Podstawy matematyki

Wykład 4 - Dobry porządek, indukcja, funkcje, bijekcje

Oskar Kędzierski

19 kwietnia 2020

Porządek – przypomnienie

Relację $R \subset X \times X$ nazywamy **porządkiem** (częściowym) jeśli jest

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

ii) antysymetryczna, tzn. $\forall_{x \in X} \forall_{y \in X}\, xRy \wedge yRx \rightarrow x = y$,

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

Jeśli jest dodatkowo spójna, tzn. $\forall_{x \in X} \forall_{y \in X}\, xRy \vee yRx \vee x = y$, to nazywamy ją relacją **porządku liniowego**.

Uwaga

Relacja pusta jest relacją porządku liniowego jedynie na zbiorze pustym. Jeśli xRy to mówimy, że x jest elementem **mniejszym lub równym** od y (lub, że y jest elementem **większym lub równym od** x), jeśli dodatkowo $x \neq y$, to mówimy, że x jest elementem **mniejszym** od y (lub, że y jest elementem **większym** od x).

Porządek liniowy – przykład

Dla zbioru $X = \mathbb{R}$ (lub $X = \mathbb{N}, \mathbb{Z}$) relacja $xRy \leftrightarrow x \leq y$ jest relacją porządku liniowego. Dla dowolnych $x, y, z \in X$

i) $x \leq x$,

ii) $x \leq y \land y \leq x \rightarrow x = y$,

iii) $x \leq y \land y \leq z \rightarrow x \leq z$,

iv) $x \leq y \lor y \leq x$.

Elementy wyróżnione

Niech $\preccurlyeq \subset X \times X$ będzie porządkiem.

Definicja

Element $a \in X$ nazywamy elementem

i) **największym**, jeśli $\forall_{x \in X}\ x \preccurlyeq a$,

ii) **najmniejszym**, jeśli $\forall_{x \in X}\ a \preccurlyeq x$,

iii) **maksymalnym**, jeśli $\forall_{x \in X}\ a \preccurlyeq x \to a = x$,

iv) **minimalnym**, jeśli $\forall_{x \in X}\ x \preccurlyeq a \to x = a$,

To znaczy, element największy (odp. najmniejszy) jest większy (odp. mniejszy) lub równy od wszystkich pozostałych elementów, a element maksymalny (odp. minimalny), to taki, dla którego nie istnieje element od niego większy (odp. mniejszy).

Elementy wyróżnione cd.

Stwierdzenie

W zbiorze X z relacją porządku $\preccurlyeq$ istnieje co najwyżej jeden element największy (odp. najmniejszy). Gdy istnieje, jest on zarazem jedynym elementem maksymalnym (odp. minimalnym).

Dowód.

Przypuśćmy, że $a, b \in X$ są elementami największymi w X. Wtedy $a \preccurlyeq b$ oraz $b \preccurlyeq a$, co z antysymetryczności daje $a = b$. Niech $a \in X$ będzie elementem największym oraz $b \in X$ elementem maksymalnym. Wtedy $b \preccurlyeq a$, co z definicji daje $b = a$.

Elementy wyróżnione cd.

Stwierdzenie

W niepustym zbiorze skończonym X z relacją porządku $\preccurlyeq \subset X \times X$ istnieje element maksymalny i minimalny.

Dowód.

Przypuścimy przeciwnie, że wszystkie elementy w X nie są maksymalne.

$$a \in X \text{ nie jest maksymalny} \leftrightarrow \exists_{x \in X}\, a \preccurlyeq x \wedge a \neq x,$$

zatem, dla każdego elementu w X istnieje element od niego większy. Elementy X można ustawić w ciąg

$$x_1 \preccurlyeq x_2, \quad x_2 \preccurlyeq x_3, \quad x_3 \preccurlyeq x_4, \ldots$$

gdzie $x_i \neq x_j$ dla $i < j$ (jeśli $x_i = x_j$, to z przechodniości i antysymetrii $x_i = x_{i+1} = \ldots = x_j$). Przeczy to skończoności X.

Przykłady

Niech $X \subset \mathbb{N}_{>0}$ będzie zbiorem z relacją porządku $\preccurlyeq$ zadaną warunkiem

$$m \preccurlyeq n \leftrightarrow m | n.$$

Wtedy, gdy

i) $X = \{2, 2^2, 2^3, \ldots\}$, to 2 jest elementem najmniejszym (i zarazem jedynym elementem minimalnym), element maksymalny nie istnieje,

ii) $X = \{3, 2, 2^2, 2^3, \ldots\}$, to nie istnieje element największy i najmniejszy, 3 jest elementem maksymalnym i minimalnym, 2 jest elementem minimalnym,

iii) $X = \{1, 2, 2^2, 2^3\}$, to 1 jest jedynym elementem najmniejszym i minimalnym, 2^3 jest jedynym elementem największym i maksymalnym,

iv) $X = \{2, 3\}$, to nie istnieje element największy i najmniejszy, 2 i 3 są zarazem elementami minimalnymi i maksymalnymi.

Ograniczenia górne i ograniczenia dolne

Niech $\preccurlyeq \subset X \times X$ będzie porządkiem (częściowym). Niech $A \subset X$ będzie podzbiorem zbioru X.

Definicja

Element $a \in X$ nazywamy **ograniczeniem górnym** zbioru A jeśli

$$\forall_{x \in X}\ x \preccurlyeq a.$$

Element $a \in X$ nazywamy **ograniczeniem dolnym** zbioru A jeśli

$$\forall_{x \in X}\ a \preccurlyeq x.$$

Uwaga

Dowolny element $a \in X$ zbioru X jest ograniczeniem górnym i dolnym zbioru pustego $A = \emptyset$.

Kres górny i kres dolny

Niech $\preccurlyeq \subset X \times X$ będzie porządkiem (częściowym). Niech $A \subset X$ będzie podzbiorem zbioru X.

Definicja

Niech B będzie zbiorem wszystkich ograniczeń górnych zbioru A. **Kresem górnym** zbioru A nazywamy najmniejszy element zbioru B (o ile istnieje) i oznaczamy $\sup A$.

Niech B będzie zbiorem wszystkich ograniczeń dolnych zbioru A. **Kresem dolnym** zbioru A nazywamy największy element zbioru B (o ile istnieje) i oznaczamy $\inf A$.

Uwaga

Kres górny i dolny, o ile istnieją, są wyznaczone jednoznacznie.

Kraty

Niech $\preccurlyeq \subset X \times X$ będzie porządkiem (częściowym).

Definicja

Zbiór X wraz z porządkiem częściowym $\preccurlyeq$ nazywamy **kratą**, jeśli dla dowolnych dwóch elementów $x, y \in X$ istnieją

$$x \vee y = \sup\{x, y\},$$

$$x \wedge y = \inf\{x, y\}.$$

Kratę nazywamy **ograniczoną**, jeśli w X istnieją elementy największy (oznaczany $1 \in X$) oraz najmniejszy (oznaczany $0 \in X$).

Przykład

Dla dowolnego zbioru A, zbiór potęgowym $P(A)$ wraz z relacją inkluzji $\subset$ jest kratą ograniczoną. Dodatkowo, jeśli $X, Y \in P(A)$, to

$$X \vee Y = X \cup Y,$$

$$X \wedge Y = X \cap Y.$$

Kraty

Stwierdzenie

Niech zbiór X z relacją porządku $\preccurlyeq$ będzie kratą. Wtedy dla dowolnych $x, y, z \in X$

i) $x \preccurlyeq y \leftrightarrow x \vee y = y$,

ii) $x \preccurlyeq y \leftrightarrow x \wedge y = x$,

iii) $x \vee x = x$,

iv) $x \wedge x = x$,

v) $x \vee y = y \vee x$,

vi) $x \wedge y = y \wedge x$,

vii) $(x \vee y) \vee z = x \vee (y \vee z)$,

viii) $(x \wedge y) \wedge z = x \wedge (y \wedge z)$,

ix) $x \wedge (x \vee y) = x$,

x) $x \vee (x \wedge y) = x$.

Kraty cd.

Dowód.

vii) z definicji zachodzą warunki (elementy są mniejsze od swoich ograniczeń górnych)

$$x \preccurlyeq x \vee y \preccurlyeq (x \vee y) \vee z,$$

$$y \preccurlyeq x \vee y \preccurlyeq (x \vee y) \vee z,$$

$$z \preccurlyeq (x \vee y) \vee z.$$

Element $(x \vee y) \vee z$ jest ograniczeniem górnym elementu y oraz elementu z, stąd

$$(y \vee z) \preccurlyeq (x \vee y) \vee z.$$

Zatem element $(x \vee y) \vee z$ jest ograniczeniem górnym elementu x oraz elementu $y \vee z$, skąd

$$x \vee (y \vee z) \preccurlyeq (x \vee y) \vee z.$$

Kraty cd.

Dowód.

ix)

x) z punktów i), ii) oraz

$$x \preccurlyeq x \vee y, \quad x \wedge y \preccurlyeq x.$$

Wniosek

Niech zbiór X z relacją porządku $\preccurlyeq$ będzie kratą.

i) dla dowolnych $x, y, z \in X$

$$x \vee y \vee z = \sup\{x, y, z\},$$

$$x \wedge y \wedge z = \inf\{x, y, z\},$$

ii) jeśli $A \subset X$ jest zbiorem skończonym, to istnieją $\sup A$, $\inf A$,

Kraty cd.

Wniosek

iii) jeśli X jest kratą ograniczoną, to dla dowolnego $x \in X$

$$x \wedge 1 = x,$$

$$x \wedge 0 = 0,$$

$$x \vee 1 = 1,$$

$$x \vee 0 = x.$$

Krata rozdzielna

Niech zbiór X z relacją porządku $\preccurlyeq$ będzie kratą.

Definicja

Mówimy, że krata X jest **rozdzielna** (lub dystrybutywna), jeśli dla dowolnych $x, y, z \in X$

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z),$$

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

Przykład

Niech $x, y, z \in X$ będą nieporównywalnymi, parami różnymi elementami kraty X. Niech $0, 1 \in X$ będą ograniczeniami odpowiednio dolnym i górnym, różnymi od x, y, z. Wtedy

$$x = x \wedge (y \vee z) \neq (x \wedge y) \vee (x \wedge z) = 0,$$

tzn. krata ta nie jest rozdzielna.

Krata zupełna

Niech zbiór X z relacją porządku $\preccurlyeq$ będzie kratą.

Definicja

Mówimy, że krata X jest **zupełna**, jeśli dla dowolnego $A \subset X$ istnieje $\sup A$ oraz $\inf A$.

Algebry Boole'a

Definicja

Ograniczoną rozdzielną kratę X z porządkiem $\preccurlyeq$ nazywamy **algebrą Boole'a** jeśli dla dowolnego elementu $x \in X$ istnieje jego **dopełnienie** $\neg x \in X$, tj. element spełniający warunki

$$x \vee \neg x = 1,$$

$$x \wedge \neg x = 0.$$

Uwaga

Dopełnienie jest jednoznacznie wyznaczone. Niech $y, z \in X$ spełniają warunki

$$x \vee y = x \vee z = 1,$$

$$x \wedge y = x \wedge z = 0.$$

Wtedy

$$y = y \wedge 1 = y \wedge (x \vee z) = 0 \vee (y \wedge z) = y \wedge z,$$

do daje $y \preccurlyeq z$. Podobnie można uzyskać $z \preccurlyeq y$, czyli $y = z$.

Algebry Boole'a

Stwierdzenie

Niech krata X z porządkiem $\preccurlyeq$ będzie algebrą Boole'a. Wtedy dla dowolnych $x, y, x', y' \in X$

i) $\neg\neg x = x$,

ii) $\neg 0 = 1,\ \neg 1 = 0$,

iii) $\neg(x \wedge y) = \neg x \vee \neg y$,

iv) $\neg(x \vee y) = \neg x \wedge \neg y$,

v) jeśli $x \preccurlyeq y,\ x' \preccurlyeq y'$, to $x \vee x' \preccurlyeq y \vee y'$ oraz $x \wedge x' \preccurlyeq y \wedge y'$,

vi) $x \preccurlyeq y \leftrightarrow \neg y \preccurlyeq \neg x \leftrightarrow x \wedge \neg y = 0$.

Dowód.

i) wynika z jednoznaczności dopełnienia,

ii) $\neg 0 = 0 \vee \neg 0 = 1$ oraz $\neg 1 = 1 \wedge \neg 1 = 0$,

Algebry Boole'a cd.

Dowód.

i) z jednoznaczności

$$(x \wedge y) \wedge (\neg x \vee \neg y) = 0,$$

$$(x \wedge y) \vee (\neg x \vee \neg y) = 1,$$

ii) j.w.

iii) jeśli $x \wedge x' \preccurlyeq x \preccurlyeq y$ oraz $x \wedge x' \preccurlyeq x' \preccurlyeq y'$, to $x \wedge x' \preccurlyeq y \wedge y'$,

iv) $(\rightarrow)$ jeśli $x \preccurlyeq y$ oraz $\neg y \preccurlyeq \neg y$, to

$$x \wedge \neg y \preccurlyeq y \wedge \neg y = 0,$$

$(\leftarrow)$ jeśli $\neg x \vee y = 1$, to

$$x = x \wedge 1 = x \wedge (\neg x \vee y) = x \wedge y.$$

Atomy, atomowe algebry Boole'a

Niech krata X z porządkiem $\preccurlyeq$ będzie algebrą Boole'a.

Definicja

Dla $x, y \in X$ definiujemy

$$x \prec y \leftrightarrow x \preccurlyeq y \text{ oraz } x \neq y.$$

Definicja

Element $a \in X$ nazywamy **atomem**, jeśli

i) $0 \prec a$,

ii) nie istnieje element $x \in X$ taki, że $0 \prec x \prec a$.

Zbiór atomów w X oznaczamy przez $\mathrm{At}\, X$. Algebrę X nazywamy **atomową algebrą Boole'a**, jeśli dla każdego $x \in X, x > 0$ istnieje atom $a \in X$ taki, że $a \preccurlyeq x$.

Własności atomów

W dowodzie poniższego stwierdzenia będzie wykorzystywana równoważność

$$x \preccurlyeq y \leftrightarrow x \wedge \neg y = 0. \tag{$\star$}$$

Niech krata X z porządkiem $\preccurlyeq$ będzie algebrą Boole'a.

Stwierdzenie

Niech $a \in X$. Następujące warunki są równoważne

i) a jest atomem w X,

ii) dla każdego $x \in X$ zachodzi $a \preccurlyeq x$ albo $a \preccurlyeq \neg x$ (tzn. oba warunki nie zachodzą naraz),

iii) $0 \prec a$ oraz dla dowolnych $x, y \in X$ zachodzi $a \preccurlyeq x \vee y \leftrightarrow a \preccurlyeq x$ lub $a \preccurlyeq y$,

iv) $0 \prec a$ oraz dla dowolnych $x, y \in X$ zachodzi $a \preccurlyeq x \wedge y \leftrightarrow a \preccurlyeq x$ oraz $a \preccurlyeq y$.

Własności atomów cd.

Dowód.

$i)\to ii)$ jeśli nie zachodzi $a \preccurlyeq x$, to nie zachodzi także $0 \prec a \wedge \neg x \preccurlyeq a$, ponieważ a jest atomem, to $a \preccurlyeq \neg x$. Jeśli $a \preccurlyeq x$ albo $a \preccurlyeq \neg x$, to $a \wedge a \preccurlyeq x \wedge \neg x = 0$.

$ii)\to iii)$ implikacja $\leftarrow$ zachodzi zawsze, bo $a \preccurlyeq x \preccurlyeq (x \vee y)$ oraz $a \preccurlyeq y \preccurlyeq (x \vee y)$. Przypuśćmy, że $a \preccurlyeq x \vee y$ ale nie zachodzi $a \preccurlyeq x$. Wtedy, $a \preccurlyeq \neg x$ oraz

$$a = a \wedge a \preccurlyeq (x \vee y) \wedge \neg x = 0 \vee (\neg x \wedge y) = (\neg x \wedge y) \preccurlyeq y.$$

Dodatkowo $a > 0$ ponieważ inaczej $a = 0 \preccurlyeq x$ oraz $a = 0 \preccurlyeq \neg x$.

Własności atomów cd.

Dowód.

iii)$\to$*i*) niech $0 \prec x \prec a$. Wtedy

$$a = a \wedge 1 = a \wedge (x \vee \neg x) = x \vee (a \wedge \neg x).$$

Z punktu *iii*) zachodzi

$$a \preccurlyeq x \text{ albo } a \preccurlyeq a \wedge \neg x,$$

przy czym pierwszy warunek jest sprzeczny z założeniem, a drugi daje $a = a \wedge \neg x$, czyli $a \preccurlyeq \neg x$. Z warunku $(\star)$ zachodzi $x = a \wedge x = 0$, czyli sprzeczność.

Klasyfikacja skończonych algebr Boole'a

Niech X będzie atomową zupełną algebrą Boole'a. Odwozorowanie zadane wzorem

$$f\colon X \in x \mapsto \{a \in \mathrm{At}\colon a \preccurlyeq x\} \in P(\mathrm{At}\, X),$$

i) jest odwzorowaniem wzajemnie jednoznacznym,

ii) dla dowolnych $x, y \in X$

$$f(x \vee y) = f(x) \cup f(y),$$

$$f(x \wedge y) = f(x) \cap f(y),$$

$$f(\neg x) = [f(x)]' = X \setminus f(x),$$

$$x \preccurlyeq y \leftrightarrow f(x) \subset f(y),$$

iii) $f(0) = \emptyset$,

iv) $f(1) = \mathrm{At}\, X$.

Klasyfikacja skończonych algebr Boole'a cd.

Dowód.

Warunki *iii*) i *iv*) są oczywiste. W warunków *ii*) – *iv*) charakteryzacji elementów atomowych, dla dowolnego $x \in X$

$$f(x) \sqcup f(\neg x) = \mathrm{At}\, X,$$

$$f(x \vee y) = f(x) \cup f(y),$$

$$f(x \wedge y) = f(x) \cap f(y).$$

Klasyfikacja skończonych algebr Boole'a cd.

Dowód.

Różnowartościowość: niech $x \neq y$ oraz, na przykład $x \wedge \neg y \neq 0$ (tzn. nie zachodzi $x \preccurlyeq y$). Ponieważ algebra X jest atomowa, to istnieje $a \in \mathrm{At}\, X$ taki, że

$$0 \prec a \preccurlyeq x \wedge \neg y,$$

co jest równoważne

$$a \preccurlyeq x \text{ oraz } a \preccurlyeq \neg y,$$

czyli

$$a \in f(x) \text{ oraz } a \notin f(y),$$

skąd $f(x) \neq f(y)$.

Klasyfikacja skończonych algebr Boole'a cd.

Dowód.

Surjektywność: niech $B \subset Y$ będzie dowolnym zbiorem oraz niech $s = \bigvee Y$ (z zupełności). Pokażemy, że $f(s) = Y$. $Y \subset f(s)$**:** jeśli $a \in Y$, to $a \preccurlyeq s$, skąd $a \in f(s)$.

$Y' \subset [f(s)]'$**:** Jeśli $a \notin Y$, to dla dowolnego $b \in Y$ nie zachodzi $0 \prec a \preccurlyeq b$, skąd, z charakteryzacji atomów, dla dowolnego $b \in Y$ zachodzi $a \preccurlyeq\neq b$, czyli $a \wedge b = 0$, skąd z rozdzielności $a \wedge s = 0$. Oznacza to, że $a \preccurlyeq\neq s$, czyli $a \notin f(s)$.

Klasyfikacja skończonych algebr Boole'a cd.

Stwierdzenie

Każda skończona algebra Boole'a jest atomowa i zupełna.

Dowód.

Nie istnieje nieskończony ciąg

$$0 \prec \ldots \prec a_3 \prec a_2 \prec a_1.$$

$$\sup\{a_1, \ldots, a_n\} = a_1 \vee \ldots \vee a_m,$$

$$\inf\{a_1, \ldots, a_n\} = a_1 \wedge \ldots \wedge a_m.$$

Wniosek

Każda skończona algebra Boole'a X jest izomorficzna z algebrą $P(\mathrm{At}\, X)$.

Klasyfikacja skończonych algebr Boole'a cd.

Wniosek

Dowolna skończona algebra Boole'a X jest izomorficzna a algebrą Boole'a $P(\mathrm{At}\, X)$ i ma 2^n elementów. Dodatkowo, dwie skończone algebry Boole'a są izomorficzne wtedy i tylko wtedy, gdy maja taką samą liczbę elementów.

Relacja dobrego porządku

Definicja

Relację $\preccurlyeq \subset X \times X$ porządku liniowego na X nazywamy relacją **dobrego porządku** jeśli spełnia warunek

$$\forall_{A \subset X}\ A \neq \emptyset \to \exists_{a \in A} \forall_{x \in A}\ a \preccurlyeq x,$$

tzn. w każdym niepustym podzbiorze A zbioru X istnieje element **najmniejszy** w A.

Stwierdzenie

Porządek $\leq$ na zbiorze liczb naturalnych $\mathbb{N}$ jest dobrym porządkiem.

Dowód.

Jest to **aksjomat** liczb naturalnych.

Relacja dobrego porządku cd.

Przykład

Relacje $\leq_{lex}$ oraz $\leq_{grlex}$ są relacjami dobrego porządku na $\mathbb{N}^n$.

Dowód.

Dla $\leq_{lex}$. Niech $A \subset \mathbb{N}^n$, $A \neq \emptyset$. Definiujemy rekurencyjnie rodzinę niepustych zbiorów $A_0, \ldots, A_n \subset \mathbb{N}^n$

$$A_0 = A,$$

$$A_k = \{\alpha \in A_{k-1} \mid \pi_k(\alpha) \text{ elt. najmniejszy w } \pi_k(A_{k-1})\},$$

dla $k = 1, \ldots, n$, gdzie

$$\pi_k \colon \mathbb{N}^n \to \mathbb{N},$$

$$\pi_k(\alpha_1, \ldots, \alpha_n) = \alpha_k \in \mathbb{N},$$

jest rzutowaniem na k-tą współrzędną. Wtedy $A_n = \{\alpha\}$, gdzie $\alpha \in \mathbb{N}$ jest elementem najmniejszym w A. Podobnie dla $\leq_{grlex}$.

Indukcja pozaskończona

Niech relacja $\preccurlyeq$ na zbiorze X będzie relacją **dobrego porządku**.

Stwierdzenie

Jeśli $P(x)$ jest funkcją zdaniową zakresem zmienności równym zbiorowi X, spełniającą warunek

$$\forall_{y\in X}\,(\forall_{x\in X}\; x \preccurlyeq y \wedge x \neq y \to P(x)) \to P(y),$$

(tzn. z prawdziwości funkcji $P(x)$ dla wszystkich elementów x mniejszych od y, wynika prawdziwość $P(y)$), to

$$\forall_{x\in X}\; P(x),$$

tzn. funkcja zdaniowa $P(x)$ jest prawdziwa w zbiorze X.

Indukcja pozaskończona cd.

Dowód.

Niech

$$A = \{x \in X \mid \neg P(x)\}$$

będzie zbiorem tych elementów $x \in X$, dla których $P(x)$ nie jest prawdą. Jeśli zbiór A jest niepusty, to istnieje w nim element najmniejszy $a \in A$. Wtedy, jeśli $b \preccurlyeq a$ oraz $b \neq a$, to zachodzi $P(b)$ (w przeciwnym razie $b \in A$, co stoi w sprzeczności z tym, że a jest elementem najmniejszym w A). Z założenia stwierdzenia, $P(b)$ zachodzi dla elementów $b \in X$ mniejszych od a, zatem zachodzi także $P(a)$, co jest sprzeczne z $a \in A$.

Zasada indukcji matematycznej

Stwierdzenie

Niech $P(n)$ będzie funkcją zdaniową z zakresem zmienności równym zbiorowi liczb naturalnych, spełniającą warunki:

i) zdanie $P(0)$ jest prawdziwe,

ii) dla dowolnego $n \in \mathbb{N}$, z prawdziwości zdań $P(0), \ldots, P(n)$ wynika prawdziwość zdania $P(n+1)$.

Wtedy zdanie $P(n)$ jest prawdziwe dla dowolnego $n \in \mathbb{N}$.

Dowód.

Wynika z indukcji pozaskończonej dla relacji dobrego porządku $\leq$ na zbiorze $\mathbb{N}$.

Uwaga

Prawdziwość $P(0)$ konieczna jest, aby warunek indukcji pozaskończonej był prawdziwy dla $y = 0$.

Indukcja – przykład

Stwierdzenie

Dla dowolnego $n \in \mathbb{N}$

$$0^2 + 1^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Dowód.

(przez indukcję matematyczną)

i) dla $n = 0$ wzór jest prawdziwy,

ii) załóżmy, że wzór jest prawdziwy dla $k < n + 1$. Wtedy

$$0^2 + 1^2 + \ldots + n^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 =$$

$$= (n+1)\frac{n(2n+1) + 6(n+1)}{6} = (n+1)\frac{2n^2 + 7n + 6}{6} =$$

$$= (n+1)\frac{(n+2)(2n+3)}{6} = \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}.$$

Wzór Faulhabera

$$\sum_{k=1}^{n} k^m = \frac{n^{m+1}}{m+1} + \frac{n^m}{2} + \sum_{k=2}^{m} \frac{B_k}{k!} \binom{m}{k-1} (k-1)! n^{m-k+1},$$

gdzie $B_2, \ldots, B_m$ są **liczbami Bernoulliego** zadanymi współczynnikami szeregu Taylora

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} \frac{B_k x^k}{k!} =$$

$$= 1 - \frac{x}{2} + \frac{x^2}{12} - \frac{x^4}{720} + \frac{x^6}{30240} - \frac{x^8}{1209600} + \frac{x^{10}}{47900160} + \ldots$$

W szczególności, dla $m = 2$

$$\sum_{k=1}^{n} k^2 = \frac{n^3}{3} + \frac{n^2}{2} + \frac{1}{12} \cdot 2 \cdot n = \frac{n\,(n+1)\,(2n+1)}{6}.$$

Funkcje – przypomnienie

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 $x \in X$ jest w relacji z **co najwyżej jednym** elementem zbioru Y.

Definicja

Relację $R \subset X \times Y$ nazywamy **funkcją**

$$\forall_{x \in X} \exists!_{y \in Y} xRy,$$

tzn. każdy $x \in X$ jest w relacji z **dokładnie jednym** elementem zbioru Y. W szczególności, funkcja jest funkcją częściową.

Kwantyfikator jednoznaczności

Definicja

Dla dowolnej funkcji zdaniowej $P(x)$ zdanie $\exists!_x P(x)$ jest równoważne zdaniu

$$\exists_x P(x) \wedge \forall_y \forall_z \left(P(y) \wedge P(z) \to y = z\right).$$

Kwantyfikator $\exists!$ nazywamy **kwantyfikatorem jednoznaczności**.

Uwaga

Z definicji

$$\neg\left(\exists!_x P(x)\right) \leftrightarrow \left[\left(\forall_x \neg P(x)\right) \vee \left(\exists_y \exists_z P(y) \wedge P(z) \wedge y \neq z\right)\right],$$

zatem zaprzeczeniem zdania „istnieje dokładnie jeden x taki, że $P(x)$" jest zdanie „nie istnieje x taki, że $P(x)$ lub istnieją dwa różne x, y takie, że $P(x)$ oraz $P(y)$.

Funkcje – przypomnienie cd.

Przykład

Dla $X = \{1, 2\}$ dane są relacje $R, S, T \subset X \times X$

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

Relacja R nie jest funkcją, relacja S jest funkcją częściową, ale nie jest funkcją.
Relacja T jest funkcją ale relacja $T^{-1} = R$ nie jest funkcją.

Funkcje – notacja

Definicja

Jeśli relacja $R \subset X \times Y$ jest funkcją, to piszemy

$$R\colon X \to Y.$$

Dla każdego $x \in X$ istnieje jednoznacznie wyznaczony element $y \in Y$, taki, że xRy. Oznaczamy go przez $R(x)$. To znaczy, dla funkcji R

$$y = R(x) \leftrightarrow xRy.$$

Piszemy też

$$R\colon X \ni x \mapsto R(x) \in Y.$$

Zbiór X nazywamy **dziedziną** funkcji f, a zbiór Y **przeciwdziedziną** funkcji f.

Uwaga

Funkcje zwyczajowo oznaczamy literami f, g, h.

Identyczność i złożenie

Definicja

Dla dowolnego zbioru X funkcję $\mathrm{id}_X : X \to X$ zadaną warunkiem

$$id_X(x) = x,$$

nazywamy funkcją **identycznościową** (lub **identycznością**) na X.

Definicja

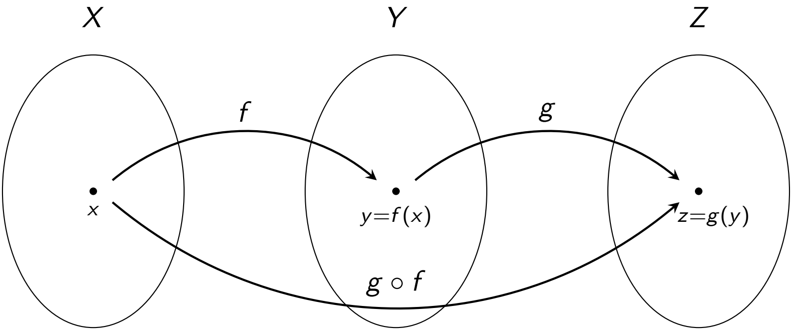
Dla funkcji $f: X \to Y$, $g: Y \to Z$ **złożeniem** g z f nazywamy funkcję $g \circ f: X \to Z$ daną warunkiem

$$(g \circ f)(x) = g(f(x)).$$

Uwaga

Jako relacja $g \circ f = f \cdot g$, gdzie po lewej stronie stoi złożenie relacji, oznaczane „$\cdot$”. Zmiana kolejności w zapisie złożenia dla funkcji pochodzi z następującego faktu

Złożenie funkcji – cd



$$x\, f\, (f(x)) \wedge f(x)\, g\, (g(f(x))) \rightarrow x\, (f \cdot g)\ (g(f(x)))\,.$$

Złożenie funkcji cd.

Stwierdzenie

Dla dowolnych funkcji $f\colon X \to Y, g\colon Y \to Z, h\colon Z \to W$

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Dowód.

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) =$$
$$= ((h \circ g) \circ f)(x).$$

Przykłady

i) dla dowolnej funkcji $f\colon X \to Y$ zachodzi $id_Y \circ f = f \circ id_X = f$,

ii) dla funkcji $f, g\colon \mathbb{R} \to \mathbb{R}$ danych wzorami $f(x) = x^2$, $g(x) = x + 3$ zachodzi

$$
\begin{aligned}
(g \circ f)(x) &= g(f(x)) = g(x^2) = x^2 + 3,\\
(f \circ g)(x) &= f(g(x)) = f(x + 3) = (x + 3)^2,\\
(g \circ g)(x) &= g(g(x)) = g(x + 3) = x + 6,\\
(f \circ f)(x) &= f(f(x)) = f(x^2) = x^4.
\end{aligned}
$$

Obrazy i przeciwobrazy

Niech $f\colon X \to Y$ będzie funkcją.

Definicja

Dla dowolnego zbioru $A \subset X$ **obrazem** zbioru A przez funkcję f nazywamy zbiór

$$f(A) = \{y \in Y \mid \exists_{x \in A} y = f(x)\} = \{f(x) \in Y \mid x \in A\}.$$

W szczególności, dla $x \in X$ zachodzi $f(\{x\}) = \{f(x)\}$.

Definicja

Dla dowolnego zbioru $B \subset Y$ **przeciwobrazem** zbioru B przez funkcję f nazywamy zbiór

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}.$$

W szczególności, **włóknem** elementu $y \in Y$ nazywamy zbiór

$$f^{-1}(y) = f^{-1}(\{y\}) = \{x \in X \mid f(x) = y\}.$$

Przykłady

Niech $f\colon \mathbb{R} \to \mathbb{R}$ będzie funkcją daną wzorem $f(x) = x^2$. Wtedy

$$
\begin{aligned}
&f((1,+\infty)) = (1,+\infty),\\
&f((-1,+\infty)) = f(\mathbb{R}) = [0,+\infty),\\
&f^{-1}(4) = \{-2,2\},\\
&f^{-1}(3) = \{-\sqrt{3},\sqrt{3}\},\\
&f^{-1}(0) = \{0\},\\
&f^{-1}(-2) = f^{-1}((-\infty,0)) = \emptyset,\\
&f^{-1}([4,+\infty)) = (-\infty,-2] \cup [2,+\infty),\\
&f^{-1}((0,+\infty)) = \mathbb{R} \setminus \{0\},\\
&f^{-1}([0,+\infty)) = f^{-1}((-1,+\infty) = f^{-1}(\mathbb{R}) = \mathbb{R}.
\end{aligned}
$$

Własności obrazów i przeciwobrazów

Niech $A, \widetilde{A} \subset X,\ B, \widetilde{B} \subset Y$ będą dowolnymi podzbiorami.

i) $A \subset \widetilde{A} \rightarrow f(A) \subset f(\widetilde{A})$,

ii) $B \subset \widetilde{B} \rightarrow f^{-1}(B) \subset f^{-1}(\widetilde{B})$,

iii) $A \subset f^{-1}(f(A))$ oraz $f(f^{-1}(B)) \subset B$,

iv) $f(A \cap \widetilde{A}) \subset f(A) \cap f(\widetilde{A})$ oraz $f(A \cup \widetilde{A}) = f(A) \cup f(\widetilde{A})$,

v) $f(A) \setminus f(\widetilde{A}) \subset f(A \setminus \widetilde{A})$,

vi) $f^{-1}(B \cap \widetilde{B}) = f^{-1}(B) \cap f^{-1}(\widetilde{B})$ oraz
$f^{-1}(B \cup \widetilde{B}) = f^{-1}(B) \cup f^{-1}(\widetilde{B})$,

vii) $f^{-1}(B) \setminus f^{-1}(\widetilde{B}) = f^{-1}(B \setminus \widetilde{B})$.

Dowód.

iii) $x \in A \rightarrow f(x) \in f(A) \rightarrow x \in f^{-1}(f(A))$,
$y \in f(f^{-1}(B)) \rightarrow \exists_{x' \in f^{-1}(B)}\ y = f(x')$ ale $f(x') \in B$,

Własności obrazów i przeciwobrazów cd.

Dowód.

iv) $y \in f(A \cap \widetilde{A}) \leftrightarrow \exists_{x \in A \cap \widetilde{A}}\, y = f(x) \leftrightarrow \exists_x\, x \in A \wedge x \in \widetilde{A} \wedge y = f(x) \rightarrow y \in f(A) \wedge y \in f(\widetilde{A})$,

v) $y \in f(A) \setminus f(\widetilde{A}) \leftrightarrow (\exists_{x \in A}\, y = f(x)) \wedge \left(\forall_{x \in \widetilde{A}} y \neq f(x)\right) \rightarrow \exists_{x \in A \setminus \widetilde{A}}\, y = f(x) \rightarrow y \in f(A \setminus \widetilde{A})$,

vi) $x \in f^{-1}(B \cap \widetilde{B}) \leftrightarrow f(x) \in B \cap \widetilde{B} \leftrightarrow f(x) \in B \wedge f(x) \in \widetilde{B} \leftrightarrow x \in f^{-1}(B) \wedge x \in f^{-1}(\widetilde{B})$,

vii) jak w vi).

Funkcja różnowartościowa

Definicja

Funkcję $f\colon X \to Y$ nazywamy **różnowartościową** (lub **injekcją**), jeśli

$$\forall_{x,x'\in X}\ f(x) = f(x') \to x = x'.$$

Równoważnie,

$$\forall_{x,x'\in X}\ x \neq x' \to f(x) \neq f(x').$$

Przykład

Funkcja $f\colon \mathbb{R} \to \mathbb{R}$ dana wzorem $f(x) = x^2$ nie jest różnowartościowa, bo $-2 \neq 2$, ale $f(-2) = f(2)$. Funkcja $g\colon \mathbb{R} \to \mathbb{R}$ dana wzorem $g(x) = 2^x$ jest różnowartościowa, bo $2^x = 2^{x'}$ implikuje $x = x'$.

Funkcja „na”

Definicja

Funkcję $f\colon X \to Y$ nazywamy **funkcją „na”** (lub **surjekcją**), jeśli

$$\forall_{y\in Y}\exists_{x\in X}\ y = f(x),$$

czyli $f(X) = Y$.

Uwaga

Funkcja f **nie jest** „na”, jeśli

$$\exists_{y\in Y}\forall_{x\in X}\ y \neq f(x).$$

Przykład

Funkcja $f\colon \mathbb{R} \to \mathbb{R}$ dana wzorem $f(x) = x^2$ nie jest „na”, bo $f(\mathbb{R}) = [0 + \infty) \neq \mathbb{R}$. Funkcja $g\colon \mathbb{R} \to [0, +\infty)$ dana wzorem $g(x) = x^2$ jest „na”.

Własności funkcji różnowartościowej

Stwierdzenie

Niech $f, f' \colon X \to Y$ oraz $g \colon Y \to Z$ będą funkcjami. Wtedy

i) jeśli f i g są różnowartościowe, to złożenie $g \circ f$ jest funkcją różnowartościową,

ii) jeśli złożenie $g \circ f$ jest funkcją różnowartościową, to f jest funkcją różnowartościową,

iii) jeśli $g \circ f = g \circ f'$ oraz g jest funkcją różnowartościową, to $f = f'$.taka, że $g \circ f = id_X$.

Dowód.

i) niech funkcje g, f będą różnowartościowe, wtedy

$$g(f(x)) = g(f(x')) \to f(x) = f(x') \to x = x',$$

Własności funkcji równowartościowej cd.

Dowód.

ii) niech $g \circ f$ będzie funkcją różnowartościową, przypuśćmy przeciwnie, że istnieją $x \neq x'$ takie, że $f(x) = f(x')$. Wtedy $g(f(x)) = g(f(x'))$, co daje sprzeczność,

iii) dla dowolnego $x \in X$ zachodzi $g(f(x)) = g(f'(x))$, co daje $f(x) = f'(x)$. pewnika wyboru istnieje selektor, to jest funkcja $g\colon f(X) \to X$, taka, że $g(y) \in f^{-1}(y)$, funkcję g można dowolnie rozszerzyć na $Y \supset f(X)$, i wtedy $g \circ f = \mathrm{id}_X$, bo $f^{-1}(\{f(x)\}) = \{x\}$.

Monomorfizm (teoria kategorii)

Niech $f\colon x \to y$ będzie morfizmem w kategorii C.

Definicja

Morfizm f jest **monomorfizmem** jeśli, dla dowolnego obiektu $z \in \mathrm{C}$ oraz dowolnych morfizmów $h_1, h_2\colon z \to x$

$$\text{jeśli } f \circ g = f \circ g', \text{ to } g = g'.$$

$$\begin{tikzcd} z \arrow[r, shift left, "g"] \arrow[r, shift right, "g'"'] & x \arrow[r, "f"] & y \end{tikzcd}$$

Wniosek

Następujące warunki są równoważne:

i) f jest monomorfizmem,

ii) dla dowolnego obiektu $z \in \mathrm{C}$ funkcja

$$f_*\colon \operatorname{Hom}(z, x) \to \operatorname{Hom}(z, y),$$

jest różnowartościowa.

Monomorfizm (teoria kategorii) cd.

Wniosek

Monomorfizmy w kategorii Set to dokładnie funkcje różnowartościowe.

Uwaga

Morfizm z obiektu końcowego jest monomorfizmem.

Uwaga

Funkcja

$$\emptyset\colon \emptyset \to Y,$$

jest różnowartościowa dla dowolnego zbioru Y.

Uwaga

Istnieją monomorfizmy, które nie są różnowartościowe.

Monomorfizm (teoria kategorii) cd.

Stwierdzenie

i) morfizm *id* jest monomorfizmem,

ii) jeśli złożenie morfizmów $f' \circ f$ jest monomorfizmem, to morfizm f jest monomorfizmem,

iii) złożenie monomorfizmów jest monomorfizmem.

Dowód.

Ćwiczenie.

Własności funkcji „na”

Niech $f\colon X \to Y$ oraz $g, g'\colon Y \to Z$ będą funkcjami.

Stwierdzenie

i) jeśli f i g są „na”, to złożenie $g \circ f$ jest funkcją „na”,

ii) jeśli złożenie $g \circ f$ jest funkcją „na”, to g jest funkcją „na”,

iii) jeśli $g \circ f = g' \circ f$ oraz f jest funkcją „na”, to $g = g'$.
$f \circ g = id_Y$.

Dowód.

i) $(g \circ f)(X) = g(f(X)) = g(Y) = Z$,

ii) dla dowolnego $z \in Z$ istnieje $x \in X$ takie, że $z = (g \circ f)(x)$, co daje $z = g(y)$, gdzie $y = f(x)$, zatem g jest funkcją „na”.

Własności funkcji „na” cd.

Dowód.

iii) z założenia, dla dowolnego $y \in Y$ istnieje $x \in X$ takie, że $y = f(x)$, zatem, dla dowolnego $y \in Y$ mamy $g(y) = g(f(x)) = g'(f(x)) = g'(y)$. wyboru istnieje selektor, to jest funkcja $g\colon Y \to X$, taka, że $g(y) \in f^{-1}(y)$, i wtedy $f \circ g = \mathrm{id}_Y$.

Epimorfizm (teoria kategorii)

Niech $f\colon x \to y$ będzie morfizmem w kategorii C.

Definicja

Morfizm f jest **epimorfizmem** jeśli, dla dowolnego obiektu $z \in \mathrm{C}$ oraz dowolnych morfizmów $g, g'\colon y \to z$

$$\text{jeśli } g \circ f = g' \circ f, \text{ to } g = g'.$$

$$\begin{tikzcd} x \arrow[r, "f"] & y \arrow[r, shift left, "g"] \arrow[r, shift right, "g'"'] & z \end{tikzcd}$$

Wniosek

Następujące warunki są równoważne:

i) f jest epimorfizmem,

ii) dla dowolnego obiektu $z \in \mathrm{C}$ funkcja

$$f^*\colon \mathrm{Hom}(y, z) \to \mathrm{Hom}(x, z),$$

jest różnowartościowa.

Epimorfizm (teoria kategorii) cd.

Wniosek
Epimorfizmy w kategorii Set to dokładnie funkcje „na”.

Uwaga
Każdy morfizm do obiektu początkowego jest epimorfizmem.

Uwaga
Funkcja
$$\emptyset\colon \emptyset \to Y,$$
jest funkcją „na” dokładnie wtedy, gdy $Y = \emptyset$.

Uwaga
Istnieją epimorfizmy, które nie są funkcjami „na”.

Epimorfizm (teoria kategorii) cd.

Stwierdzenie

i) morfizm *id* jest epimorfizmem,

ii) jeśli złożenie morfizmów $f \circ f'$ jest epimorfizmem, to morfizm f jest epimorfizmem,

iii) złożenie epimorfizmów jest epimorfizmem.

Dowód.

Ćwiczenie.

Obcięcie i rozszerzenie funkcji

Definicja

Dla dowolnej funkcji $f\colon X \to Y$ oraz zbioru $A \subset X$ relacja

$$f|_A = f \cap (A \times Y) \subset A \times Y$$

jest funkcją, nazywaną **obcięciem** funkcji f do zbioru A.

Definicja

Dla dowolnego zbioru $A \subset X$ oraz dowolnej funkcji $g\colon A \to Y$ funkcję $f\colon X \to Y$ nazywamy **rozszerzeniem** funkcji g do zbioru X, jeśli $f|_A = g$.

Stwierdzenie

Obcięcie funkcji różnowartościowej jest funkcją różnowartościową. Rozszerzenie funkcji „na” jest funkcją „na”.

Zmiana przeciwdziedziny

Uwaga

Funkcja $f\colon X \to Y$ jest wyznaczona jednoznacznie przez swoje wartości **oraz** dziedzinę i przeciwdziedzinę.

Stwierdzenie

Dla dowolnej funkcji $f\colon X \to Y$ istnieje funkcja „na”

$$f'\colon X \to f(X),$$

o tej samej dziedzinie i tych samych wartościach, tj. $f(x) = f'(x)$ dla $x \in X$.

Dowód.

$f' = f \cap (X \times f(X)) \subset X \times f(X)$

Uwaga

Zachowując wartości i dziedzinę, za przeciwdziedzinę można ustalić dowolny zbiór $Z \supset f(X)$.

Aksjomat wyboru w języku funkcji

Uwaga

Aksjomat wyboru jest równoważny następującemu stwierdzeniu: dla dowolnego zbioru $I \neq \emptyset$ oraz dowolnej, indeksowanej przez I, rodziny niepustych, parami rozłącznych zbiorów $\{A_i\}_{i \in I}$ tzn.,

$$A_i \neq \emptyset \text{ dla } i \in I \text{ oraz } A_i \cap A_j = \emptyset \text{ dla } i, j \in I,\ i \neq j,$$

istnieje **selektor** s, to jest funkcja

$$s\colon I \to \bigcup_{i \in I} A_i$$

taka, że

$$f(i) \in A_i.$$

Lewa i prawa odwrotność

Stwierdzenie

Niech $f\colon X \to Y$ będzie funkcją. Wtedy

i) f jest funkcją różnowartościową wtedy i tylko wtedy, gdy istnieje funkcja $g\colon Y \to X$ taka, że $g \circ f = \mathrm{id}_X$,

ii) f jest funkcją „na" wtedy i tylko wtedy, gdy istnieje funkcja $g\colon Y \to X$ taka, że $f \circ g = \mathrm{id}_Y$.

W przypadku i), funkcję g nazywamy **lewostronną odwrotnością**, a w przypadku ii) **prawostronną odwrotnością** funkcji f.

Dowód.

i) $(\leftarrow)$ wynika z własności funkcji różnowartościowej, id_X jest funkcją różnowartościową, $(\rightarrow)$ relację f^{-1} rozszerzamy dowolnie do funkcji $g\colon Y \to X$, dla $y \in f(X)$

$$y(f^{-1})x \wedge y(f^{-1})x' \to y = f(x) \wedge y = f(x') \to x = x',$$

czyli relacja $f^{-1} \subset Y \times X$ jest funkcją częściową.

Lewa i prawa odwrotność– cd

Dowód.

ii) $(\leftarrow)$ wynika z własności funkcji „na”, id_Y jest funkcją na, $(\rightarrow)$ rodzina $\{f^{-1}(y)\}_{y\in Y}$, indeksowana przez zbiór Y jest rodziną niepustych, parami rozłącznych zbiorów, na mocy pewnika wyboru istnieje selektor, to jest funkcja

$$g\colon Y \to X = \bigcup_{y\in Y} f^{-1}(y)$$

taka, że $g(y) \in f^{-1}(y)$ dla $y \in Y$. Zatem $f(g(y)) = y$.

Funkcja wzajemnie jednoznaczna

Definicja

Funkcję $f\colon X \to Y$ nazywamy funkcją **wzajemnie jednoznaczną** (lub **bijekcją**) jeśli jest funkcją różnowartościową i funkcją „na".

Stwierdzenie

Funkcja $f\colon X \to Y$ jest funkcją wzajemnie jednoznaczną wtedy i tylko wtedy, gdy istnieje funkcja $g\colon Y \to X$ taka, że

$$g \circ f = \mathrm{id}_X, \qquad f \circ g = \mathrm{id}_Y\,.$$

Dowód.

($\leftarrow$) oczywiste,

Funkcja wzajemnie jednoznaczna– cd.

Dowód.

($\rightarrow$) z własności funkcji różnowartościowych i funkcji „na”, istnieją $g, g' \colon Y \rightarrow X$ takie, że

$$g \circ f = \mathrm{id}_X, \qquad f \circ g' = \mathrm{id}_Y\,.$$

Zatem $g = g \circ (f \circ g') = (g \circ f) \circ g' = g'$. Dodatkowo, jako relacje $g = f^{-1}$.

Stwierdzenie

Dla funkcji wzajemnie jednoznacznej $f \colon X \rightarrow Y$ istnieje dokładnie jedna **funkcja odwrotna** $f^{-1} \colon Y \rightarrow X$, spełniająca warunki

$$f^{-1} \circ f = \mathrm{id}_X, \qquad f \circ f^{-1} = \mathrm{id}_Y\,.$$

Funkcja odwrotna jest także funkcją wzajemnie jednoznaczną oraz $(f^{-1})^{-1} = f$.

Izomorfizm (teoria kategorii)

Niech $f : x \to y$ będzie morfizmem w kategorii C.

Definicja

Morfizm f jest **izomofizmem** w kategorii C jeśli istnieje morfizm $g : y \to x$ taki, że

$$g \circ f = \mathrm{id}, \quad f \circ g = \mathrm{id}\,.$$

Wniosek

Izomorfizm jest monomorfizmem i epimorfizmem.

Uwaga

W kategorii Set izomorfizmy, to dokładnie funkcje wzajemnie jednoznaczne.

Przykłady

i) funkcja $f\colon \mathbb{R} \to \mathbb{R}$ zadana wzorem $f(x) = -x$ jest wzajemnie jednoznaczna oraz $f^{-1} = f$.

ii) funkcja $f\colon \mathbb{R} \to \mathbb{R}$ zadana wzorem $f(x) = 2^x$ nie jest wzajemnie jednoznaczna (jest funkcją różnowartościową ale nie jest „na”),

iii) funkcja $f\colon \mathbb{R} \to \mathbb{R}$ zadana wzorem $f(x) = x^3 - x$ nie jest wzajemnie jednoznaczna (nie jest funkcją różnowartościową ale jest „na”),

iv) dla dowolnej sumy prostej $\mathbb{R}^n = V \oplus W$ symetria $S\colon \mathbb{R}^n \to \mathbb{R}^n$ względem podprzestrzeni V równolegle do podprzestrzeni W jest funkcją wzajemnie jednoznaczną (bo $S \circ S = \mathrm{id}_{\mathbb{R}^n}$),

v) odwzorowanie liniowe $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ jest funkcją wzajemnie jednoznaczną wtedy i tylko wtedy, gdy $\det M(\varphi)_{\mathcal{A}}^{\mathcal{A}} \neq 0$ dla dowolnej bazy $\mathcal{A}$ przestrzeni $\mathbb{R}^n$,

Przykłady

vi) funkcja $f : \mathbb{R} \to \mathbb{R}$ zadana wzorem $f(x) = ax + b$ jest wzajemnie jednoznaczna dla $a \neq 0$ oraz

$$y = ax + b \leftrightarrow ax = y - b \leftrightarrow x = \frac{y - b}{a},$$

zatem funkcja odwrotna jest równa $f^{-1}(x) = \frac{x-b}{a}$,

vii) dla dowolnego $n \geq 2$ funkcja $f : \mathbb{C} \to \mathbb{C}$ zadana wzorem $f(z) = z^n$ nie jest wzajemnie jednoznaczna (nie jest funkcją różnowartościową ale jest „na" z podstawowego twierdzenia algebry).

Funkcje – notacja cd.

Stwierdzenie

Dla dowolnego zbioru X, zbiór wszystkich podzbiorów $P(X)$ można utożsamić ze zbiorem $\{0,1\}^X$. Funkcja

$$F\colon \{0,1\}^X \ni f \mapsto f^{-1}(1) \in P(X)$$

jest wzajemnie jednoznaczna, z funkcją odwrotną

$$F^{-1}\colon P(X) \ni A \mapsto \left(X \ni x \mapsto \begin{cases} 0 & x \notin A \\ 1 & x \in A \end{cases} \right) \in \{0,1\}^X.$$

Currying

Uwaga

Zbiór wszystkich funkcji ze zbioru X do zbioru Y oznaczamy

$$Y^X = \{f \subset X \times Y \mid f \colon X \to Y\}.$$

Stwierdzenie

Dla dowolnych zbiorów X, Y, Z istniej funkcja wzajemnie jednoznaczna

$$Z^{X \times Y} \ni f \mapsto (x \ni X \mapsto (Y \ni y \mapsto f(x, y) \in Z)) \in (Z^Y)^X.$$

Dowód.

Ćwiczenie. Funkcja odwrotna, to

$$(Z^Y)^X \ni g \mapsto (X \times Y \ni (x, y) \mapsto (g(x))(y) \in Z) \in Z^{X \times Y}.$$

Currying (teoria kategorii)

W języku teorii kategorii, istnieje **naturalny izomorfizm** w X, Y, Z

$$\mathrm{Hom}(X \times Y, Z) \cong \mathrm{Hom}(X, \mathrm{Hom}(Y, Z)),$$

gdzie $\mathrm{Hom}(X, Y)$ w kategorii zbiorów Set oznacza zbiór wszystkich funkcji ze zbioru X do zbioru Y.

Równoważnie, funktory

$$\cdot \times Y \colon \mathrm{Set} \to \mathrm{Set},$$

$$\mathrm{Hom}(Y, \cdot) \colon \mathrm{Set} \to \mathrm{Set},$$

są sprzężone/dołączone (ang. adjoint). Funktor $\cdot \times Y$ jest lewym funktorem dołączonym do funktora $\mathrm{Hom}(Y, \cdot)$. Funktor $\mathrm{Hom}(Y, \cdot)$ jest prawym funktorem dołączonym do funktora $\cdot \times Y$.

Currying (teoria kategorii) cd.

Lewy funktor dołączony zachowuje kogranice, w szczególności koprodukty. W kategorii zbiorów Set, koprodukt zbiorów X, Y to suma rozłączna $X \sqcup Y$, zatem[1]

$$(X \sqcup Y) \times Z \cong X \times Z \sqcup Y \times Z.$$

Prawy funktor dołączony zachowuje granice, w szczególności produkty. W kategorii zbiorów Set produkt zbiorów X, Y to iloczyn kartezjański $X \times Y$, zatem

$$\mathrm{Hom}(X, Y \times Z) \cong \mathrm{Hom}(X, Y) \times \mathrm{Hom}(X, Z).$$

[1] w obu przypadkach $\cong$ oznacza naturalny izomorfizm

Ideały w pierścieniu $\mathbb{Z}$

Definicja

Ideałem pierścienia $\mathbb{Z}$ nazywamy dowolny zbiór $I \subset \mathbb{Z}$ taki, że

a) $\mathbb{Z}I \subset I$,

b) $I + I \subset I$.

Piszemy $I \lhd \mathbb{Z}$.

Definicja

Ideał $I \lhd \mathbb{Z}$ nazywamy **głównym** jeśli

$$I = (a) = \{na \in \mathbb{Z} \mid n \in \mathbb{Z}\}.$$

Ideały w pierścieniu $\mathbb{Z}$ cd.

Stwierdzenie

Każdy ideał w pierścieniu $\mathbb{Z}$ jest główny.

Dowód.

Niech $J = I \cap \mathbb{N}$. Niech $a \in J$ będzie najmniejszym elementem w zwykłym porządku. Wtedy $(a) \subset I$. Jeśli $b \in I$ oraz $b > 0$ to

$$b = ar + q,$$

gdzie $0 \leq q < a$ oraz $q \in I$. Stąd $q = 0$ czyli $I \subset (a)$.

Własności ideałów

Stwierdzenie

i) $a|b \leftrightarrow (b) \subset (a)$,

ii) $(a) = (b) \leftrightarrow a = \pm b$,

iii) $(a) \subsetneq \mathbb{Z} \leftrightarrow a \neq \pm 1$,

iv) $d|a, d|b \leftrightarrow (a) \subset (d), (b) \subset (d) \leftrightarrow (a) + (b) \subset (d)$,

v) $a|d, b|d \leftrightarrow (d) \subset (a), (d) \subset (b) \leftrightarrow (d) \subset (a) \cap (b)$.

Dowód.

Ćwiczenie.

Liczby pierwsze

Definicja

Liczbę $p \in \mathbb{Z},\ p \geq 2$ nazywamy liczbę pierwszą, jeśli dla dowolnej liczby $n \in \mathbb{Z}, n \neq 0$

$$\text{jeśli } n|p, \text{ to } n = 1 \text{ lub } n = p,$$

lub równoważnie

$$\text{jeśli } (p) \subset (n), \text{to } (n) = (1) \text{ lub } (n) = (p).$$

Definicja

Jeśli $I \lhd \mathbb{Z},\ I \neq \mathbb{Z}$ jest ideałem oraz dla dowolnego ideału $J \lhd \mathbb{Z}$,

$$\text{jeśli } I \subset J, \text{ to } I = J \text{ lub } I = \mathbb{Z},$$

to I nazywamy **ideałem maksymalnym**.

Wniosek

Liczby pierwsze, to dokładnie dodatnie generatory ideałów maksymalnych.

Lemat Euklidesa

Stwierdzenie

Niech $p \geq 2$ będzie liczbą pierwszą. Dla dowolnych liczb $a, b \in \mathbb{Z}$

$$\text{jeśli } p|ab, \text{ to } p|a \text{ lub } p|b,$$

lub równoważnie

$$\text{jeśli } (ab) \subset (p), \text{ to } (a) \subset (p) \text{ lub } (b) \subset (p).$$

Dowód.

Niech $(ab) \subset (p)$, przypuśćmy, że $(a) \not\subset (p)$. Wtedy $(p) \subsetneq (a) + (p) \subset (1) = \mathbb{Z}$ skąd $(a) + (p) = (1)$. Istnieją zatem $k, l \in \mathbb{Z}$ takie, że

$$ka + lp = 1.$$

Mnożąc obustronnie przez b dostajemy

$$kab + lpb = b,$$

NWD i NWW

Definicja

Niech $a, b \in \mathbb{N}_{>0}$. **Najmniejszą wspólną wielokrotnością** (tj. NWW) liczb a i b nazywamy liczbę $d = \mathrm{NWW}(a, b) \in \mathbb{N}_{>0}$ taką, że

i) $a|d, b|d$,

ii) jeśli $a|d', b|d'$, to $d|d'$,

lub równoważnie, na mocy powyższego stwierdzenia

i) $(d) \subset (a) \cap (b)$,

ii) jeśli $(d) \subset (a) \cap (b)$ to $(d') \subset (d)$, liczba d generuje największy ideał główny zawarty w ideale $(a) \cap (b)$.

Wniosek

$$(\mathrm{NWW}(a, b)) = (a) \cap (b).$$

NWD i NWW cd.

Definicja

Niech $a, b \in \mathbb{N}_{>0}$. **Największym wspólnym dzielnikiem** (tj. NWD) liczb $a, b \in \mathbb{Z}$ nazywamy liczbę $d = \mathrm{NWD}(a, b) \in \mathbb{N}_{>0}$ taką, że

i) $d|a, d|b$,

ii) jeśli $d'|a, d'|b$, to $d'|d$,

lub równoważnie, na mocy powyższego stwierdzenia

i) $(a) + (b) \subset (d)$,

ii) jeśli $(a) + (b) \subset (d')$ to $(d) \subset (d')$, tzn. liczba jest dodatnia i d generuje najmniejszy ideał główny zawierający ideał $(a) + (b)$.

Wniosek

$$(\mathrm{NWD}(a, b)) = (a) + (b).$$

NWD i NWW cd.

Wniosek

Jeśli $d = \mathrm{NWD}(a, b)$, to istnieją $k, l \in \mathbb{Z}$ takie, że

$$ak + bl = d.$$

Wniosek

Element $[a] \in \mathbb{Z}/n\mathbb{Z}$ jest odwracalny wtedy i tylko wtedy, gdy $\mathrm{NWD}(a, n) = 1$.

Dowód.

Jeśli $[a]$ jest odwracalny, to istnieje $b \in \mathbb{Z}$ taki, że $ab - 1 = kn$ dla pewnego $k \in \mathbb{Z}$, skąd a i n nie mają wspólnych dzielników. Jeśli $\mathrm{NWD}(a, n) = 1$ to istnieją $k, l \in \mathbb{Z}$ takie, że $ak + ln = 1$ skąd $[a][k] = [1]$.

Twierdzenie chińskie o resztach

Stwierdzenie

Jeśli $\mathrm{NWD}(m, n) = 1$, to

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$

gdzie $\simeq$ oznacza izomorfizm pierścieni.

Dowód.

Odwzorowanie

$$x \pmod{mn} \mapsto (x \pmod{m}, x \pmod{n}),$$

zadaje homomorfizm równolicznych pierścieni. Jest on różnowartościowy, bo jeśli $m|x$ oraz $n|x$, to $mn|x$ (korzystamy z jednoznaczności rozkładu na iloczyn potęg liczb pierwszych).

Twierdzenie chińskie o resztach cd.

Wniosek

Jeśli liczby $n_1, \ldots, n_k \in \mathbb{N}_{>1}$ są parami względnie pierwsze, to dla dowolnych $a_1, \ldots, a_k \in \mathbb{Z}$ układ kongruencji

$$\begin{cases} x \equiv a_1 \pmod{n_1}, \\ x \equiv a_2 \pmod{n_2}, \\ \qquad\vdots \\ x \equiv a_k \pmod{n_k}, \end{cases}$$

ma dokładnie jedno rozwiązanie

$$x \equiv \sum_{i_1}^{k} a_i \frac{n}{n_i} \left(\frac{n}{n_i}\right)^{-1},$$

modulo $n = n_1 \cdot \ldots \cdot n_k$, gdzie $\left(\frac{n}{n_i}\right)^{-1}$ jest dowolnym reprezentantem odwrotności $\frac{n}{n_i}$ modulo n_i.

Funkcja Eulera

Definicja

Dla $n \geq 2$ niech

$$\varphi(n) = |\{a \in \{0, \ldots, n-1\} \mid \mathrm{NWD}(a, n) = 1\}| =$$

$$= \text{liczba elementów odwracalnych w } \mathbb{Z}/n\mathbb{Z}.$$

Stwierdzenie

i) $\varphi(p^n) = p^n - p^{n-1}$ dla dowolnej liczby pierwszej p,

ii) $\varphi(mn) = \varphi(m)\varphi(n)$ dla dowolnych liczb m, n takich, że $\mathrm{NWD}(m, n) = 1$,

iii) jeśli $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, to

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Funkcja Eulera cd.

Dowód.

Wystarczy udowodnić punkt *ii*). Z chińskiego twierdzenie o resztach wynika, że liczba a jest jednością modulo mn wtedy i tylko wtedy, gdy jest jednością modulo m i jest jednością modulo n.

Małe twierdzenie Fermata

Twierdzenie
Jeśli NWD$(a, n) = 1$, *to*

$$a^{\varphi(n)} \equiv 1 \ (mod \ n).$$

Dowód.
Liczba a (dokładnie, jej warstwa $[a] \in \mathbb{Z}/n\mathbb{Z}$) jest jednością w pierścieniu $\mathbb{Z}/n\mathbb{Z}$ a $\varphi(n)$ jest rzędem grupy jedności.

Wniosek

$$a^{-1} \equiv a^{\varphi(n)-1} \pmod{n}.$$

Przykład

Jaka jest odwrotność do 11 modulo 150?

$$\varphi(150) = \varphi(2)\varphi(3)\varphi(5^2) = 1 \cdot 2 \cdot (5^2 - 5) = 40.$$

$$11^{39} \equiv 11(11^{19})^2,$$

$$11^{19} \equiv 11(11^9)^2,$$

$$11^9 \equiv 11(11^4)^2,$$

$$11^4 \equiv (11^2)2 \equiv 121^2 \equiv 14641 \equiv 91,$$

$$11^9 \equiv 11 \cdot 91^2 \equiv 93104 \equiv 41,$$

$$11^{19} \equiv 11 \cdot 41^2 \equiv 18491 \equiv 41,$$

$$11^{39} \equiv 11 \cdot 41^2 \equiv 41.$$

Rzeczywiście

$$11 \cdot 41 = 3 \cdot 150 + 1.$$

Przykład

W grupie co najwyżej 30 osób ustawiano wszystkich po kolei w parach, trojkach i piątkach i zawsze zostawały odpowiednio jedna, dwie i trzy osoby. Ile osób było w grupie?

$$\begin{cases} x \equiv 1 \pmod{2}, \\ x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5}, \end{cases}$$

Można sprawdzić, że

$$(3 \cdot 5)^{-1} \equiv 1 \pmod{2},$$

$$(2 \cdot 5)^{-1} \equiv 1 \pmod{3},$$

$$(2 \cdot 3)^{-1} \equiv 6 \pmod{5},$$

$$x \equiv 1 \cdot 3 \cdot 5 \cdot 1 + 2 \cdot 2 \cdot 5 \cdot 1 + 3 \cdot 2 \cdot 3 \cdot 6 \equiv 15 + 20 + 108 \equiv 23.$$

Krata liczb naturalnych z relacją podzielności

Przykład

Zbiór $X = \mathbb{N}_{>0}$ z relacją

$$a \preccurlyeq b \leftrightarrow a|b,$$

jest kratą rozdzielną, ograniczoną z dołu, gdzie

$$a \wedge b = \mathrm{NWD}(a, b),$$

$$a \vee b = \mathrm{NWW}(a, b).$$