\mathbb{Z}_n$:*

- *$a +_n b$ to reszta z dzielenia przez n liczby $a + b$,*
- *$a \cdot_n b$ to reszta z dzielenia przez n liczby $a \cdot b$.*

Wyróżniamy też elementy $0, 1$ w $\mathbb{Z}_n$. Wówczas $(\mathbb{Z}_n, +_n, \cdot_n, 0, 1)$ jest ciałem wtedy i tylko wtedy, gdy p jest liczbą pierwszą.

Przykłady ilustrujące powyżej zdefiniowane działania:

- $1 +_3 2 = 0$ w ciele $\mathbb{Z}_3$, więc 1 i 2 są elementami wzajemnie przeciwnymi w $\mathbb{Z}_3$,
- $3 \cdot_{23} 8 = 1$ w ciele $\mathbb{Z}_{23}$, więc 3 i 8 są elementami wzajemnie odwrotnymi w $\mathbb{Z}_{23}$,
- $2 +_4 2 = 0$ w zbiorze $\mathbb{Z}_4$.

Dowód Twierdzenia 2 jest ćwiczeniem z elementarnej teorii liczb. Z uwagi na jego wagę przedstawimy szkic rozumowania. Jak się okazuje, piątka $(\mathbb{Z}_n, +_n, \cdot_n, 0, 1)$ spełnia wszystkie aksjomaty ciała, poza aksjomatem (8) istnienia elementu odwrotnego, który nie jest spełniony, o ile n nie jest liczbą pierwszą. Spełnianie pozostałych aksjomatów jest rutynowym ćwiczeniem, korzystającym z dwóch faktów:

- aksjomaty ciała (1)-(7) oraz (9) są spełnione przez zbiór liczb całkowitych ze standardowymi działaniami dodawania i mnożenia oraz elementami 0, 1,
- jeśli przez $[x]_n$ oznaczymy resztę z dzielenia przez n liczby całkowitej x, to dla dowolnych całkowitych a, b mamy:
$$[a]_n \ +_n \ [b]_n = [a+b]_n, \qquad [a]_n \ \cdot_n \ [b]_n = [ab]_n.$$

Istnienie elementu odwrotnego do każdego elementu niezerowego w $\mathbb{Z}_n$ zagwarantowane jest jedynie, gdy $n = p$. Wymaga to wykorzystania następującego rezultatu.

Lemat 1 (Bezout)**.** *Dla niezerowej liczby całkowitej a oraz dowolnej liczby całkowitej b istnieją takie liczby całkowite x, y, że:*

$$ax + by = NWD(a, b).$$

Pokażmy, w jaki sposób wykorzystać powyższy lemat do zakończenia dowodu. Biorąc dowolną niezerową resztę a z dzielenia przez liczbę pierwszą p mamy $NWD(a, p) = 1$. Istnieją wiec liczby całkowite x, y takie, że

$$ax + py = 1.$$

A zatem reszta z dzielenia x przez p jest odwrotnością do a w $\mathbb{Z}_p$. Z drugiej strony, jeśli $n = rs$, gdzie $r, s > 1$, to nie istnieje takie k, że $r \cdot_n k = 1$. To by bowiem oznaczało, że $rk = qn + 1$, dla pewnego $q \in \mathbb{Z}$. To z kolei implikuje $rk - qrs = 1$. Jednak $r > 1$, co daje sprzeczność. Dowód twierdzenia jest zakończony. Inny (ogólniejszy) argument polega na wykorzystaniu następującego faktu.

Twierdzenie 3. *Niech K będzie ciałem. Wówczas jeśli $a, b \in K$ oraz $ab = 0$, to $a = 0$ lub $b = 0$.*

Dowód. Niech $x, y \in K$. Wyprowadzimy kolejne wnioski z aksjomatów ciała.

(i) Jeśli $x + y = x$, to $-x + (x + y) = (-x + x) + y = 0 + y = y = -x + x = 0$.

(ii) Mamy $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$. Zatem na mocy (i) mamy $0 \cdot x = 0$.

(iii) Jeśli $a \neq 0$, to na mocy (ii) mamy $0 = a^{-1} \cdot 0 = a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b = b$.

□

Ze względu na dużą wagę uogólnień Lematu Bezout w algebrze, pokażemy jego dowód.

Dowód. Uznamy, że znane są dwa fakty[4]:

1. twierdzenie o dzieleniu z resztą,
2. twierdzenie o istnieniu NWD pary liczb całkowitych.

Ograniczymy się do przypadku, gdy a, b są dodatnie (resztę łatwo uzupełnić). Rozważmy zbiór L wszystkich **dodatnich** liczb postaci $ax + by, \quad x, y \in \mathbb{Z}$. Skoro a, b są dodatnie, to zbiór ten jest niepusty i **istnieje najmniejszy jego element**, który nazwiemy d. Twierdzimy, że $d = NWD(a, b)$.

Jest jasne, że $NWD(a, b)$ jest dzielnikiem każdej liczby postaci $ax + by$ (bo każdy wspólny dzielnik a, b jest dzielnikiem $ax + by$), więc $d \geqslant NWD(a, b)$. Aby pokazać przeciwną nierówność wykażemy, że d to wspólny dzielnik a oraz b.

Załóżmy, wbrew temu co oczekujemy, że d nie jest dzielnikiem a. Zatem na mocy twierdzenia o dzieleniu z resztą istnieje liczba $0 < r < d$ oraz $k \geqslant 1$ taka, że:

$$a = kd + r.$$

To oznacza, że $r = a - kd$. To jest niemożliwe, bo przecież:

$$r = a - kd = a - k(ax + by) = a(1 - lkx) - kby,$$

jest również (dodatnim, jako reszta!) elementem zbioru L, i to mniejszym niż d, sprzeczność. A zatem d jest dzielnikiem a. Analogicznie pokazujemy, że d jest dzielnikiem b. A zatem d rzeczywiście jest wspólnym dzielnikiem a oraz b, co oznacza, że $d \leqslant NWD(a, b)$. Dowód Lematu Bezout jest zakończony. □

Zobaczmy jak wyglądają tabelki ciał $\mathbb{Z}_2$ oraz $\mathbb{Z}_3$. W dodatku pokażemy, że są to jedyne ciała odpowiednio dwu- i trzyelementowe.

$+_2$	0	1
0	0	1
1	1	0

$\cdot_2$	0	1
0	0	0
1	0	1

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Spróbujmy rozwiązać układ równań liniowych o współczynnikach w ciele $\mathbb{Z}_3$:

$$\begin{cases} x_1 + x_2 = 2 \\ 2x_1 + x_2 = 1 \end{cases} \quad \text{o macierzy} \quad \left[\begin{array}{cc|c} 1 & 1 & 2 \\ 2 & 1 & 1 \end{array}\right] \in M_{3\times 2}(\mathbb{Z}_3).$$

Odejmujemy pierwszy wiersz przemnożony przez 2. Jaką on ma postać? Otóż jest to wiersz postaci $2\,2\,|1$, bo działania wykonujemy modulo 3. A zatem po tej operacji mamy (to samo, co po dodaniu wierszy):

$$\left[\begin{array}{cc|c} 1 & 1 & 2 \\ 0 & 2 & 0 \end{array}\right].$$

Cóż więc pozostaje? Przemnożyć drugi wiersz przez... odwrotność 2, czyli 2 (bo $2 \cdot_3 2 = 1$). A zatem mnożymy drugi wiersz przez 2 i odejmujemy od pierwszego. Dostajemy:

$$\left[\begin{array}{cc|c} 1 & 0 & 2 \\ 0 & 1 & 0 \end{array}\right].$$

A zatem rozwiązaniem tego układu jest para $(x_1, x_2) = (2, 0)$. Ten układ był tak prosty, że to rozwiązanie byłoby widoczne i bez sprowadzania macierzy do postaci schodkowej. **Układ równań liniowych o współczynnikach w ciele skończonym ma zawsze skończenie wiele rozwiązań!** Rozwiązania ogólne mogą być jednak nadal reprezentowane przez zmienne zależne i niezależne. Np. zbiorem rozwiązań równania $x_1 + x_2 = 0$ o współczynnikach w ciele skończonym $\mathbb{Z}_p$ są wszystkie pary $\{(-t, t) \,|\, t \in \mathbb{Z}_p\}$, a więc równanie to ma p rozwiązań. Równanie $x_1 + x_2 + x_3 = 0$ ma p^2 rozwiązań w ciele $\mathbb{Z}_p$.

Przejdziemy teraz do drugiego fundamentalnego przykładu ciała, liczb zespolonych.

[4]Pełen dowód Lematu i faktów pomocniczych, i więcej o elementarnych aspektach NWD, np. w tekście dla nauczycieli: `https://mimuw.edu.pl/~amecel/semNWD.pdf`.

Definicja 4. ***Ciało liczb zespolonych*** *to piątka* $(\mathbb{R}^2, \oplus, \otimes, (0,0), (1,0))$*, oznaczana przez* $\mathbb{C}$*, którego elementami są wszystkie uporządkowane pary liczb rzeczywistych, i w którym działania* $\oplus, \otimes$ *określone są za pomocą działań* $+$ *oraz* $\cdot$ *w* $\mathbb{R}$ *wzorami:*

$$(a,b) \oplus (c,d) = (a+c, b+d), \quad (a,b) \otimes (c,d) = (ac-bd, ad+bc).$$

Dla dowolnej liczby zespolonej $z = (a,b)$ *wprowadzamy oznaczenia:*

- a *nazywamy* ***częścią rzeczywistą*** *liczby* z *i oznaczamy ją przez* $\mathrm{Re}(z)$*,*
- b *nazywamy* ***częścią urojoną*** *liczby* z *i oznaczamy* $\mathrm{Im}(z)$*,*
- *liczbę* $\sqrt{a^2+b^2}$ *nazywamy* ***modułem liczby*** z *i oznaczamy jako* $|z|$*.*

Zobaczmy kilka przykładowych działań w ciele $\mathbb{C}$.

- $(3,0) \oplus (4,0) = (7,0)$,
- $(0,1) \oplus (1,0) = (1,1)$,
- $(0,1) \otimes (0,1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1,0)$,
- $(2,1) \otimes (2,-1) = (2 \cdot 2 - 1 \cdot (-1), 2 \cdot (-1) + 1 \cdot 2) = (5,0)$.

Widzimy, że definicja mnożenia liczb zespolonych nie wygląda na zbyt naturalną. Spróbujmy wyjaśnić ją przyjmując nieco inną, algebraiczną konwencję zapisu liczb zespolonych.

Przyporządkowanie $a \mapsto (a,0)$ zadaje utożsamienie zbioru liczb rzeczywistych z podzbiorem zbioru liczb zespolonych złożonym ze wszystkich liczb postaci $(r,0)$. Przy tym utożsamieniu działania na liczbach rzeczywistych odpowiadają działaniom na ich odpowiednikach w zbiorze liczb zespolonych. Mamy bowiem:

$$(a,0) \oplus (a',0) = (a+a',0), \quad (a,0) \otimes (a',0) = (aa'-0, 0+0) = (aa',0).$$

W tym przyporządkowaniu:

- liczbę postaci $(a,0)$ będziemy zapisywać jako a, dla każdego $a \in \mathbb{R}$,
- liczbę $(0,1)$ oznaczać będziemy jako i.

Używając tych oznaczeń mamy na przykład:

$$(a,b) = (a,0) \oplus (0,b) = (a,0) \oplus (b,0) \otimes (0,1) = a + bi, \quad i^2 = (0,1) \otimes (0,1) = (-1,0) = -1.$$

Widzimy więc, że liczbę $z = (a,b)$ zapisywać możemy w **postaci ogólnej** (algebraicznej)

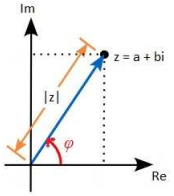
$$z = a + bi,$$

przyjmując umowę, że jeśli $a + bi = c + di$, to $a = c$ oraz $b = d$.

W przyjętej konwencji dodawanie i mnożenie liczb zespolonych staje się bardziej zrozumiałe i pozwala na opuszczenie oznaczeń $\oplus, \otimes$. Dodawanie i mnożenie sprowadzają się bowiem do wykonywania operacji algebraicznych, uwzględniających zasadę: $i^2 = -1$, czyli np.:

$$(a+bi)(c+di) = ac + adi + bci + bdi^2 = (ac-bd) + (ad+bc)i.$$

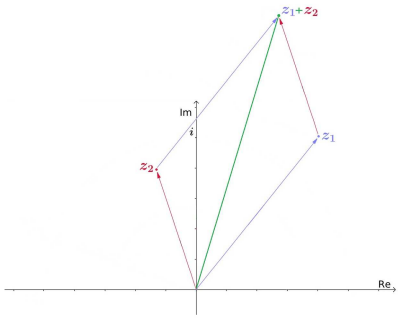
Aby jeszcze lepiej zrozumieć mnożenie liczb zespolonych, odwołamy się teraz do niezwykle ważnej, geometrycznej interpretacji. Liczby zespolone to pary punktów i możliwe jest reprezentowanie liczb zespolonych na tzw. płaszczyźnie zespolonej. Oś odpowiadającą współrzędnej $\mathrm{Re}(z)$ liczby zespolonej z oznaczamy Re, a oś odpowiadającą $\mathrm{Im}(z)$ oznaczamy przez Im. Moduł $|z|$ liczby zespolonej z intepretować możemy, zgodnie z twierdzeniem Pitagorasa, jako odległość (euklidesową) punktu (reprezentującego) z od punktu (reprezentującego) $(0,0)$.



Rys. 1. Płaszczyzna zespolona. Moduł i argument liczby zespolonej. Źródło: Wikipedia (z modyfikacjami).

Zauważmy, że dodawanie liczb zespolonych przypomina dodawanie wektorów. Mamy:

$$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i.$$



Rys. 2. Interpretacja geometryczna dodawania liczb zespolonych.

Niech $z = a + bi \neq 0$ będzie liczbą zespoloną i niech $\varphi \in \mathbb{R}$ oznacza miarę łukową kąta między półprostą o początku $(0,0)$ przechodzącą przez $(0,1)$, a półprostą o początku $(0,0)$, przechodzącą przez z. Wówczas korzystając ze szkolnej definicji funkcji trygonometrycznych i z tw. Pitagorasa mamy:

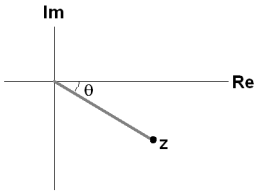
$$\cos\varphi = \frac{a}{\sqrt{a^2+b^2}} = \frac{a}{|z|}, \quad \sin\varphi = \frac{b}{\sqrt{a^2+b^2}} = \frac{b}{|z|}.$$

Stąd $a = |z|\cos\varphi$ oraz $b = |z|\sin\varphi$, a więc:

$$z = a + bi = |z|\cos\varphi + (|z|\sin\varphi)i = |z|(\cos\varphi + i\sin\varphi).$$

Jest to **postać trygonometryczna liczby zespolonej** $z \neq 0$. Liczbę φ nazywamy **argumentem** liczby z i oznaczamy $\arg(z)$. Argument liczby zespolonej $z \neq 0$ jest więc wyznaczony z dokładnością do całkowitej wielokrotności 2π. Liczbie 0 przypisujemy moduł 0 i dowolny argument $\varphi \in \mathbb{R}$.

Przykład: znajdziemy postać trygonometryczną liczby $z = \sqrt{3} - i$.

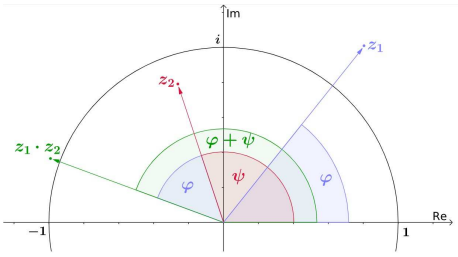


Mamy $|z| = \sqrt{\sqrt{3}^2 + (-1)^2} = 2$ oraz:

$$z = 2\left(\frac{\sqrt{3}}{2} - \frac{1}{2}\cdot i\right) = 2\left(\cos\frac{11\pi}{6} + i\cdot\sin\frac{11\pi}{6}\right) = 2\left(\cos\frac{-\pi}{6} + i\cdot\sin\frac{-\pi}{6}\right).$$

Wniosek 1. *Dla niezerowych liczb zespolonych w, z zachodzą równości*

$$\arg(z\cdot w) = \arg(z) + \arg(w), \quad |zw| = |z|\cdot|w|.$$



Rys. 2. Mnożenie liczb zespolonych z_1 i z_2 w interpretacji geometrycznej. Zródło: Wikipedia (z modyfikacjami).

Dowód. Następujące obliczenie pokazuje jak zachowuje się argument przy mnożeniu liczb zespolonych z, w danych w postaciach trygonometrycznych:

$$\begin{aligned} z \cdot w &= |z|(\cos\varphi + i\sin\varphi) \cdot |w|(\cos\psi + i\sin\psi) = \\ &= |z||w|(\cos\varphi\cos\psi - \sin\varphi\sin\psi) + i(\sin\varphi\cos\psi + \cos\varphi\sin\psi)) = \\ &= |z||w|(\cos(\varphi+\psi) + i\sin(\varphi+\psi)). \end{aligned}$$

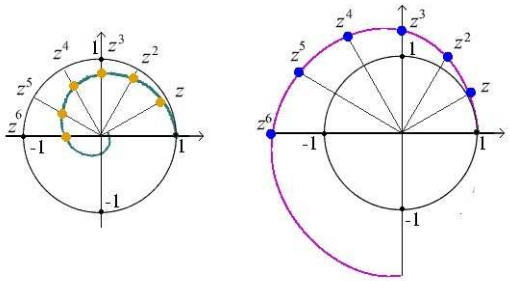
Pokażmy jeszcze, że $|z| \cdot |w| = |zw|$. Niech $z = a + bi, w = c + di \in \mathbb{C}$. Wówczas

$$\begin{aligned} |z \cdot w| &= |(a+bi)(c+di)| = |(ac-bd) + (bc+ad)i| = \\ &= \sqrt{(ac-bd)^2 + (bc+ad)^2} = \sqrt{a^2c^2 + b^2d^2 + b^2c^2 + a^2d^2} = \\ &= \sqrt{(a^2+b^2)(c^2+d^2)} = |z| \cdot |w|. \end{aligned}$$

□

Wniosek 2 (Wzór de Moivre'a, 1730)**.** *Niech $z = |z|(\cos\varphi + i\cdot\sin\varphi)$. Wówczas dla każdego n całkowitego dodatniego mamy:*

$$z^n = |z|^n(\cos(n\cdot\varphi) + i\cdot\sin(n\cdot\varphi)).$$



Rys. 4. Interpretacja geometryczna potęgowania liczb zespolonych. Źródło: http://www.suitcaseofdreams.net/.

Wszystko to wygląda bardzo obiecująco, ale nie uzasadniliśmy w ogóle, że $\mathbb{C}$ jest ciałem. I nie będziemy tego robić. To, że aksjomaty ciała są istotnie spełnione w zasadzie sprowadza się do manipulacji algebraicznych i może nie być w każdym przypadku natychmiastowo widoczne (dowód łączności mnożenia czy rozdzielności). Elementy takich rachunków mogą być przeprowadzone w ramach ćwiczeń. Nie mają one wielkiego waloru poznawczego, a przedstawiona interpretacja geometryczna w zasadzie pozwala sprowadzić niektóre punkty do faktów czysto geometrycznych (i odwrotnie, co może się podobać). W tym momencie odnotujmy tylko, że dla każdego $(a, b) \neq (0, 0)$ mamy:

$$(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right).$$

W ramach naszych zajęć ważna będzie jeszcze jedna definicja, związana z liczbami zespolonymi.

Definicja 5. *Niech $z = a + bi$ będze liczbą zespoloną.* ***Sprzężeniem*** *liczby zespolonej z nazywamy liczbę $a - bi$, oznaczaną przez $\overline{z}$. Na płaszczyźnie zespolonej punkt $\overline{z}$ jest obrazem z w symetrii względem osi* $\mathrm{Re}(z)$. *W szczególności $|z| = |\overline{z}|$ oraz* $\arg(z) = -\arg(\overline{z})$.

Do sprawdzenia przez Państwa (na przykład na ćwiczeniach) pozostawiam następujące proste własności wprowadzonych wyżej pojęć. Mianowicie dla dowolnych $z, z_1, z_2 \in \mathbb{C}$ mamy:

(a) $z + \overline{z} = 2\,\mathrm{Re}(z), z \cdot \overline{z} = |z|^2$,

(b) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$, $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$,

(c) $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$ oraz gdy $|z_2| \neq 0$ mamy też $\left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|}$,

(d) $|z_1 + z_2| \leqslant |z_1| + |z_2|$, $||z_1| - |z_2|| \leqslant |z_1 - z_2|$.

Ciało reszt z dzielenia przez liczbę pierwszą oraz ciało liczb zespolonych reprezentują dwie niezwykle ważne klasy ciał. Pierwsza to ciała skończone, którym poświęcony będzie dzisiejszy dodatek. Druga – to tak zwane ciała algebraicznie domknięte, czyli takie, że wielomiany o współczynnikach w tych ciałach mają zawsze pierwiastki. Dyskusji tego drugiego zagadnienia poświęcony będzie kolejny wykład. Na koniec warto poruszyć jeszcze jeden istotny aspekt – kluczowy dla bardzo wielu zagadnień algebraicznych i pozwalający podawać nowe przykłady ciał. Zacznijmy od definicji.

Definicja 6. *Mówimy, że piątka* $(K', +', \cdot', 0', 1')$ *jest* ***podciałem*** *ciała* $(K, +, \cdot, 0, 1)$ *jeśli* K' *jest podzbiorem ciała* K*,* $0' = 0$*,* $1' = 1$ *oraz działania* $+'$ *i* $\cdot'$ *powstają przez ograniczenie działań* $+, \cdot$ *określonych na* $K \times K$ *do zbioru* $K' \times K'$*.*

Najbardziej znanym podciałem ciała liczb rzeczywistych jest ciało liczb wymiernych $\mathbb{Q}$ ze zwykłymi działaniami dodawania, mnożenia oraz z wyróżnionymi elementami 0 i 1. Innym przykładem podciała (pozostawiam sprawdzenie Państwu – dla przypomnienia sobie wyciągania niewymierności z mianownika) ciała $\mathbb{R}$ jest zbiór:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}.$$

Jest to tak zwane rozszerzenie kwadratowe ciała $\mathbb{Q}$ o $\sqrt{2}$. Więcej o informacji o rozszerzeniach znajdą Państwo w materiałach prof. Wiśniewskiego. Temat ten jest niezwykle ważny na Algebrze 2.

Definicja 7. *Ciało* K*, które nie ma podciał właściwych, czyli różnych od siebie, nazywamy* ***prostym****.*

Jak się okazuje, przykładem ciała prostego jest ciało liczb wymiernych (dowód zobaczycie Państwo na ćwiczeniach). Jest to, jak się również okaże, jedyne nieskończone ciało proste. W dodatku pokażemy natomiast, że jedynymi skończonymi ciałami prostymi są ciała p-elementowe, gdzie p jest liczbą pierwszą. Ciała proste i ciała algebraicznie domknięte są na przeciwnym spektrum „złożoności". Pomiędzy ciałem liczb wymiernych, a ciałem liczb zespolonych znajduje się bardzo bogaty świat ciał. Jak to zobaczyć?

Obserwacja 2. *Rozważmy dowolną rodzinę podciał* K_t *ciała* L*, gdzie* $t \in T$*. Wówczas część wspólna wszystkich ciał* K_t *jest podciałem ciała* K*.*

Obserwacja 3. *Dla każdego podciała* K *ciała* L *oraz podzbioru* S *zbioru* L *istnieje najmniejsze podciało* $K(S)$ *ciała* L*, które zawiera jednocześnie ciało* K *oraz zbiór* S*.*

Oto przykłady podciał ciała liczb rzeczywistych, utworzone w oparciu o powyższe obserwacje:

- ciała $\mathbb{Q}(\sqrt{p})$, gdzie p jest liczbą pierwszą,
- ciała $\mathbb{Q}(\sqrt{p}, \sqrt{q})$, gdzie p, q są liczbami pierwszymi,
- najmniejsze ciało zawierające $\mathbb{Q}$ i pierwiastki z wszystkich liczb pierwszych,
- ciała typu $\mathbb{Q}(\pi)$, $\mathbb{Q}(\sqrt{2}, \pi)$, $\mathbb{Q}(\pi, \pi^2, \pi^3, \ldots)$ itd.

Ostatnim ważnym przykładem, jaki chciałbym pokazać jest ciało funkcji wymiernych. W tym celu przytoczę definicję, od której wystartuje kolejny wykład.

Definicja 8. ***Wielomianem*** *zmiennej* x *o współczynnikach w ciele* K *nazywamy wyrażenie:*

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,$$

gdzie n *jest liczbą całkowitą nieujemną oraz* $a_0, a_1, \ldots, a_n \in K$*. Utożsamiamy przy tym takie napisy, jeśli różnią się o składniki postaci* $0 \cdot x^i$ *oraz jeśli różnią się kolejnością składników. Elementy* a_i *nazywamy* ***współczynnikami*** *wielomianu. Zbiór wielomianów o współczynnikach z ciała* K *oznaczamy przez* $K[x]$*.*

Obserwacja 4. ***Ciałem funkcji wymiernych*** $K(x)$ *zmiennej* x *o współczynnikach w ciele* K *nazywamy zbiór wyrażeń formalnych:*

$$\frac{f}{g}, \quad f, g \in K[x].g \neq 0.$$

z naturalnymi działaniami dodawania i mnożenia funkcji wymiernych. Zerem i jedynką w ciele $K(x)$ *są odpowiednio* $0/1$ *i* $1/1$*.*

Z formalnego punktu widzenia $K(x)$ jest najmniejszym ciałem zawierającym K oraz zmienną x, która nie tylko nie jest elementem ciała K, ale żaden element ciała K nie może być uzyskany z x (ani jego odwrotności) w wyniku wielokrotnego wykonania działania dodawania lub mnożenia, a więc nie może być rozwiązaniem żadnego równania $f(s) = 0$, gdzie $f \in K[x]$. O takim rozszerzeniu mówimy, że jest **przestępne**. Jest to inna sytuacja, niż w przypadku **algebraicznego** rozszerzenia ciała $\mathbb{Q}$ o $\sqrt{2}$, który jest pierwiastkiem równania $x^2 - 2 = 0$, i $x^2 - 2 \in \mathbb{Q}[x]$. Można na przykład pokazać, że ciała $\mathbb{Q}(x)$ oraz $\mathbb{Q}(\pi)$ są *w istocie* tym samym ciałem (trzeba jeszcze wiedzieć, że π jest przestępne i co to znaczy: *w istocie*).

Uzupełnienie. Tabelki działań i ciało czteroelementowe

Na wykładzie poznaliśmy ciała $\mathbb{Z}_p$ reszt z dzielenia przez p, gdzie p jest liczbą pierwszą. Nie są to jedyne ciała skończone. Aby się o tym przekonać pokażemy, że istnieje ciało czteroelementowe o elementach $\{0, 1, a, b\}$. Spróbujemy to jednak zrobić w taki sposób, by dyskusja miała możliwie uniwersalny charakter i pozwalała wprowadzać nowe pojęcia. Po przedstawieniu konstrukcji sformułujemy bez dowodów kilka ogólnych wyników. Powiedzmy jeszcze tyle, że ciała skończone są niezwykle istotnymi obiektami, zarówno w samej matematyce, jak i w zastosowaniach, zwłaszcza w kryptografii i teorii kodów.

Zaczniemy zupełnie naiwnie. Mamy zbiór n elementowy i chcemy na nim określać jakieś dwuargumentowe działania. Ile jest tych działań? Które są łączne? Które są przemienne? Jak wygodnie określać te działania? Spójrzmy na tabelkę pewnego działania dwuargumentowego $*$ na zbiorze $\{a, b, c\}$:

$*$	a	b	c
a	b	c	b
b	a	c	b
c	c	a	a

Oczywiście działanie to nie jest przemienne – tabelka musiałaby mieć określoną symetrię. Mamy na przykład $a*b = c$ oraz $b*a = a$. Trudniej dostrzec brak łączności, ale po chwili widać, że $a*(b*c) = a*b = c$, podczas gdy $(a*b)*c = c*c = a$. Warto powiedzieć, że istnieje stosunkowo efektywna procedura sprawdzania czy tabelka danego działania dwuargumentowego opisuje działanie łączne, zwana testem łączności Lighta z 1949 roku (można poczytać hasło *Light's associativity test* na Wikipedii).

Nietrudno policzyć liczbę działań dwuargumentowych na zbiorze n elementowym, a także liczbę działań przemiennych, czy działań, w których jest element neutralny. Liczby te równe są odpowiednio:

$$n^{(n^2)}, \quad n^{\frac{n(n+1)}{2}}, \quad n^{(n-1)^2+1}.$$

Osobom, które byłyby zainteresowane tabelkami działań i zliczaniem niedużych tabelek o określonych własnościach polecam całkowicie elementarny tekst *Associative Operations on a Three-Element Set* autorstwa F. Diego oraz K. Jónsdóttir (dostępny on-line). Na koniec tego wstępu powiem tylko, że parę $(X, \circ)$, gdzie $\circ$ jest łącznym działaniem dwuargumentowym nazywamy **półgrupą**. Półgrup jest bardzo dużo. Istotnie różnych (nie chcę się tu wgłębiać w to, co to znaczy) półgrup 3-elementowych jest 18. Półgrup czteroelementowych, istotnie różnych, jest już 126, a pięcioelementowych – 1160 (patrz https://oeis.org/A001423).

W przypadku zliczania ciał skończonych potężnym narzędziem jest żądanie łączności aż dwóch działań dwuargumentowych, związanych prawem rozdzielności. Podstawowe obserwacje niezbędne do dalszej pracy zebrane są w następującym stwierdzeniu (dowód jest analogiczny do przedstawionych na wykładzie).

Obserwacja 5. *Niech K będzie ciałem.*

- *Dla każdych $x, y, z \in K$ równość $x + y = x + z$ implikuje $y = z$.*
- *Dla $x \neq 0$ oraz $y, z \in K$ równość $xy = xz$ implikuje $y = z$.*

W języku algebraicznym mówimy, że dodawanie i mnożenie w ciele są „skracalne". Wniosek z tych obserwacji jest następujący: w tabelkach opisujących działania w ciele skończonym K w każdym wierszu i w każdej kolumnie występować muszą wszystkie elementy z ciała – każdy dokładnie raz. Jeśli wiemy dodatkowo, że dla każdego $a \in K$ zachodzą równości:

$$a + 0 = a, \quad a \cdot 0 = 0, \quad a \cdot 1 = 1,$$

to wnioskujemy, że jest jedynie jedno ciało dwuelementowe i trzyelementowe – nie da się bowiem wypełnić tabelek dodawania i mnożenia ciał dwu i trzyelementowych inaczej, niż wypełnione są tabelki przedstawione w zasadniczej części wykładu. W przypadku tabelki ciała czteroelementowego napotkamy jednak na pewien problem. Oto tabelki działań w tym ciele, wypełnione zgodnie z wiedzą przedstawioną wyżej.

$+$	0	1	a	b
0	0	1	a	b
1	1			
a	a			
b	b			

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a		
b	0	b		

W rzeczywistości, tabelkę mnożenia wypełnić można jeszcze dokładniej. Zauważmy bowiem, że $a \cdot b \neq b$. W przeciwnym bowiem razie wiedząc, że $b \neq 0$ mamy $a = 1$, co jest nieprawdą. A zatem $a \cdot b = 1$, nie ma innej możliwości uzupełnienia trzeciego wiersza tabelki. W szczególności mamy:

+	0	1	a	b
0	0	1	a	b
1	1			
a	a			
b	b			

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

.

Co natomiast z dodawaniem? Tutaj użyjemy nieco innego podejścia, związanego z pojęciem podciała. Zauważmy, że każde ciało zawiera element 1 oraz wszystkie elementy postaci:

$$m \cdot 1 = \underbrace{1 + 1 + \ldots + 1}_{m}.$$

Zauważmy jednak, że jeśli mamy ciało n elementowe i $m > n$, to z zasady szufladkowej Dirichleta wynika, że pewne dwie liczby powyżej są równe. Na przykład dla ciała czteroelementowego pewne dwa z elementów:

$$1, \quad 1+1, \quad 1+1+1, \quad 1+1+1+1, \quad 1+1+1+1+1$$

są równe. Które dwa? Na pewno żadne sąsiednie dwa, bowiem z prawa skracania mamy $1 = 1+1 \Rightarrow 0 = 1$. Gdyby było $1 + 1 + 1 = 0$ oraz $1 + 1 \neq 0$, to nasze ciało miałoby za mało elementów, bowiem 1 oraz $a = 1 + 1$ byłyby przeciwne, a więc czwarty element (niezerowy) musiałby być przeciwny do samego siebie, tzn. $b + b = 0$. Ale $b + b = b(1 + 1)$ byłoby iloczynem dwóch niezerowych elementów, sprzeczność. A zatem musi być $1 + 1 = 0$. Co więcej, mamy:

$$(1 + 1)(1 + 1) = 1 + 1 + 1 + 1 = 0.$$

Oczywiście gdyby $1 + 1 + 1 + 1 = (1 + 1)(1 + 1) = 0$, to $1 + 1 = 0$ (to jest bardzo ważny argument potrzebny niżej). Mamy więc $1+1 = a+a = b+b = 0$. co pozwala do końca uzupełnić powyższe tabelki.

+	0	1	a	b
0	0	1	a	b
1	1	0		
a	a		0	
b	b			0

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

.

Teraz możemy już zauważyć, że $a + 1 \neq a$, czyli $a + 1 = b$. Analogicznie $b + 1 = a$, co daje:

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

.

Pokazaliśmy, że istnieje dokładnie jedno ciało 4-elementowe. Zauważmy ciekawą rzecz: zachodzą równości:

$$a^2 + a + 1 = 0, \quad b^2 + b + 1 = 0.$$

Dlaczego nas to interesuje? Otóż wyrażenie x^2+x+1 nie jest równe 0, dla żadnego $x \in \mathbb{Z}_2$. Używając języka wykładu można powiedzieć, że uzyskane ciało czteroelementowe jest rozszerzeniem ciała $\mathbb{Z}_2$ o pierwiastki wielomianu, który w tym ciele pierwiastków nie ma. Po zakończeniu kolejnego wykładu pokażemy, że nie jest to przypadek. Póki co odnotujmy fundamentalną obserwację wynikającą z naszych rozważań.

Obserwacja 6. *Dla każdego ciała skończonego K istnieje liczba pierwsza p taka, że w ciele tym zachodzi równość $\underbrace{1 + 1 + \ldots + 1}_{p} = 0$. W takim przypadku mówimy, że ciało K ma **charakterystykę** równą p.*

Warto odnotować, że również ciała nieskończone mogą mieć charakterystykę dodatnią (prosty przykład to ciało funkcji wymiernych $\mathbb{Z}_2(x)$).

Na koniec sformułuję twierdzenie, które można udowodnić zupełnie elementarnie (zachęcam), a po dwóch kolejnych wykładach – niemal natychmiastowo.

Twierdzenie 4. *Każde ciało skończone ma p^n elementów, gdzie p jest pewną liczbą pierwszą, a n pewną liczbą całkowitą dodatnią. Dla każdej pary p, n istnieje ciało p^n-elementowe.*

Faktem wymagającym nieco większej liczby pojęć jest również to, że dla każdej pary p, n istnieje tylko jedna tabelka ciała p^n-elementowego. W tym momencie się na razie zatrzymamy.

Dodatek. Liczby p-adyczne

Na wykładzie z analizy matematycznej rozważa się dwie konstrukcje liczb rzeczywistych pochodzące od Dedekinda i Cantora. Pierwsza oparta jest na przekrojach, a druga na ciągach Cauchy'ego. Obydwie pochodzą z lat 70' XIX wieku. Wcześniejsze próby rygorystycznego opisu liczb rzeczywistych, podejmowane nawet w XVI wieku (Stevin), a potem intensywnie w wieku XIX (Bolzano, Hamilton, Weierstrass) były jedynie częściowo rygorystyczne. W XX wieku doczekaliśmy się wielu alternatywnych konstrukcji, bardziej lub mniej elementarnych[5]. Z naszego punktu widzenia szczególnie ciekawa jest konstrukcja Cantora.

W dużym skrócie, konstrukcja Cantora jest oparta na obserwacji, że każda liczba rzeczywista a jest granicą ciągu (q_n) liczb wymiernych. Co więcej, dowolne dwa ciągi zbieżne (q_n) oraz (q'_n) są zbieżne do tej samej granicy wtedy i tylko wtedy, gdy $|q_n - q'_n| \xrightarrow[n\to\infty]{} 0$. Kluczowym narzędziem są ciągi Cauchy'ego liczb wymiernych, czyli takie ciągi (q_n), że dla każdego $\epsilon > 0$ istnieje $k_0 \in \mathbb{N}$ takie, że $|q_n - q_m| < \epsilon$, o ile tylko $n, m > k_0$. Na czym polega? Bierzemy zbiór C wszystkich ciągów Cauchy'ego liczb wymiernych i mówimy, że dwa elementy zbioru C postaci (q_n) oraz (q'_n) są równoważne, o ile $|q_n - q'_n| \xrightarrow[n\to\infty]{} 0$, co oznaczamy jako $(q_n) \sim (q'_n)$. A zatem zbiór C rozbija się na podzbiory postaci $[(q_n)]$, z których każdy złożony jest równoważnych sobie ciągów Cauchy'ego (oczywiście zbiór $[(q_n)]$ zawiera (q_n)). Konstrukcja Cantora liczb rzeczywistych polega na utożsamieniu ich z owymi podzbiorami, które oznaczymy nieco umownie przez $C/\sim$ (za jakiś czas poznacie Państwo ogólną teorię takich konstrukcji na wstępie do matematyki). I wreszcie, definiujemy **działania** dwuargumentowe $\oplus, \otimes$ na owych podzbiorach:

$$[(q_n)] \oplus [(q'_n)] = [(q_n + q'_n)], \quad [(q_n)] \otimes [(q'_n)] = [(q_n \cdot q'_n)],$$

gdzie $+, \cdot$ są dodawaniem i mnożeniem w $\mathbb{Q}$. Trzeba pokazać, że działania te są dobrze określone, tzn. że dla każdego ciągu (t_n) w $[(q_n)]$ oraz dla każdego ciągu (t'_n) w $[(q'_n)]$ mamy:

$$[(t_n) + (t'_n)] = [(q_n) + (q'_n)], \quad [(t_n t'_n)] = [(q_n q'_n)].$$

Gdy to zrobimy, pozostaje uzasadnić, że spełnione są wszystkie aksjomaty ciała. Na przykład dla dowolnego ciągu Cauchy'ego (q_n) nierównoważnego z ciągiem zerowym trzeba znaleźć ciąg Cauchy'ego (q'_n) taki, że $(q_n q'_n)$ jest ciągiem należącym do $[(1)]$, gdzie $[(k)]$ jest ciągiem stałym, o każdym wyrazie równym k (w ten sposób widzimy, że $\mathbb{Q}$ jest podciałem tak określonego ciała $\mathbb{R}$). W rezultacie $\oplus$ oraz $\otimes$ staną się znanym nam dodawaniem i mnożeniem liczb rzeczywistych.

Co to wszystko ma wspólnego z algebrą liniową i ciałami? Z pewnością konstrukcja działań na zbiorach ciągów, prowadzących do pojęcia ciała, jest ciekawa sama w sobie. Natomiast kluczowy jest dla nas element, którego nie porusza się na początku studiów: definicja ciągu Cauchy'ego na zbiorze liczb wymiernych oparta jest o pojęcie odległości w $\mathbb{Q}$: odległość liczb $p, q \in Q$ równa jest $|p - q|$. Jak się okazuje, nie jest to jedyny „sensowny" sposób określania odległości w $\mathbb{Q}$ (to temat na osobny wykład). Okazuje się, że można wprowadzić inną odległość, związaną z tzw. normą p-adyczną.[6]

Definicja 9. *Niech p będzie dowolną liczbą pierwszą, zaś z – niezerową liczbą całkowitą.*

- *Przez $v_p(z)$ oznaczamy największe n całkowite takie, że*

$$p^n \mid z,$$

  zwane ***wykładnikiem p-adycznym liczby z.***
- *Jeśli $x = \frac{a}{b}$, gdzie $a, b \in \mathbb{Z}$, $b \neq 0$, to określamy:*

$$v_p(x) = v_p(a) - v_p(b).$$

- ***Normą p-adyczną*** *nazywamy funkcję $|.|_p : \mathbb{Q} \to [0, \infty)$ określoną wzorem:*

$$|x|_p = \begin{cases} p^{-v_p(x)} & , x \neq 0 \\ 0 & , x = 0. \end{cases}.$$

- ***Odległością p-adyczną liczb wymiernych*** *x, y nazywamy liczbę wymierną $|x - y|_p$.*

[5] I. Weiss: *The Real Numbers - a survey of constructions*, https://arxiv.org/pdf/1506.03467.pdf.

[6] Rozszerzoną wersję tej opowieści znajdą Państwo pod adresem: `https://mimuw.edu.pl/~amecel/2021l/gal21/p-adyczne1.pdf`., a także w kolejnym wykładzie z poprzedniego roku: `https://mimuw.edu.pl/~amecel/2021l/gal21/p-adyczne2.pdf`.

Zobaczmy kilka przykładów:

- $|2|_2 = 2^{-v_2(2)} = \frac{1}{2}$,
- $|3|_2 = 2^{-v_2(3)} = 1$,
- $|4|_2 = 2^{-v_2(4)} = \frac{1}{4}$,
- $|-\frac{128}{7}|_2 = |\frac{2^7}{-7}|_2 = 2^{-v_2(2^7)+v_2(-7)} = 2^{-7} = 1/128$.
- $|13, 23|_3 = 1/27$, bo $13 + \frac{23}{100} = \frac{1323}{100} = \frac{3^3 \cdot 49}{100}$.

To, co może Państwa zainteresować to fakt, że nie ma żadnych przeszkód, aby wprowadzić ciągi Cauchy'ego zdefiniowane nie w oparciu o wartość bezwzględną, ale o odległość p-adyczną! A jak to zrobimy, to możemy powtórzyć konstrukcję Cantora i dostać... no właśnie, co dostaniemy? Jak się okazuje, dostaniemy nie liczby rzeczywiste, ale tzw. ciało p-adyczne $\mathbb{Q}_p$! I dowód nie jest w zasadzie w jakikolwiek sposób inny niż ten, przedstawiony na Analizie. Czym jest $\mathbb{Q}_p$? I jak opisywać jego elementy? Okazuje się, że podobnie jak liczby rzeczywiste można opisywać przy pomocy rozwinięć, np. dziesiętnego, tak liczby p-adyczne przedstawia się za pomocą tzw. rozwinięcia p-adycznego (czyli w zasadzie za pomocą szeregów). Nie będę definiował czym jest to rozwinięcie, ale pokażę kilka przykładów i powiem, że dla liczb całkowitych pokrywa się ono z rozwinięciem w bazie o podstawie p.

- Liczba 320 ma rozwinięcie $5 + 3 \cdot 7 + 6 \cdot 7^2 = 635$.
- Liczba -1 ma przedstawienie $-1 = 6 + 6 \cdot 7 + 6 \cdot 7^2 + 6 \cdot 7^3 = \ldots 6666$.
- Liczba $\frac{1}{2}$ ma przedstawienie $3 + 2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + \ldots = \ldots 2223$.

Powyższe rozwinięcia mogą Państwa nieco dziwić. Dlaczego szereg określający -1 jest zbieżny, i dlaczego to jest ten szereg? Jak się okazuje liczbie p-adycznej przypisujemy rozwinięcie, które po przecinku może mieć jedynie skończenie wiele elementów, ale na lewo od przecinka może mieć ich nieskończenie wiele. Intuicja jest taka, że wprowadzona odległość zachowuje się jakby odwrotnie do zwykłej wartości bezwzględnej, a to dlaczego, że $|p^n|_p = \frac{1}{n}$. Ogólnie, dla dowolnych $x, y \in \mathbb{Q}_p$ mamy:

$$\|x + y\|_p \leqslant \max(\|x\|_p, \|y\|_p).$$

Jest to nierówność zwana mocną nierównością trójkąta, albo nierównością ultrametryczną.

Ciała p-adyczne mają wiele bardzo ciekawych własności, a uprawiana na nich analiza czy geometria zupełnie nie przypomina tego, czego będziecie się Państwo uczyć (i jest ciekawa). A jednak od ponad 100 lat stanowią one bardzo ważne narzędzie współczesnej matematyki. Jeden z medalistów Fieldsa z 2018 roku, Peter Scholze, otrzymał to najbardziej prestiżowe dla matematyka wyróżnienie właśnie za rozwój geometrii p-adycznej. Zachęcam do obejrzenia filmu z prezentacją Laureata: `https://youtu.be/yEVlCZTqht8`.

Na koniec chcę zwrócić uwagę na jeszcze jedno, głębokie i zaskakujące zagadnienie. Po przeczytaniu powyższego dodatku, ktoś mógłby słusznie zapytać: czy skoro z $\mathbb{Q}$ można konstruować, za pomocą ciągów Cauchy'ego liczby rzeczywiste i ciała p-adyczne, to czy można w podobny sposób konstruować inne ciała? Może są jeszcze jakieś inne „odległości" na $\mathbb{Q}$ pozwalające na uzyskanie takiej konstrukcji? Zaskakująca jest odpowiedź: nie można. Mówi o tym twierdzenie Ostrowskiego z 1916 roku. Okazuje się, że każda odległość na $\mathbb{Q}$ (wciąż nie napisałem czym jest odległość) jest „równoważna" odległości zadanej przez wartość bezwzględną lub odległość p-adyczną! To wynik bardzo przemawiający do wyobraźni, ale nie chciałbym zabierać się tu za wprowadzanie niezbędnych definicji i wyjaśnianie szczegółów. Zachęcam do zajrzenia do mojego wykładu z poprzedniego roku, a w celu znalezienia dowodu tw. Ostrowskiego (nic specjalnie skomplikowanego) odsyłam do tekstu prof. Tomaszewskiego: Twierdzenie Ostrowskiego (tekst jest dostępny on-line, ale można do niego dotrzeć również przez `https://mimuw.edu.pl/~amecel/2021l/gal21/ostr.pdf`), gdzie zagadnienie to omówione jest w sposób niezwykle przystępny.

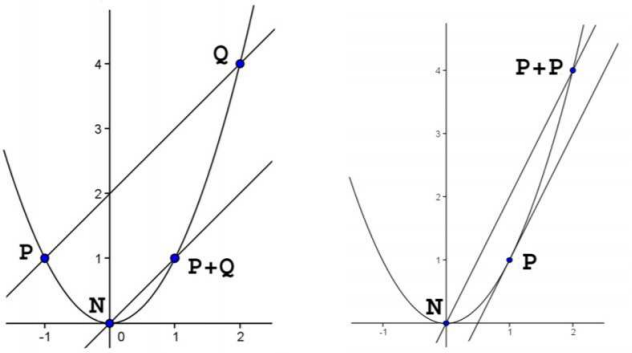
Dodam jeszcze, że twórcą/odkrywcą (niepotrzebne skreślić) liczb p-adycznych był Kurt Hensel, a pionierskie badania w tej dziedzinie prowadził na przełomie XIX i XX wieku. Wielkie znaczenie tych ciał zrozumiane zostało po raz pierwszy dzięki niezwykle ważnemu rezultatowi teorioliczbowemu: zasadzie lokalno-globalnej Hassego z 1921 roku. Wspomnimy o tym wyniku w drugim semestrze. Są również elementarne zastosowania normy p-adycznej, np. następujące ciekawe twierdzenie Monsky'ego[7] z 1970 roku: *Kwadratu nie można podzielić na nieparzystą liczbę trójkątów o równych polach.*

[7] Patrz np. `http://math.uchicago.edu/~may/REU2019/REUPapers/Sablan.pdf` lub *Monsky's theorem.* Wikipedia.

Trivia. Ciało na paraboli

Dziwna może się wydawać definicja ciała liczb zespolonych, gdy patrzymy na nią z punktu widzenia działania na parach liczb. Przypomnę jednak uwagę z wykładu: zbiór $\mathbb{R}^2$ z działaniami dodawania i mnożenia „po współrzędnych" (tzn. z mnożeniem $(a,b)\otimes(c,d)=(ac,bd)$) nie jest ciałem! Ale nie o tym jest ten dodatek. Chciałbym w nim wspomnieć o mało znanym przykładzie ciała, w którym działania dodawania i mnożenia wyglądają bardziej intuicyjnie niż w $\mathbb{C}$, ale zdefiniowane są na dość nietypowym obiekcie.

Rozważamy mianowicie parabolę $\mathcal{P}$ o równaniu $y=x^2$. Pokażemy najpierw, że można wprowadzić na niej strukturę przemiennego dodawania. Niech $N=(0,0)$. Określamy sumę $P\oplus Q$ dwóch punktów paraboli $\mathcal{P}$ jako drugi punkt przecięcia paraboli oraz prostej równoległej do prostej PQ przechodzącej przez punkt N. Jeśli $P=Q$, to zastępujemy prostą PQ przez prostą styczną do paraboli w punkcie P. Poniższe (zapożyczone) rysunki pokazują odpowiednio działania postaci $(-1,1)\oplus(2,4)=(1,1)$ oraz $(1,1)\oplus(1,1)=(2,4)$.



Źródło: Franz Lemmermeyer. *Pell Conics. An Alternative Approach to Elementary Number Theory.* http://www.rzuser.uni-heidelberg.de/~hb3/pell.html

Weryfikacja przypuszczenia, że wprowadzone działanie dwuargumentowe $\oplus$ zadaje na $\mathcal{P}$ działanie łączne z elementem neutralnym N wymaga odrobiny wiedzy szkolnej i wytrwałości. Wyznaczmy wzory na dodawanie dwóch punktów $P_1=(x_1,x_1^2)$ oraz $P_2=(x_2,x_2^2)$. Jeśli $P_1\neq P_2$, to prosta przechodząca przez P_1 oraz P_2 ma współczynnik kierunkowy postaci: $m=(x_2^2-x_1^2)/(x_2-x_1)=x_1+x_2$. Prosta równoległa do prostej P_1P_2 przechodząca przez punkt $N=(0,0)$ ma równanie postaci $y=mx$. Aby znaleźć jej drugi punkt przecięcia z parabolą potrzebujemy rozwiązać równanie $mx=x^2$. To zaś daje nam dwa punkty przecięcia: $N=(0,0)$ oraz $R=(m,m^2)$. A zatem na mocy naszej definicji działania $\oplus$ mamy:

$$(x_1,x_1^2)\oplus(x_2,x_2^2)=(x_1+x_2,(x_1+x_2)^2).$$

Powyższa formuła pozostaje prawdziwa także gdy $P_1=P_2$.

Ktoś powie: *to w zasadzie nic ciekawego*. Matematyk od razu widzi, że zdefiniowane działanie to „właściwie" (nie znamy pojęcia izomorfizmu) dodawanie liczb rzeczywistych. W podobny sposób na hiperboli $xy=1$ wprowadzić można działanie mnożenia, które jest „izomorficzną kopią" mnożenia liczb rzeczywistych. Czy umielibyście Państwo zaproponować geometryczną konstrukcję mnożenia punktów na hiperboli? Aby dowiedzieć się więcej o podobnych konstrukcjach na stożkowych (i nie tylko) zachęcam do lektury książki, do której odsyłam pod powyższym obrazkiem. Znajdziecie tam Państwo łagodny wstęp do teorii punktów wymiernych na krzywych i ich zastosowań. W latach 90' zaawansowane metody teorii krzywych eliptycznych zaowocowały dowodem Wielkiego Twierdzenia Fermata przez Andrew Wilesa. Polecam poglądowy wykład Wilesa i następujący po nim inspirujący wywiad mówiący o życiu zawodowego matematyka. Adres: `https://www.youtube.com/watch?v=uQgcpzKA5jk`.

To jednak nie koniec opowieści. Parabola ma tę szczególną cechę, że można na niej wprowadzić nie tylko strukturę tzw. grupy algebraicznej, ale i strukturę ciała. Spróbujmy więc określić działanie mnożenia. Niech $I=(1,1)$. Dla punktów $P,Q\in\mathcal{P}$ definiujemy mnożenie w następujący sposób: prosta PQ przecina oś OY w punkcie A oraz prosta IA przecina parabolę $\mathcal{P}$ w punkcie $B:=P\star Q$ (proszę to dopracować).

Czy potraficie Państwo napisać algebraiczną formułę opisującą działanie $\star$? Czy potraficie Państwo pokazać, za pomocą tych wzorów, że $(\mathcal{P},\oplus,\star,N,I)$ jest ciałem? Okazuje się, że wcale nie potrzeba tu algebry. Zarówno łączność mnożenia, jak i rozdzielność mnożenia względem dodawania można udowodnić geometrycznie. Czy ktoś z Państwa potrafiłby to zrobić? Fakt ten, co zaskakujące, pochodzi z 2003 roku.

Notka historyczna. Liczby urojone

Być może część, a nawet większość z Państwa słyszała kiedyś o liczbach zespolonych w kontekście tajemniczego „wyciągania pierwiastków z liczb ujemnych". Definicja, którą oglądaliśmy na wykładzie pochodzi z roku 1833 i jest zasługą Hamiltona – który zasłynął jako odkrywca kwaternionów. Była ona swego rodzaju ukoronowaniem 300 lat wysiłków matematyków, którzy od 1545 roku mierzyli się z konsekwencjami wyników opisanych w dziele *Ars Magna* (`Wielka Sztuka`) autorstwa (jak mówią historycy – wybitnego uczonego, ale oszusta) Girolamo Cardano. Wyjawiona w nich była metoda rozwiązywania równań wielomianowych stopnia trzeciego i czwartego zakładająca konieczność wyciągania pierwiastków z liczb ujemnych. Więcej o tym zagadnieniu powiemy w przyszłym tygodniu.

W dziełach starożytnych napotkać można dwie sytuacje – dwa problemy, w których słynni Heron i Diofantos próbują rozwiązać konkretne zadania i zapisują wprost działania wymagające pierwiastkowania liczb ujemnych – oczywiście nie potrafiąc ich wykonać. Jeden z tych problemów zapisany w dziele *Arithmetica* Diofantosa (275 r.) jest następujący[8]: „*Trójkąt prostokątny ma pole równe siedmiu jednostkom kwadratowym oraz obwód równy 12 jednostkom. Znajdź długości jego boków.*" Nie potrzeba długo się zastanawiać by przekonać się, że nie ma takiego trójkąta. Diofantos też to zauważa, bo formułuje odpowiednio równanie kwadratowe, wypisuje rozwiązania zgodnie ze wzorami (choć używał innych oznaczeń) – by stwierdzić wreszcie niemożliwość istnienia takiego rozwiązania (nie wchodząc już w dalsze szczegóły).

Poznając liczby zespolone będziemy cofać się do coraz wcześniejszych interpretacji: od abstrakcyjnie określonych działań na parach liczb, do interpretacji geometrycznej, aż po rozwiązywanie równań wielomianowych i badanie pierwiastków z jedynki. Im historia odleglejsza, tym matematyka wydaje się bardziej obca, niezrozumiała - motywacje i notacja trudne i siermiężne. Cechą charakterystyczną wykładu akademickiego jest to, że nie jest w stanie wprowadzić Państwa w całą zawiłość historycznego procesu formowania się tego, czy innego pojęcia. Nie jest to zresztą pożądane, bo postęp pełen jest zakrętów i ślepych zaułków. Ujęcie rezultatów i teorii rozważanych ponad 100 czy 150 lat temu ulegało zmianie wraz ze zmianą języka matematycznego, konsolidacją notacji w danej teorii i wieloma latami jej wykładu.

Proces tworzenia się teorii matematycznych przypomina historię eksploracji wielkich ścian himalajskich czy tatrzańskich. Wszystko zaczynało się od wielomiesięcznych, siermiężnych wypraw, gdzie szukano jakiejkolwiek drogi na szczyt i często popełniano błędy kosztujące zdrowie i życie. Następnie poprawiano pionierskie drogi, pokonywano je ponownie szybciej, krócej, logiczniej, znajdowano drogi wspinaczkowe, następnie wiele alternatywnych dróg, które później cierpliwie, latami „prostowano", uzyskując słynne „direttissimy" - drogi idące wprost przez ścianę. Oczywiście stosując to porównanie można powiedzieć, że dopiero zaczynamy pierwsze wędrówki i dłuższe wspinaczki, poznajemy sprzęt i chodzimy dawno utartymi, niełatwymi wszakże ścieżkami. Jednak już za dwa, trzy lata, a może szybciej, niektórzy z Państwa zaprowadzeni zostaną, jeśli zechcą, na drogi dopiero wytyczane, w tereny bez map i przewodnika.

W przyszłym tygodniu dowiemy się, że każde równanie wielomianowe o współczynnikach w ciele liczb zespolonych ma pierwiastek (inaczej niż równania wielomianowe o współczynnikach w $\mathbb{R}$), poznając przy okazji podstawową terminologię związaną z wielomianami, ich pierwiastkami oraz funkcjami wielomianowymi. Od XVII wieku formułowano w różnych postaciach przypuszczenie, że wielomian stopnia n ma n pierwiastków (pierwszy był Albert Girard w 1629 roku). Nie rozumiano jednak wówczas natury liczb zespolonych, podając przez lata rozmaite dowody, lub kontrprzykłady. Dotyczyło to nawet wielkich matematyków. Jedną z przyczyn była zapewne ogólna nieufność i brak języka, związane z nazywaniem liczb zespolonych *liczbami urojonymi* w zasadzie do początków XX wieku. Jeden z najbardziej znanych profesorów polskiej emigracji Henryk Niewęgłowski tak pisze w wydanej w 1870 roku ponad czterystustronicowej monografii pt. *Trygonometrya z teoryą ilości urojonych i z notami*[9]:

`Zaiste, ilości urojone grają dziś wielką rolę w wysokiej analizie... Nie dawno temu, jeden z mistrzów umiejętności, zapowiedział, że posiada klucz ilości urojonych. Na nieszczęście, zamiast tym kluczem otworzyć tajemnicę, otworzył wejście do manowców z których sam niełatwo się wydostał; ale w których inni pobłąkali, rozprawiając o ilościach urojonych jak gdyby były istotnemi rzeczywistościami"!`

[8] Odsyłam do: Green D.R.: *The Historical Development of Complex Numbers*, The Mathematical Gazette 60 (1976), 99-107.

[9] Książkę tą, podobnie jak i wiele innych białych kruków, można znaleźć w ogólnodostępnej bibliotece cyfrowej POLONA: https://polona.pl/.