Ćwiczenia 13. Indukcja matematyczna. Relacje równoważności i porządkujące

Definicje indukcyjne dodawania i mnożenia liczb naturalnych Dla wszystkich $m, n \in \mathbb{N}$:
$m + 0 = m$
$m + S(n) = S(m + n)$
$m \cdot 0 = 0$
$m \cdot S(n) = m \cdot n + m$ (przyjmujemy wyższy priorytet $\cdot$ wobec $+$)
Na wykładzie udowodniliśmy prawa arytmetyki:
$\forall_{m,n\in\mathbb{N}}(S(m) = S(n) \Rightarrow m = n)$
$\forall_{n\in\mathbb{N}}(n + 1 = S(n))$, gdzie $1 = S(0)$
$\forall_{k,m,n\in\mathbb{N}}[(k + m) + n = k + (m + n)]$ (łączność dodawania)

Zadanie 1. Udowodnij przez indukcję względem n prawa arytmetyki:
(a) $\forall_{k,m,n\in\mathbb{N}}(k \cdot (m + n) = k \cdot m + k \cdot n)$ (rozdzielność $\cdot$ względem $+$)
(b) $\forall_{m,n\in\mathbb{N}}(m + n = n + m)$ (przemienność $+$)
(c) $\forall_{k,m,n\in\mathbb{N}}(k + n = m + n \Rightarrow k = m)$ (prawo skracania)

Dowody
(a) Dowodzimy $\forall_{n\in\mathbb{N}}(k \cdot (m + n) = k \cdot m + k \cdot n)$.
$n = 0$
$k \cdot (m + 0) = k \cdot m = k \cdot m + 0 = k \cdot m + k \cdot 0$
ZI: $k \cdot (m + n) = k \cdot m + k \cdot n$
TI: $k \cdot (m + S(n)) = k \cdot m + k \cdot S(n)$
$k \cdot (m + S(n)) = k \cdot S(m + n) = k \cdot (m + n) + k \overset{ZI}{=} (k \cdot m + k \cdot n) + k =$
$k \cdot m + (k \cdot n + k) = k \cdot m + k \cdot S(n)$
(b) Najpierw udowodnimy dwa lematy.
(L1) $\forall_{n\in\mathbb{N}}(0 + n = n)$
(L2) $\forall_{m,n\in\mathbb{N}}(S(m) + n = S(m + n))$
Dowodzimy (L1) przez indukcję względem n.
$n = 0$
$0 + 0 = 0$ na mocy definicji $+$
ZI: $0 + n = n$
TI: $0 + S(n) = S(n)$
$0 + S(n) = S(0 + n) \overset{ZI}{=} S(n)$
Dowodzimy (L2) przez indukcję względem n.
$n = 0$
$S(m) + 0 = S(m) = S(m + 0)$
ZI: $S(m) + n = S(m + n)$
TI: $S(m) + S(n) = S(m + S(n))$
$S(m) + S(n) = S(S(m) + n) \overset{ZI}{=} S(S(m + n)) = S(m + S(n))$
Dowodzimy $\forall_{n\in\mathbb{N}}(m + n = n + m)$ przez indukcję względem n.
$n = 0$
$m + 0 = m \overset{L1}{=} 0 + m$
ZI: $m + n = n + m$

TI: $m + S(n) = S(n) + m$

$m + S(n) = S(m+n) \overset{ZI}{=} S(n+m) \overset{L2}{=} S(n) + m$

(c) Dowodzimy $\forall_{n\in\mathbb{N}}(k + n = m + n \Rightarrow k = m)$ przez indukcję względem n.

$n = 0$. Cel: $k + 0 = m + 0 \Rightarrow k = m$. Zakładamy $k + 0 = m + 0$. Wtedy $k = k + 0 = m + 0 = m$.

ZI: $k + n = m + n \Rightarrow k = m$

TI: $k + S(n) = m + S(n) \Rightarrow k = m$.

Zakładamy $k + S(n) = m + S(n)$. Mamy $k + S(n) = S(k + n)$ i $m + S(n) = S(m+n)$. Stąd $S(k+n) = S(m+n)$, a więc $k+m = k+n$. Na mocy ZI $k = m$.

Zadanie domowe 1. Udowodnij prawa arytmetyki.

(a) $\forall_{n\in\mathbb{N}}(n \cdot 1 = n)$ (bez indukcji)

(b) $\forall_{m,n\in\mathbb{N}}(m \cdot n = n \cdot m)$. Najpierw udowodnij dwa lematy.

(L3) $\forall_{n\in\mathbb{N}}(0 \cdot n = 0)$

(L4) $\forall_{m,n\in\mathbb{N}}(S(m) \cdot n = m \cdot n + n)$

(c) $\forall_{k,m,n\in\mathbb{N}}[(k \cdot m) \cdot n = k \cdot (m \cdot n)]$ (łączność mnożenia)

Określiliśmy $R_n \subset \mathbb{Z}^2$, $n \geq 2$:

$xR_ny \Leftrightarrow n|(y - x)$.

Działania ilorazowe na zbiorze $\mathbb{Z}/R_n$ określiliśmy tak (tu $R = R_n$):

$[x]_R +_R [y]_R = [x + y]_R$

$[x]_R \cdot_R [y]_R = [x \cdot y]_R$

dla $x, y \in \mathbb{Z}$.

Zadanie 2. Wykaż, że $+_R$ jest przemienne i łączne.

$[x] +_R [y] = [x + y] = [y + x] = [y] +_R [x]$

$([x] +_R [y]) +_R [z] = [x + y] +_R [z] = [(x + y) + z] = [x + (y + z)] =$

$= [x] +_R [y + z] = [x] +_R ([y] +_R [z])$

Zadanie domowe 2. Wykaż, że działanie $\cdot_R$ jest przemienne, łączne i rozdzielne względem $+_R$. **Uwaga.** Wiemy, że te własności mają odpowiednie działania na $\mathbb{Z}$.

Definicja. Relację $R \subset A^2$ nazywamy relacją *porządkującą* na zbiorze A, jeżeli jest zwrotna (na A), antysymetryczna i przechodnia. Wtedy parę (A, R) nazywamy *zbiorem uporządkowanym.*

Definicja. Relację $R \subset A^2$ nazywamy relacją *liniowo porządkującą* na zbiorze A, jeżeli jest porządkująca i spójna (na A).

Mówimy "porządek" zamiast "relacja porządkująca"; podobnie "liniowy porządek" zamiast "relacja liniowo porządkująca".

Zamiast "porządek" można mówić "częściowy porządek", ale my stosujemy ten drugi termin do porządków, które nie są liniowe.

Diagramy Hassego skończonych zbiorów uporządkowanych

Niech $\leq$ będzie porządkiem na A. *Ostry porządek* $<$ wyznaczony przez $\leq$ określamy tak:

$$x < y \Leftrightarrow x \leq y \wedge x \neq y$$

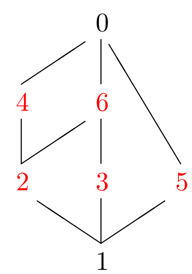
Niech $(A, \leq)$ będzie zbiorem uporządkowanym. Element $y \in A$ nazywamy *następnikiem* elementu $x \in A$, jeżeli $x < y$, lecz nie istnieje $z \in A$ takie, że $x < z$ i $z < y$.

W diagramie Hassego przedstawiamy elementy zbioru jako wierzchołki i prowadzimy krawędzie od każdego wierzchołka do wszystkich następników tego wierzchołka, umieszczonych wyżej.

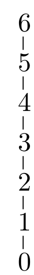
Mamy: $x \leq y$ wtedy i tylko wtedy, gdy w diagramie istnieje droga, idąca w górę, od x do y (dowolnej długości $n \geq 0$).

Droga jest to trasa, która nie przechodzi dwukrotnie przez żaden wierzchołek. Długość drogi: liczba krawędzi, przez które przechodzi ta droga.

Poniżej przedstawiamy diagramy Hassego dla zbioru $A = \{0, 1, 2, 3, 4, 5, 6\}$ z relacją podzielności ograniczoną do tego zbioru oraz naturalnym porządkiem $\leq$ ograniczonym do tego zbioru (pierwsza jest częściowo porządkująca, druga liniowo porządkująca).



Relacja podzielności



Naturalny porządek

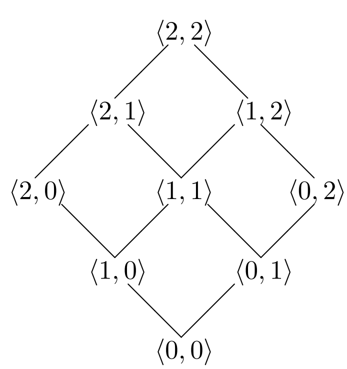


Diagram Hassego dla relacji $\leq_p$ na $\mathbb{N}^2$ ograniczonej do $\{0, 1, 2\}^2$

$$\langle x_1, y_1 \rangle \leq_p \langle x_2, y_2 \rangle \Leftrightarrow x_1 \leq x_2 \wedge y_1 \leq y_2$$

$$
\begin{tikzcd}[column sep=small]
 & \{a,b\} \arrow[dl, dash] \arrow[dr, dash] & \\
\{a\} \arrow[dr, dash] & & \{b\} \arrow[dl, dash] \\
 & \emptyset &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}[column sep=small]
 & \langle 1,1\rangle \arrow[dl, dash] \arrow[dr, dash] & \\
\langle 1,0\rangle \arrow[dr, dash] & & \langle 0,1\rangle \arrow[dl, dash] \\
 & \langle 0,0\rangle &
\end{tikzcd}
$$

$(P(\{a,b\}),\subset)$ $\qquad\qquad$ $(\{0,1\}^2, \leq_p)$

Zadanie domowe 3. (a) Narysuj diagram Hassego dla zbioru $\{1,2,3,4,5,6,7,8,9\}$ z relacją podzielności ograniczoną do tego zbioru. Wyznacz element najmniejszy i elementy maksymalne.

(b) Na tym diagramie zaznacz podzbiór $X = \{2,3,6,8,9\}$, np. otaczając każdy element kółkiem. Wyznacz:

(1) elementy minimalne i elementy maksymalne w X,

(2) wszystkie ograniczenia dolne i ograniczenia górme zbioru X (jeżeli istnieją),

(3) kres dolny i kres górny zbioru X (jeżeli istnieją).

Zadanie domowe 4. Narysuj diagram Hassego dla $(\mathcal{P}(\{a,b,c\}),\subset)$. Niech X będzie rodziną wszystkich niepustych podzbiorów zbioru $\{a,b,c\}$. Oczywiście $X \subset \mathcal{P}(\{a,b,c\})$. Wyznacz elementy (1), (2), (3) jak w (b) powyżej.