Matematyka

Teoria Liczb Rzeczywistych

Aleksander Denisiuk

`denisjuk@euh-e.edu.pl`

Elbląska Uczelnia Humanistyczno-Ekonomiczna

ul. Lotnicza 2

82-300 Elbląg

Teoria Liczb Rzeczywistych

Najnowsza wersja tego dokumentu dostępna jest pod adresem

`http://denisjuk.euh-e.edu.pl/`

Zbiory Liczbowe

- $\mathbb{N} = \{1, 2, \ldots\}$ — zbiór liczb naturalnych,
- $\mathbb{Z}$ — zbiór liczb całkowitych,
- $\mathbb{Q}$ — zbiór liczb wymiernych,
- $\mathbb{R}$ — zbiór liczb rzeczywistych.

Liczby wymierne

- $\mathbb{Q}^* = \left\{ \frac{m}{n} \,\middle|\, m, n \in \mathbb{Z},\ n \neq 0 \right\}$,
- $\frac{m_1}{n_1} \sim \frac{m_2}{n_2} \iff m_1 n_2 = m_2 n_1$,
- $\mathbb{Q} = \mathbb{Q}^* / \sim$,
- $\mathbb{Q}$ jest ciałem ułamków ciała $\mathbb{Z}$.

Dodawanie liczb wymiernych

Definicja 1.

$\frac{m_1}{n_1} + \frac{m_2}{n_2} = \frac{m_1 n_2 + n_1 m_2}{n_1 n_2}$

Własności dodawania

- $\forall x, y \in \mathbb{Q} \quad x + y = y + x$ (przemienność dodawania),
- $\forall x, y, z \in \mathbb{Q} \quad (x + y) + z = x + (y + z)$ (łączność dodawania),
- Istnieje liczba $0 \in \mathbb{Q}$, taka że $\forall x \in \mathbb{Q} \quad x + 0 = 0 + x = x$ (liczba neutralna),
- $\forall x \in \mathbb{Q}$ istnieje liczba przeciwna $(-x) \in \mathbb{Q}$, taka że $x + (-x) = (-x) + x = 0$.

Mnożenie liczb wymiernych

Definicja 2.

$$\frac{m_1}{n_1} \cdot \frac{m_2}{n_2} = \frac{m_1 m_2}{n_1 n_2}$$

Własności mnożenia

- $\forall x, y \in \mathbb{Q} \quad xy = yx$ (przemienność mnożenia),
- $\forall x, y, z \in \mathbb{Q} \quad (xy)z = x(yz)$ (łączność mnożenia),
- Istnieje liczba $1 \in \mathbb{Q}$, taka że $\forall x \in \mathbb{Q} \quad 1 \cdot x = x \cdot 1 = x$.
- $\forall x, y, z \in \mathbb{Q} \quad x(y + z) = xy + xz$ oraz $(x + y)z = xz + yz$ (rozdzielność mnożenia względem dodawania),
- $\forall x \in \mathbb{Q},\ x \neq 0 \quad \exists x^{-1} \in \mathbb{Q}$ (element odwrotny) taki że $x \cdot x^{-1} = x^{-1} \cdot x = 1$

Porównywanie liczb wymiernych

Definicja 3.

$$\frac{m_1}{n_1} < \frac{m_2}{n_2} \iff \begin{array}{l} \big(m_1 n_2 < m_2 n_1 \text{ i } n_1 n_2 > 0\big) \\ \text{albo} \\ \big(m_1 n_2 > m_2 n_1 \text{ i } n_1 n_2 < 0\big) \end{array}$$

Własności relacji uporządkowania

- $a > b \Rightarrow a + c > b + c$,
- $a > b, c > 0 \Rightarrow ac > bc$.

Aksjomat Archimedesa

Twierdzenie 4. *Dla dowolnej liczby $a \in \mathbb{Q}$ jedynkę (1) można powtórzyć tyle razy, że suma zostanie większa od a.*

- Nieograniczoność zbioru liczb wymiernych.
- Dowolny odcinek jest krótszy od pewnej wielokrotności każdego innego odcinka.

Podstawowe własnoći liczb wymiernych

- Dowolna własność liczb wymiernych jest wnioskiem 16 podstawowych.

Przykład 5. Niech $a > b$ oraz $c > d$. Wtedy $a + c > b + d$.

Niezupełność zbioru liczb wymiernych

Twierdzenie 6.

$$\sqrt{2} \neq \mathbb{Q}$$

Dowód.

- Załóżmy, że

$$\sqrt{2} = \frac{m}{n} \quad \text{(ułamek nieskracalny).} \tag{1}$$

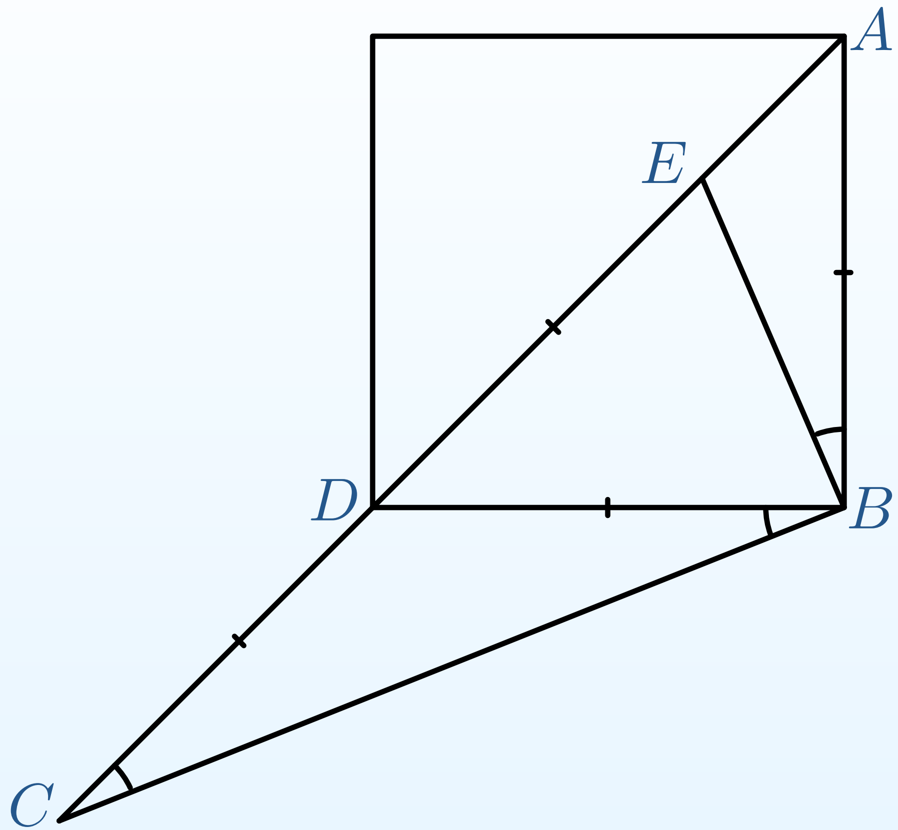
- Wtedy $m^2 = 2n^2$ czyli m jest liczbą parzystą, $m = 2m_1$.
- Podstawiając do (1), otrzymamy po skróceniu

$$2m_1^2 = n^2,$$

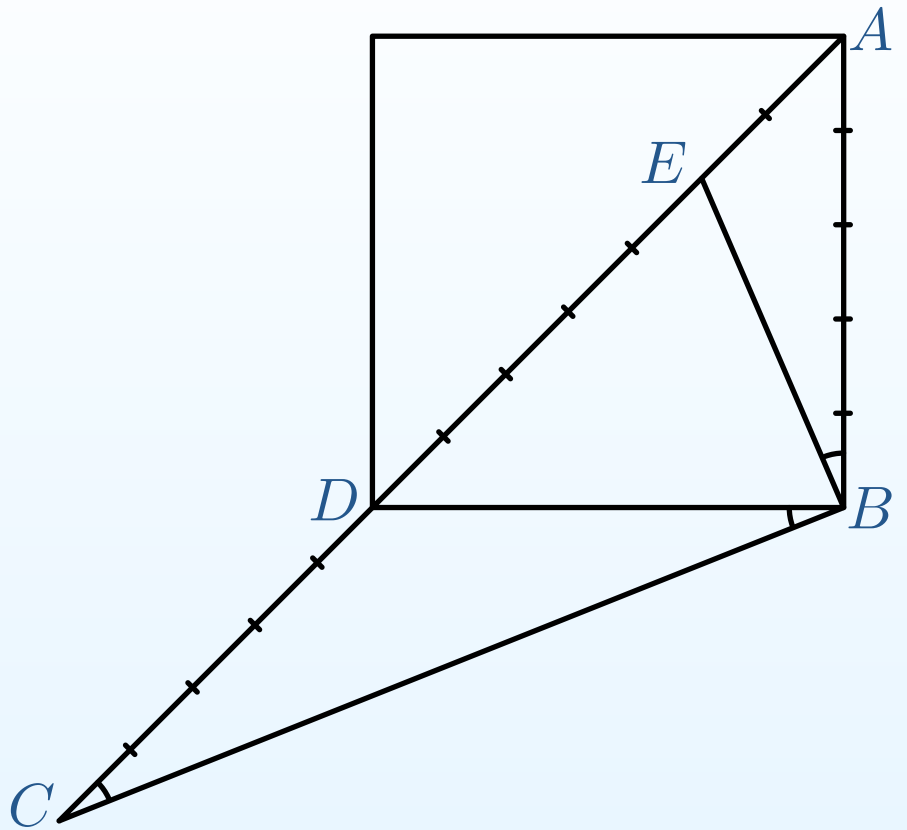
  czyli n też jest liczbą parzystą.
- Sprzeczność.

□

Niezupełność zbioru liczb wymiernych



Niezupełność zbioru liczb wymiernych



Liczby rzeczywiste

- Zbiór $\mathbb{R}$ jest uzupełnieniem zbioru $\mathbb{Q}$:
  - jest polem względem dodawania i mnożenia,
  - okreslona relacja mniejszoćsi,
  - spełniony jest aksjomat Archimedesa,
  - spełniony jest aksjomat ciągłości

Aksjomat ciągłości

Aksjomat 7. *Niech zbiór $\mathbb{R}$ będzie podzielony na dwa niepuste podzbiory A i B: $\mathbb{R} = A \cup B$ w ten sposób, że każda liczba A jest mniejsza od każdej liczby B, to wówczas zachodzi jedna z dwóch możliwości: albo w zbiorze A istnieje największy element, albo w zbiorze B istnieje najmniejszy element.*

Liczby rzeczywiste. Sposób konstruktywny

- $a = a_0{,}a_1a_2a_3\ldots, \quad a_i \in \{0, 1, 2, \ldots, 9\}$ dla $i > 0$,
- $a_0{,}a_1a_2a_3\ldots a_n000\ldots = a_0{,}a_1a_2a_3\ldots(a_n - 1)999\ldots$
- $0{,}5000\ldots = 0{,}4999\ldots$

Kresy zbioru

- Niech A będzie podzbiorem zbioru liczb rzeczywistych, $A \subset \mathbb{R}$.

Definicja 8. Zbiór A jest *ograniczonycm z góry (z dołu),* jeżeli istnieje liczba $M \in \mathbb{R}$, taka że $\forall x \in A \Rightarrow x \leqslant M$ (względnie $x \geqslant M$). Zbiór, ograniczony z dołu i z góry nazywa się *ograniczonym.*

Definicja 9. Element $M \in A$ nazywa się *maksymalnym (minimalnym),* jeżeli $\forall x \in A \Rightarrow x \leqslant M$ $(x \geqslant M)$: $\quad M = \max A \, (\min A)$.

Definicja 10. Najmniejsza z liczb $M \in \mathbb{R}$, takich że $\forall x \in A \Rightarrow x \leqslant M$, jest *górnym kresem* zbioru A: $\quad M = \sup A$.

Definicja 11. Największa z liczb $M \in \mathbb{R}$, takich że $\forall x \in A \Rightarrow x \geqslant M$, jest *dolnym kresem* zbioru A: $\quad M = \inf A$.

Kresy zbioru. twierdzenie

Twierdzenie 12. *Niepusty zbiór ograniczony z góry (z dołu) ma górny (dolny) kres.*

Dowód.

- Rozważamy zbiór ograniczony z góry.
- Określimy dwa podzbiory $\mathbb{R}$: $A_1 = \{ y \in \mathbb{R} \mid \forall x \in A, x \leqslant y \}$ i $A_2 = \{ z \in \mathbb{R} \mid \exists x \in A, x > z \}$.
- A_1 jest *dopełnieniem* A_2.
- A_1 jest niepustym.
- A_2 jest niepustym.
- $\forall y \in A_1, \forall z \in A_2$ spełnia się nierówność $z < y$, ponieważ $\exists x \in A$, $z < x$ i $x \leqslant y$.
- Za mocą aksjomatu ciągłości istnieje albo najmniejszy element A_1, albo największy element A_2.

–verte–

Kresy zbioru, cd

Dowód. cd.

- A_2 nie ma największego elementu.
- A więc $\min A_1 = \sup A$.

$\square$

Przykład 13. Niech $A = \{\, 1/n \mid n \in \mathbb{N} \,\} \subset \mathbb{R}$. Wtedy:

- $\sup A = 1$,
- $\inf A = 0$,
- $\max A = 1$,
- $\min A$ nie istnieje.

Wartość bezwzględna

Definicja 14.

$$|x| = \begin{cases} x, & x \geqslant 0 \\ -x, & x < 0 \end{cases}$$

Twierdzenie 15. *1.* $|ab| = |a| \cdot |b|$,

2. $|a + b| \leqslant |a| + |b|$.

Dowód.
$-|a| \leqslant a \leqslant |a|,\ -|b| \leqslant b \leqslant |b| \Rightarrow -(|a|+|b|) \leqslant a+b \leqslant (|a|+|b|)$ $\square$

Podzbiory $\mathbb{R}$

Definicja 16.

- Zbiór $\{\, x \in \mathbb{R} \mid a \leqslant x \leqslant b \,\}$, gdzie $a < b$, nazywa się *przedziałem domkniętym,* oznacza się przez $[a, b]$. Punkty a i b — to są *kresy* albo *końce* przedziału, a dowolna liczba x, $a < x < b$ jest punktem wewnętrznym przedziału.
- Zbiór $\{\, x \in \mathbb{R} \mid a < x < b \,\}$, gdzie $a < b$, nazywa się *przedziałem otwartym,* oznacza się przez (a, b).
- Zbiór $\{\, x \in \mathbb{R} \mid a \leqslant x < b \,\}$ ($\{\, x \in \mathbb{R} \mid a < x \leqslant b \,\}$) nazywa się *przedziałem półotwartym,* oznacza się przez $[a, b)$ (względnie $(a, b]$).
- Zbiór $\mathbb{R}$ oznaczamy przez $(-\infty, +\infty)$, nazywamy również *prostą.* Jeżeli $x < y$, to mówimy, że x jest *po lewej* od y, y jest *po prawej* od x.
- Zbiór $\{\, x \in \mathbb{R} \mid a \leqslant x \,\}$ ($\{\, x \in \mathbb{R} \mid x \leqslant b \,\}$) nazywa się *półprostą,* oznacza się przez $[a, +\infty)$ (względnie $(-\infty, b]$).
- Zbiór $\{\, x \in \mathbb{R} \mid a < x \,\}$ ($\{\, x \in \mathbb{R} \mid x < b \,\}$) nazywa się *półprostą otwartą,* oznacza się przez $(a, +\infty)$ (względnie $(-\infty, b)$).

Otoczenia punktu

Definicja 17.

- Przedział $(a-\varepsilon, a+\varepsilon)$ (gdzie $\varepsilon > 0$) jest ε-*otoczeniem* punktu a.
- Dowolny przedział otwarty, zawierający punkt a jest *otoczeniem* punktu a.
- Przedział $(a-\varepsilon a) \cup (a, a+\varepsilon)$ (gdzie $\varepsilon > 0$) jest ε-*sąsiedztwem* punktu a.
- Dowolny przedział otwarty, zawierający punkt a z wyłączeniem jego samego jest *sąsiedztwem* punktu a.
- Przedział $(a-\varepsilon, a)$ (gdzie $\varepsilon > 0$) jest *lewym otoczeniem* punktu a.
- Przedział $(a, a+\varepsilon)$ (gdzie $\varepsilon > 0$) jest *prawym otoczeniem* punktu a.

Otoczenie nieskończoności

Definicja 18.

- Zbiór $\{\, x \in \mathbb{R} \mid A < |x| \,\}$, gdzie $A > 0$, nazywa się *otoczeniem nieskończoności* (∞).
- Zbiór $\{\, x \in \mathbb{R} \mid A < x \,\}$, gdzie $A > 0$, nazywa się *otoczeniem plus nieskończoności* ($+\infty$).
- Zbiór $\{\, x \in \mathbb{R} \mid x < -A \,\}$, gdzie $A > 0$, nazywa się *otoczeniem minus nieskończoności* ($-\infty$).

Uwaga 19. Przedział nazywa się również *odcinkiem.* Zamiast nawiasów kwadratowych $[\,]$ używa się również nawiasów kątowych: $\langle\,\rangle$.