

ALGEBRA R 1



Algebra jest słowem pochodzenia perskiego (Iran) a „wzięła się z tytułu książki perskiego matematyka Muhammada ibn Musa al Khwarizmi. Tytuł po persku brzmiał mniej więcej

1

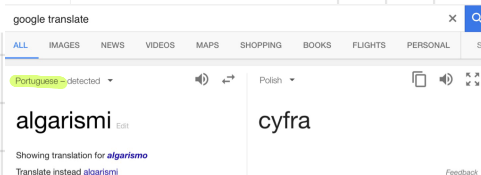
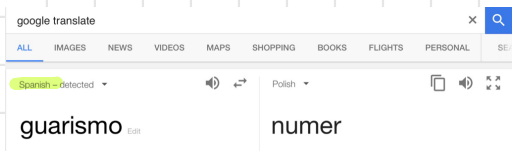
Al-kitāb al-mukhtaṣar fī ḥisāb al-ğabr wa'l-muqābala

algebra

Angielskie tłumaczenie tego tytułu to „The compendious book on calculation by completion and balancing”. Słowo al-ğabr oznacza jedną z tych czynności – completion, balancing (niestety nie wiem którą). Książka dotyczy metod rozwiązywania równań liniowych i kwadratowych.

Sam Al Khwarizmi zapisał się w historii matematyki jako badacz wielu zagadnień, ale także zostawił więcej niż jeden ślad w terminologii.

Jedno z jego dzieł ma łaciński tytuł „Algorithmi de numero indorum”. Choć o „Al Khwarizmi (dzieło o) liczbach indyjskich”. Łacińska wersja nazwiska Al Khwarizmi w postaci Algorithmi jest źródłem rdzenia słowa algorytm w wielu językach. Ponadto, zgodnie z księgą ... de numero indorum:



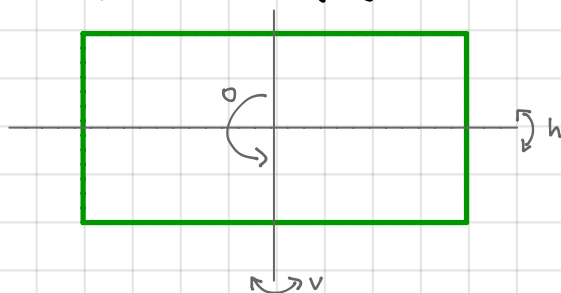
Algebra jako dział matematyki zajmuje się badaniem własności zbiorów wraz z operacjami na nich zadanymi. Jeśli S jest zbiorem, to operację na tym zbiorze nazwiemy odwzorowaniem $S \times S \rightarrow S$.

Na przykład dodawanie jest operacją na zbiorze liczb naturalnych $+: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ $(k, l) \mapsto k+l$. Dodawanie na różnych zbiorach liczbowych może mieć różne własności, dlatego **struktura algebraiczna** to jest **zbiór** wraz z **operacją algebraiczną** i rozważamy jej własności. Struktura algebraiczna może obejmować więcej niż jedno działanie, np. $(\mathbb{R}, +, \cdot)$ – liczby rzeczywiste z dodawaniem i mnożeniem. Przykłady, które do tej pory się pojawiały dotyczyły zbiorów liczbowych bo do nich jesteśmy wszyscy przyzwyczajeni. Przyjmijmy się jednak jeszcze jednemu przykładowi, który jest zupełnie inny:

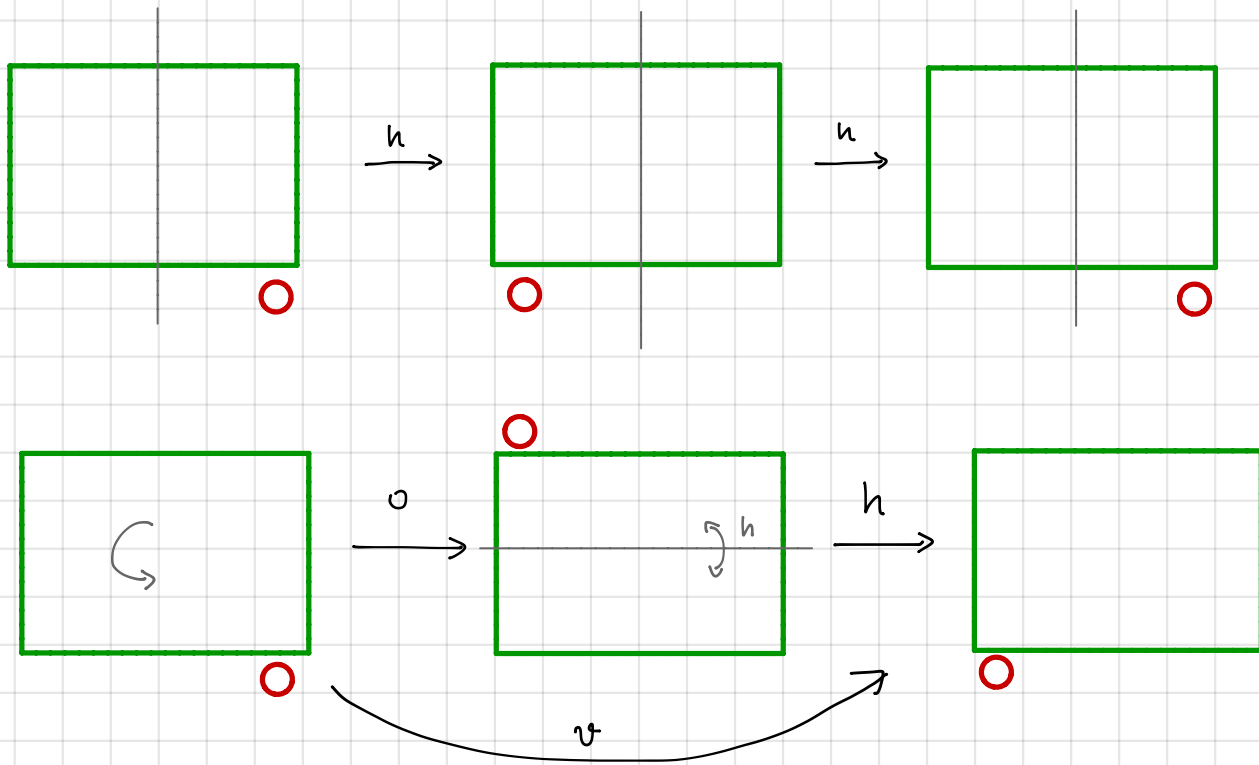
GRUPA CZWÓRKOWA KLEINA

Viererguppe

Felix Klein



Rozważmy płaszczyznę a na niej wyróżniony prostokąt o koniecznie różnych bokach. Rozważamy zbiór izometrii płaszczyzny zachowujących ten prostokąt. Okazuje się, że istnieje trzy takie niechwilalne izometrie. Odbicie względem osi poziomej (h) odbicie względem osi pionowej (v), obrót o 180° względem środka (o). Zauważmy że wykonanie dwóch operacji jedna po drugiej jest też symetrią prostokąta. Ponadto wykonanie każdej z nich dwa razy prowadzi do stanu wyjściowego.



Jeśli więc dołączymy do $\{h, v, o\}$ jeszcze "id" czyli "nicnierobienie" (odwzorowanie identycznościowe) i rozważymy składanie odwzorowań jako operację w $\{id, v, o, h\} = V$ dostaniemy pewną strukturę algebraiczną, którą opisać można tabelką:

	id	o	v	h
id	id	o	v	h
o	o	id	h	v
v	v	h	id	o
h	h	v	o	id

Struktura algebraiczna może więc mieć zbiór inny niż liczbowy i operacje inne niż arytmetyczne. Żeby mieć jeszcze trochę zagmatwać rozważmy zbiór par liczb 0 i 1, ten $S = \{00, 01, 10, 11\}$. Można o nim myśleć jako o wszystkich możliwych stanach dwóch uporządkowanych bitów informacji. Rozważmy teraz na tych bitach operację XOR, czyli alternatywę mocny. Na jednobitowym stanie XOR działa tak

$$0 \text{ XOR } 0 = 0, 1 \text{ XOR } 0 = 1, 0 \text{ XOR } 1 = 1, 1 \text{ XOR } 1 = 0$$

Na dwubitowym stanie przeprowadzamy XOR na każdej pozycji oddzielnie:

$h = v \circ o$ — składanie odwzorowań

$10 \text{ XOR } 01 = 11, 11 \text{ XOR } 10 = 01, \text{ itd.}$ Zrobmy tabelkę

	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

Porównajmy obie tabelki. Zauważmy, że jeśli przyporządkujemy $id \leftrightarrow 00, o \leftrightarrow 01, v \leftrightarrow 10, h \leftrightarrow 11$ to obie tabelki okażą się identyczne!!! Zbiory V i S z operacjami odpowiednio składanie odwzorowań i XOR reprezentują w pewnym sensie (w algebraicznym sensie) tę samą strukturę. Oznacza to, że wszystkie własności obu tych zbiorów, które da się wypowiedzieć wyłącznie w języku odpowiednich operacji

algebraicznych będą dla tych zbiorów jednakowe. Si V są „wcieleńiami” albo realizacjami tej samej struktury algebraicznej którą nazywamy grupą ciałkową Kleina i oznaczamy, zazwyczaj V_4 . Na naszym wykładzie zajmować się będziemy głównie algebrą liniową. Prawdopodobnie liniowy odnosi się zarówno do wektorów. Pracować będziemy więc nad własnościami przestrzeni wektorowych. Wkrótce wyjaśni się dokładnie co to jest. Nazwa słusnie wskazuje, że rzecz dotyczy obiektów takich jak prędkość, siła... Na początek jednak musimy uzupełnić podstawę wiedzę dotyczącą zbiorów liczbowych.

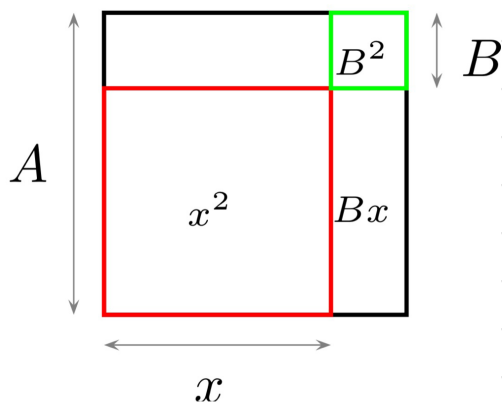
Na razie mamy państwo zapewne $\mathbb{N} = \{1, 2, 3, \dots\}$ zbiór liczb naturalnych, $\mathbb{Z} = \{\dots, -7, \dots, -1, 0, 1, 2, \dots\}$ zbiór liczb całkowitych, $\mathbb{Q}$ zbiór liczb wymiernych, $\mathbb{R}$ - zbiór liczb rzeczywistych. W każdym z tych zbiorów zdefiniowane są operacje $+$ i $\cdot$. W zależności od zbioru operacje te mają różną własność. Założę, że te masz już państwu znane. Następny w kolejności będzie $\mathbb{C}$ - zbiór liczb zespolonych.

LICZBY ZESPOLONE - MOTYWACJA

Rozwiązywanie równań kwadratowych metodą perską: W książce do algebry autorstwa Al-Khwarizmi dyskutowane są różne typy równań kwadratowych. Ponieważ w czasie nie używano zera i liczb ujemnych należało rozważać oddzielnie równanie

$$x^2 + bx = c, \quad x^2 + c = bx, \quad x^2 = bx + c, \quad x^2 = bx, \quad x^2 = c \quad \text{dla } b, c > 0$$

Zajmijmy się rozwiązywaniem równania pierwszego typu metodą perską: Konsystamy z obrazka:



$$x = A - B \Rightarrow x + B = A$$

$$A^2 = x^2 + B^2 + 2Bx$$

$$b = 2B$$

$$c = A^2 - B^2$$

$$A^2 - B^2 = x^2 + 2Bx$$

$$B = \frac{b}{2}$$

$$A = \sqrt{c + \frac{b^2}{4}}$$

$$x = A - B = \sqrt{c + \frac{b^2}{4}} - \frac{b}{2}$$

Dostajemy jedno rozwiązanie. Drugiego nie, bo musiałoby być ujemne (dla $A = -\sqrt{\dots}$). Pójdźmy dalej, to spróbujemy zrobić to samo dla równań trzeciego stopnia:

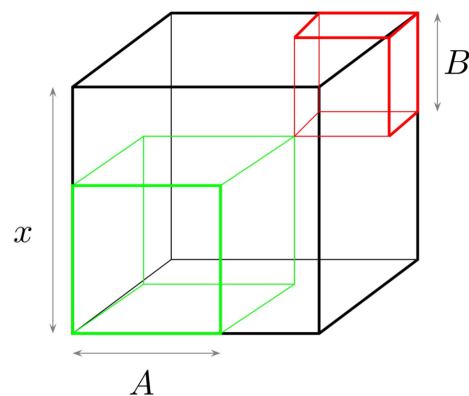
$$x^3 = px + q$$

$$x = A + B$$

$$x^3 = A^3 + 3A^2B + 3AB^2 + B^3$$

$$x^3 = 3AB(A + B) + A^3 + B^3$$

$$x^3 = \underbrace{3ABx}_p + \underbrace{A^3 + B^3}_q$$



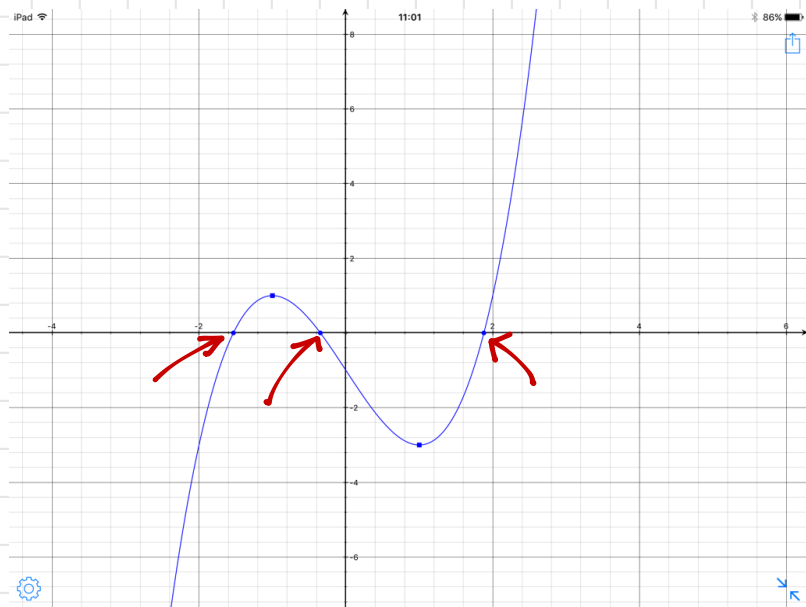
$$p = 3AB \quad q = A^3 + B^3$$

$$p^3 = 27A^3B^3$$

$$\rightarrow \text{równanie kwadratowe na } A^3: p^3 = 27A^3q - 27(A^3)^2$$

Rozwiązujemy to równanie i mamy wynik... Może nie wszystkie rozwiązań, ale jakieś. No dobrze, ale są równania trzeciego stopnia, np. takie

$x^3 = 3x + 1$ które sprawiają kłopoty. Mają rozwiązanie rzeczywiste, w tym jedno dodatnie, pasujące do obrazka, ale sprawiają trudności.



Co robić???

Spróbujemy użyć metody perskiej

$$x^3 = 3x + 1$$

$$x^3 = 3ABx + A^3 + B^3$$

$$AB = 1 \quad A^3 + B^3 = 1$$

$$\downarrow$$

$$A^3B^3 = 1 \quad B^3 = 1/A^3$$

$$A^3 + \frac{1}{A^3} = 1$$

$$(A^3)^2 + 1 = A^3 \quad (A^3)^2 - A^3 + 1 = 0$$

$$\Delta = 1 - 4 = -3 < 0 \quad \text{⚡}$$

Pomysł jest taki, żeby rozszerzyć zbiór liczb rzeczywistych w taki sposób, żeby równanie $x^3 + 1 = 0$ miało rozwiązanie i można było posługiwać się nimi jak „normalnymi” liczbami. Oczywiście trzeba doprecyzować — co to znaczy „rozszerzyć” i co to znaczy „posługiwać się jak liczbami”.

Wypiszmy znane własności operacji dodawanie i mnożenie w $\mathbb{R}$

DODAWANIE

→ jest łączne $\forall x, y, z \in \mathbb{R} \quad (x+y)+z = x+(y+z)$ D1

→ jest przemienne $\forall x, y \in \mathbb{R} \quad x+y = y+x$ D2

→ istnieje element neutralny $x+0 = x = 0+x$ D3

→ istnieje element odwrotny $\forall x \in \mathbb{R} \exists y \in \mathbb{R} : x+y = 0 = y+x$ D4

MNOŻENIE

→ jest łączne $\forall x, y, z \quad (xy)z = x(yz)$ M1

→ jest przemienne $\forall x, y \in \mathbb{R} \quad xy = yx$ M2

→ istnieje element neutralny $\forall x \quad 1 \cdot x = x = x \cdot 1$ M3

→ istnieje element odwrotny $\forall x \neq 0 \exists y : xy = 1 = yx$ M4

WSPÓLNE

→ niechwilność $0 \neq 1$ C1 → rozdzielność $\forall x, y, z \in \mathbb{R} \quad x(y+z) = xy + xz$ C2

DEFINICJA Zbiór K z dwiema operacjami $+: K \times K \rightarrow K$ i $\cdot: K \times K \rightarrow K$ spełniającymi warunki D1-D4, M1-M4, C1, C2 nazywamy **ciałem**. 5

Liczby rzeczywiste z dodawaniem i mnożeniem są ciałem, podobnie liczby wymierne. Jeśli zmniejszymy ten zbiór, np. weźmiemy $(\mathbb{Z}, +, \cdot)$ to stwierdzimy, że nie jest to ciało, gdyż nie zachodzi warunek M4. Mówiąc, że chcemy, aby tymi nowymi liczbami dalo się porządkować tak jak liczbami rzeczywistymi, będziemy mieć na myśli, że zbiór ten ma być wyposażony w działanie $+$, $\cdot$ takie, żeby spełniały warunki bycia ciałem.

Oprócz $(\mathbb{R}, +, \cdot)$ i $(\mathbb{Q}, +, \cdot)$ istnieją też inne ciała. Najmniejszym (w sensie liczby elementów zbioru) ciałem jest $\mathbb{Z}_2$. Jako zbiór jest to $\{0, 1\}$ a działania to:

+	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

łatwo rozpoznać, że są to „zwykłe” działania na resztach z dzielenia przez 2. Więcej o różnych ciałach na ćwiczeniach. ale nie za dużo! Jeśli ktoś chce wiedzieć musi dowieść się sam!

Pozostaje odpowiedzieć na pytanie o rozszerzenie. Chodzi tu o to, żeby nowe liczby zawierały liczby rzeczywiste jako podzbiór wraz z działaniami o zwykłych własnościach, tak żeby te rzeczywiste rozwiązanie równań dalej nimi były. Formalnie rzecz biorąc musi istnieć wyróżnione odwzorowanie

$\mathbb{R} \xrightarrow{\varphi} \mathbb{C}$ różnowartościowe (injekcja) i zachowujące działanie (homomorfizm ciał)

$$\varphi(x) = \varphi(y) \Rightarrow x = y$$

$$\varphi(x+y) = \varphi(x) + \varphi(y)$$

$$\varphi(x \cdot y) = \varphi(x) \varphi(y)$$

$$\varphi(0) = 0$$

$$\varphi(1) = 1$$

Załóżmy teraz że mamy ciało K takie, że (1) $\mathbb{R} \subset K$ jako podciało (tzn. j.w.)
(2) istnieje $i \in K$ takie, że $i^2 = -1$. Rozważmy podzbiór K zdefiniowany jako

$$\mathbb{C} = \{x + iy : x, y \in \mathbb{R}\}$$

Pokażemy (prawie), że ten zbiór jest ciałem. Po pierwsze sprawdzimy, że działanie nie wyprowadzając poza ten zbiór:

$$(x+iy)(a+ib) = xa + iya + xib + iyib = (xa - yb) + i(ya + xb) \quad \text{ok}$$

$$(x+iy) + (a+ib) = (x+a) + i(y+b) \quad \text{ok}$$

Łączności i przemienności nie sprawdzamy, bo to długie a łatwe...

0 bierzemy z $\mathbb{R}$ tzn. $0 + i0$, 1 też z $\mathbb{R}$ $1 + 0i$ i sprawdzamy, że działają jak trzeba

Element odwrotny względem dodawania dla $x+iy$ to $(-x) + (-y)i$

Element odwrotny względem mnożenia ... hmm... policzmy:

6

$$1 = (x+iy)(a+ib) = (xa-yb) + i(xb+ya) \Rightarrow xa-yb=1 \text{ i } xb+ya=0$$

$$b = -\frac{ya}{x} \quad (\text{dla } x \neq 0)$$

$$1 = xa - yb = xa + y\frac{a}{x} \Rightarrow x = (x^2 + y^2)a \Rightarrow a = \frac{x}{x^2 + y^2}, \quad b = \frac{-y}{x^2 + y^2}$$

$$(x+iy)^{-1} = \frac{x}{x^2+y^2} - i \frac{y}{x^2+y^2} \quad (*)$$

Gdy $x=0$ mamy liczbę iy . Odwrotna do niej to $-\frac{i}{y}$. Widać, że to samo dostaniemy ze wzoru (*) mimo, że do wyprowadzenia użyliśmy założenie $x \neq 0$. Jeśli $x=y=0$ to odwrotna nie istnieje (i nie musi).

Rozdzielność sprawdzamy rachunkiem, niechwilność widać. Zbiór $\mathbb{C}$ jest więc ciałem. No dobra, ale zaczęliśmy od założenie, że mamy $\mathbb{K}$. Pytanie czy je mamy? Można wziąć np:

$$\mathbb{K} = \mathbb{R}^2 \text{ jako zbiór, działania } (x,y) + (a,b) = (x+a, y+b)$$

$$(x,y) \cdot (a,b) = (xa-yb, xb+ya)$$

Wtedy $1_{\mathbb{K}} = (1,0)$, $0_{\mathbb{K}} = (0,0)$ i rachunkami sprawdzamy że wszystko działa. Sprawdzamy też, że $i = (0,1)$

Oczywiście każdy zauważy od razu, że zawieranie $\mathbb{C} \subset \mathbb{K}$ jest trywialne, to znaczy tak naprawdę mamy równość! Podsumowując te wszystkie rozważania formalnie mamy:

DEFINICJA Zbiór $\mathbb{C} = \mathbb{R}^2$ z działaniami $+$ i $\cdot$ zdefiniowanymi wzorami

$$(x,y) + (a,b) = (x+a, y+b)$$

$$(x,y) \cdot (a,b) = (xa-yb, xb+ya)$$

nazywamy zbiorem liczb zespolonych.

TWIERDZENIE $(\mathbb{C}, +, \cdot)$ jest ciałem

DOWÓD Już był

TWIERDZENIE Odwzorowanie $\mathbb{R} \rightarrow \mathbb{C}, \quad x \mapsto (x,0)$ jest iniektywnym homomorfizmem ciał

DOWÓD Nudne rachunki

TWIERDZENIE $\mathbb{C}$ jest najmniejszym (z dokładnością do izomorfizmu) rozszerzeniem ciała $\mathbb{R}$ zawierającym element $i : i^2 = -1$. Oznacza to, że jeśli jakieś ciało $\mathbb{K}$ spełnia te warunki to istnieje iniektywny homomorfizm $\varphi : \mathbb{C} \rightarrow \mathbb{K}$.

DOWÓD: Dowód w zasadzie już przeprowadziliśmy. Pozostaje uporządkować rozumowanie: ① Ciało będące rozszerzeniem $\mathbb{R}$ i zawierające i takie że $i^2 = -1$