I Logika i teoria mnogości

4) Aksjomatyka Peano liczb naturalnych. Indukcja matemetyczna.

(z notatek z wykładu dr W. Kraśkiewicza)

Aksjomatyka Peano (Elementarna własność liczb $\mathbb{N}$, $n \in \mathbb{N}$)

Pojęcia pierwotne:

zbiór liczb naturalnych $\mathbb{N}$

liczba naturalna 0 (najmniejsza)

następnik * (w dalszym zapisie *=@)

Aksjomaty:

1. $0 \in \mathbb{N}$
2. $n \in \mathbb{N} \Rightarrow n^{@} \in \mathbb{N}$
3. $0 \neq n^{@}$
4. $m^{@} = n^{@} \Rightarrow m = n$
5. Aksjomat indukcji:
   Jeżeli A jest podzbiorem zbioru liczb naturalnych takim, że
   1. $0 \in A$
   2. $\forall_{n \in \mathbb{N}} n \in A \Rightarrow n^{@} \in A$

   To z 1. i 2. wynika, że $A = \mathbb{N}$

Twierdzenie:

Dla każdej liczby naturalnej $n \in \mathbb{N}$ różnej od 0 istnieje liczba $m \in \mathbb{N}$ taka, że $n = m^{@}$

Dowód:

$$A = \left\{ n \in \mathbb{N} | n = 0 \vee \exists_{n \in \mathbb{N}} n = m^{@} \right\}$$

1. Czy $0 \in A$?
   $0 \in A$ na mocy definicji zbioru A.
2. Niech n_0 będzie ustalonym elementem zbioru A.
   $n_0^{@} \in A$?
   $n_0^{@} \in A$ na mocy definicji zbioru A.

Z aksjomatu indukcji 5. wynika, że $A = \mathbb{N}$

$n_1 \in \mathbb{N}, n_1 \neq 0$

$n_1 \in A$ tylko wtedy, gdy $n = 0 \vee \exists_{n \in \mathbb{N}} n = m^{@}$

$v(\exists_{n \in \mathbb{N}} n = m^{@}) = 1$

Definicja dodawania:

D_0 $\quad n + 0 = n$

$D_{@}$ $\quad n + m^{@} = (n + m)^{@}$

$1 \stackrel{def}{=} 0^{@}$

$2 \stackrel{def}{=} 1^{@}$

$$n + 2 \stackrel{def}{=} n + 1^{@} \stackrel{D_{@}}{=} (n+1)^{@} \stackrel{def}{=} (n + 0^{@})^{@} \stackrel{D_{@}}{=} ((n+0)^{@})^{@} \stackrel{D_0}{=} (n^{@})^{@}$$

Własności dodawania

(1) $0 + n = n$

Dowód:

$$B = \{ n \in \mathbb{N} | 0 + n = n \}$$

Czy $0=B$?

D_0 z $n=0, 0+0=0$

$0+n=n$ dla $n=0$

$0\in B$

Niech $n\in B$ czy $n^{@}\in B$?

$n\in B\Rightarrow 0+n=n$

$0+n^{@}\overset{D_@}{=}(0+n)^{@}=n^{@}, n^{@}\in B$ (z aksjomatu 5)

$B\subset\mathbb{N}$

(2) $(m+n)+k=m+(n+k)$

<u>Dowód:</u>

dowolne, ale ustalone m, n

$C=\{k\in\mathbb{N}|(m+n)+k=m+(n+k)\}$

Czy $0\in C$?

$(m+n)+0\overset{D_0}{=}m+n$

$m+(n+0)\overset{D_0}{=}m+n$

$0\in C$

Załóżmy, że dla pewnego $k, k\in C$

Czy $k^{@}\in C$?

$(m+n)+k^{@}\overset{D_@}{=}[(m+n)+k]^{@}\underset{z\,zał.}{=}[m+(n+k)]^{@}\overset{D_@}{=}m+(n+k)^{@}\overset{D_@}{=}m+(n+k^{@})$

$k^{@}\in C$

Z aksjomatu 5 (A5) $C\subset\mathbb{N}$

(3) $n^{@}+m=n+m^{@}$

<u>Dowód:</u>

ustalmy n

$D=\{n\in\mathbb{N}|n^{@}+m=n+m^{@}\}$

Czy $0\in D$?

$n^{@}+0\overset{D_0}{=}n^{@}$

$n+0^{@}\overset{D_@}{=}(n+0)^{@}\overset{D_0}{=}n^{@}$

$0\in D$

Czy jeśli $m\in D$ to $m^{@}\in D$?

$m\in D, n^{@}+m=n+m^{@}$

$n^{@}+m^{@}\overset{D_@}{=}(n^{@}+m)^{@}\underset{z\,zał.}{=}(n+m^{@})^{@}\overset{D_@}{=}n+(m^{@})^{@}$

$m^{@}\in D$

z aksjomatu 5 $D=\mathbb{N}$

(4) $n+m=m+n$

<u>Dowód:</u>

ustalmy n

$E=\{m\in\mathbb{N}|n+m=m+n\}$

$0\in E$?

$n+0\overset{D_0}{=}n$

$0+n\underset{wł.(1)}{=}n$

$0\in E$

Niech $m\in E$

Czy $m^{@}\in E$?

$n+m^{@}\overset{D_@}{=}(n+m)^{@}\underset{z\,zał.}{=}(m+n)^{@}\overset{D_@}{=}m+n^{@}\underset{wł.(3)}{=}m^{@}+n$

$m^{@}\in E$

z aksjomatu 5 $E\in\mathbb{N}$

Definicja mnożenia:

$$M_p,\ n*0=0$$

$$M_@,\ n*m^@=n*m+n$$

$$n*1\overset{\text{def}}{=}n*0^@\overset{M_@}{=}n*0+n\overset{M_0}{=}0+n\underset{wł.dod.(1)}{=}n$$

Definicja porządku w liczbach naturalnych:

$$m\leqslant n\overset{def.}{\Leftrightarrow}\underset{k}{\exists}\, n=m+k$$

Własność =<

(1) $n\leqslant n,\ n=n+0$ (własność zwrotności)

(2) $m\leqslant n\wedge n\leqslant p\Rightarrow m\leqslant p$ (przechodniość)

$$n=m+k_{1,}\ k_1\in\mathbb{N}$$

$$p=n+k_{2,}\ k_2\in\mathbb{N}$$

$$p=n+k_2=(m+k_1)+k_2\underset{wł.dod.(2)}{=}m+(k_1+k_2)$$

Z definicji porządku oznacza to, że $m\leqslant p$ jest prawdą.

(3) $m\leqslant n\wedge n\leqslant m\Rightarrow n=m$ (własność antysymetrii)

$$n=m+k_1$$

$$m=n+k_2$$

$$n=m+k_1=n+k_2+k_1=n(k_2+k_1)=n$$

$k_2+k_1=0$ (intuicyjnie)

(4) $0\leqslant n$ 0 jest najmniejszą liczbą naturalną

$$n=0+n$$

Reguły dowodowe wynikające z aksjomatu indukcji (aksjomatu A5)

$$A\subset\mathbb{N}$$

$$0\in A$$

$$\underset{n}{\forall}(n\in A\Rightarrow n^@\in A)$$

$$A=\mathbb{N}$$

$\phi(n)$ - funkcja zdaniowa, w której zmienna przebiega zbiór liczb naturalnych.

Załóżmy, że:

$$v(\phi(0))=1$$

Jeżeli

$$\underset{n}{\forall}(\phi(n)\Rightarrow\phi(n^@))$$

$$\underset{n}{\forall}\phi(n)$$

$$A=\{n\in\mathbb{N}|\phi(n)\}$$

Jeżeli $\phi(0)$ jest prawdziwe to $0>A$. Niech $n\in\mathbb{N}$ załóżmy, że $n\in A$ stąd zachodzi $\phi(n)$ z założenia, że $\underset{n}{\forall}(\phi(n)\Rightarrow\phi(n^@))$ wynika, że zachodzi $\phi(n^@)$. Jeżeli zachodzi $\phi(n^@)$ to $n^@\in A$ z aksjomatu A5 wynika, że A jest zbiorem wszystkich $\mathbb{N}$.

$$A\subset\mathbb{N}=\{n\in\mathbb{N}|\phi(n)\}\underset{n}{\forall}\phi(n)$$

Indukcja uogólniona (uogólniona zasada indukcji)

$$k\in\mathbb{N},\ A\subset\mathbb{N}$$

$$k\in A$$

$$\underset{n\geqslant k}{\forall}(n\in A\Rightarrow n+1\in A)$$

$$\{n|n\geqslant k\}\subset A$$

$$\phi(k)$$

$$\underset{n\geqslant k}{\forall}(\phi(n)\Rightarrow\phi(n+1))$$

$$\underset{n\geqslant k}{\forall}\phi(n)$$

Dowód: $B=\{n\in\mathbb{N}|n<k\vee n\in A\}$

(1) Czy $n=0\in B$?

(a) $k=0$

$0\in B$ bo $0=k\in A$

(b) $k>0$

$0<k$ to $0\in B$ na mocy $n<k$

(2) Załóżmy, że dla pewnego ustalonego $n\in\mathbb{N}$ zachodzi, że $n\in B$.

Jeżeli $n\in B$, to $n<k\vee n\in A$.

Jeżeli $n<k$ to $n+1<k+1\wedge n+1<k\vee n+1=k$

$n+1\in B$ na mocy definicji.

Jeżeli $n\in A$ to z założenia $n+1\in A$, więc z definicji zbioru $B, n+1\in B$. Z aksjomatu 5 (A5) zbiór B jest zbiorem $B\subset N$ $B=\{n\in\mathbb{N}|n<k\vee n\in A\}$. Niech $n\in\mathbb{N}$ taki, że $n\geqslant k$, $n\in B\wedge\neg(n<k)$ więc z definicji B musi zachodzić $n\in A$.

Mocna zasada indukcji

$$\frac{\begin{array}{c}A\subset\mathbb{N}\\ 0\in A\\ \forall_n((\forall_{k\leqslant n} k\in A)\Rightarrow k+1\in A)\end{array}}{A=\mathbb{N}}$$

$$\frac{\begin{array}{c}\phi(0)\\ \forall_n(\forall_{k\leqslant n}\phi(k))\Rightarrow\phi(k+1)\end{array}}{\forall_n\phi(n)}$$

Dowód: $C=\{n\in\mathbb{N}|\forall_{k\leqslant n} n\in A\}$

(1) Czy $0\in C$?

$0\in A$ z założenia

$k\leqslant 0$ to $k=0$ (bo $k\in\mathbb{N}$) stąd wniosek $\forall_k(k\leqslant 0\Rightarrow k\in A)$

(2) Ustalmy $n\in C$

Czy $n+1\in C$?

$\forall_{k\leqslant n} k\in A$

$n+1\in A$ z drugiego założenia twierdzenia.

Jeżeli $k\leqslant n+1\Rightarrow k\leqslant n\vee k=n+1$

Jeżeli $k\leqslant n\Rightarrow k\in A$

Jeżeli $k=n+1\Rightarrow k\in A$ z założenia

Z definicji C: $n+1\in C$ na mocy aksjomatu 5 (A5) $C\subset\mathbb{N}$. Pokazaliśmy inkluzję $A\supset\mathbb{N}$.

Wykażemy $\mathbb{N}\subset A$ niech $n\in\mathbb{N}=C, n\in C$. Z definicji C $\forall_{k\leqslant n} k\in A, n\leqslant n$ więc $n\in A$.

Twierdzenie (zasada minimum)

W każdym niepustym podzbiorze zbioru $\mathbb{N}$ istnieje element najmniejszy.

$A\subset\mathbb{N}, A\notin\emptyset\Rightarrow\exists_{a\in A}\forall_{b\in A} a\leqslant b$

Dowód:

Niech $B=\mathbb{N}/A$. Załóżmy, że w zbiorze A nie ma elementu najmniejszego. Stosujemy mocną zasadę indukcji:

(1) Czy $0\in B$?

Gdy $0\notin B$ to $0\in A$ i 0 byłoby najmniejszą liczbą w A, założenie że $0\notin B$ prowadzi do sprzeczności wobec tego $0\in B$.

(2) Niech n będzie ustaloną liczbą naturalną i załóżmy, że $\forall_{k\leqslant n} k\in B, \forall_{k\leqslant n} k\notin A$. Gdyby $n+1\notin B$ to $n+1\in A$ byłoby najmniejsze w A jest sprzeczne z czego wynika, że $n+1\in B$.

Czyli $n+1\in B, B=\mathbb{N}, \mathbb{N}=B=\mathbb{N}/A, A=\emptyset$ sprzeczne z założeniem, że $A\notin\emptyset$.

To prowadzi do sprzeczności, że w A nie ma elementu najmniejszego, więc to znaczy, że w A jest element najmniejszy.

Twierdzenie (zasada maksimum)

W każdym niepustym i ograniczonym (z góry) podzbiorze $\mathbb{N}$ istnieje element największy.

Reguły dowodowe indukcji matematycznej w skrócie:

- zupełna

$$\frac{\phi(0) \qquad \forall_{n}[\phi(n) \Rightarrow \phi(n+1)]}{\forall_{n} \phi(n)}$$

- uogólniona

$$\frac{\phi(k) \qquad \forall_{n \geqslant k}[\phi(n) \Rightarrow \phi(n+1)]}{\forall_{n \geqslant k} \phi(n)}$$

- mocna

$$\frac{\phi(0) \qquad \forall_{n}[(\forall_{k \leqslant n} \phi(k)) \Rightarrow \phi(n+1)]}{\forall_{n} \phi(n)}$$

- połączenie uogólnionej z mocną

$$\frac{\phi(k) \qquad \forall_{n \geqslant k}[(\forall_{k \leqslant n} \phi(k)) \Rightarrow \phi(n+1)]}{\forall_{n \geqslant k} \phi(n)}$$

- zasada minimum

$$\frac{A \subset \mathbb{N} \qquad A \neq \emptyset}{\exists_{a \in A} \forall_{b \in A} a \leqslant b}$$

- zasada maksimum

$$\frac{A \subset \mathbb{N} \qquad A \neq \emptyset \qquad \exists_{M \in \mathbb{N}} \forall_{a \in A} a \leqslant M}{\exists_{a \in A} \forall_{b \in A} b \leqslant a}$$

„Metatwierdzenie”:

Jeżeli w aksjomatyce Peano zastąpić aksjomat 5 – aksjomat indukcji (A5) mocnym aksjomatem indukcji, zasadą minimum lub zasadą maksimum. Otrzymamy równoważną teorię, to znaczy w teorii tej będą prawdziwe dokładnie te same twierdzenia, które wynikają z aksjomatów Peano.