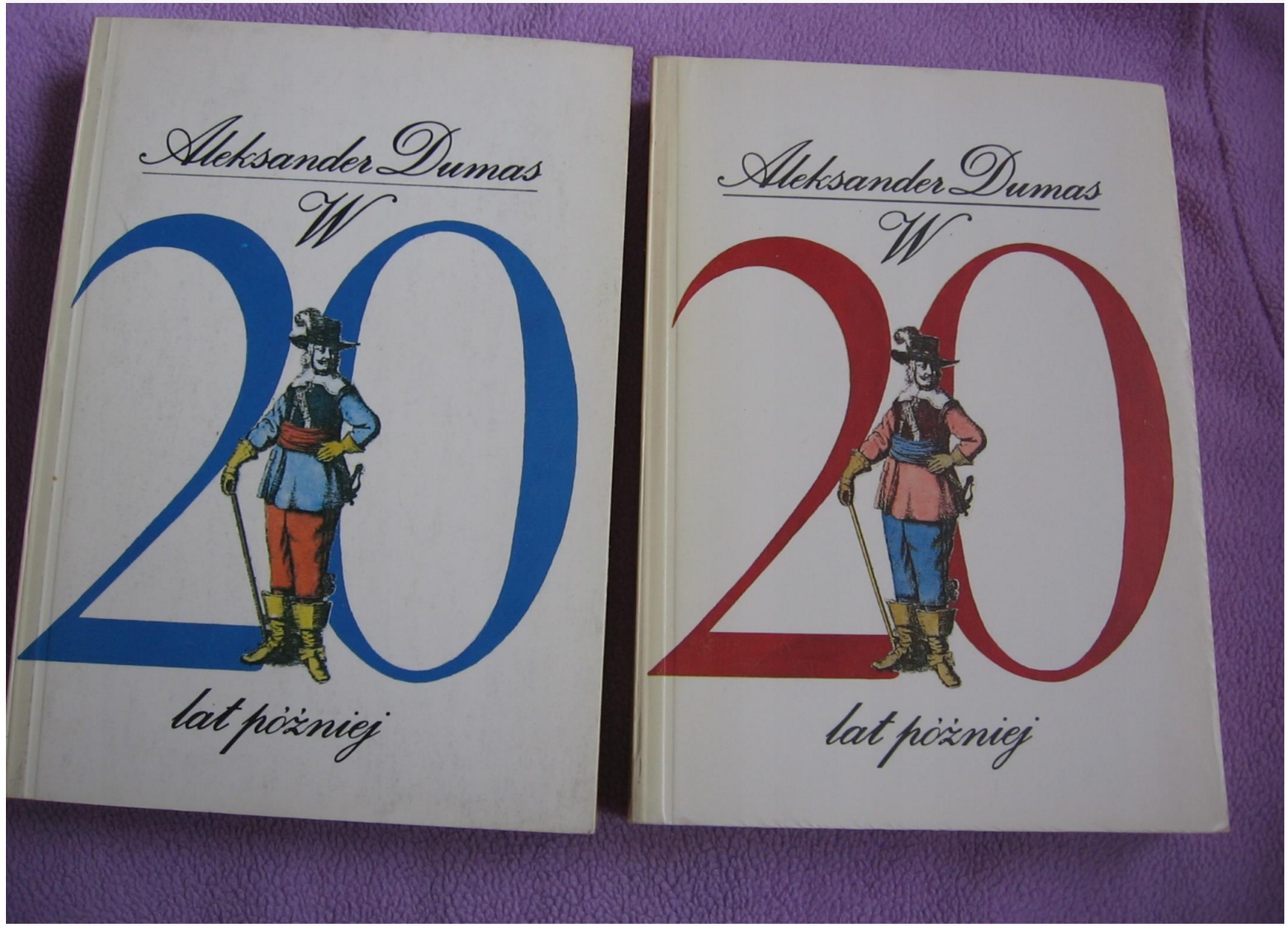
Liczby idealne

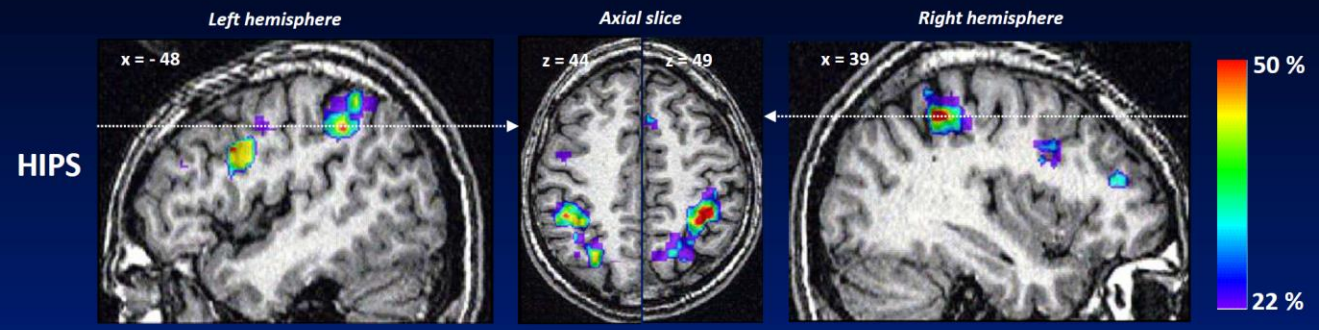
Zbigniew Marciniak

LX Szkoła Matematyki Poglądowej


Aleksander Dumas
W
20
lat później
Aleksander Dumas
W
20
lat później

Liczby idealne

Number sense and the horizontal segment of the intraparietal sulcus (HIPS)



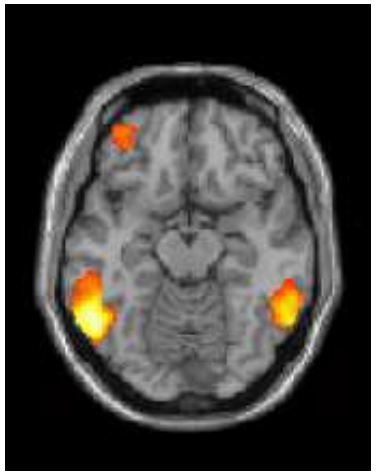
- All numerical tasks activate this region
  (e.g. addition, subtraction, comparison, approximation, digit detection…)

- This region fulfils two criteria for a semantic-level representation:

-It responds to number in various formats (Arabic digits, written or spoken words), more than to other categories of objects (e.g. letters, colors, animals…)

-Its activation varies according to a semantic metric (numerical distance, number size)

Dehaene, S., Piazza, M., Pinel, P., & Cohen, L. (2003).
Cognitive Neuropsychology



A Survey of Modern Algebra

Garrett Birkhoff
Saunders Mac Lane

Liczby rzeczywiste $\mathbb{R}$, cokolwiek by to nie było, mają następujące własności:

1. tworzą ciało:
   - $(x+y)+z = x+(y+z), \quad x+y = y+x, \quad 0+x = x, \quad x+(-x) = 0$
   - $(x \cdot y) \cdot z = x \cdot (y \cdot z), \quad x \cdot y = y \cdot x, \quad 1 \cdot x = x, \quad x \cdot x^{-1} = 1 \quad (x \neq 0)$
   - $(x+y) \cdot z = x \cdot z + y \cdot z$

2. tworzą zbiór liniowo uporządkowany:
   - $x \geqslant x, \quad x \geqslant y,\ y \geqslant x \Rightarrow x = y, \quad x \geqslant y,\ y \geqslant z \Rightarrow x \geqslant z$
   - $x \geqslant y \Rightarrow x+z \geqslant y+z, \quad x \geqslant 0,\ y \geqslant 0 \Rightarrow xy \geqslant 0$

3. każdy niepusty i ograniczony z góry podzbiór $\mathbb{R}$ ma kres górny.

Odwoływanie sie do intuicji geometrycznych w pierwszej prezentacji rachunku różniczkowego uważam za niezmiernie użyteczne z dydaktycznego punktu widzenia, a nawet za niezastąpione, gdy nie chcemy tracić zbyt dużo czasu. Temu jednak, że taka forma wprowadzenia w rachunek różniczkowy nie może rościć sobie pretensji do bycia naukową, nikt nie zaprzeczy. Poczucie niezadowolenia było we mnie tak przemożne, ze podjąłem zdecydowane postanowienie, aby rozmyślać nad tym problemem, dopóki nie znajdę czysto arytmetycznego i doskonale rygorystycznego ugruntowania zasad analizy infinitezymalnej.

Często słyszy się, ze rachunek różniczkowy zajmuje sie wielkościami ciągłymi, ale nie podaje sie nigdy wyjaśnienia, czym jest ta ciagłość. (...) [Należało wiec] zagwarantować rzeczywistą definicję istoty ciągłości. Osiągnąłem ten cel 24 listopada roku 1858, a kilka dni później przedstawiłem wyniki swych rozmyślań memu drogiemu przyjacielowi Durege, z którym odbyłem długa i żywą dyskusję. (Richard Dedekind 1872)

Przekroje Dedekinda zbioru liczb wymiernych

$$\{x \in \mathbb{Q} : x < 1\} \cup \{x \in \mathbb{Q} : x \geqslant 1\}$$

$$\{x \in \mathbb{Q} : x^2 < 2\} \cup \{x \in \mathbb{Q} : x^2 > 2\}$$

„W każdym przypadku kiedy mamy przekrój $L \cup P$ nieodpowiadający żadnej liczbie wymiernej, wyznaczamy nową liczbę niewymierną, którą można uważać za całkowicie określoną przez ten przekrój; będziemy mówić że ta liczba odpowiada przekrojowi lub że produkuje ona ten przekrój.”

Działania na przekrojach:

$$\{x \in \mathbb{Q} : x \geqslant 2\} + \{x \in \mathbb{Q} : x \geqslant 3\} = \{x \in \mathbb{Q} : x \geqslant 5\}$$

Działania na przekrojach:

$$\{x \in \mathbb{Q} : x \geqslant 2\} + \{x \in \mathbb{Q} : x \geqslant 3\} = \{x \in \mathbb{Q} : x \geqslant 5\}$$

$$P_1 + P_2 = \{x_1 + x_2 : x_1 \in P_1, x_2 \in P_2\} \subset \mathbb{Q}$$

Działania na przekrojach:

$$\{x \in \mathbb{Q} : x \geqslant 2\} + \{x \in \mathbb{Q} : x \geqslant 3\} = \{x \in \mathbb{Q} : x \geqslant 5\}$$

$$P_1 + P_2 = \{x_1 + x_2 : x_1 \in P_1, x_2 \in P_2\} \subset \mathbb{Q}$$

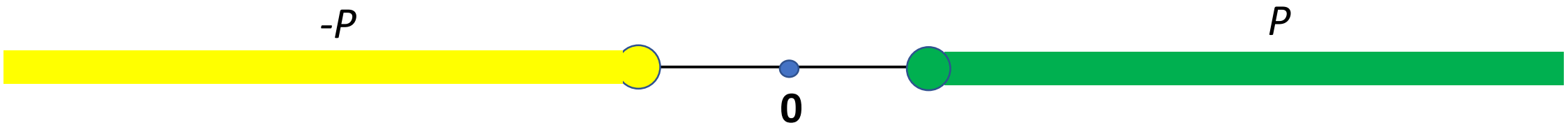
$$-P = \{-x : x \in P\}$$

Działania na przekrojach:

$$\{x \in \mathbb{Q} : x \geqslant 2\} + \{x \in \mathbb{Q} : x \geqslant 3\} = \{x \in \mathbb{Q} : x \geqslant 5\}$$

$$P_1 + P_2 = \{x_1 + x_2 : x_1 \in P_1, x_2 \in P_2\} \subset \mathbb{Q}$$

$$-P = \{-x : x \in P\}$$

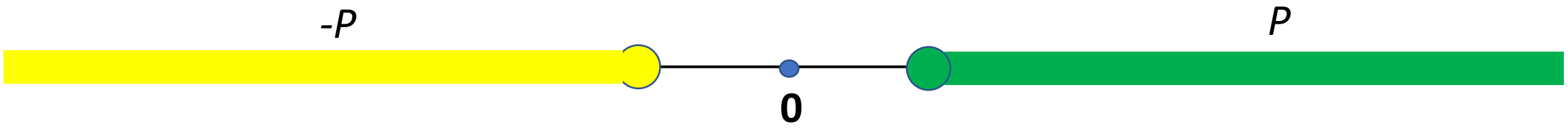


Działania na przekrojach:

$$\{x \in \mathbb{Q} : x \geqslant 2\} + \{x \in \mathbb{Q} : x \geqslant 3\} = \{x \in \mathbb{Q} : x \geqslant 5\}$$

$$P_1 + P_2 = \{x_1 + x_2 : x_1 \in P_1, x_2 \in P_2\} \subset \mathbb{Q}$$

$$-P = \{-x : x \in P\}$$



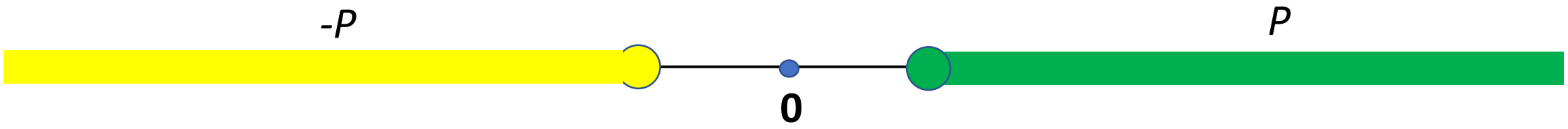
$$-P = \mathbb{Q} \setminus \{-x : x \in P\} \cup \{\text{ewentualnie element najmniejszy}\}$$

Działania na przekrojach:

$$\{x \in \mathbb{Q} : x \geqslant 2\} + \{x \in \mathbb{Q} : x \geqslant 3\} = \{x \in \mathbb{Q} : x \geqslant 5\}$$

$$P_1 + P_2 = \{x_1 + x_2 : x_1 \in P_1, x_2 \in P_2\} \subset \mathbb{Q}$$

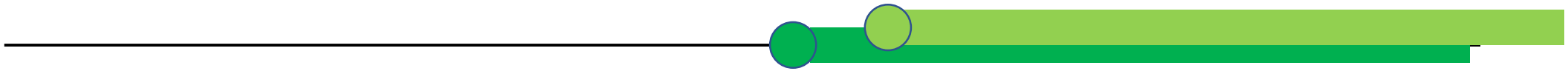
$$-P = \{-x : x \in P\}$$



$$-P = \mathbb{Q} \setminus \{-x : x \in P\} \cup \{\text{ewentualnie element najmniejszy}\}$$

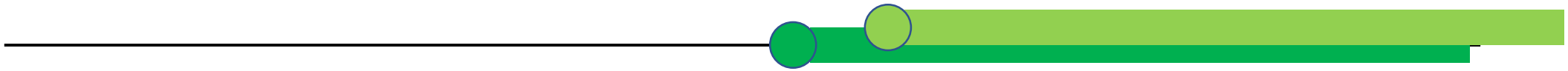
Uporządkowanie przekrojów:

$$P_1 \geqslant P_2 \Leftrightarrow P_1 \subseteq P_2$$



Uporządkowanie przekrojów:

$$P_1 \geqslant P_2 \Leftrightarrow P_1 \subseteq P_2$$



Istnienie kresów górnych:

$$\sup\{P_t\} = \bigcap_t P_t$$

Twierdzenie. Ciało liczb rzeczywistych jest jedyne z dokładnością do izomorfizmu.

Twierdzenie. Ciało liczb rzeczywistych jest jedyne z dokładnością do izomorfizmu.

Dowód.

$$\mathbb{R}_1 \supset \mathbb{Q} \longleftrightarrow \mathbb{Q} \subset \mathbb{R}_2$$

Twierdzenie. Ciało liczb rzeczywistych jest jedyne z dokładnością do izomorfizmu.

Dowód.

$$\mathbb{R}_1 \supset \mathbb{Q} \longleftrightarrow \mathbb{Q} \subset \mathbb{R}_2$$

$$\begin{array}{ccccccc} \mathbb{R}_1 & \supset & \mathbb{Q} & \longleftrightarrow & \mathbb{Q} & \subset & \mathbb{R}_2 \\ & & \cup & & \cup & & \\ & & P & \longleftrightarrow & P & & \end{array}$$

Twierdzenie. Ciało liczb rzeczywistych jest jedyne z dokładnością do izomorfizmu.

Dowód.

$$\mathbb{R}_1 \supset \mathbb{Q} \longleftrightarrow \mathbb{Q} \subset \mathbb{R}_2$$

$$\begin{array}{ccccccc} \mathbb{R}_1 & \supset & \mathbb{Q} & \longleftrightarrow & \mathbb{Q} & \subset & \mathbb{R}_2 \\ & & \cup & & \cup & & \\ & & P & \longleftrightarrow & P & & \end{array}$$

□

Arithmeticorum Liber II. 61

interuallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos esse ad 2. & adhuc superaddere 10. Ter igitur 2. adscitis vnitatibus 10. æquatur 4 N. + 4. & fit 1 N. 3. Erit ergo minor 3. maior 5. & satisfaciunt quæstioni.

ς^ν ἐστὶ. ὁ ἄρα μεῖζων ἔσται ς^ς ἑνὸς μ^ο β̄. δεῖ-σει ἄρα ἀριθμὸς δ̄ μονάδας δ̄ τριπλασίονας ξ̄ζ̄ μ^ο β̄. ℂ ἔστι ὑπερέχειν μ^ο ῑ̄. τρὶς ἄρα μονάδες ϛ̄ μ̄ζ̄ μ^ο ῑ̄. ἴσαι εἰσὶν ς^ις δ̄ μονάσι δ̄. καὶ γίνεται ὁ ἀριθμὸς μ^ο γ̄. ἔσται ὁ μὲν ἐλάσσων μ^ο γ̄. ὁ δὲ μείζων μ^ο ε̄. καὶ ποιοῦσι τὸ προβλημα.

IN QVÆSTIONEM VII.

CONDITIONIS appositæ eadem ratio est quæ & appositæ præcedenti quæstioni, nil enim aliud requirit quàm vt quadratus interualli numerorum sit minor interuallo quadratorum, & Canones iidem hic etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 — 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto a 2 N. — 4. ipse igitur quadratus erit 4 Q. + 16. — 16 N. hæc æquabuntur vnitatibus 16 — 1 Q. Communis adiiciatur vtrimque defectus, & a similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$. Erit igitur alter quadratorum $\frac{256}{25}$. alter vero $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

ΤΟΝ ὁπταχθέντα τετράγωνον διελεῖν εἰς δύο τετραγώνους. ἐπιτετάχθω δὴ ὁ ῑ̄ϛ̄ διελεῖν εἰς δύο τετραγώνους. καὶ τετάχθω ὁ πρῶτος δυνάμεως μιᾶς. δεήσει ἄρα μονάδας ῑ̄ϛ̄ λεῖψει δυνάμεως μιᾶς ἴσας ξ̄ζ̄ τετραγώνῳ. πλάσω τὸ τετράγωνον ἀπὸ ϛ̄ς̄. ὅσων δὴ ποτε λείψει τοσάκων μ^ο ὅσαν ἔχει ἡ ὑ̄ ῑ̄ϛ̄ μ^ο πλευρά. ἔστω ϛ̄ς̄ β̄ λεῖψει μ^ο δ̄. αὐτὸς ἄρα ὁ πρῶτός ἐστι δυνάμεων δ̄ μ^ο ῑ̄ϛ̄ λείψει ϛ̄ς̄ ῑ̄ϛ̄. ταῦτα ἴσα μονάσι ῑ̄ϛ̄ λείψει δυνάμεως μιᾶς. κοινὴ προσκείσθω ἡ λεῖψις. καὶ ἀπὸ ὁμοίων ὅμοια. δυνάμεις ἄρα ε̄ ἴσαι ἀριθμοῖς ῑ̄ϛ̄. καὶ γίνεται ὁ ἀριθμὸς ῑ̄ϛ̄. πέμπτων. ἔσται ὁ μὲν σπ̄ς̄ εἰκοσιπέμπτων. ὁ δὲ ρμδ̄ εἰκοσιπέμπτων, ℂ οἱ δύο συντιθέντες ποιοῦσι τὸν εἰκοσιπεμπτα, ἥτοι μονάδας ῑ̄ϛ̄. καὶ ἔστιν ἑκάτερος τετράγωνος.

OBSERVATIO DOMINI PETRI DE FERMAT.

CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò

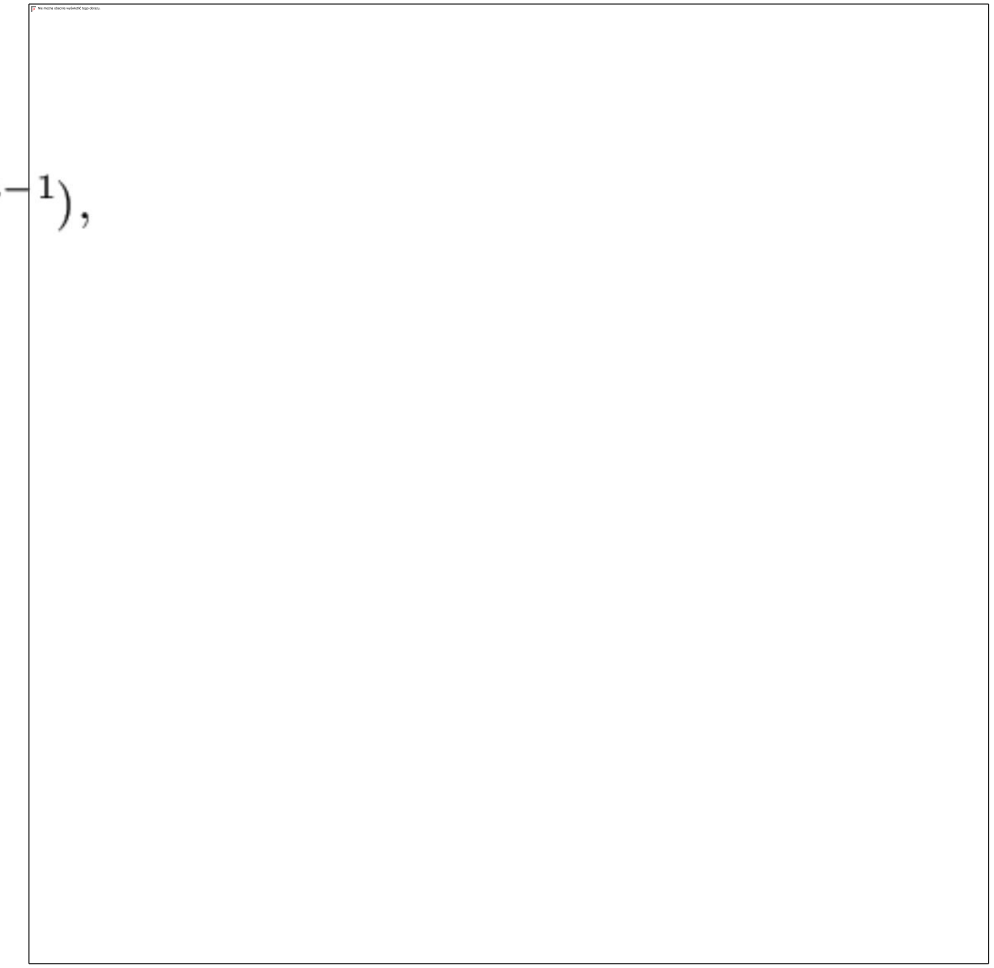
ΕΣΤΩ δὴ πάλιν τὸν ῑ̄ϛ̄ τετράγωνον διελεῖν εἰς δύο τετραγώνους. τετάχθω πάλιν ἡ τοῦ πρώτου πλευρὰ ς^ις ἑνὸς, ἡ δὲ τοῦ ἑτέρου

Jest niemożliwe rozłożyć sześcian na dwa sześciany, czwartą potęgę na dwie czwarte potęgi i ogólnie potęgę wyższą niż druga na dwie takie potęgi; znalazłem naprawdę zadziwiający dowód tego, jednak margines jest za mały, by go pomieścić.

$$x^n + y^n = z^n$$

$$X^n - 1 = (X-1)(X-\xi)(X-\xi^2)\cdots(X-\xi^{n-1}),$$

$\xi -$ pierwiastek z 1 stopnia n



$$X^n - 1 = (X-1)(X-\xi)(X-\xi^2)\cdots(X-\xi^{n-1}),$$

$\xi -$ pierwiastek z 1 stopnia n

$X = \dfrac{z}{y}$:

$$\left(\frac{z}{y}\right)^n - 1 = \left(\frac{z}{y} - 1\right)\left(\frac{z}{y} - \xi\right)\cdots\left(\frac{z}{y} - \xi^{n-1}\right)$$

$$x^n = z^n - y^n = (z-y)(z-\xi y)(z-\xi^2 y)\cdots(z-\xi^{n-1}y) \in \mathbb{Z}[\xi]$$

Każda liczba naturalna posiada jednoznaczny (z dokładnością do kolejności czynników) rozkład na liczby nierozkładalne, czyli pierwsze.

Każda liczba naturalna posiada jednoznaczny (z dokładnością do kolejności czynników) rozkład na liczby nierozkładalne, czyli pierwsze.

W pierścieniu liczb całkowitych $\mathbb{Z}$ mamy $2 = (-1)(-2)$, więc rozkład jest jednoznaczny tylko z dokładnością do znaku, czyli do elementu odwracalnego ± 1.

Każda liczba naturalna posiada jednoznaczny (z dokładnością do kolejności czynników) rozkład na liczby nierozkładalne, czyli pierwsze.

W pierścieniu liczb całkowitych $\mathbb{Z}$ mamy $2 = (-1)(-2)$, więc rozkład jest jednoznaczny tylko z dokładnością do znaku, czyli do elementu odwracalnego ± 1.

R - dowolny pierścień przemienny z jedynką.

Element a jest nierozkładalny, jeśli z równości $a = bc$ wynika, że b lub c jest elementem odwracalnym.

Pierścień R ma własność jednoznaczności rozkładu, jeśli każdy element $a \in R$ może być zapisany w postaci iloczynu elementów nierozkładalnych, które są wyznaczone jednoznacznie z dokładnością do kolejności i czynników odwracalnych.

Czy pierścienie $\mathbb{Z}[\xi]$ mają własność jednoznaczności rozkładu?

Można założyć, że n jest liczbą pierwszą nieparzystą p.

Tak dla $p < 23$.

Dla $p = 23$ liczba 47 nie ma jednoznacznego rozkładu.

W pewnych pierścieniach przemiennych niektóre elementy można rozkładać bez końca:

Na przykład w pierścieniu

$$R = \mathbb{Z}[\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \sqrt[16]{2}, \ldots] \subseteq \mathbb{C}$$

mamy

$$2 = \sqrt{2} \cdot \sqrt{2} = \sqrt[4]{2} \cdot \sqrt[4]{2} \cdot \sqrt[4]{2} \cdot \sqrt[4]{2} = \cdots$$

Jeśli $a = bc$, to mówimy, że $b|a$.

Jeśli $a = bc$, to mówimy, że $b|a$.

Załóżmy, że $a|b$ oraz $b|a$.

Wówczas

$$b = ac, \quad a = bd \Rightarrow b = bdc$$

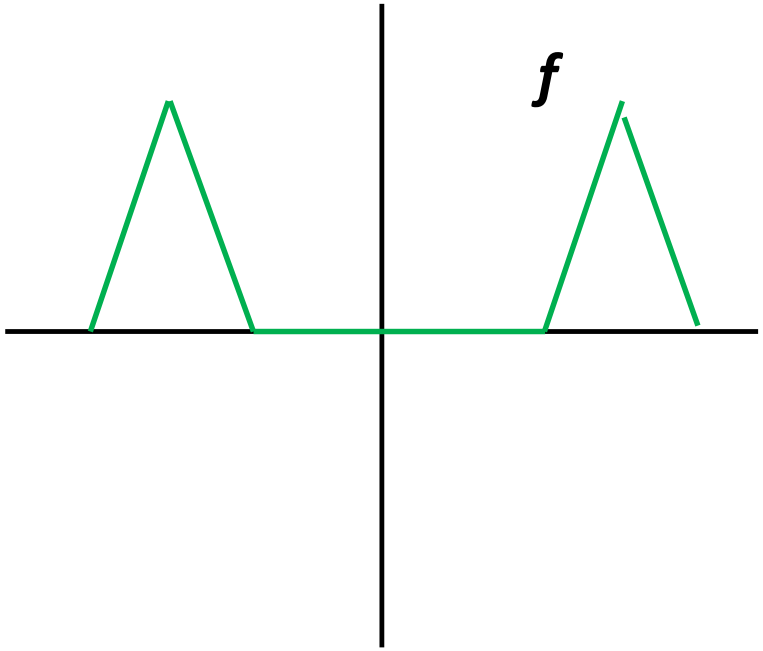
Jeśli pierścień R nie ma dzielników zera, to

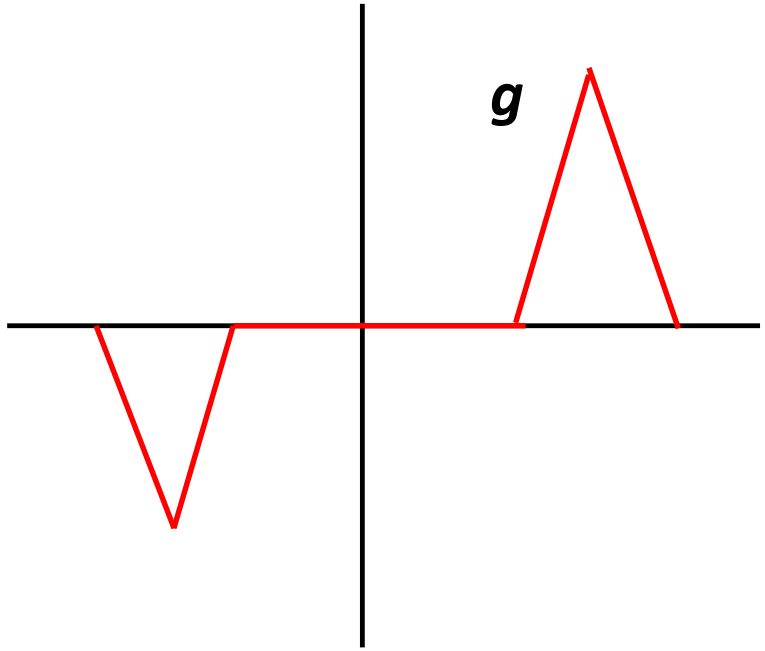
$$b = bdc \Rightarrow 1 = dc, \quad d - \text{odwracalny oraz} \quad b = ac.$$

Zatem elementy a, b są stowarzyszone, to znaczy różnią się o czynnik odwracalny.

Gdy pierścień R ma dzielniki zera, sytuacja wymyka się spod kontroli.

Niech $R = C(\mathbb{R})$.





Dalej rozważamy tylko pierścienie bez dzielników zera.

Dalej rozważamy tylko pierścienie bez dzielników zera.

W $\mathbb{Z}[-14]$ mamy

$$3 \cdot 5 = (1 + \sqrt{-14})(1 - \sqrt{-14})$$

$$3 \cdot 3 \cdot 3 \cdot 3 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14})$$

$$2 \cdot (-7) = (\sqrt{-14})^2$$

Niech

$$R = \{f \in \mathbb{C}[X] : f = a_0 + a_2 X^2 + \cdots + a_n X^n, \quad n \geqslant 0\}$$

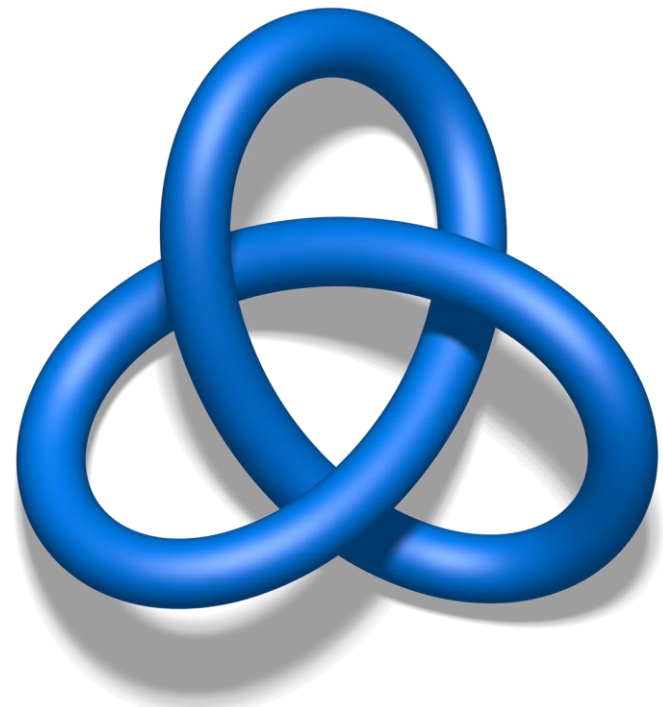
$$X^2 \cdot X^2 \cdot X^2 = X^3 \cdot X^3$$

Niech

$$R = \{f \in \mathbb{C}[X] : f = a_0 + a_2 X^2 + \cdots + a_n X^n, \quad n \geqslant 0\}$$

$$X^2 \cdot X^2 \cdot X^2 = X^3 \cdot X^3$$

$$R \approx \mathbb{C}[U, V]/(U^2 - V^3)$$



$$\{f \in \mathbb{C}[X] : f = a_0 + a_2 X^2 + \cdots + a_n X^n, \quad n \geqslant 0\} \subset \mathbb{C}[X]$$

$$\{f \in \mathbb{C}[X] : f = a_0 + a_2 X^2 + \cdots + a_n X^n, \quad n \geqslant 0\} \subset \mathbb{C}[X]$$

$$R \supset R^* = R \setminus \{0\} \text{ – półgrupa przemienna z mnożeniem}$$

$R^* \longrightarrow \mathcal{D}$, gdzie $\mathcal{D}$ jest półgrupą z jednoznacznością rozkładu

$x \mapsto (x)$

$$\{f \in \mathbb{C}[X] : f = a_0 + a_2 X^2 + \cdots + a_n X^n, \quad n \geqslant 0\} \subset \mathbb{C}[X]$$

$$R \supset R^* = R \setminus \{0\} \text{ – półgrupa przemienna z mnożeniem}$$

$R^* \longrightarrow \mathcal{D}$, gdzie $\mathcal{D}$ jest półgrupą z jednoznacznością rozkładu

$x \mapsto (x)$

Postulujemy:

- $x|y \Leftrightarrow (x)|(y)$
- $d \in \mathcal{D}, \quad d|(x)$ and $d|(y) \Rightarrow d|(x \pm y)$
- $\{d \in \mathcal{D} : d|(x)\} = \{d \in \mathcal{D} : d|(y)\} \Rightarrow x = y$

Skąd wziąć taką półgrupę z jednoznacznością rozkładu?

$$\mathcal{D} = \mathbb{N} \oplus \mathbb{N} \oplus \mathbb{N} \oplus \cdots$$

Skąd wziąć taką półgrupę z jednoznacznością rozkładu?

$$\mathcal{D} = \mathbb{N} \oplus \mathbb{N} \oplus \mathbb{N} \oplus \cdots$$

Przykład.

$$\nu_p : \mathbb{Q} \longrightarrow \mathbb{Z}, \quad \nu_p\left(\frac{p^n a}{b}\right) = n.$$

Skąd wziąć taką półgrupę z jednoznacznością rozkładu?

$$\mathcal{D} = \mathbb{N} \oplus \mathbb{N} \oplus \mathbb{N} \oplus \cdots$$

Skąd wziąć homomorfizm półgrup $R^* \longrightarrow \mathcal{D}$?

$$R \subseteq \mathbb{F} \xrightarrow{waluacje} \mathbb{N}$$

DEFINICJA. Waluacją na ciele $\mathbb{F}$ nazywamy funkcję $\nu\colon \mathbb{F} \longrightarrow \mathbb{Z}$ taką, że

$$\nu(x \cdot y) = \nu(x) + \nu(y)$$
$$\nu(x + y) \geqslant \min(\nu(x), \nu(y))$$

PRZYKŁAD.

$$\nu_p\colon \mathbb{Q} \longrightarrow \mathbb{Z}, \quad \nu_p\left(\frac{p^n a}{b}\right) = n.$$

Czy nie można brakujących elementów – liczb idealnych – znaleźć w obrębie pierścienia R?

Zbiór R^* nie jest częściowo uporządkowany relacją podzielności:

$$x \leqslant y \Leftrightarrow x|y$$

ale zbiór klas stowarzyszenia – jest.

Zbiór R^* nie jest częściowo uporządkowany relacją podzielności:

$$x \leqslant y \Leftrightarrow x|y$$

ale zbiór klas stowarzyszenia – jest.

$$\{x \subset R : a \leqslant x\} = \{x \in R : x = ab\} = aR$$

Ideały są brakującymi liczbami idealnymi.

Ideał I to niepusty podzbiór pierścienia R, który

- jest podgrupą ze względu na dodawanie: $x, y \in I \Rightarrow x - y \in I$
- jest pułapką ze względu na mnożenie: $x \in I, r \in R \Rightarrow rx \in I$

„Przedziałom z końcem” odpowiadają ideały postaci xR, czyli ideały główne.

Działania na ideałach:

$$I + J = \{x + y : x \in I, y \in J\}$$

$$I \cdot J = \{\sum x_i y_i : x_i \in I, y_i \in J\}$$

Działania na ideałach:

$$I + J = \{x + y : x \in I, y \in J\}$$

$$I \cdot J = \{\sum x_i y_i : x_i \in I, y_i \in J\}$$

Elementom nierozkładalnym odpowiadają ideały pierwsze:

$$xy \in I \Rightarrow x \in I \ \text{ lub } \ y \in I$$

Działania na ideałach:

$$I + J = \{x + y : x \in I, y \in J\}$$

$$I \cdot J = \{\sum x_i y_i : x_i \in I, y_i \in J\}$$

Elementom nierozkładalnym odpowiadają ideały pierwsze:

$$xy \in I \Rightarrow x \in I \ \text{ lub } \ y \in I$$

TWIERDZENIE. Jeśli R jest pierścieniem liczb całkowitych w skończonym rozszerzeniu ciała $\mathbb{Q}$ (np. $R = \mathbb{Z}[\xi]$), to każdy ideał w R posiada jednoznaczny rozkład na iloczyn ideałów pierwszych.

$$2 \cdot (-7) = (\sqrt{-14})^2$$

$$I = (2, \sqrt{-14}), \quad J = (7, \sqrt{-14})$$

Wtedy

$$I^2 = (2), \quad J^2 = (-7), \quad IJ = (\sqrt{-14})$$

zatem

$$I^2 \cdot J^2 = (IJ)^2$$