Elementy teorii mnogości

Część I

Wojciech Buszkowski

Zakład Teorii Obliczeń
Wydział Matematyki i Informatyki
Uniwersytet im. Adama Mickiewicza

1. Pojęcia podstawowe.

Teoria mnogości bada własności dowolnych *zbiorów* i pojęć pochodnych.

Teoria mnogości jest uniwersalną teorią matematyczną w następującym sensie.

I. *Wszystkie pojęcia matematyczne można zdefiniować na gruncie pojęć teorii mnogości.*

II. *Wszystkie twierdzenia matematyczne można udowodnić w teorii mnogości.*

MATEMATYKA = TEORIA MNOGOŚCI

Mówiąc ściślej, tak można scharakteryzować stan obecny, lecz to nie odpowiada historycznemu rozwojowi matematyki. Faktycznie teoria mnogości stanowi pewną rekonstrukcję matematyki, niekoniecznie odzwierciedlając wiernie wszystkie intuicje matematyków.

Za twórcę teorii mnogości uważa się Georga Cantora (1845-1918), chociaż zbiorami zajmowali się też inni matematycy XIX w. Dojrzałą postać uzyskała w pierwszej połowie XX w.

Wyróżniamy trzy pojęcia *pierwotne*:

pojęcie zbioru,

pojęcie należenia (elementu do zbioru),

pojęcie równości.

Pojęcie zbioru wyrażamy przez predykat jednoargumentowy $\mathcal{Z}$, pojęcie należenia przez predykat dwuargumentowy $\in$, a pojęcie równości - jak zwykle - przez predykat dwuargumentowy $=$.

$\mathcal{Z}(x)$: x jest zbiorem

$x \in y$: x należy do zbioru y, x jest elementem zbioru y

$x = y$: x jest równe y

Przykład. Formuła $\forall_x \exists_{y:\mathcal{Z}(y)} (x \in y)$ wyraża stwierdzenie: każdy obiekt jest elementem pewnego zbioru.

Obiekty to dowolne zbiory oraz przedmioty nie będące zbiorami, zwane *atomami* (lub: urelementami).

Dla potrzeb czystej matematyki rozważa się teorię mnogości bez atomów. Wszystkie obiekty są zbiorami, elementami zbiorów są tylko zbiory. Takie obiekty, jak np. liczby, funkcje, przestrzenie funkcyjne, mogą być zdefiniowane jako pewne zbiory. Niektóre konstrukcje tego rodzaju poznamy w następnych rozdziałach.

W zastosowaniach matematyki naturalne jest dopuszczenie zbiorów, których elementy są atomami.

Przykłady: zbiór wszystkich studentów znajdujących się w tej chwili w tej sali, zbiór wszystkich ciał w Układzie Słonecznym.

Dlatego rozważamy teorię mnogości z atomami. Nie zakładamy jednak niczego o liczbie i naturze atomów. Żadne dalsze konstrukcje ani twierdzenia nie zależą istotnie od tego, czy uwzględniamy jakieś atomy, czy nie.

Dla uproszczenia symboliki przyjmujemy, że wszystkie małe litery alfabetu łacińskiego, tj. $a, b, c, ..., x, y, z$, są zmiennymi reprezentującymi dowolne obiekty, natomiast duże litery, tj. $A, B, C, ..., X, Y, Z$, są zmiennymi reprezentującymi zbiory.

Wobec tego poprzednią formułę zapiszemy: $\forall_x \exists_Y (x \in Y)$

Każdą formułę zawierającą zmienne dla zbiorów (duże litery) można prztłumaczyć na formułę zawierającą tylko zmienne dla dowolnych obiektów (małe litery) i symbol $\mathcal{Z}$, ale ten drugi zapis jest zwykle mniej czytelny.

Dla podstawiania stosujemy notację popularną. Piszemy $\varphi(t)$ zamiast $\varphi[x/t]$. Oczywiście w kontekście naszych rozważań musi występować oznaczenie $\varphi(x)$ (lub $\varphi(y)$, $\varphi(z)$ itp.), żeby było wiadomo za którą zmienną podstawiamy t.

Za zmienne dla zbiorów wolno podstawiać tylko wyrażenia (termy) reprezentujące zbiory.

Teoria mnogości opiera się na KRPR. Poza prawami i regułami KRP przyjmujemy wszystkie aksjomaty równości dla tego języka.

Zatem wyprowadzalne są *twierdzenia o równości*:

(TR1) $s = t \Rightarrow u(s) = u(t)$ dla dowolnych termów s, t i $u(x)$,

(TR2) $s = t \Rightarrow (\varphi(s) \Leftrightarrow \varphi(t))$ dla dowolnych formuł $\varphi(x)$ i termów s, t podstawialnych za x w $\varphi(x)$.

W szczególności otrzymujemy:

(1) $x = y \Rightarrow (x \in Z \Leftrightarrow y \in Z)$ (z (TR2))

(2) $X = Y \Rightarrow (z \in X \Leftrightarrow z \in Y)$ (z (TR2))

(3) $X = Y \Rightarrow \forall_z (z \in X \Leftrightarrow z \in Y)$ Stosujemy DD$\forall$ do (2), przy czym $\forall_z (X = Y)$ jest logicznie równoważne $X = Y$.

Implikacja odwrotna do (3) nie jest prawem KRPR. Przyjmujemy ją jako pozalogiczny aksjomat teorii mnogości, nazywany *aksjomatem ekstensjonalności*.

$$\text{(Ext)}\ \forall_z (z \in X \Leftrightarrow z \in Y) \Rightarrow X = Y$$

Podamy sformułowanie słowne.

Aksjomat ekstensjonalności. Jeżeli dwa zbiory mają dokładnie te same elementy, to te zbiory są równe.

Poprzednik (Ext) wyraża to, że X i Y mają dokładnie te same elementy. Dla każdego obiektu z, $z \in X$ jest równoważne $z \in Y$, czyli albo jednocześnie $z \in X$ i $z \in Y$, albo jednocześnie $z \notin X$ i $z \notin Y$. $z \notin X$ jest skrótem dla: $\neg(z \in X)$.

Zbiór jest jednoznacznie wyznaczony przez swoje elementy.

Zdefiniujemy ważny stosunek *inkluzji* (zawierania), oznaczany symbolem $\subset$.

Definicja 1. Mówimy, że zbiór X *zawiera się* w zbiorze Y, jeżeli każdy element zbioru X jest elementem zbioru Y.

(D $\subset$) $X \subset Y \Leftrightarrow \forall_z (z \in X \Rightarrow z \in Y)$

$X \subset Y$ czytamy też: zbiór X jest zawarty w zbiorze Y, X jest podzbiorem zbioru Y, zbiór Y zawiera zbiór X, Y jest nadzbiorem zbioru X.

Przykład. Zbiór wszystkich Polaków zawiera się w zbiorze wszystkich Europejczyków. Zbiór wszystkich Europejczyków zawiera zbiór wszystkich Polaków.

Niech $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ i $\mathbb{R}$ oznaczają kolejno zbiory (wszystkich) liczb naturalnych, całkowitych, wymiernych i rzeczywistych.

Mamy: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Mówimy, że zbiór X jest *właściwym podzbiorem* zbioru Y (albo: inkluzja $X \subset Y$ jest właściwa), jeżeli $X \subset Y$ i $X \neq Y$.

$x \neq y$ jest skrótem dla: $\neg(x = y)$.

Wszystkie inkluzje wymienione w ostatnim przykładzie są właściwe.

Uwaga. Niektórzy autorzy stosują symbol $\subseteq$ dla inkluzji, a $\subset$ dla inkluzji właściwej. Tu nie stosujemy tych oznaczeń, podobnie jak większość matematyków.

Fakt 1 (podstawowe własności inkluzji). Dla dowolnych zbiorów X, Y, Z:

(a) $X \subset X$ (prawo zwrotności inkluzji),

(b) $X \subset Y \wedge Y \subset Z \Rightarrow X \subset Z$ (prawo przechodniości inkluzji),

(c) $X \subset Y \wedge Y \subset X \Rightarrow X = Y$ (prawo antysymetrii inkluzji).

DOWÓD.

(a). Postawiając w (D $\subset$) X za Y, otrzymujemy:

$X \subset X \Leftrightarrow \forall_z(z \in X \Rightarrow z \in X)$.

$z \in X \Rightarrow z \in X$ jest prawem logiki, a więc $\forall_z(z \in X \Rightarrow z \in X)$ jest też prawem logiki na mocy reguły generalizacji. Wobec tego powyższa równoważność jest prawdziwa i jej prawa strona jest prawdziwa, a więc $X \subset X$ jest prawdą.

(b). Zakładamy, że $X \subset Y$ i $Y \subset Z$. Na mocy (D $\subset$) mamy $\forall_z(z \in X \Rightarrow z \in Y)$ i $\forall_z(z \in Y \Rightarrow z \in Z)$. Niech z będzie dowolnym obiektem. Z praw podstawiania KRP mamy:

(1) $z \in X \Rightarrow z \in Y$, (2) $z \in Y \Rightarrow z \in Z$.

Stąd na mocy reguły (SYL): (3) $z \in X \Rightarrow z \in Z$.

Z (3) na mocy (GEN): $\forall_z(z \in X \Rightarrow z \in Z)$, a więc $X \subset Z$ na mocy (D $\subset$).

(c). Zakładamy, że $X \subset Y$ i $Y \subset X$. Stąd $\forall_z (z \in X \Rightarrow z \in Y)$ i $\forall_z (z \in Y \Rightarrow z \in X)$. Dla dowolnego z mamy:

(1) $z \in X \Rightarrow z \in Y$, (2) $z \in Y \Rightarrow z \in X$,

a więc: (3) $z \in X \Leftrightarrow z \in Y$, na mocy reguły wprowadzania równoważności. Stąd $\forall_z (z \in X \Leftrightarrow z \in Y)$ na mocy reguły generalizacji, a więc $X = Y$ na mocy (Ext). Q.E.D.

Powyższy dowód można zapisać w stylu półformalnym jako skrócony dowód implikacyjny.

$X \subset Y \wedge Y \subset X \to \forall_z (z \in X \Rightarrow z \in Y) \wedge \forall_z (z \in Y \Rightarrow z \in X) \to$

$\forall_z [(z \in X \Rightarrow z \in Y) \wedge (z \in Y \Rightarrow z \in X)] \to$

$\forall_z (z \in X \Leftrightarrow z \in Y) \to X = Y$

Podobnie można zapisać dowód (b).

2. Podstawowe konstrukcje zbiorów

2.1. Zbiory skończone

Zbiór, którego (wszystkimi) elementami są $a_1, \ldots, a_n$ oznaczamy $\{a_1, \ldots, a_n\}$. Znaczenie tej symboliki reguluje definicja formalna:

(D$\{,\}$) $x \in \{a_1, \ldots, a_n\} \Leftrightarrow x = a_1 \vee \cdots \vee x = a_n$

W szczególności:

$x \in \{a\} \Leftrightarrow x = a$

$x \in \{a, b\} \Leftrightarrow x = a \vee x = b$

Zbiór $\{a\}$ nazywamy *zbiorem jednoelementowym* z elementem a.

Zbiór $\{a, b\}$ nazywamy *parą nieuporządkowaną* elementów a i b.

Fakt 2. $\{a, b\} = \{b, a\}$ dla dowolnych obiektów a, b.

Formalnie: $\forall_{a,b}(\{a, b\} = \{b, a\})$

Dowód.

Wykażemy: $x \in \{a, b\} \Leftrightarrow x \in \{b, a\}$.

$x \in \{a, b\} \leftrightarrow x = a \vee x = b \leftrightarrow x = b \vee x = a \leftrightarrow x \in \{b, a\}$

Na mocy reguły generalizacji $\forall_x (x \in \{a, b\} \Leftrightarrow x \in \{b, a\})$, a więc $\{a, b\} = \{b, a\}$ na mocy (Ext). Q.E.D.

Podobnie możemy wykazać, że $\{a, b, c\} = \{c, b, a\}$ i ogólnie:

$\{a_1, \ldots, a_n\} = \{a_{i_1}, \ldots, a_{i_n}\}$ dla dowolnej permutacji $(i_1, \ldots, i_n)$ ciągu $(1, \ldots, n)$.

Zatem dla tej konstrukcji zbiorów skończonych kolejność elementów nie jest istotna.

Nie są też istotne powtórzenia. Mamy $\{a, a\} = \{a\}$, $\{a, b\} = \{a, b, b\}$ itp. Zwykle podajemy listę elementów bez powtórzeń i w pewnej ustalonej (naturalnej) kolejności, np. $\{1, 2, 3\}$, $\{a, b, c\}$.

Oczywiście $\{a\} \subset \{a, b\} \subset \{a, b, c\}$ itd.

Aksjomat zbioru pustego. Istnieje zbiór nie mający żadnych elementów.

Formalnie: $\exists_X \forall_x (x \notin X)$

Na mocy (Ext) istnieje dokładnie jeden taki zbiór. Ten zbiór nazywamy *zbiorem pustym* i oznaczamy symbolem $\emptyset$.

(D $\emptyset$) $\mathcal{Z}(\emptyset) \wedge \forall_x (x \notin \emptyset)$.

Fakt 3. Zbiór pusty jest podzbiorem każdego zbioru.

DOWÓD. Mamy: $\emptyset \subset X \Leftrightarrow \forall_x (x \in \emptyset \Rightarrow x \in X)$. Implikacja $x \in \emptyset \Rightarrow x \in X$ jest prawdziwa jako implikacja o fałszywym poprzedniku, więc $\forall_x (x \in \emptyset \Rightarrow x \in X)$ jest prawdą na mocy reguły generalizacji. Zatem $\emptyset \subset X$ jest prawdą dla dowolnego zbioru X. Q.E.D.

2.2. Zbiór wyznaczony przez warunek

Nie zawsze można podać listę wszystkich elementów zbioru, np. nie można wypisać wszystkich elementów zbioru nieskończonego.

Często określamy zbiór, podając warunek, który spełniają wszystkie elementy tego zbioru i żadne inne obiekty.

$\{x : \varphi(x)\}$ oznacza zbiór tych wszystkich obiektów x, które spełniają $\varphi(x)$ (krótko: zbiór tych x, że $\varphi(x)$).

(D{:}) $x \in \{x : \varphi(x)\} \Leftrightarrow \varphi(x)$

UWAGA. Każde wystąpienie x w wyrażeniu $\{x : \varphi(x)\}$ jest związane, natomiast pierwsze wystąpienie x w (D{:}) jest wolne, a w formule $\varphi(x)$ może być wolne wystąpienie x. Zatem podstawiając y za x w (D{:}), otrzymujemy:

$y \in \{x : \varphi(x)\} \Leftrightarrow \varphi(y)$, przy czym $\varphi(y) \equiv \varphi[x/y]$.

Przykład. $\{x : x \in \mathbb{N} \wedge x > 5\}$ oznacza zbiór wszystkich liczb naturalnych większych od 5. $\{x : x \neq x\}$ oznacza zbiór pusty.

Antynomia Russella

Nieograniczone stosowanie tej konstrukcji prowadzi do sprzeczności. Tzw. "naiwna teoria mnogości", rozwijana przez G. Cantora i innych w XIX w., przyjmowała, że dla dowolnego, sensownego warunku $\varphi(x)$ istnieje zbiór tych x, że $\varphi(x)$.

W 1901 r. B. Russell zauważył, że nie istnieje zbiór tych wszystkich zbiorów, które nie są własnymi elementami, czyli $\{X : X \notin X\}$ (inaczej: $\{x : \mathcal{Z}(x) \wedge x \notin x\}$).

Przypuśćmy, że ten zbiór istnieje. Wychodząc od wersji (D{:}) dla zbiorów jako elementów:

$$X \in \{X : X \notin X\} \Leftrightarrow X \notin X,$$

otrzymujemy przez podstawienie $\{X : X \notin X\}$ za zmienną X:

$$\{X : X \notin X\} \in \{X : X \notin X\} \Leftrightarrow \{X : X \notin X\} \notin \{X : X \notin X\},$$

co jest fałszem logicznym. Schemat logiczny tego zdania na gruncie KRZ to $p \Leftrightarrow \neg p$, a $\neg(p \Leftrightarrow \neg p)$ jest tautologią KRZ.

Żeby uniknąć tych kłopotów, stworzono różne systemy *aksjomatycznej teorii mnogości*. Największą popularność wśród matematyków zdobył system zaproponowany prze E. Zermelo w 1908 r. Teoria Zermelo przyjmuje pewne *aksjomaty istnienia zbiorów*, które postulują istnienie zbioru tych x, że $\varphi(x)$, dla poszczególnych (nie dowolnych) warunków $\varphi(x)$.

Aksjomat wyróżniania. Niech $\varphi(x)$ będzie dowolną formułą języka teorii mnogości. Dla dowolnego zbioru A istnieje zbiór tych wszystkich elementów zbioru A, które spełniają $\varphi(x)$.

Formalnie: $\forall_A \exists_X \forall_x (x \in X \Leftrightarrow x \in A \wedge \varphi(x))$.

Inaczej: $\{x : x \in A \wedge \varphi(x)\}$ istnieje dla dowolnego zbioru A i dowolnego warunku $\varphi(x)$.

Inne oznaczenie: $\{x \in A : \varphi(x)\}$, np. $\{x \in \mathbb{N} : x > 5\}$.

(D{:}) $x \in \{x \in A : \varphi(x)\} \Leftrightarrow x \in A \wedge \varphi(x)$

Aksjomat pary. Dla dowolnych obiektów a, b istnieje zbiór, którego jedynymi elementami są a i b.

Formalnie: $\forall_{a,b} \exists_X \forall_x (x \in X \Leftrightarrow x = a \vee x = b)$.

Inaczej: dla dowolnych a, b istnieje para nieuporządkowana $\{a, b\}$, czyli $\{x : x = a \vee x = b\}$.

Aksjomat sumy (słaba wersja). Dla dowolnych zbiorów A, B istnieje zbiór tych wszystkich obiektów, które należą do A lub do B.

Formalnie: $\forall_{A,B} \exists_X \forall_x (x \in X \Leftrightarrow x \in A \vee x \in B)$.

Inaczej: $\{x : x \in A \vee x \in B\}$ istnieje dla dowolnych zbiorów A, B. Ten zbiór nazywamy *sumą* zbiorów A i B i oznaczamy $A \cup B$.

(D$\cup$) $x \in A \cup B \Leftrightarrow x \in A \vee x \in B$.

Zatem istnieją zbiory $\{a\} = \{a, a\}$, $\{a, b, c\} = \{a, b\} \cup \{c\}$ itd.

2.3. Zbiór potęgowy i rodziny zbiorów

Aksjomat zbioru potęgowego. Dla dowolnego zbioru A istnieje zbiór, którego elementami są wszystkie podzbiory zbioru A i tylko te obiekty.

Formalnie: $\forall_A \exists_X \forall_x (x \in X \Leftrightarrow \mathcal{Z}(x) \wedge x \subset A)$

Inaczej: $\{B : B \subset A\}$, czyli zbiór wszystkich podzbiorów zbioru A, istnieje dla dowolnego zbioru A.

Ten zbiór nazywamy *zbiorem potęgowym* zbioru A i oznaczamy $\mathcal{P}(A)$ (inne oznaczenie: 2^A).

$\mathcal{P}(A) = \{X : X \subset A\}$

(D$\mathcal{P}$) $X \in \mathcal{P}(A) \Leftrightarrow X \subset A$

Mamy: $\mathcal{P}(\emptyset) = \{\emptyset\}$, $\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$,
$\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

$|A|$ oznacza liczbę elementów skończonego zbioru A.

$|\emptyset| = 0$, $|\{a_1, \ldots, a_n\}| = n$ (jeżeli na liście nie ma powtórzeń)

Fakt 3(m). Jeżeli $|A| = n$, to $|\mathcal{P}(A)| = 2^n$.

Dowód. Dla $n = 0$ mamy $A = \emptyset$, więc $\mathcal{P}(A) = \{\emptyset\}$. Stąd $|\mathcal{P}(A)| = 1 = 2^0$.

Niech $A = \{a_1, \ldots, a_n\}$. Liczba wszystkich podzbiorów zbioru A jest równa liczbie wszystkich ciągów binarnych długości n, ponieważ dowolny podzbiór X zbioru A można jednoznacznie opisać ciągiem $(b_1, \ldots, b_n)$ takim, że $b_i = 1$ jeżeli $a_i \in X$, $b_i = 0$ jeżeli $a_i \notin X$. Q.E.D.

Przykład. Podzbiory zbioru $\{a, b, c\}$ odpowiadają następującym ciągom binarnym.

$\emptyset$: $(0, 0, 0)$, $\{a\}$: $(1, 0, 0)$, $\{b\}$: $(0, 1, 0)$, $\{c\}$: $(0, 0, 1)$

$\{a, b\}$: $(1, 1, 0)$, $\{a, c\}$: $(1, 0, 1)$, $\{b, c\}$: $(0, 1, 1)$, $\{a, b, c\}$: $(1, 1, 1)$

Zbiór, którego wszystkie elementy są zbiorami, nazywamy *rodziną zbiorów*.

$\mathcal{P}(A)$ jest rodziną zbiorów. Rodzinami zbiorów są też zbiory zawarte w $\mathcal{P}(A)$, np. $\{\emptyset, \{a, b, c\}\} \subset \mathcal{P}(\{a, b, c\})$.

Inny przykład: rodzina wszystkich skończonych podzbiorów zbioru $\mathbb{N}$ jest zawarta w $\mathcal{P}(\mathbb{N})$.

Aksjomat sumy (mocna wersja). Dla dowolnego zbioru A istnieje zbiór, którego elementami są te wszystkie obiekty, które należą do przynajmniej jednego zbioru należącego do A.

Formalnie: $\forall_A \exists_X \forall_x (x \in X \Leftrightarrow \exists_Y (Y \in A \wedge x \in Y))$.

Inaczej: $\{x : \exists_Y (Y \in A \wedge x \in Y)\}$ istnieje dla dowolnego zbioru A. Ten zbiór nazywamy sumą zbioru A i oznaczamy $\bigcup A$.

Zazwyczaj stosujemy tę konstrukcję, gdy A jest rodziną zbiorów.

Fakt 4. $A \cup B = \bigcup \{A, B\}$.

2.4. Klasy

W podrozdziale 2.2 stwierdziliśmy, że nie istnieje $\{X : X \notin X\}$.

Wynika stąd nieistnienie zbioru wszystkich zbiorów. Przypuśćmy, że istnieje zbiór V, którego elementami są wszystkie zbiory. Na mocy aksjomatu wyróżniania istnieje zbiór $\{x \in V : x \notin x\}$, czyli w innej notacji $\{X : X \notin X\}$. Doszliśmy do sprzeczności. Zatem nie istnieje zbiór wszystkich zbiorów.

Niektóre systemy teorii mnogości opierają się na pojęciu *klasy*. Zbiory określa się jako klasy będące elementami innych klas. Każdy zbiór jest klasą, lecz nie każda klasa jest zbiorem. Elementami klas mogą być tylko zbiory i atomy.

Klasy, które nie są zbiorami, nazywamy *klasami właściwymi*.

Przykłady klas właściwych: klasa wszystkich zbiorów, klasa wszystkich zbiorów jednoelementowych (wykaż to!).

3. Algebra zbiorów

3.1. Podstawowe działania na zbiorach

Definicja 2. Dla dowolnych zbiorów A, B określamy ich *sumę* $A \cup B$, iloczyn $A \cap B$ i różnicę $A \setminus B$ w następujący sposób:

$A \cup B = \{x : x \in A \vee x \in B\}$,

$A \cap B = \{x : x \in A \wedge x \in B\}$,

$A \setminus B = \{x : x \in A \wedge x \notin B\}$.

$A \cup B$ czytamy 'A plus B', $A \cap B$ czytamy 'A razy B', $A \setminus B$ czytamy 'A minus B'.

Iloczyn $A \cap B$ nazywamy też *przekrojem* lub *częścią wspólną* zbiorów A i B.

(D$\cup$) $x \in A \cup B \Leftrightarrow x \in A \vee x \in B$

(D$\cap$) $x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$

(D$\setminus$) $x \in A \setminus B \Leftrightarrow x \in A \wedge \neg(x \in B)$

Przykłady.

$\{a, b\} \cup \{b, c\} = \{a, b, c\}$

$\{a, b\} \cap \{b, c\} = \{b\}$

$\{a, b\} \setminus \{b, c\} = \{a\}$

Zauważmy, że dla dowolnych zbiorów A, B zbiór $A \cup B$ istnieje na mocy aksjomatu sumy, natomiast zbiory $A \cap B$ i $A \setminus B$ istnieją na mocy aksjomatu wyróżniania, ponieważ:

$A \cap B = \{x \in A : x \in B\}$ oraz $A \setminus B = \{x \in A : x \notin B\}$.

Definicja 3. Mówimy, że zbiór A jest *rozłączny* ze zbiorem B (albo: zbiory A i B są rozłączne), jeżeli $A \cap B = \emptyset$.

Przykłady. Zbiór wszystkich lewych butów jest rozłączny ze zbiorem wszystkich prawych butów. Zbiory $\{1, 2\}$ i $\{3, 4\}$ są rozłączne.

Prawa dla sumy i iloczynu zbiorów

prawa idempotentości

$A \cup A = A$, $A \cap A = A$

prawa przemienności

$A \cup B = B \cup A$, $A \cap B = B \cap A$

prawa łączności

$(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$

prawa rozdzielności

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (rozdzielność sumy względem iloczynu)

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (rozdzielność iloczynu względem sumy)

prawa dla zbioru pustego

$A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$

Podstawowy sposób dowodzenia tych praw korzysta z aksjomatu ekstensjonalności. Żeby udowodnić $L = P$, dowodzimy: $x \in L \Leftrightarrow x \in P$. Stąd $\forall_x (x \in L \Leftrightarrow x \in P)$ na mocy reguły generalizacji, a więc $L = P$ na mocy (Ext).

$A \cup B = B \cup A$. Wykazujemy: $x \in A \cup B \Leftrightarrow x \in B \cup A$.

$x \in A \cup B \leftrightarrow x \in A \vee x \in B \leftrightarrow x \in B \vee x \in A \leftrightarrow x \in B \cup A$

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$x \in A \cup (B \cap C) \leftrightarrow x \in A \vee x \in B \cap C \leftrightarrow$

$x \in A \vee (x \in B \wedge x \in C) \leftrightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \leftrightarrow$

$x \in A \cup B \wedge x \in A \cup C \leftrightarrow x \in (A \cup B) \cap (A \cup C)$

$A \cup \emptyset = A$

$x \in A \cup \emptyset \leftrightarrow x \in A \vee x \in \emptyset \leftrightarrow x \in A$ (bo $x \in \emptyset$ jest fałszem)

Prawa dla różnicy zbiorów

$A \setminus A = \emptyset$, $A \setminus \emptyset = A$, $\emptyset \setminus A = \emptyset$

prawa De Morgana dla różnicy zbiorów

$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

Inne prawa

$(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$

$(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$

$(A \setminus B) \setminus C = A \setminus (B \cup C)$

$A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$

Prawa z inkluzją

$A \subset A \cup B$, $B \subset A \cup B$

$A \subset C \wedge B \subset C \Rightarrow A \cup B \subset C$ (zachodzi $\Leftrightarrow$)

Wyprowadzimy te prawa.

$x \in A \Rightarrow x \in A \vee x \in B \Rightarrow x \in A \cup B$. Stąd $\forall_x (x \in A \Rightarrow x \in A \cup B)$, czyli $A \subset A \cup B$. Podobnie dowodzimy drugie prawo. Dowód trzeciego prawa jest bardziej skomplikowany.

Zakładamy, że $A \subset C$ i $B \subset C$. Na mocy (D $\subset$), dla dowolnego x mamy:

$x \in A \Rightarrow x \in C$ i $x \in B \Rightarrow x \in C$.

Stąd $x \in A \vee x \in B \Rightarrow x \in C$ na mocy reguły wnioskowania KRZ. Na mocy (D$\cup$), $x \in A \vee x \in B \Leftrightarrow x \in A \cup B$. Zatem $x \in A \cup B \Rightarrow x \in C$ dla dowolnego x, czyli $A \cup B \subset C$.

Ten dowód można przedstawić półformalnie.

$A \subset C \wedge B \subset C \rightarrow \forall_x (x \in A \Rightarrow x \in C) \wedge \forall_x (x \in B \Rightarrow x \in C) \rightarrow$

$\forall_x ((x \in A \Rightarrow x \in C) \wedge (x \in B \Rightarrow x \in C)) \rightarrow$

$\forall_x (x \in A \vee x \in B \Rightarrow x \in C) \rightarrow$

$\forall_x (x \in A \cup B \Rightarrow x \in C) \rightarrow A \cup B \subset C$

Matematycy często prowadzą takie dowody całkiem nieformalnie.

Zakładamy, że $A \subset C$ i $B \subset C$. Wykażemy $A \cup B \subset C$. Niech $x \in A \cup B$. Wtedy $x \in A$ lub $x \in B$.

Rozważamy dwa przypadki. 1°. $x \in A$. Wtedy $x \in C$, ponieważ $A \subset C$. 2°. $x \in B$. Wtedy $x \in C$, ponieważ $B \subset C$. Zatem w obu przypadkach $x \in C$. Wykazaliśmy, że każdy element zbioru $A \cup B$ należy do C, a więc $A \cup B \subset C$.

Podobne prawa dla inkluzji i iloczynu zbiorów

$A \cap B \subset A$, $A \cap B \subset B$

$A \subset B \wedge A \subset C \Rightarrow A \subset B \cap C$ (zachodzi $\Leftrightarrow$)

Podobne prawa dla inkluzji i różnicy zbiorów

$A \setminus B \subset A$, $(A \setminus B) \cap B = \emptyset$

$A \subset B \wedge A \cap C = \emptyset \Rightarrow A \subset B \setminus C$ (zachodzi $\Leftrightarrow$)

Prawa monotoniczności działań sumy, iloczynu i różnicy zbiorów

$A_1 \subset B_1 \wedge A_2 \subset B_2 \Rightarrow A_1 \cup A_2 \subset B_1 \cup B_2$

$A_1 \subset B_1 \wedge A_2 \subset B_2 \Rightarrow A_1 \cap A_2 \subset B_1 \cap B_2$

$A_1 \subset B_1 \wedge A_2 \subset B_2 \Rightarrow A_1 \setminus B_2 \subset B_1 \setminus A_2$

Prawa definiujące inkluzję przez działania na zbiorach

$A \subset B \Leftrightarrow A \cup B = B$

$A \subset B \Leftrightarrow A \cap B = A$

$A \subset B \Leftrightarrow A \setminus B = \emptyset$

Udowodnimy pierwsze prawo.

($\Rightarrow$). Zakładamy $A \subset B$. Ponieważ $A \subset B$ i $B \subset B$, więc $A \cup B \subset B$ na mocy wcześniejszego prawa. Mamy też $B \subset A \cup B$, a więc $A \cup B = B$ na mocy prawa antysymetrii inkluzji.

($\Leftarrow$). Zakładamy $A \cup B = B$. Ponieważ $A \subset A \cup B$, więc $A \subset B$ (tu korzystamy z praw dla równości).

Różnica symetryczna

Określamy nowe działanie:

$A \dot{-} B = (A \setminus B) \cup (B \setminus A)$.

Zbiór $A \dot{-} B$ nazywamy *różnicą symetryczną* zbiorów A i B.

Prawa dla różnicy symetrycznej

$A \dot{-} B = B \dot{-} A$ (przemienność)

$(A \dot{-} B) \dot{-} C = A \dot{-} (B \dot{-} C)$ (łączność)

$A \dot{-} A = \emptyset$, $A \dot{-} \emptyset = A = \emptyset \dot{-} A$

W dowodzie prawa łączności można skorzystać z prawa:
$x \in A \dot{-} B \Leftrightarrow (x \in A \wedge \neg(x \in B)) \vee (x \in B \wedge \neg(x \in A))$ oraz tautologii:

$\neg(p \Leftrightarrow q) \Leftrightarrow (p \wedge \neg q) \vee (q \wedge \neg p)$

$\neg(p \Leftrightarrow q) \Leftrightarrow (\neg p \Leftrightarrow q)$, $\neg(p \Leftrightarrow q) \Leftrightarrow (p \Leftrightarrow \neg q)$

$[(p \Leftrightarrow q) \Leftrightarrow r] \Leftrightarrow [p \Leftrightarrow (q \Leftrightarrow r)]$

3.2. Działanie dopełnienia

Często wykonujemy działania na podzbiorach ustalonego zbioru U, zwanego wtedy *uniwersum*.

Wtedy wprowadzamy dodatkowe działanie:

$A' = U \setminus A$ dla $A \subset U$.

Zbiór A' nazywamy *dopełnieniem zbioru* A (do uniwersum U).

Prawa dopełnienia

$U' = \emptyset$, $\emptyset' = U$, $A'' = A$, $A \cup A' = U$, $A \cap A' = \emptyset$

$(A \cup B)' = A' \cap B'$, $(A \cap B)' = A' \cup B'$ (prawa De Morgana dla dopełnienia)

$A \subset B \Rightarrow B' \subset A'$ (prawo antytoniczności dopełnienia)

Te prawa można wyprowadzić z praw dla różnicy zbiorów.

$(A \cup B)' = U \setminus (A \cup B) = (U \setminus A) \cap (U \setminus B) = A' \cap B'$

3.3. Aksjomaty algebry Boole'a

Wszystkie prawa algebry zbiorów można wyprowadzić z następujących praw, zwanych *aksjomatami algebry Boole'a*.

(B1) $A \cup B = B \cup A$ (prawa

(B1') $A \cap B = B \cap A$ przemienności)

(B2) $(A \cup B) \cup C = A \cup (B \cup C)$ (prawa

(B2') $(A \cap B) \cap C = A \cap (B \cap C)$ łączności)

(B3) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (prawa

(B3') $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ rozdzielności)

(B4) $A \cup \emptyset = A$ (prawo zbioru pustego)

(B4') $A \cap U = A$ (prawo uniwersum)

(B5) $A \cup A' = U$ (prawa

(B5') $A \cap A' = \emptyset$ dopełnienia)

(TB1) $A \cup A = A$

$A =_{(B4)} A \cup \emptyset =_{(B5')} A \cup (A \cap A') =_{(B3)}$

$(A \cup A) \cap (A \cup A') =_{(B5)} (A \cup A) \cap U =_{(B4')} A \cup A$

(TB1') $A \cap A = A$

$A =_{(B4')} A \cap U =_{(B5)} A \cap (A \cup A') =_{(B3')}$

$(A \cap A) \cup (A \cap A') =_{(B5')} (A \cap A) \cup \emptyset =_{(B4)} A \cap A$

Prawo (TB1') jest *dualne* do prawa (TB1) i odwrotnie.

Formuła φ^d dualna do φ powstaje przez zamianę każdego symbolu $\cup$ na $\cap$, $\cap$ na $\cup$, $\emptyset$ na U i U na $\emptyset$.

Zauważmy, że aksjomaty (Bi) i (Bi') są wzajemnie dualne dla $i = 1, \ldots, 5$. W rezultacie każde wyprowadzenie prawa φ z tych aksjomatów można przekształcić w wyprowadzenie prawa φ^d przez dualizację każdego kroku wyprowadzenia.

(TB2) $A \cup U = U$, (TB2') $A \cap \emptyset = \emptyset$

$A \cup U = A \cup (A \cup A') = (A \cup A) \cup A' = A \cup A' = U$

$A \cap \emptyset = A \cap (A \cap A') = (A \cap A) \cap A' = A \cap A' = \emptyset$

(TB3) $A \cup (A \cap B) = A$, (TB3') $A \cap (A \cup B) = A$

$A \cup (A \cap B) = (A \cap U) \cup (A \cap B) = A \cap (U \cup B) =$

$A \cap (B \cup U) = A \cap U = A$

(TB4) $A \cup B = B \Leftrightarrow A \cap B = A$

($\Rightarrow$). Zakładamy $A \cup B = B$. Mamy:

$A \cap B = A \cap (A \cup B) = A$.

($\Leftarrow$). Zakładamy $A \cap B = A$. Mamy:

$A \cup B = A \cup (A \cap B) = A$.

(DB1) $A \subset B \Leftrightarrow A \cup B = B$

(TB5) $A \subset B \Leftrightarrow A \cap B = A$

UWAGA. Dualizacja prawa z inkluzją wymaga zamiany kierunku inkluzji. Dla dowolnych termów s, t mamy:

$(s \subset t)^d \leftrightarrow (s \cup t = t)^d \leftrightarrow s^d \cap t^d = t^d \leftrightarrow t^d \cap s^d = t^d \leftrightarrow t^d \subset s^d$

(TB6) $A \subset A$

$A \subset A \Leftrightarrow A \cup A = A$ na mocy (DB1). Prawa strona jest prawdziwa na mocy (TB1).

(TB7) $A \subset B \wedge B \subset C \Rightarrow A \subset C$

Zakładamy, że $A \subset B$ i $B \subset C$. Z (DB1) mamy $A \cup B = B$ i $B \cup C = C$. Stąd:

$A \cup C = A \cup B \cup C = B \cup C = C$. Zatem $A \subset C$.

(DB2) $A \setminus B = A \cap B'$

4. Pary uporządkowane, iloczyn kartezjański, relacje

4.1. Pary uporządkowane

Stosunki dwuargumentowe można traktować jako własności par obiektów. Na przykład, $2 < 5$ jest pewną własnością pary 2 i 5.

Ponieważ $2 < 5$, lecz $\neg(5 < 2)$, więc tej pary nie można reprezentować przez parę nieuporządkowaną $\{2, 5\}$. Potrzebne jest pojęcie pary uporządkowanej, która odróżnia pierwszy element od drugiego.

Definicja 4. *Parą uporządkowaną* elementów a i b nazywamy zbiór $\{\{a\}, \{a, b\}\}$. Ten zbiór oznaczamy $\langle a, b\rangle$.

$\langle a, b\rangle = \{\{a\}, \{a, b\}\}$ (definicja K. Kuratowskiego)

Inne oznaczenie: (a, b).

Nie będziemy używać tego drugiego oznaczenia, żeby nie myliło się z oznaczeniem przedziału otwartego $(a, b) = \{x \in \mathbb{R} : a < x < b\}$.

Lemat 1 (o parach uporządkowanych). Dla dowolnych obiektów a, b, c, d:

$\langle a, b\rangle = \langle c, d\rangle \Leftrightarrow a = c \wedge b = d\,.$

Słownie: Dwie pary uporządkowane są równe wtw, gdy ich pierwsze elementy są równe i drugie elementy są równe.

Dowód. Implikacja ($\Leftarrow$) powyższej równoważności jest prawem KRPR. Dowodzimy ($\Rightarrow$).

Zakładamy $\langle a, b\rangle = \langle c, d\rangle$. Stąd $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$.

Jeżeli $a \neq c$, to $\{a\} \neq \{c\}$ i $\{a\} \neq \{c, d\}$, co jest niemożliwe. Zatem $a = c$.

Stąd $\{\{a\}, \{a, b\}\} = \{\{a\}, \{a, d\}\}$. Niech $\{a, b\} = \{a\}$. Wtedy $a = b$, więc $\{\{a\}, \{a, b\}\} = \{\{a\}\}$; stąd $\{a, d\} = \{a\}$, a więc $b = a = d$. Niech $\{a, b\} \neq \{a\}$. Wtedy $a \neq b$ i $\{a, b\} = \{a, d\}$, a więc $b = d$. Zatem $b = d$. Q.E.D.

Wniosek. Jeżeli $a \neq b$, to $\langle a, b\rangle \neq \langle b, a\rangle$.

Definicja 5. Dla dowolnych obiektów $a_1, \ldots, a_n$, gdzie n jest dodatnią liczbą naturalną, określamy $n-$elementowy *układ uporządkowany* (krótko: $n-$krotkę) $\langle a_1, \ldots, a_n\rangle$ przez następującą definicję rekurencyjną:

$\langle a_1\rangle = a_1$,

$\langle a_1, \ldots, a_n, a_{n+1}\rangle = \langle\langle a_1, \ldots a_n\rangle, a_{n+1}\rangle$.

Przykład. $\langle 1, 2, 3\rangle = \langle\langle 1, 2\rangle, 3\rangle$ (*trójka uporządkowana*)

Lemat 2 (o n-krotkach)**.** Dla dowolnych obiektów $a_1, \ldots, a_n$:

$\langle a_1, \ldots, a_n\rangle = \langle b_1, \ldots b_n\rangle \Leftrightarrow a_1 = b_1 \wedge \cdots \wedge a_n = b_n$.

Dowód przebiega przez indukcję względem n z wykorzystaniem Lematu 1.

4.2. Iloczyn kartezjański

Definicja 6. Dla dowolnych zbiorów A i B określamy zbiór $A \times B$ wzorem:

$$A \times B = \{\langle x, y\rangle : x \in A \wedge y \in B\}\,.$$

Zbiór $A \times B$ nazywamy *iloczynem kartezjańskim* (albo: produktem kartezjańskim) zbiorów A i B.

$$\{\langle x, y\rangle : x \in A \wedge y \in B\} = \{z : \exists_{x,y}(x \in A \wedge y \in B \wedge z = \langle x, y\rangle)\}$$

$A \times B \subset \mathcal{P}(\mathcal{P}(A \cup B))$. Istnienie $A \times B$ wynika z aksjomatów sumy, zbioru potęgowego i wyróżniania.

(D$\times$) $\langle x, y\rangle \in A \times B \Leftrightarrow x \in A \wedge y \in B$

Przykłady. Niech $A = \{1, 2, 3\}$, $B = \{4, 5\}$. Wtedy

$$A \times B = \{\langle 1, 4\rangle, \langle 1, 5\rangle, \langle 2, 4\rangle, \langle 2, 5\rangle, \langle 3, 4\rangle, \langle 3, 5\rangle\}\,.$$

$\mathbb{R} \times \mathbb{R}$ przedstawia zbiór wszystkich punktów płaszczyzny wyposażonej w układ współrzędnych prostokątnych.

Prawa dla iloczynu kartezjańskiego

$\emptyset \times A = \emptyset$, $A \times \emptyset = \emptyset$

Iloczyn kartezjański nie jest przemienny ani łączny. Na ogół:

$A \times B \neq B \times A$, $(A \times B) \times C \neq A \times (B \times C)$.

Zachodzą prawa rozdzielności iloczynu kartezjańskiego względem działań boolowskich.

$(A \cup B) \times C = (A \times C) \cup (B \times C)$

$A \times (B \cup C) = (A \times B) \cup (A \times C)$

$(A \cap B) \times C = (A \times C) \cap (B \times C)$

$A \times (B \cap C) = (A \times B) \cap (A \times C)$

$(A \setminus B) \times C = (A \times C) \setminus (B \times C)$

$A \times (B \setminus C) = (A \times B) \setminus (A \times C)$

Wyprowadzimy ostatnie prawo:
$A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

Wykazujemy: $\langle x, y\rangle \in A \times (B \setminus C) \Leftrightarrow \langle x, y\rangle \in (A \times B) \setminus (A \times C)$.

$\langle x, y\rangle \in (A \times B) \setminus (A \times C) \leftrightarrow$

$\langle x, y\rangle \in A \times B \wedge \neg(\langle x, y\rangle \in A \times C) \leftrightarrow$

$(x \in A \wedge y \in B) \wedge \neg(x \in A \wedge y \in C) \leftrightarrow$

$(x \in A \wedge y \in B) \wedge (\neg(x \in A) \vee \neg(y \in C)) \leftrightarrow$

$(x \in A \wedge y \in B \wedge \neg(x \in A)) \vee (x \in A \wedge y \in B \wedge \neg(y \in C)) \leftrightarrow$

$0 \vee (x \in A \wedge y \in B \wedge \neg(y \in C)) \leftrightarrow$

$x \in A \wedge y \in B \setminus C \leftrightarrow$

$\langle x, y\rangle \in A \times (B \setminus C)$

Niech $n \geq 1$. *$n-$krotny iloczyn kartezjański* $A_1 \times A_2 \times \cdots \times A_n$ określamy rekurencyjnie:

Dla $n = 1$ $A_1 \times \cdots \times A_n = A_1$.

$A_1 \times \cdots \times A_n \times A_{n+1} = (A_1 \times \cdots \times A_n) \times A_{n+1}$

W szczególności:

$A \times B \times C = (A \times B) \times C$

$A \times B \times C \times D = (A \times B \times C) \times D = ((A \times B) \times C) \times D$

Zatem w wyrażeniach $A_1 \times \cdots \times A_n$ wstawiamy nawiasy od lewej strony.

Fakt 4. Niech $n \geq 1$. Wtedy:

$A_1 \times \cdots \times A_n = \{\langle x_1, \ldots, x_n \rangle : x_1 \in A_1 \wedge \cdots \wedge x_n \in A_n\}$.

Niech $n \geq 1$. Określamy rekurencyjnie zbiór A^n, zwany $n-$*tą potęgą kartezjańską* zbioru A.

$A^1 = A$

$A^{n+1} = A^n \times A$

W szczególności:

$A^2 = A \times A$, $A^3 = A \times A \times A$ itd.

Przykłady.

$\mathbb{R}^2$ przedstawia płaszczyznę kartezjańską.

$\mathbb{R}^3$ przedstawia trójwymiarową przestrzeń kartezjańską.

$\mathbb{R}^3 = \{\langle x, y, z\rangle : x, y, z \in \mathbb{R}\}$

Piszemy $x, y, z \in \mathbb{R}$ zamiast $x \in \mathbb{R} \wedge y \in \mathbb{R} \wedge z \in \mathbb{R}$.

4.3. Relacje

Definicja 7. Niech $n \geq 1$. *Relacją $n-$argumentową* nazywamy zbiór, którego wszystkie elementy są $n-$elementowymi układami uporządkowanymi.

Relacje jednoargumentowe nazywamy też *unarnymi*, a dwuargumentowe *binarnymi*.

Każda relacja binarna jest zbiorem par uporządkowanych.

Definicja 8. Podzbiory zbioru $A_1 \times \cdots \times A_n$ nazywamy *relacjami na iloczynie kartezjańskim* $A_1 \times \cdots \times A_n$.

Definicja 9. Niech $n \geq 1$. Podzbiory zbioru A^n nazywamy $n-$argumentowymi relacjami *na zbiorze* A.

Relacje unarne na zbiorze A są podzbiorami zbioru A.

Relacje binarne na zbiorze A są podzbiorami zbioru $A \times A$.

Relacje binarne odpowiadają stosunkom dwuargumentowym.

Na przykład stosunek $<$ na zbiorze $\{1, 2, 3\}$ jest reprezentowany przez relację $\{\langle 1, 2\rangle, \langle 1, 3\rangle, \langle 2, 3\rangle\}$.

Stosunek $<$ na zbiorze $\mathbb{N}$ jest reprezentowany przez relację nieskończoną, którą możemy zapisać tylko częściowo jako listę par: $\{\langle 0, 1\rangle, \langle 0, 2\rangle, \ldots, \langle 1, 2\rangle, \langle 1, 3\rangle, \ldots, \langle 2, 3\rangle, \langle 2, 4\rangle, \ldots\}$

albo jako relację wyznaczoną przez warunek:
$\{\langle m, n\rangle \in \mathbb{N}^2 : m < n\}$.

Podobnie relacje trójargumentowe odpowiadają stosunkom trójargumentowym.

Rozważmy zbiór A, którego elementami są Anna, Barbara, Jan, Piotr, Kasia i Zosia, przy czym Kasia jest córką Anny i Jana, a Zosia jest córką Barbary i Piotra. Wtedy stosunek 'x jest córką y (matki) i z (ojca)' jest reprezentowany przez relację:

$\{\langle$ Kasia, Anna , Jan $\rangle, \langle$ Zosia, Barbara, Piotr $\rangle\}$

Specjalne relacje binarne na zbiorze A:

$\emptyset$ - *relacja pusta*,

$\mathrm{I}_A = \{\langle x, y\rangle \in A^2 : x = y\} = \{\langle x, x\rangle : x \in A\}$ - *relacja identyczności na zbiorze* A,

$A \times A$ - *relacja totalna na zbiorze* A.

Definicja 10. Dla dowolnej relacji binarnej R określamy zbiory:

$D(R) = \{x : \exists_y(\langle x, y\rangle \in R)\}$,

$D^*(R) = \{y : \exists_x(\langle x, y\rangle \in R)\}$.

Zbiór $D(R)$ nazywamy *dziedziną*, a zbiór $D^*(R)$ *przeciwdziedziną* relacji R.

Mamy: $D(R) \subset \bigcup\bigcup R$, $D^*(R) \subset \bigcup\bigcup R$. Istnienie $D(R)$ i $D^*(R)$ wynika z aksjomatów sumy i wyróżniania.

Mamy: $R \subset D(R) \times D^*(R)$.

Przykłady.

I. $R = \{\langle 1, 2\rangle, \langle 2, 3\rangle\}$. Wtedy $D(R) = \{1, 2\}$, $D^*(R) = \{2, 3\}$.

II. $R = \{\langle m, n\rangle \in \mathbb{N}^2 : m < n\}$. Wtedy $D(R) = \mathbb{N}$,
$D^*(R) = \mathbb{N}^+ = \mathbb{N} \setminus \{0\}$.

Definicja 11. *Relacją odwrotną* do relacji binarnej R nazywamy relację:

$R^{-1} = \{\langle x, y\rangle : \langle y, x\rangle \in R\}$.

Przykłady.

I. $R = \{\langle 1, 2\rangle, \langle 2, 3\rangle\}$. Wtedy $R^{-1} = \{\langle 2, 1\rangle, \langle 3, 2\rangle\}$.

II. $R = \{\langle m, n\rangle \in \mathbb{N}^2 : m < n\}$. Wtedy
$R^{-1} = \{\langle n, m\rangle \in \mathbb{N}^2 : m < n\} = \{\langle m, n\rangle \in \mathbb{N}^2 : m > n\}$.

Mamy: $D(R^{-1}) = D^*(R)$, $D^*(R^{-1}) = D(R)$, $(R^{-1})^{-1} = R$.

Definicja 12. Niech R i S będą relacjami binarnymi. *Złożeniem relacji* R i S nazywamy relację:

$S \circ R = \{\langle x, y\rangle : \exists_z(\langle x, z\rangle \in R \wedge \langle z, y\rangle \in S)\}$.

Przykłady.

I. $R = \{\langle 1, 2\rangle, \langle 1, 3\rangle\}$, $S = \{\langle 2, 3\rangle, \langle 2, 4\rangle\}$.

Wtedy $S \circ R = \{\langle 1, 3\rangle, \langle 1, 4\rangle\}$, $R \circ S = \emptyset$.

Złożenie relacji nie jest działaniem przemiennym!

II. Niech R, S będą relacjami binarnymi na zbiorze wszystkich ludzi L, określonymi następująco:

$R = \{\langle x, y\rangle \in L^2 : x$ jest mężem $y\}$,

$S = \{\langle x, y\rangle \in L^2 : x$ jest córką $y\}$.

Wtedy $S \circ R = \{\langle x, y\rangle \in L^2 : x$ jest zięciem $y\}$.

Prawa algebry relacji binarnych

Dla dowolnych relacji binarnych R, S, T prawdziwe są następujące równości.

$(T \circ S) \circ R = T \circ (S \circ R)$ (prawo łączności złożenia relacji)

$(S \circ R)^{-1} = R^{-1} \circ S^{-1}$ (prawo złożenia relacji odwrotnych)

$(S_1 \cup S_2) \circ R = (S_1 \circ R) \cup (S_2 \circ R)$ (prawa rozdzielności

$S \circ (R_1 \cup R_2) = (S \circ R_1) \cup (S \circ R_2)$ złożenia względem sumy)

Dla dowolnej relacji $R \subset A^2$ prawdziwe są równości.

$\mathrm{I}_A \circ R = R$, $R \circ \mathrm{I}_A = R$.

Ponadto mamy prawa rozdzielności dla relacji odwrotnej.

$(R \cup S)^{-1} = R^{-1} \cup S^{-1}$, $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$

$(R \setminus S)^{-1} = R^{-1} \setminus S^{-1}$

Wyprowadzimy prawo: $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Korzystamy z równoważności wynikających z definicji.

(D.$^{-1}$) $\langle x, y\rangle \in R^{-1} \Leftrightarrow \langle y, x\rangle \in R$

(D $\circ$) $\langle x, y\rangle \in S \circ R \Leftrightarrow \exists_z(\langle x, z\rangle \in R \wedge \langle z, y\rangle \in S)$

$\langle x, y\rangle \in (S \circ R)^{-1} \leftrightarrow \langle y, x\rangle \in S \circ R \leftrightarrow$

$\leftrightarrow \exists_z(\langle y, z\rangle \in R \wedge \langle z, x\rangle \in S) \leftrightarrow$

$\leftrightarrow \exists_z(\langle z, y\rangle \in R^{-1} \wedge \langle x, z\rangle \in S^{-1}) \leftrightarrow$

$\leftrightarrow \exists_z(\langle x, z\rangle \in S^{-1} \wedge \langle z, y\rangle \in R^{-1}) \leftrightarrow$

$\leftrightarrow \langle x, y\rangle \in R^{-1} \circ S^{-1}$

Wykażemy: $R \circ \mathrm{I}_A = R$ dla $R \subset A^2$.

$\langle x, y\rangle \in R \circ \mathrm{I}_A \leftrightarrow \exists_z(\langle x, z\rangle \in \mathrm{I}_A \wedge \langle z, y\rangle \in R) \leftrightarrow$

$\leftrightarrow \exists_z(x = z \wedge \langle z, y\rangle \in R) \leftrightarrow \langle x, y\rangle \in R$

Ważne rodzaje relacji binarnych

Definicja 13. Relację $R \subset A^2$ nazywamy:

zwrotną na zbiorze A, jeżeli $\forall_{x \in A}(\langle x, x\rangle \in R)$,

symetryczną, jeżeli $\forall_{x,y}(\langle x, y\rangle \in R \Rightarrow \langle y, x\rangle \in R)$,

przechodnią, jeżeli $\forall_{x,y,z}(\langle x, y\rangle \in R \wedge \langle y, z\rangle \in R \Rightarrow \langle x, z\rangle \in R)$,

antysymetryczną, jeżeli $\forall_{x,y}(\langle x, y\rangle \in R \wedge \langle y, x\rangle \in R \Rightarrow x = y)$,

spójną na zbiorze A, jeżeli $\forall_{x,y \in A}(\langle x, y\rangle \in R \vee \langle y, x\rangle \in R)$.

przeciwzwrotną na zbiorze A, jeżeli $\forall_{x \in A}(\langle x, x\rangle \notin R)$,

przeciwsymetryczną, jeżeli $\forall_{x,y}(\langle x, y\rangle \in R \Rightarrow \langle y, x\rangle \notin R)$,

słabo spójną na zbiorze A, jeżeli
$\forall_{x,y \in A}(\langle x, y\rangle \in R \vee x = y \vee \langle y, x\rangle \in R)$.

Dla relacji binarnych często piszemy xRy zamiast: $\langle x, y\rangle \in R$. Ta symbolika przypomina, że relacje binarne odpowiadają stosunkom dwuargumentowym, które zwykle zapisuje się w notacji infiksowej, np. $x = y$, $x < y$. W tej notacji warunki Definicji 13 przyjmują formę:

zwrotna na zbiorze A: $\forall_{x\in A}(xRx)$,

symetryczna: $\forall_{x,y}(xRy \Rightarrow yRx)$,

przechodnia: $\forall_{x,y,z}(xRy \wedge yRz \Rightarrow xRz)$,

antysymetryczna: $\forall_{x,y}(xRy \wedge yRx \Rightarrow x = y)$,

spójna na zbiorze A: $\forall_{x,y\in A}(xRy \vee yRx)$,

przeciwzwrotna na zbiorze A: $\forall_{x\in A}\neg(xRx)$,

przeciwsymetryczna: $\forall_{x,y}(xRy \Rightarrow \neg(yRx))$,

słabo spójna na zbiorze A: $\forall_{x,y\in A}(xRy \vee x = y \vee yRx)$.

Przykłady podano na tablicy!

Fakt 5. Relacja $R \subset A^2$ jest:

zwrotna na zbiorze A wtw, gdy $\mathrm{I}_A \subset R$,

symetryczna wtw, gdy $R = R^{-1}$,

przechodnia wtw, gdy $R \circ R \subset R$,

antysymetryczna wtw, gdy $R \cap R^{-1} \subset \mathrm{I}_A$,

spójna na zbiorze A wtw, gdy $R \cup R^{-1} = A^2$,

przeciwzwrotna na zbiorze A wtw, gdy $R \cap \mathrm{I}_A = \emptyset$,

przeciwsymetryczna wtw, gdy $R \cap R^{-1} = \emptyset$,

słabo spójna na zbiorze A wtw, gdy $R \cup \mathrm{I}_A \cup R^{-1} = A^2$.

Wniosek. Każda relacja przeciwsymetryczna jest antysymetryczna. Każda relacja spójna na zbiorze A jest słabo spójna na zbiorze A.

5. Funkcje

5.1. Funkcje i odwzorowania

Przez funkcję rozumiemy przyporządkowanie elementom pewnego zbioru X elementów pewnego zbioru Y w taki sposób, że każdemu elementowi zbioru X przyporządkowano dokładnie jeden element zbioru Y.

Powyższa definicja jest nieprecyzyjna. W teorii mnogości przyjmuje się ścisłą definicję funkcji jako relacji.

Definicja 14. *Funkcją* nazywamy relację binarną R, spełniającą warunek *prawostronnej jednoznaczności*:

$$\forall_{x,y,z}(\langle x, y\rangle \in R \wedge \langle x, z\rangle \in R \Rightarrow y = z).$$

Zgodnie z tym warunkiem, dla każdego obiektu x istnieje najwyżej jeden obiekt y taki, że $\langle x, y\rangle \in R$.

Równoważnie: dla każdego $x \in D(R)$ istnieje dokładnie jedno y takie, że $\langle x, y\rangle \in R$.

Przykłady.

Relacja $\{\langle 1,2\rangle,\langle 2,3\rangle,\langle 3,1\rangle\}$ jest funkcją.

Relacja $\{\langle 1,2\rangle,\langle 1,3\rangle,\langle 2,4\rangle\}$ nie jest funkcją.

Relacja $\{\langle m,n\rangle \in \mathbb{N}^2 : m < n\}$ nie jest funkcją.

Relacja $\{\langle x,y\rangle \in \mathbb{R}^2 : x^2 = y\}$ jest funkcją.

Relacja $\{\langle x,y\rangle \in \mathbb{R}^2 : x = y^2\}$ nie jest funkcją.

Relacja pusta jest funkcją; nazywamy ją *funkcją pustą*.

Dla dowolnego zbioru A relacja I_A jest funkcją; nazywamy ją *funkcją identycznościową na zbiorze A*.

Funkcje często oznaczamy literami f, g, h, F, G, H.

Definicja 15. Niech f będzie funkcją. Dla $x \in D(f)$ jedyny element y taki, że $\langle x, y\rangle \in f$ oznaczamy przez $f(x)$ i nazywamy *wartością funkcji f dla argumentu x.*

(D$f(x)$) $\forall_{x\in D(f)}\forall_y(f(x) = y \Leftrightarrow \langle x, y\rangle \in f)$

Zbiór $D(f)$ jest dziedziną funkcji f.

Mamy: $D^*(f) = \{f(x) : x \in D(f)\}$. Zbiór $D^*(f)$, czyli przeciwdziedzinę funkcji f, nazywamy też *zbiorem wartości* funkcji f.

Definicja 16. Niech f będzie funkcją. Mówimy, że funkcja f *odwzorowuje zbiór X w zbiór Y* (piszemy: $f : X \mapsto Y$), jeżeli $D(f) = X$ i $D^*(f) \subset Y$.

UWAGA. $f : D(f) \mapsto Y$ dla dowolnego zbioru Y zawierającego $D^*(f)$. $D^*(f)$ jest najmniejszym zbiorem Y takim, że $f : D(f) \mapsto Y$.

Definicja 17. Niech f będzie funkcją. Mówimy, że funkcja f odwzorowuje zbiór X *na* zbiór Y, jeżeli $D(f) = X$ i $D^*(f) = Y$.

Przykłady.

Rozważmy funkcję $f : \mathbb{R} \mapsto \mathbb{R}$ określoną wzorem:

$f(x) = x + 1$ dla $x \in \mathbb{R}$.

f odwzorowuje $\mathbb{R}$ na $\mathbb{R}$, ponieważ każda liczba $y \in \mathbb{R}$ jest wartością funkcji f. Żeby to stwierdzić, z równania $y = x + 1$ otrzymujemy $x = y - 1$. Zatem $y = f(y - 1)$.

Funkcja g określona wzorem:

$g(x) = x^2 + 1$ dla $x \in \mathbb{R}$

odwzorowuje $\mathbb{R}$ w $\mathbb{R}$, lecz nie na $\mathbb{R}$. Mamy $D^*(g) = [1, \infty)$, a więc $D^*(g)$ jest właściwym podzbiorem zbioru $\mathbb{R}$.

Definicja 18. Funkcję f nazywamy *różnowartościową* (albo: wzajemnie jednoznaczną, jedno-jednoznaczną), jeżeli spełnia warunek:

$\forall_{x_1,x_2\in D(f)}(f(x_1)=f(x_2)\Rightarrow x_1=x_2)$.

Równoważnie: $\forall_{x_1,x_2\in D(f)}(x_1\neq x_2\Rightarrow f(x_1)\neq f(x_2))$.

Przykłady.

Funkcja $f:\mathbb{R}\mapsto\mathbb{R}$ określona wzorem:

$f(x)=x+1$ dla $x\in\mathbb{R}$

jest różnowartościowa. Wykazujemy to.

Niech $x_1,x_2\in\mathbb{R}$ spełniają równanie $f(x_1)=f(x_2)$. Stąd $x_1+1=x_2+1$, a więc $x_1=x_2$.

Funkcja $g:\mathbb{R}\mapsto\mathbb{R}$ określona wzorem:

$g(x)=x^2+x$ dla $x\in\mathbb{R}$

nie jest różnowartościowa. Mamy: $g(0)=0$ i $g(-1)=0$.

Definicja 19. *Odwzorowaniem* nazywamy trójkę $\langle f, X, Y\rangle$ taką, że f jest funkcją, X, Y są zbiorami i $f : X \mapsto Y$.

Mniej formalnie: odwzorowanie to funkcja f z wyraźnie podanymi zbiorami X, Y takimi, że $f : X \mapsto Y$.

Zamiast 'odwzorowanie $\langle f, X, Y\rangle$' często piszemy: odwzorowanie $f : X \mapsto Y$.

Definicja 20. Odwzorowanie $f : X \mapsto Y$ nazywamy:

iniekcją, jeżeli funkcja f jest różnowartościowa,

suriekcją, jeżeli f odwzorowuje X na Y,

bijekcją, jeżeli jest iniekcją i suriekcją.

Przykłady. Odwzorowanie $\mathrm{I}_A : A \mapsto A$ jest bijekcją.

Odwzorowanie $f : \mathbb{R} \mapsto \mathbb{R}$ określone wzorem: $f(x) = x + 1$ jest bijekcją.

Pewne dodatkowe pojęcia

Mówimy, że funkcja f *jest określona na zbiorze* X, jeżeli $D(f) = X$. Zbiór $D(f)$ nazywamy też *zbiorem argumentów* funkcji f.

Funkcję f taką, że $D(f) = X^n$ dla pewnego zbioru X i $n \geq 1$, nazywamy *funkcją* $n-$*argumentową określoną na zbiorze* X. Dla funkcji $n-$argumentowej f piszemy $f(x_1, \ldots, x_n)$ zamiast $f(\langle x_1, \ldots, x_n \rangle)$.

Odwzorowanie $f : X^n \mapsto X$ nazywamy $n-$argumentową *operacją* (albo: $n-$argumentowym *działaniem wewnętrznym*) *na zbiorze* X.

Najczęściej rozważa się działania jednoargumentowe i dwuargumentowe. Przykładami działań dwuargumentowych są działania dodawania i mnożenia na zbiorze $\mathbb{R}$.

Niech f będzie funkcją określoną na zbiorze X. Niech $A \subset X$. Przez $f|A$ oznaczamy *ograniczenie funkcji f na zbiór A*, tj. funkcję:

$f|A = \{\langle x, y\rangle \in f : x \in A\}$.

Mamy: $D(f|A) = A$ oraz $(f|A)(x) = f(x)$ dla każdego $x \in A$.

Symbolem Y^X oznaczamy zbiór wszystkich funkcji f takich, że $f : X \mapsto Y$.

Fakt 6(m). Jeżeli $|X| = n$ i $|Y| = m$, to $|Y^X| = m^n$.

Dowód przebiega przez indukcję względem n.

Ciągi

Funkcję f określoną na zbiorze $\mathbb{N}^+$ albo $\mathbb{N}$ nazywamy *ciągiem nieskończonym*.

Zwykle ciąg nieskończony oznaczamy $(a_n)_{n\geq 1}$, $(a_n)_{n\geq 0}$ itp. Wtedy a_n jest wartością tej funkcji dla argumentu n, zwaną *$n-$tym wyrazem ciągu.*

Ciąg uogólniony $(a_i)_{i\in I}$ określamy jako funkcję f taką, że $D(f) = I$ oraz $f(i) = a_i$ dla każdego $i \in I$.

Ciąg skończony określamy jako ciąg uogólniony $(a_i)_{i\in\{1,2,\ldots,n\}}$ lub $(a_i)_{i\in\{0,1,\ldots,n-1\}}$ dla pewnej liczby naturalnej n (zwanej *długością* tego ciągu).

Inne oznaczenia: $(a_i)_{1\leq i\leq n}$ lub $(a_1, \ldots, a_n)$

$(a_i)_{i<n}$ lub $(a_0, \ldots, a_{n-1})$

Fakt 7. Niech f, g będą funkcjami określonymi na zbiorze X. Wtedy:

$$f = g \Leftrightarrow \forall_{x \in X}(f(x) = g(x)).$$

Dowód. Jeżeli $f = g$ i $x \in X$, to $f(x) = g(x)$ na mocy praw równości. Wykażemy przeciwną implikację. Zakładamy prawą stronę. Stąd na mocy praw równości:

$$\forall_{x \in X} \forall_y (f(x) = y \Leftrightarrow g(x) = y),$$

a to jest równoważne:

$$\forall_{x,y}(\langle x, y \rangle \in f \Leftrightarrow \langle x, y \rangle \in g).$$

Zatem $f = g$ na mocy aksjomatu ekstensjonalności. Q.E.D.

Wniosek. $(a_i)_{i \in I} = (b_i)_{i \in I} \Leftrightarrow \forall_{i \in I}(a_i = b_i)$.

Uogólniony ciąg zbiorów $(A_i)_{i\in I}$ nazywamy też *indeksowaną rodziną zbiorów*, a zbiór I nazywamy *zbiorem indeksów* tej rodziny.

Inne oznaczenie: $\{A_i\}_{i\in I}$.

Definicja 21. Niech $\{A_i\}_{i\in I}$ będzie indeksowaną rodziną zbiorów. Określamy zbiory:

$\bigcup_{i\in I} A_i = \{x : \exists_{i\in I}(x \in A_i)\}$ (*suma* rodziny $\{A_i\}_{i\in I}$),

$\bigcap_{i\in I} A_i = \{x : \forall_{i\in I}(x \in A_i)\}$ (*iloczyn* rodziny $\{A_i\}_{i\in I}$) dla $I \neq \emptyset$,

$\Pi_{i\in I} A_i = \{(a_i)_{i\in I} : \forall_{i\in I}(a_i \in A_i)\}$ (*produkt kartezjański* rodziny $\{A_i\}_{i\in I}$).

Tak określone działania sumy, iloczynu i produktu kartezjańskiego nazywamy *działaniami nieskończonymi* lub *uogólnionymi*.

Mamy: $\bigcup_{i\in I} A_i = \bigcup D^*(\{A_i\}_{i\in I})$.

5.2. Funkcja odwrotna i złożenie funkcji

Dla dowolnej funkcji f istnieje relacja odwrotna do funkcji f:

$f^{-1} = \{\langle y, x\rangle : \langle x, y\rangle \in f\}$.

Fakt 8. Niech f będzie funkcją. Relacja f^{-1} jest funkcją wtw, gdy f jest funkcją różnowartościową.

DOWÓD. Zauważmy, że f jest funkcją różnowartościową wtw, gdy spełnia warunek *lewostronnej jednoznaczności*:

(LJ) $\forall_{x,y,z}(\langle x, z\rangle \in f \wedge \langle y, z\rangle \in f \Rightarrow x = y)$

Warunek (LJ) dla f jest równoważny warunkowi prawostronnej jednoznaczności dla f^{-1}:

$\forall_{x,y,z}(\langle z, x\rangle \in f^{-1} \wedge \langle z, y\rangle \in f^{-1} \Rightarrow x = y)$. Q.E.D.

Definicja 22. Niech f będzie funkcją różnowartościową. Funkcję f^{-1} nazywamy *funkcją odwrotną do funkcji* f.

Oczywiście $D(f^{-1}) = D^*(f)$ i $D^*(f^{-1}) = D(f)$ (tak jest dla dowolnych relacji).

Fakt 9. Niech f będzie funkcją różnowartościową. Wtedy odwzorowanie $f^{-1} : D^*(f) \mapsto D(f)$ jest bijekcją.

Dowód. Z powyższych równości wynika, że to odwzorowanie jest suriekcją. Warunek prawostronnej jednoznaczności dla f jest równoważny warunkowi lewostronnej jednoznaczności dla f^{-1}, a więc to odwzorowanie jest iniekcją. Q.E.D.

Przykłady.

Mamy: $\mathrm{I}_A^{-1} = \mathrm{I}_A$.

Niech funkcja $f : \mathbb{R} \mapsto \mathbb{R}$ będzie określona wzorem:

$f(x) = 2x + 1$ dla $x \in \mathbb{R}$.

Wtedy $f^{-1}(x) = \frac{x-1}{2}$ dla $x \in \mathbb{R}$.

Niech $g = \{\langle 1, 2\rangle, \langle 2, 4\rangle\}$. Wtedy $g^{-1} = \{\langle 2, 1\rangle, \langle 4, 2\rangle\}$.

Fakt 10. Jeżeli f i g są funkcjami, to $g \circ f$ jest funkcją.

Dowód. Wykażemy warunek prawostronnej jednoznaczności dla $g \circ f$ przy założeniu, że f i g spełniają ten warunek.

Niech $\langle x, y \rangle \in g \circ f$ i $\langle x, z \rangle \in g \circ f$. Istnieją z_1, z_2 takie, że $\langle x, z_1 \rangle \in f$, $\langle z_1, y \rangle \in g$, $\langle x, z_2 \rangle \in f$, $\langle z_2, z \rangle \in g$. Stąd $z_1 = z_2$, a więc $\langle z_1, y \rangle \in g$ i $\langle z_1, z \rangle \in g$. Zatem $y = z$. Q.E.D.

Mamy: $D(g \circ f) \subset D(f)$, $D^*(g \circ f) \subset D^*(g)$ (jak dla relacji).

Fakt 11. Jeżeli $f : X \mapsto Y$ i $g : Y \mapsto Z$, to $g \circ f : X \mapsto Z$.

Dowód. Zakładamy, że $f : X \mapsto Y$ i $g : Y \mapsto Z$. Z powyższych inkluzji mamy: $D(g \circ f) \subset X$ i $D^*(g \circ f) \subset Z$. Niech $x \in X$. Wtedy istnieje $y \in Y$ takie, że $\langle x, y \rangle \in f$, oraz istnieje $z \in Z$ takie, że $\langle y, z \rangle \in g$. Stąd $\langle x, z \rangle \in g \circ f$, a więc $x \in D(g \circ f)$. Wykazaliśmy $X \subset D(g \circ f)$, a więc $D(g \circ f) = X$. Q.E.D.

Fakt 12. Niech $f : X \mapsto Y$ i $g : Y \mapsto Z$.

(a) $(g \circ f)(x) = g(f(x))$ dla każdego $x \in X$.

(b) Jeżeli te odwzorowania są iniekcjami, to $g \circ f : X \mapsto Z$ jest iniekcją.

(c) Jeżeli te odwzorowania są suriekcjami, to $g \circ f : X \mapsto Z$ jest suriekcją.

(d) Jeżeli te odwzorowania są bijekcjami, to $g \circ f : X \mapsto Z$ jest bijekcją.

(e) Jeżeli $f : X \mapsto Y$ jest bijekcją, to $f^{-1} : Y \mapsto X$ jest bijekcją.

Dowód. (a) Niech $x \in X$ i $z = (g \circ f)(x)$. Stąd $\langle x, z\rangle \in g \circ f$, a więc istnieje y takie, że $\langle x, y\rangle \in f$ i $\langle y, z\rangle \in g$. Mamy: $f(x) = y$ i $y \in Y$. Mamy też: $g(y) = z$. Stąd $g(f(x)) = z$. Zatem $(g \circ f)(x) = g(f(x))$.

Pozostałe punkty wykazujemy na tablicy. Q.E.D.

5.3. Obraz i przeciwobraz

Niech $f : X \mapsto Y$.

Dla dowolnego $A \subset X$ określamy zbiór:

$f[A] = \{f(x) : x \in A\} = \{y : \exists_x (x \in A \wedge y = f(x))\}$,

zwany *obrazem zbioru* A *danym przez funkcję* f.

Dla dowolnego $B \subset Y$ określamy zbiór:

$f^{-1}[B] = \{x \in X : f(x) \in B\}$,

zwany *przeciwobrazem zbioru* B *danym przez funkcję* f.

Przykład. Niech $f : \mathbb{R} \mapsto \mathbb{R}$, $f(x) = x^2$ dla $x \in \mathbb{R}$.

$f[[-2, 2]] = [0, 4]$, $f^{-1}[[0, 3]] = [-\sqrt{3}, \sqrt{3}]$

Prawa dla obrazu i przeciwobrazu Niech $f : X \mapsto Y$.

$f[A_1 \cup A_2] = f[A_1] \cup f[A_2]$ dla $A_1, A_2 \subset X$

$f[\bigcup_{i \in I} A_i] = \bigcup_{i \in I} f[A_i]$ dla $A_i \subset X$ przy $i \in I$

$f^{-1}[B_1 * B_2] = f^{-1}[B_1] * f^{-1}[B_2]$ dla $* \in \{\cup, \cap, \setminus\}$, $B_1, B_2 \subset Y$

$f^{-1}[\bigcup_{i \in I} B_i] = \bigcup_{i \in I} f^{-1}[B_i]$ dla $B_i \subset Y$ przy $i \in I$

$f^{-1}[\bigcap_{i \in I} B_i] = \bigcap_{i \in I} f^{-1}[B_i]$ dla $B_i \subset Y$ przy $i \in I$, $I \neq \emptyset$

$f[f^{-1}[B]] \subset B$ dla $B \subset Y$

$A \subset f^{-1}[f[A]]$ dla $A \subset X$

Mamy: $f[X] = D^*(f)$ i $f^{-1}[Y] = X$.