Podstawy matematyki

Wykład 3 - Twierdzenia matematyczne, operacje nieskończone, relacje

Oskar Kędzierski

29 marca 2020

Twierdzenia w matematyce

Typowa postać twierdzenia w matematyce, to implikacja.

Twierdzenie

Jeśli A, to B.

$$A \to B$$

Zdanie A (poprzednik implikacji) nazywamy **warunkiem wystarczającym** na to, żeby B.

Zdanie B (następnik implikacji) nazywamy **warunkiem koniecznym**, na to, żeby A.

Zdanie A nazywa się tez **założeniem**, a zdanie B **tezą** twierdzenia.

Twierdzenie postaci $A \to B$ nazywamy **twierdzeniem prostym**.

Twierdzenia w matematyce – przykład

Dla dowolnego $n \in \mathbb{N}$ zachodzi następująca implikacja

$$6|n \rightarrow 3|n,$$

tzn. jeśli liczba n jest podzielna przez 6, to liczba n jest podzielna przez 3.

Dla $n \in \mathbb{N}$ warunkiem wystarczającym na bycie podzielnym przez 3 jest bycie podzielnym przez 6.

Dla $n \in \mathbb{N}$ warunkiem koniecznym na bycie podzielnym przez 6 jest bycie podzielnym przez 3.

Twierdzenia proste, odwrotne, przeciwstawne, przeciwne

Twierdzenie (proste)

Jeśli A, to B.

$$A \rightarrow B$$

Dla ustalonego twierdzenia prostego, możemy napisać twierdzenia do niego **odwrotne, przeciwstawne** i **przeciwne**.

Twierdzenie (odwrotne)

Jeśli B, to A.

$$B \rightarrow A$$

Twierdzenia proste, odwrotne, przeciwstawne, przeciwne

Twierdzenie (przeciwstawne)

Jeśli nieprawda, że B, to nieprawda, że A.

$$\neg B \rightarrow \neg A$$

Twierdzenie (przeciwne)

Jeśli nieprawda, że A, to nieprawda, że B.

$$\neg A \rightarrow \neg B$$

Twierdzenia proste, odwrotne, przeciwstawne, przeciwne – cd.

Na mocy prawa transpozycji (tautologii rachunku zdań)

$$(p \to q) \leftrightarrow (\neg q \to \neg p)$$

twierdzenie proste jest równoważne twierdzeniu przeciwstawnemu, a twierdzenie odwrotne jest równoważne twierdzeniu przeciwnemu.

Z prawdziwości twierdzenia prostego, nie wynika prawdziwość twierdzenia odwrotnego, i na odwrót.

Twierdzenia proste, odwrotne, przeciwstawne, przeciwne – przykład

Dla dowolnego $n \in \mathbb{N}$ prawdziwa jest implikacja

$$6|n \rightarrow 3|n,$$

ale nieprawdziwa jest implikacja odwrotna

$$3|n \rightarrow 6|n,$$

bo, na przykład $n = 3$ jest liczbą podzielną przez 3, a nie jest liczbą podzielna przez 6.

Twierdzenia proste, odwrotne, przeciwstawne, przeciwne – przykład

Dla dowolnego $n \in \mathbb{N}$ prawdziwa jest implikacja

$$3 \not| n \to 6 \not| n.$$

Dla $n \in \mathbb{N}$ warunkiem koniecznym na nie bycie podzielnym przez 3 jest nie bycie podzielnym przez 6.

Dla $n \in \mathbb{N}$ warunkiem wystarczającym na nie bycie podzielnym przez 6 jest nie bycie podzielnym przez 3.

Warunek konieczny i wystarczający

Gdy twierdzenie proste i twierdzenie do niego odwrotne są prawdziwe, wtedy mówimy, że A jest **warunkiem koniecznym i wystarczającym** na to, że B. Równoważnie, mówimy, że A zachodzi, **wtedy i tylko wtedy**, gdy B.

Twierdzenie

A zachodzi wtedy i tylko wtedy, gdy B.

$$A \leftrightarrow B.$$

Odpowiada to prawu logicznemu (tautologii rachunku zdań)

$$(p \leftrightarrow q) \leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p).$$

Warunek konieczny i wystarczający – przykład

Twierdzenie

Trójkąt o bokach o długości a, b, c jest prostokątny i bok o długości c jest przeciwprostokątną wtedy i tylko wtedy, gdy

$$a^2 + b^2 = c^2.$$

Twierdzenie

Dla $n \in \mathbb{N}$

$$3|n \leftrightarrow 3|n^2.$$

Metody dowodzenia twierdzeń

Aby dowieść twierdzenia postaci $A \leftrightarrow B$, należy dowieść implikacji $A \rightarrow B$ oraz $B \rightarrow A$.

W ogólności, aby dowieść **równoważności** warunków $A_1, \ldots, A_n$ (tzn. $A_i \leftrightarrow A_j$ dla $i, j = 1, \ldots, n$) wystarczy dowieść implikacji

$$A_1 \rightarrow A_2, \quad A_2 \rightarrow A_3, \ldots, A_{n-1} \rightarrow A_n, \quad A_n \rightarrow A_1.$$

Korzystamy tu z prawa sylogizmu (prawa przechodniości implikacji)

$$(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r).$$

Metody dowodzenia twierdzeń – dowód nie wprost

Dowodem **nie wprost (apagogicznym, przez sprowadzenie do sprzeczności)** nazywamy dowód, który pokazujemy, ze zaprzeczenie pewnego zdania prowadzi do sprzeczności. Odpowiada to regule dowodzenia

$$\frac{\neg A \to (B \wedge \neg B)}{A}.$$

W szczególności, gdy chcemy dowieść implikacji $A \to B$, to zakładamy negację tego zdania, czyli $A \wedge \neg B$.

Dowód nie wprost – przykład

Twierdzenie

Nie istnieje największa liczba pierwsza.

Dowód.

Załóżmy przeciwnie, że istnieje największa liczba pierwsza. Zatem zbiór wszystkich liczb pierwszych jest skończony i możemy je oznaczyć $p_1, \ldots, p_n$. Wtedy, z praw arytmetyki, liczba

$$N = p_1 \cdots p_n + 1$$

rozkłada się na iloczyn liczb pierwszych, zatem jest podzielna przez pewną liczbę pierwszą. Z drugiej strony, z definicji, liczba N nie dzieli się przez żadną liczbę pierwsza (daje przy dzieleniu resztę 1). Sprzeczność, zatem nie istnieje największa liczba pierwsza.

Zbiór podzbiorów

Definicja

Dla ustalonego zbioru X, **zbiorem podzbiorów** X (lub **zbiorem potęgowym** zbioru X) nazywamy zbiór, którego elementami są dokładnie wszystkie podzbiory zbioru X. Oznaczamy go $P(X)$.

$$A \in P(X) \leftrightarrow A \subset X$$

Istnienie takiego zbioru wynika z aksjomatów teorii mnogości.

Przykład

i) $P(\emptyset) = \{\emptyset\}$,

ii) $P(\{1\}) = \{\emptyset, \{1\}\}$,

iii) $P(P(\{1\})) = \{\emptyset, \{\emptyset\}, \{\{1\}\}, \{\emptyset, \{1\}\}\}$,

iv) $P(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$.

Zbiór podzbiorów – cd.

Definicja

Jeśli zbiór A jest skończony, to liczbę jego elementów oznaczamy przez $|A|$.

Na przykład $|\emptyset| = 0$, $|\{1,2\}| = 2$, $|\{\emptyset, \{1,2\}\}| = 2$.

Stwierdzenie

Jeśli $|X| = n$, to $|P(X)| = 2^n$.

Dowód.

Każdy podzbiór zbioru X jest wyznaczony jednoznacznie przez elementy, które do niego należą. Dla każdego elementu mamy dokładnie 2 możliwości: element należy do podzbioru lub nie należy. Daje to $\underbrace{2 \cdot 2 \cdots 2}_{n} = 2^n$ możliwości.

Własności zbioru potęgowego

i) $P(X) \neq \emptyset$,
ii) $X \subset Y \leftrightarrow P(X) \subset P(Y)$,
iii) $P(X) \cap P(Y) = P(X \cap Y)$.

Dowód.

i) $\emptyset \in P(X)$,
ii) $(\rightarrow)$ jeśli $X \subset Y$ oraz $A \in P(X)$, to $A \subset X \subset Y$, zatem $A \in P(Y)$,
$(\leftarrow)$ jeśli $P(X) \subset P(Y)$, to w szczególności $X \in P(X)$, skąd $X \in P(Y)$, zatem $X \subset Y$,
iii) $A \in P(X) \cap P(Y) \leftrightarrow A \in P(X) \wedge A \in P(Y) \leftrightarrow A \subset X \wedge A \subset Y \leftrightarrow A \subset X \cap Y$.

Uogólnione rodziny zbiorów

Niech I będzie niepustym zbiorem a X dowolnym zbiorem. **Rodziną zbiorów** indeksowaną przez zbiór I nazywamy dowolną funkcję f ze zbioru I do zbioru $P(X)$ (tj. przyporządkowanie każdemu elementowi $i \in I$ pewnego zbioru $A_i \in P(X)$)

$$f : I \ni i \mapsto A_i \in P(X).$$

Rodzinę zbiorów indeksowanych przez I oznaczamy także przez

$$\{A_i\}_{i \in I},$$

gdzie $A_i = f(i)$.

Powyższa konstrukcja pozwala na konstrukcję *nieskończonych* rodzin zbiorów.

Uogólnione rodziny zbiorów – przykład

Niech $I = \mathbb{N}$ oraz $X = \mathbb{R}$. Definiujemy rodzinę zbiorów $\{A_n\}_{n \in \mathbb{N}}$ warunkiem

$$A_n = \{x \in \mathbb{R} \mid x \geq n\}.$$

Wtedy

$$\begin{aligned} A_0 &= [0, +\infty), \\ A_1 &= [1, +\infty), \\ &\text{itd.} \end{aligned}$$

Uogólnione działania na zbiorach

Dla dowolnej rodzin zbiorów $\{A_i\}_{i\in I}$ indeksowanej przez zbiór I takiej, że $A_i \in P(X)$ definiujemy **przecięcie rodziny** $\{A_i\}_{i\in I}$

$$\bigcap_{i\in I} A_i = \{x \in X \mid \forall_{i\in I}\, x \in A_i\},$$

oraz **sumę rodziny** $\{A_i\}_{i\in I}$

$$\bigcup_{i\in I} A_i = \{x \in X \mid \exists_{i\in I}\, x \in A_i\}.$$

Przecięcie rodziny $\{A_i\}_{i\in I}$ to zbiór elementów zbioru X, które należą *do wszystkich* zbiorów A_i, a suma rodziny $\{A_i\}_{i\in I}$ to zbiór elementów zbioru X, które należą *do pewnego* zbioru A_i.

Uogólnione działania na zbiorach – przykład

Jeśli

$$A_n = \{x \in \mathbb{R} \mid x \geq n\} = [n, +\infty).$$

dla $n \in \mathbb{N}$, to

$$\bigcap_{n \in \mathbb{N}} A_n = \emptyset,$$

$$\bigcup_{n \in \mathbb{N}} A_n = [0, +\infty).$$

Własności uogólnionych działań na zbiorach

Dla dowolnych rodzin $\{A_i\}_{i\in I}$, $\{B_i\}_{i\in I}$ indeksowanych przez I zachodzi,

i) jeśli $A \subset A_i$ dla $i \in I$, to $A \subset \bigcap_{i\in I} A_i$,

ii) jeśli $A_i \subset A$ dla $i \in I$, to $\bigcup_{i\in I} A_i \subset A$,

iii) $\bigcap_{i\in I} A_i \cap \bigcap_{i\in I} B_i = \bigcap_{i\in I}(A_i \cap B_i)$,

iv) $\bigcup_{i\in I} A_i \cup \bigcup_{i\in I} B_i = \bigcup_{i\in I}(A_i \cup B_i)$,

v) $\bigcap_{i\in I} A_i \cup \bigcap_{i\in I} B_i \subset \bigcap_{i\in I}(A_i \cup B_i)$,

vi) $\bigcup_{i\in I} A_i \cap \bigcup_{i\in I} B_i \supset \bigcup_{i\in I}(A_i \cap B_i)$.

Kontrprzykład dla równości w v) oraz vi), dla dowolnego, niepustego zbioru I otrzymujemy biorąc rodzinę podzbiorów I

$$A_i = \{i\}, \quad B_i = I \setminus \{i\}.$$

Dowody powyższych własności opierają sie na prawach rachunku kwantyfikatorów.

Prawa de Morgana dla uogólnionych działań na zbiorach

Dla dowolnego zbioru $A \subset X$ oraz dowolnej rodziny $\{A_i\}_{i \in I}$ podzbiorów zbioru X, z praw de Morgana rachunku kwantyfikatorów wynikają następujące równości

$$A \setminus \bigcap_{i \in I} A_i = \bigcup_{i \in I} (A \setminus A_i),$$

$$A \setminus \bigcup_{i \in I} A_i = \bigcap_{i \in I} (A \setminus A_i).$$

Dowód.

Pierwsza tożsamość

$$x \in A \setminus \bigcap_{i \in I} A_i \leftrightarrow x \in A \wedge x \notin \bigcap_{i \in I} A_i \leftrightarrow x \in A \wedge \neg \forall_{i \in I}\, x \in A_i \leftrightarrow$$

$$\leftrightarrow x \in A \wedge \exists_{i \in I}\, x \notin A_i \leftrightarrow \exists_{i \in I}\, x \in A \wedge x \notin A_i \leftrightarrow x \in \bigcup_{i \in I} (A \setminus A_i)$$

Prawa de Morgana dla uogólnionych działań na zbiorach – cd.

W szczególności, gdy $A = X$ oraz $A_i \subset X$ dostajemy

$$\left(\bigcap_{i\in I} A_i\right)' = \bigcup_{i\in I} A_i',$$

$$\left(\bigcup_{i\in I} A_i\right)' = \bigcap_{i\in I} A_i'.$$

Pary elementów

Definicja (K. Kuratowski)

Dla dowolnych zbiorów X, Y oraz $x \in X,\ y \in Y$ definiujemy **parę** elementów $(x, y) \in P(P(X \cup Y))$

$$(x, y) = \{\{x\}, \{x, y\}\} \subset P(X \cup Y),$$

tzn. (x, y), to zbiór dwuelementowy, którego elementami są zbiory $\{x\}$ oraz $\{x, y\}$.

Stwierdzenie

Dla $x, z \in X$ oraz $y, w \in Y$ zachodzi

$$(x, y) = (z, w) \leftrightarrow (x = z) \wedge (y = w).$$

Dowód.

$(\leftarrow)$ oczywiste

Pary elementów – cd.

Dowód.

$(\rightarrow)$ rozpatrzmy dwa przypadki

i) $|(x, y)| = |(z, w)| = 1$, wtedy $x = y$ oraz $z = w$, ponadto $\{\{x\}\} = \{\{z\}\}$, skąd $x = y = z = w$,

ii) $|(x, y)| = |(z, w)| = 2$, wtedy $x \neq y$ oraz $z \neq w$, ponadto $\{x\} = \{z\}$ oraz $\{x, y\} = \{z, w\}$ skąd $x = z$ oraz $y = w$.

Iloczyn kartezjański

Definicja

Iloczynem kartezjańskim zbiorów X, Y nazywamy zbiór $X \times Y$ wszystkich par (x, y), gdzie $x \in X$ oraz $y \in Y$, tzn.

$$X \times Y = \{(x, y) \in P(P(X \cup Y)) \mid x \in X \wedge y \in Y\},$$

$$(x, y) \in X \times Y \leftrightarrow x \in X \wedge y \in Y.$$

Przykład

$$\{1, 2, 3\} \times \{3, 4\} = \{(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)\}$$
$$\{3, 4\} \times \{1, 2, 3\} = \{(3, 1), (3, 2), (3, 3), (4, 1), (4, 2), (4, 3)\}$$
$$\emptyset \times \{1, 2, 3\} = \emptyset$$

Podstawowe własności iloczynu kartezjańskiego

Dla dowolnych zbiorów X, Y, Z zachodzi

i) $|X| = m, |Y| = n \to |X \times Y| = mn$,
ii) $X \times Y = \emptyset \leftrightarrow X = \emptyset \vee Y = \emptyset$,
iii) $X \times Y = Y \times X \leftrightarrow X = Y \vee X = \emptyset \vee Y = \emptyset$,
iv) $(X \cap Y) \times Z = (X \times Z) \cap (Y \times Z)$,
v) $(X \cup Y) \times Z = (X \times Z) \cup (Y \times Z)$,
vi) $(X \setminus Y) \times Z = (X \times Z) \setminus (Y \times Z)$.

Dowód.

iv) $(x, y) \in (X \times Z) \cap (Y \times Z) \leftrightarrow (x, y) \in X \times Z \wedge (x, y) \in Y \times Z \leftrightarrow x \in X \wedge y \in Z \wedge x \in Y \wedge y \in Z \leftrightarrow x \in (X \cap Y) \wedge y \in Z \leftrightarrow (x, y) \in (X \cap Y) \times Z$.

Iloczyn kartezjański wielu zbiorów

Definicja

Dla dowolnych zbiorów $X_1, X_2, \ldots, X_n$ definiujemy ich iloczyn kartezjański przez

$$X_1 \times X_2 \times \cdots \times X_n = (X_1 \times X_2 \times \cdots \times X_{n-1}) \times X_n.$$

Uwaga

Z formalnego punktu widzenia, na ogół

$$X_1 \times (X_2 \times X_3) \neq (X_1 \times X_2) \times X_3,$$

jednak istnieje naturalne utożsamienie obu zbiorów.

Nieskończony iloczyn kartezjański

Niech $\{A_i\}_{i\in I}$ będzie rodziną zbiorów indeksowaną przez zbiór I.

Definicja

Iloczynem kartezjańskim (zbiorów) rodziny $\{A_i\}_{i\in I}$ nazywamy zbiór

$$\prod_{i\in I} A_i = \{f\colon I \to \bigcup_{i\in I} A_i \mid f(i) \in A_i\}.$$

Uwaga

Istnieje naturalne utożsamienie zbioru $A_1 \times A_2$ ze zbiorem $\prod_{i\in\{1,2\}} A_i$.

Uwaga

Przy założeniu pewnika wyboru (do dowodu implikacji $\to$)

$$\forall_{i\in I}\ A_i \neq \emptyset \leftrightarrow \prod_{i\in I} A_i \neq \emptyset.$$

Nieskończony iloczyn kartezjański cd.

Definicja

Rzutem iloczynu kartezjańskiego $\prod_{i \in I} A_i$ rodziny zbiorów $\{A_i\}_{i \in I}$ na j-tą współrzędną, gdzie $j \in I$, nazywamy funkcję

$$\mathrm{pr}_j \colon \prod_{i \in I} A_i \to A_j,$$

daną wzorem

$$\mathrm{pr}_j(f) = f(j).$$

Uwaga

Gdy $I = \emptyset$ przyjmuje się, że

$$\prod_{i \in \emptyset} A_i = \{*\},$$

jest zbiorem jednoelementowym (składającym się z funkcji pustej).

Relacje

Definicja

Relacją (binarną, dwuargumentową, dwuczłonową) pomiędzy elementami zbioru X i Y nazywamy dowolny podzbiór $R \subset X \times Y$. Dla $x \in X, y \in Y$ stosujemy notację

$$xRy \leftrightarrow (x, y) \in R.$$

Definicja

Dziedziną relacji $R \subset X \times Y$ nazywamy zbiór

$$D(R) = \{x \in X \mid \exists_{y \in Y}\ xRy\} = \mathrm{pr}_X(R).$$

Przeciwdziedziną relacji $R \subset X \times Y$ nazywamy zbiór

$$D^*(R) = \{y \in Y \mid \exists_{x \in X}\ xRy\} = \mathrm{pr}_Y(R).$$

Relacje – cd.

Definicja

Relacją odwrotną do relacji $R \subset X \times Y$ nazywamy relację $R^{-1} \subset Y \times X$ zadaną warunkiem

$$yR^{-1}x \leftrightarrow xRy.$$

Definicja

Złożeniem relacji $R \subset X \times Y$ oraz $S \subset Y \times Z$ nazywamy relację oznaczaną przez $R \cdot S \subset X \times Z$, zadaną warunkiem

$$x(R \cdot S)z \leftrightarrow \exists_{y \in Y}\ xRy \wedge ySz.$$

Definicja

Relację $R \subset X \times Y$ nazywamy **funkcją częściową**, jeśli

$$\forall_{x \in X} \forall_{y \in Y} \forall_{y' \in Y}\ xRy \wedge xRy' \rightarrow y = y',$$

tzn. każdy x jest w relacji z co najwyżej jednym elementem zbioru Y.

Relacje – cd.

Definicja

Relację $R \subset X \times Y$ nazywamy **funkcją** jeśli jest funkcją częściową oraz

$$\forall_{x \in X} \exists_{y \in Y} xRy,$$

tzn. każdy $x \in X$ jest w relacji z dokładnie jednym elementem zbioru Y.

Definicja

Relację R nazywamy **pełną** jeśli $R = X \times Y$.

Relacje – przykłady

Niech $X = \{1, 2, 3\}$, $Y = \{3, 4\}$, $Z = \{1, 2, 3\}$. Ustalamy relacje $R \subset X \times Y$ oraz $S \subset Y \times Z$

$$R = \{(1, 3), (2, 3), (3, 4)\},$$

$$S = \{(3, 1), (3, 2), (4, 1)\}.$$

Wtedy

$$D(R) = X, \quad D^*(R) = Y, \quad D(S) = Y, \quad D^*(S) = \{1, 2\},$$

relacja R jest funkcją,

relacja S nie jest funkcją, bo $3S1 \wedge 3S2 \wedge 1 \neq 2$,

$$R^{-1} = \{(3, 1), (3, 2), (4, 3)\},$$

$$R \cdot S = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 1)\}.$$

Własności relacji

Relację $R \subset X \times X$ nazywamy

i) **zwrotną**, jeśli $\forall_{x \in X}\ xRx$,
ii) **przeciwzwrotną**, jeśli $\forall_{x \in X}\ \neg xRx$,
iii) **symetryczną**, jeśli $\forall_{x \in X} \forall_{y \in X}\ xRy \rightarrow yRx$,
iv) **asymetryczną**, jeśli $\forall_{x \in X} \forall_{y \in X}\ xRy \rightarrow \neg yRx$,
v) **antysymetryczną**, jeśli $\forall_{x \in X} \forall_{y \in X}\ xRy \wedge yRx \rightarrow x = y$,
vi) **przechodnią**, jeśli $\forall_{x \in X} \forall_{y \in X} \forall_{z \in X}\ xRy \wedge yRz \rightarrow xRz$,
vii) **spójną**, jeśli $\forall_{x \in X} \forall_{y \in X}\ xRy \vee yRx \vee x = y$.

Przykład

Relacja $R \subset \mathbb{R} \times \mathbb{R}$ zadana warunkiem $xRy \leftrightarrow x \leq y$ jest zwrotna, nie jest przeciwzrotna (np. $0R0$), nie jest symetryczna (np. $1R2 \wedge \neg(2R1)$), nie jest asymetryczna (np. $\neg(0R0 \rightarrow \neg 0R0)$), jest antysymetryczna, jest przechodnia, jest spójna.

Relacja częściowego porządku

Definicja

Relację $R \subset X \times X$ nazywamy relacją **częściowego porządku**, jeśli jest zwrotna, antysymetryczna oraz przechodnia. Relację R nazywamy relacją **porządku liniowego**, jeśli jest relacją częściowego porządku i jest spójna.

Przykład

Dla niepustego zbioru X niech R będzie relacją na $P(X)$ zadaną warunkiem $ARB \leftrightarrow A \subset B$. Relacja R jest relacją częściowego porządku i jest relacją porządku liniowego dokładnie wtedy, gdy zbiór X ma co najwyżej jeden element.

i) $A \subset A$,

ii) $A \subset B \wedge B \subset A \rightarrow A = B$,

iii) $A \subset B \wedge B \subset C \rightarrow A \subset C$.

Relacja podzielności

Definicja

Dla $m, n \in \mathbb{Z}$ oraz $m \neq 0$ mówimy, że liczba n jest podzielna przez liczbę m jeśli istnieje $k \in \mathbb{Z}$ takie, że $n = km$. Piszemy $m|n$.

$$m|n \leftrightarrow \exists_{k \in \mathbb{Z}}\ n = km.$$

Stwierdzenie

Relacja $R \subset \mathbb{N}_{>0} \times \mathbb{N}_{>0}$ zadana warunkiem

$$mRn \leftrightarrow m|n,$$

czyli relacja podzielności jest relacja częściowego porządku.

Relacja podzielności – dowód

i) $n = 1 \cdot n$ zatem $n|n$,

ii) jeśli $n|m$ oraz $m|n$, to istnieją $k, k' \in \mathbb{N}$ takie, że $m = kn, n = k'm$, zatem $m = kk'm$, skąd $k = k' = 1$, zatem $m = n$.

iii) jeśli $m|n$ oraz $n|l$, to istnieją $k, k' \in \mathbb{N}$ takie, że $n = km$ oraz $l = k'n$, zatem $l = kk'm$, czyli $m|l$.

Porządek leksykograficzny

Definicja

Relacja **porządku leksykograficznego**

$$\leq_{lex} \subset \mathbb{N}^n \times \mathbb{N}^n$$

zadana warunkiem

$$\alpha \leq_{lex} \beta \quad \leftrightarrow \quad (\alpha_1 < \beta_1) \vee ((\alpha_1 = \beta_1) \wedge (\alpha_2, \ldots, \alpha_n) \leq_{lex} (\beta_2, \ldots, \beta_n)),$$

gdzie $\alpha_n \leq_{lex} \beta_n$, jeśli $\alpha_n \leq \beta_n$, jest porządkiem liniowym.

Porządek leksykograficzny cd.

Przykład

$$
\begin{aligned}
&(0,0) \leq_{lex} (0,1) \leq_{lex} (0,2) \leq_{lex} (0,3) \leq_{lex} \dots \\
\leq_{lex}&(1,0) \leq_{lex} (1,1) \leq_{lex} (1,2) \leq_{lex} (1,3) \leq_{lex} \dots \\
\leq_{lex}&(2,0) \leq_{lex} (2,1) \leq_{lex} (2,2) \leq_{lex} (2,3) \leq_{lex} \dots \\
&\vdots
\end{aligned}
$$

Porządek leksykograficzny z gradacją

Definicja

Dla $\alpha \in \mathbb{N}^n$ niech

$$|\alpha| = \alpha_1 + \ldots + \alpha_n.$$

Definicja

Relacja **porządku leksykograficznego z gradacją**

$$\leq_{grlex} \subset \mathbb{N}^n \times \mathbb{N}^n$$

zadana warunkiem

$$\alpha \leq_{grlex} \beta \quad \leftrightarrow \quad (|\alpha| < |\beta|) \vee (|\alpha| = |\beta| \wedge \alpha \leq_{lex} \beta),$$

jest porządkiem liniowym.

Porządek leksykograficzny z gradacją cd.

Przykład

$$
\begin{aligned}
(0,0) &\leq_{grlex} (0,1) \leq_{grlex} (1,0) \leq_{grlex} \\
\leq_{grlex} (0,2) &\leq_{grlex} (1,1) \leq_{grlex} (2,0) \leq_{grlex} \\
\leq_{grlex} (0,3) &\leq_{grlex} (1,2) \leq_{grlex} (2,1) \leq_{grlex} (3,0) \leq_{grlex} \dots \\
&\vdots
\end{aligned}
$$

Porządki jednomianowe

Uwaga

Oba porządki są dobre (zobacz następny wykład) i spełniają warunek

$$\alpha \leq_{lex} \beta \quad \rightarrow \quad \alpha + \gamma \leq_{lex} \beta + \gamma,$$

dla dowolnego $\gamma \in \mathbb{N}^n$ i przenoszą się na jednomiany w zmiennych $x_1, \ldots, x_n$, tzn.

$$x^\alpha \leq_{lex} x^\beta \quad \leftrightarrow \quad \alpha \leq_{lex} \beta,$$

gdzie

$$x^\alpha = x_1^{\alpha_1} \ldots, x_n^{\alpha_n}.$$

Uwaga

Porządki $\leq_{lex}$ i $\leq_{grlex}$ to **porządki wielomianowe**, używane przy obliczeniach związanych z **bazami Groebnera**.

Przykłady

W pierścieniu wielomianów z dwoma zmiennymi x_1, x_2

$$
\begin{aligned}
1 &\le_{lex} x_2 \le_{lex} x_2^2 \le_{lex} x_2^3 \le_{lex} \cdots \\
\le_{lex} x_1 &\le_{lex} x_1 x_2 \le_{lex} x_1 x_2^2 \le_{lex} x_1 x_2^3 \le_{lex} \cdots \\
\le_{lex} x_1^2 &\le_{lex} x_1^2 x_2 \le_{lex} x_1^2 x_2^2 \le_{lex} x_1^2 x_2^3 \le_{lex} \cdots \\
&\vdots
\end{aligned}
$$

$$
\begin{aligned}
1 &\le_{grlex} x_2 \le_{grlex} x_1 \le_{grlex} \\
\le_{grlex} x_2^2 &\le_{grlex} x_1 x_2 \le_{grlex} x_2^2 \le_{grlex} \\
\le_{grlex} x_2^3 &\le_{grlex} x_1 x_2^2 \le_{grlex} x_1^2 x_2 \le_{grlex} x_1^3 \le_{grlex} \cdots \\
&\vdots
\end{aligned}
$$

Diagram Hassego

Definicja

Dla relacji częściowego porządku $R \subset X \times X$ na skończonym zbiorze X, **diagramem Hassego** nazywamy niezorientowany graf, którego wierzchołkami są elementy zbioru X, a wierzchołki $x, y \in X$ są połączone krawędzią, gdy xRy oraz $\forall_{z \in X} xRz \wedge zRy \rightarrow (z = x) \vee (z = y)$. Dodatkowo, wtedy wierzchołek x jest położony niżej od wierzchołka y.

Diagram Hassego – cd.

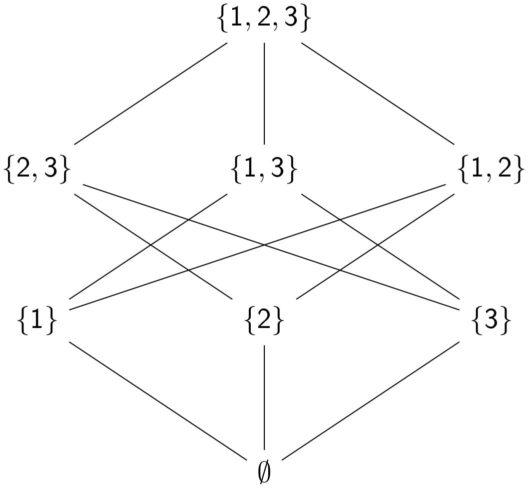

diagram Hassego dla relacji zawierania na $P(\{1,2,3\})$

Monoid

Definicja

Monoidem nazywamy dowolną parę $(M, \cdot)$, gdzie M jest zbiorem a

$$\cdot \colon M \times M \to M,$$

funkcją spełniającą warunki

i) istnieje element $e \in M$ taki, że $em = me = m$ dla dowolnego $m \in M$ (element neutralny),

ii) dla dowolnych $m, n, k \in M$ zachodzi $(mn)k = m(nk)$ (łączność).

Uwaga

Element neutralny jest wyznaczony jednoznacznie, bo jeśli e oraz e' spełniają są elementami neutralnymi, to

$$e = ee' = e'.$$

Monoid cd.

Monoid M można zdefiniować nie odwołując się wprost do elementów zbioru M.

Stwierdzenie

Zbiór M jest monoidem wtedy i tylko wtedy, gdy istnieją funkcje

$$\eta\colon \{1\} \to M,$$

$$\mu\colon M \times M \to M,$$

takie, że następujące diagramy są przemienne

$$\begin{tikzcd}
M \times \{1\} \arrow[r, "\mathrm{id}_M \times \eta"] \arrow[dr, "\mathrm{pr}_1"'] & M \times M \arrow[d, "\mu"] & \{1\} \times M \arrow[l, "\eta \times \mathrm{id}_M"'] \arrow[dl, "\mathrm{pr}_2"] \\
 & M &
\end{tikzcd}
\qquad
\begin{tikzcd}
M \times M \times M \arrow[r, "\mu \times \mathrm{id}_M"] \arrow[d, "\mathrm{id}_M \times \mu"] & M \times M \arrow[d, "\mu"'] \\
M \times M \arrow[r, "\mu"'] & M
\end{tikzcd}$$

gdzie $\mathrm{pr}_1, \mathrm{pr}_2$ oznaczają rzuty odpowiednio na pierwszą i drugą współrzędną.

Monoid cd.

Dowód.

Jeśli

$$\eta(1) = e,$$

$$\mu(m, n) = mn,$$

to przemienność diagramów jest równoważna zachodzeniu warunków *i*) oraz *ii*) w definicji monoidu.

Uwaga

Mówimy, że diagram jest **przemienny** jeśli dowolne dwa złożenia funkcji (odpowiadających strzałkom w diagramie) o wspólnych dziedzinach i przeciwdziedzinach jest równe.

Quasi–porządek

Definicja

Relację $R \subset X \times X$ na zbiorze X nazywamy **quasi–porządkiem/praporządkiem** (ang. preorder), jeśli jest

i) **zwrotna**, tzn. $\forall_{x \in X}\ xRx$,

ii) **przechodnia**, tzn. $\forall_{x \in X} \forall_{y \in X} \forall_{z \in X}\ xRy \wedge yRz \rightarrow xRz$.

Przykład

Quasi–porządkiem jest, na przykład, relacja osiągalności na zbiorze wierzchołków grafu skierowanego.

Stwierdzenie

Niech $(M, \cdot)$ będzie monoidem. Wtedy relacja $R \subset M \times M$ zadana warunkiem

$$xRy \leftrightarrow \exists_{z \in M}\ y = xz,$$

jest quasi–porządkiem.

Quasi–porządek cd.

Dowód.

Ćwiczenie.

Uwaga

Każdy porządek częściowy jest quasi–porządkiem.

Monady

Uwagi

Modyfikując definicję posługującą się przemiennością diagramów, można podać definicję monoidu, zastępując zbiór M obiektem ścisłej kategorii monoidalnej (tj. kategorii posiadającą funktor $\otimes$, nazywany **iloczynem tensorowym**, o własnościach podobnych do iloczynu kartezjańskiego).

Przykładem ścisłej kategorii monoidalnej jest np. kategoria zbiorów Set, ale także kategoria endofunktorów pewnej kategorii C. Obiektami tej kategorii są funktory $F\colon \mathsf{C} \to \mathsf{C}$, morfizmami transformacje naturalne (2-funktory), a iloczynem tensorowym składanie endofunktorów.

Monada to wybór endofunktora $F\colon \mathsf{C} \to \mathsf{C}$ oraz zadanie na nim struktury monoidu w ścisłej monoidalnej kategorii endofunktorów.

Szczegółowe definicje pojawią się w wykładzie nr 7.

Kategoryjna definicja iloczynu kartezjańskiego

Dla dowolnej rodziny zbiorów $\{A_i\}_{i \in I}$ indeksowanej przez zbiór I, zbiór $\prod_{i \in I} A_i$ posiada następującą **własność uniwersalną**.

Stwierdzenie

Dla dowolnego zbioru B oraz rodziny funkcji $\{g_i \colon B \to A_i\}_{i \in I}$ istnieje **dokładnie jedna** funkcja $h \colon B \to \prod_{i \in I} A_i$ taka, że

$$g_i = \operatorname{pr}_i \circ h,$$

gdzie pr_i jest rzutem na i-tą współrzędna w iloczynie kartezjańskim.

Dowód.

Jeśli pewne $X_i = \emptyset$, wtedy także $Y = \emptyset$, a funkcja $h = \emptyset$ spełnia warunki stwierdzenia. Gdy $I = \emptyset$ istnieje dokładnie jedna funkcja $h \colon B \to \{\emptyset\}$, a warunek złożenia jest pusto spełniony. W pozostałych przypadkach, dla dowolnego $b \in B$

$$(h(b))(i) = g_i(b).$$

Kategoryjna definicja iloczynu kartezjańskiego cd.

Uwaga

Powyższą własność można przyjąć jako definicję iloczynu kartezjańskiego w kategorii zbiorów. Definiuje ona iloczyn kartezjański z **dokładnością do jednoznacznie ustalonego izomorfizmu**.

W przypadku gdy $I = \{1, 2\}$ definicję można przedstawić na diagramie przemiennym

$$\begin{tikzcd}
& B \arrow[ddl, "g_1"'] \arrow[d, dashed, "h"'] \arrow[ddr, "g_2"] & \\
& A_1 \times A_2 \arrow[dl, "\mathrm{pr}_1"] \arrow[dr, "\mathrm{pr}_2"'] & \\
A_1 & & A_2
\end{tikzcd}$$

Zadanie

Niech $k_1 \circ \mathrm{pr}_1 = k_2 \circ \mathrm{pr}_2$. Jaki zbiór C jest zdefiniowany warunkiem: dla dowolnego zbioru B oraz funkcji $g_i \colon B \to A_i$ dla $i = 1, 2$ takich, że $g_1 \circ \mathrm{pr}_1 = g_2 \circ \mathrm{pr}_2$ istnieje dokładnie jedna funkcja $h \colon B \to C$ taka, że

$$\mathrm{pr}_i \circ h = g_i \text{ dla } i = 1, 2?$$

$$\begin{tikzcd}
 & B \arrow[d, dashed, "h"'] \arrow[ddl, "g_1"'] \arrow[ddr, "g_2"] & \\
 & C \arrow[dl, "\mathrm{pr}_1"] \arrow[dr, "\mathrm{pr}_2"'] & \\
A_1 \arrow[dr, "k_1"'] & & A_2 \arrow[dl, "k_2"] \\
 & A &
\end{tikzcd}$$