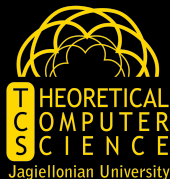


METODY FORMALNE INFORMATYKI

Marek Zaionc

<https://marekzaionc.staff.tcs.uj.edu.pl/>



Wykłady 11, 12 w dniach 12 i 19 listopada 2024

Aksjomat regularności

Aksjomat regularności

Nazywamy czasami aksjomatem dobrego ufundowania.

$$\forall x (x \neq \emptyset \implies \exists y (y \in x \wedge y \cap x = \emptyset))$$

Aksjomat regularności

Z aksjomatu regularności wynika w szczególności, że:

$$\forall x \ x \notin x$$

Aksjomat regularności

Również nie jest możliwe zbudowanie żadnego skończonego ciągu zbiorów tak by pierwszym i ostatnim był ten sam zbiór:

$$x \in y \in x \quad (1)$$

$$x \in y \in z \in x \quad (2)$$

$$x \in y \in z \in t \in x \quad (3)$$

Konstrukcja von Neumanna



John von Neumann
(Budapest 1903 - Princeton 1957)

Konstrukcja von Neumanna

następnik

Następnikiem zbioru x nazywamy zbiór $x \cup \{x\}$ i oznaczamy go przez x' .

Aksjomat

$$\exists x \ (\emptyset \in x \wedge \forall y \ (y \in x \Rightarrow y' \in x))$$

Definicja

Każdy taki zbiór x który spełnia aksjomat nieskończoności nosi nazwę zbioru induktywnego.

Lemat

Niech I będzie pewną niepustą rodziną zbiorów induktywnych.

Teza: $\bigcap I$ jest też zbiorem induktywnym.

Definicja $\mathbb{N}$

Twierdzenie

Istnieje najmniejszy zbiór induktywny. Zbiór ten jest jedyny.

Definicja

Zbiór ten oznaczamy przez $\mathbb{N}$ a elementy tego zbioru nazywamy liczbami naturalnymi.

Twierdzenie o indukcji

Twierdzenie (o indukcji)

Niech zbiór $P \subset \mathbb{N}$ będzie taki że

▶ $\emptyset \in P$

▶ *jeżeli $x \in P$ to $x' \in P$*

to $P = \mathbb{N}$.

Własności liczb naturalnych

Lemat

Dla dowolnych liczb naturalnych $n, m \in \mathbb{N}$ jest:

- 1. jeżeli $m \in n$ to $m \subset n$*
- 2. $n \notin n$*
- 3. jeżeli $m' = n'$ to $n = m$*
- 4. jeżeli $m \subset n$ oraz $m \neq n$ to $m \in n$*
- 5. $m \subset n$ lub $n \subset m$*
- 6. $m = n$ albo $m \in n$ albo $n \in m$*

Definicja

Dla dowolnych liczb naturalnych $n, m \in \mathbb{N}$ oznaczamy

$n < m$ gdy $n \in m$

$n \leq m$ gdy $n \subset m$

Lemat

*Każda liczba naturalna za wyjątkiem 0 ma poprzednik.
Poprzednik jest jedyny.*

Własności porządku na $\mathbb{N}$

Lemat

Dla dowolnych liczb naturalnych $n, m, k \in \mathbb{N}$ zachodzi:

- 1. jeżeli $n \leq m$ oraz $m \leq k$ to $n \leq k$*
- 2. jeżeli $n \leq m$ oraz $m < k$ to $n < k$*
- 3. jeżeli $n < m$ oraz $m \leq k$ to $n < k$*

Porządek na $\mathbb{N}$

Trywialne własności porządku na $\mathbb{N}$.

- ▶ $0 \leq x$
- ▶ jeżeli $n < q$ to $n' \leq q$
- ▶ jeżeli $n' \leq q$ to $n < q$
- ▶ jeżeli $n < q'$ to $n \leq q$
- ▶ pomiędzy n a n' nie ma żadnej liczby naturalnej

Zasada minimum

Twierdzenie (Zasada minimum)

Każdy niepusty zbiór liczb naturalnych posiada element najmniejszy.

Zasada maksimum

Definicja

Zbiór $Z \subset \mathbb{N}$ jest ograniczony od góry gdy

$$\exists n \in \mathbb{N} \quad \forall m \in Z \quad m < n$$

Twierdzenie (Zasada maksimum)

Każdy niepusty ograniczony od góry zbiór liczb naturalnych posiada element największy.

Definiowanie przez indukcję

Twierdzenie (Definiowanie przez schemat rekursji prostej)

Niech A, Z będą zbiorami. Niech $g : A \rightarrow Z$ oraz niech $h : Z \times \mathbb{N} \times A \rightarrow Z$. Istnieje jedyna funkcja $f : \mathbb{N} \times A \rightarrow Z$ taka że:

$$f(0, a) = g(a) \quad (4)$$

$$f(n', a) = h(f(n, a), n, a) \quad (5)$$

Definiowanie przez indukcję

Dla dowodu należy rozważyć zbiór:

$$P := \{n \in \mathbb{N} : \exists_{f_n} f_n : n' \times A \rightarrow Z \text{ oraz } (*)\}$$

Warunek $(*)$ jest następujący

1. $\forall_{a \in A} f_n(0, a) = g(a)$
2. $\forall_{a \in A, k < n} f_n(k', a) = h(f_n(k, a), k, a)$

Definicja

Niech $A = Z = \mathbb{N}$. Niech $g = 1_{\mathbb{N}}$. Niech $h : \mathbb{N}^3 \rightarrow \mathbb{N}$ będzie zdefiniowane przez $h(p, n, a) = p'$. Otrzymaną z funkcji g i h funkcję $f : \mathbb{N}^2 \rightarrow \mathbb{N}$ nazywamy dodawaniem i oznaczamy przez $+$. Będziemy stosowali dla niej notację infiksową.

Niech $A = Z = \mathbb{N}$. Niech $g(x) = 0$. Niech $h : \mathbb{N}^3 \rightarrow \mathbb{N}$ będzie zdefiniowane przez $h(p, n, a) = p + a$. Otrzymaną z funkcji g i h funkcje $f : \mathbb{N}^2 \rightarrow \mathbb{N}$ nazywamy mnożeniem i oznaczamy przez $\times$. Będziemy stosowali dla niej notację infiksową.

Dodawanie i mnożenie

W notacji infiksowej dodawanie i mnożenie definiujemy:

1. $0 + n = n$

2. $k' + n = (k + n)'$

3. $0 \times n = 0$

4. $k' \times n = (k \times n) + n$

Własności dodawania.

1. łączność dodawania $n + (k + p) = (n + k) + p$, dowód - indukcja na n .
2. $n + 0 = n$
3. $m' + n = m + n'$ dowód - indukcja na m .
4. przemienność dodawania $n + k = k + n$, dowód - indukcja na n .

Własności dodawania.

1. prawo skreśleń. Jeżeli $n + p = k + p$ to $n = k$, dowód indukcyjna na p .
2. Jeżeli $n > k$ to istnieje $p \neq 0$ takie że $n = k + p$.
(indukcja na n)

Własności mnożenia.

1. rozdzielnosc $n \cdot (k + p) = n \cdot k + n \cdot p$
2. łączność mnożenia $n \cdot (k \cdot p) = (n \cdot k) \cdot p$, dowód - indukcja na n .
3. $n \cdot 0 = 0$
4. przemienność mnożenia $n \cdot k = k \cdot n$, dowód - indukcja na n .
5. prawo skracania. Jeżeli $n \cdot p = k \cdot p$ i $p \neq 0$ to $n = k$, dowód indukcja na p .

Konstrukcja liczb całkowitych

Definicja

Niech $\approx$ będzie relacją określoną na $\mathbb{N} \times \mathbb{N}$ następująco:

$$(n, k) \approx (p, q) \text{ wtw } n + q = k + p$$

Fakt

Relacja $\approx$ jest relacją równoważności o polu $\mathbb{N} \times \mathbb{N}$.

Konstrukcja liczb całkowitych

Definicja

$$\text{Niech } \mathbb{Z} = \mathbb{N} \times \mathbb{N} / \approx$$

Operacje na $\mathbb{Z}$

Zero $0 \in \mathbb{Z}$ to element $[(0, 0)]_{\approx}$.

Element przeciwny do danego:

jeżeli $x = [(n, k)]_{\approx}$ to przez $-x = [(k, n)]_{\approx}$

Dodawanie:

$$[(n, k)]_{\approx} + [(p, q)]_{\approx} = [(n + p, k + q)]_{\approx}$$

Mnożenie:

$$[(n, k)]_{\approx} \cdot [(p, q)]_{\approx} = [(n \cdot p + k \cdot q, n \cdot q + k \cdot p)]_{\approx}$$

Odejmowanie: $x - y = x + (-y)$

Włożenie $\mathbb{N}$ w $\mathbb{Z}$

Rozważmy funkcję $i : \mathbb{N} \rightarrow \mathbb{Z}$ zadaną wzorem $i(n) = [(n, 0)]_{\approx}$. Funkcja ta jest naturalnym włożeniem zbioru $\mathbb{N}$ w zbiór $\mathbb{Z}$. Jest iniektywna i zgodna z działaniami.

1. $i(0) = 0$
2. $i(n + m) = i(n) + i(m)$
3. $i(n \cdot m) = i(n) \cdot i(m)$

Dzięki włożeniu i będziemy utożsamiali liczbę naturalną n z odpowiadającą jej liczbą całkowitą $i(n)$.

Własności działań na liczbach całkowitych

1. $x + y = y + x$

2. $x \cdot y = y \cdot x$

3. $x \cdot y = z \cdot y$ oraz $y \neq 0$ to $x = z$ (prawo skracania)

4. $x \cdot (y + z) = x \cdot y + x \cdot z$

Konstrukcja liczb wymiernych

Niech $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$. Określamy relację $\sim$ na zbiorze $\mathbb{Z} \times \mathbb{Z}^*$ następująco.

$$(a, b) \sim (c, d) \text{ wtw } a \cdot d = c \cdot b$$

Fakt

Relacja $\sim$ jest równoważnością.

Definicja

$$\text{Niech } \mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^* / \sim$$

Oznaczenie

$$[(a, b)]_{\sim} = \frac{a}{b}$$

Działania na ułamkach

- ▶ $-[(a, b)]_{\sim} = [(-a, b)]_{\sim}$
- ▶ dodawanie $[(a, b)]_{\sim} + [(c, d)]_{\sim} = [(ad + bc, bd)]_{\sim}$
- ▶ odejmowanie $[(a, b)]_{\sim} - [(c, d)]_{\sim} = [(ad - bc, bd)]_{\sim}$
- ▶ mnożenie $[(a, b)]_{\sim} \cdot [(c, d)]_{\sim} = [(ac, bd)]_{\sim}$
- ▶ dzielenie, $[(a, b)]_{\sim} : [(c, d)]_{\sim} = [(ad, bc)]_{\sim}$ gdy $[(c, d)]_{\sim} \neq [(0, d)]_{\sim}$

Porządek na ułamkach

$$\frac{a}{b} > 0 \text{ gdy } a \cdot b > 0.$$

$$\frac{a}{b} > \frac{c}{d} \text{ gdy } \frac{a}{b} - \frac{c}{d} > 0$$

wartość bezwzględna

$$|x| = \begin{cases} x & \text{gdy } , x \geq 0 \\ -x & \text{w przeciwnym przypadku.} \end{cases}$$

Włożenie $\mathbb{Z}$ w $\mathbb{Q}$

Rozważmy funkcję $j : \mathbb{Z} \rightarrow \mathbb{Q}$ zadaną wzorem $j(a) = [(a, 1)]_{\sim}$. Funkcja ta jest naturalnym włożeniem zbioru $\mathbb{Z}$ w zbiór $\mathbb{Q}$. Jest iniektywna i zgodna z działaniami.

1. $j(a + b) = j(a) + j(b)$
2. $j(a - b) = j(a) - j(b)$
3. $j(a \cdot b) = j(a) \cdot j(b)$

Dzięki włożeniu j będziemy utożsamiali liczbę całkowitą a z odpowiadającą jej liczbą wymierną $j(a)$.