

ELEMENTY LOGIKI I TEORII MNOGOŚCI
NOTATKI DO WYKŁADU DLA STUDENTÓW MATEMATYKI
I ROKU STUDIÓW ZAOCZNYCH 2013/14

KATARZYNA GRYGIEL

SPIS TREŚCI

Literatura	1
Do studentów	2
Część 1. Elementy logiki	2
1.1. Klasyczny rachunek zdań	2
1.2. Rachunek predykatów	7
Część 2. Elementy teorii zbiorów	9
2.1. Podstawowe działania na zbiorach	10
2.2. Uogólnione działania na zbiorach	14
Część 3. Relacje	16
3.1. Dziedzina, przeciwdziedzina i operacje na relacjach	17
3.2. Rodzaje relacji	18
3.3. Relacja równoważności i klasy abstrakcji	20
Część 4. Funkcje	21
Część 5. Teoria mocy	24
5.1. Zbiory przeliczalne	25
5.2. Zbiory nieprzeliczalne	27
5.3. Twierdzenie Cantora-Bernsteina	27
5.4. Twierdzenie Cantora	28
Część 6. Teoria porządku	29
Część 7. Aksjomat wyboru i równoważne twierdzenia	31

LITERATURA

- [1] K. Kuratowski, A. Mostowski, *Teoria mnogości wraz ze wstępem do opisowej teorii mnogości*, PWN, Warszawa 1978
- [2] K. Kuratowski, *Wstęp do teorii mnogości i topologii*, PWN, Warszawa 1971
- [3] W. Marek, J. Onyszkiewicz, *Elementy logiki i teorii mnogości w zadaniach*, PWN, Warszawa 1998
- [4] H. Rasiowa, *Wstęp do matematyki współczesnej*, PWN, Warszawa 1999 (od 1968)
- [5] W. Guzicki, P. Zakrzewski, *Wstęp do matematyki. Zbiór zadań*, PWN, Warszawa 2005
- [6] W. Guzicki, P. Zakrzewski, *Wykłady ze wstępu do matematyki*, PWN, Warszawa 2005
- [7] J. Kraszewski, *Wstęp do matematyki*, WNT, Warszawa 2007
- [8] P. Urzyczyn, wykłady z Podstaw Matematyki dostępne na stronie <http://www.mimuw.edu.pl/~urzy/Pmat/>
- [9] http://wazniak.mimuw.edu.pl/index.php?title=Logika_i_teoria_mnogo%C5%9Bci

Do studentów

Poniższe notatki dopiero powstają. Można je potraktować jako dodatek do własnych zapisków z wykładów, natomiast nie należy polegać na nich bezkrytycznie. Aktualna wersja jest daleka od zamierzonej, niektóre tematy są niemal w ogóle nieopracowane, natomiast spisane części zawierają liczne usterki, zarówno redakcyjne, jak i merytoryczne. W związku z powyższym bardzo proszę o nierozpowszechnianie notatek w obecnej postaci. Pragnę zwrócić uwagę, że istnieje wiele fantastycznych opracowań (nie tylko w literaturze polskiej), do których lektury gorąco zachęcam. Tworząc wykład starałam się jak najwięcej czerpać od innych, dlatego w żadnym razie nie twierdzę, że poniższe notatki stanowią moją własność intelektualną.

Wykłady te powstały z myślą o słuchaczach studiów niestacjonarnych I roku matematyki na Wydziale Matematyki i Nauk Informacyjnych Politechniki Warszawskiej. Kurs „Elementy logiki i teorii mnogości” ma na celu zapoznanie studentów z podstawowymi pojęciami i twierdzeniami dotyczącymi logiki i teorii zbiorów. Przede wszystkim powinien jednak nauczyć poruszać się wśród fundamentów matematyki, których opanowanie jest konieczne do dalszego zgłębiania tajników królowej nauk.

Część 1. Elementy logiki

1.1. KLASYCZNY RACHUNEK ZDAŃ

Definicja 1.1 (Zdanie logiczne). *Zdaniem logicznym* nazywamy zdanie, któremu możemy przyporządkować jedną z dwóch wartości logicznych: prawdę lub fałsz.

Przykład 1.2. Zdaniem logicznymi nie są żadne z poniższych:

Nie idź dzisiaj na wykład, chodź na piwo.

Kiedy jest wykład?

Poszedłbym na piwo.

Przykład 1.3. Rozważmy następujące zdania:

(a) *Jeżeli* Księżyc jest zielony, *to* Warszawa jest stolicą Polski.

(b) *Jeżeli* Warszawa jest stolicą Polski, *to* Księżyc jest zielony.

(c) *Jeżeli* Warszawa jest stolicą Polski *i* koale rozmnażają się przez pączkowanie, *to* Księżyc jest zielony.

Zdania (a) i (c) są prawdziwe, natomiast zdanie (b) jest fałszywe.

Użyjmy następujących skrótów:

p — „Warszawa jest stolicą Polski”,

q — „Księżyc jest zielony”,

r — „Koale rozmnażają się przez pączkowanie”.

Wówczas zdania (a), (b) i (c) możemy zapisać w następujący sposób:

(a) $q \rightarrow p$,

(b) $p \rightarrow q$,

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

Przy takim zapisie powyższe zdania stają się tylko ciągiem symboli. Rachunek zdań pozwoli nam precyzyjnie opisywać schematy wnioskowania i zdania złożone oraz oceniać ich prawdziwość.

Niech $V = \{p, q, r, \dots\}$ będzie zbiorem zmiennych zdaniowych.

Definicja 1.4 (Formuła rachunku zdań). Formuły rachunku zdań definiujemy w następujący sposób:

(i) Każda zmienna zdaniowa jest formułą.

(ii) Jeśli p jest formułą, to $\neg p$ (negacja) jest formułą (czytamy: „nieprawda że p ”).

(iii) Jeśli p oraz q są formułami, to $(p \rightarrow q)$ (implikacja) jest formułą (czytamy: „jeżeli p , to q ”).

(iv) Jeżeli p oraz q są formułami, to $(p \wedge q)$ (koniunkcja) jest formułą (czytamy: „ p i q ”).

(v) Jeżeli p oraz q są formułami, to $(p \vee q)$ (alternatywa) jest formułą (czytamy: „ p lub q ”).

- (vi) Jeżeli p oraz q są formułami, to $(p \leftrightarrow q)$ (równoważność) jest formułą (czytamy: „ p wtedy i tylko wtedy, gdy q ”).
- (vii) Nic innego nie jest formułą.

Występujące powyżej symbole $\neg, \rightarrow, \wedge, \vee, \leftrightarrow$ nazywamy ogólnie *funktorami zdaniotwórczymi* lub po prostu *spójnikami*. Dla czytelności zapisu będziemy pomijać niektóre z nawiasów według następującej konwencji:

- (i) pomijamy zewnętrzne nawiasy,
- (ii) koniunkcja i alternatywa wiążą silniej niż implikacja i równoważność,
- (iii) koniunkcja i alternatywa są łączne,
- (iv) negacja wiąże silniej niż którykolwiek z pozostałych spójników.

Przykład 1.5. Formułę $((p \wedge q) \rightarrow (r \vee \neg p))$ możemy zapisać w postaci $p \wedge q \rightarrow r \vee \neg p$.

Przykład 1.6. Formułami są następujące napisy: $\neg(p \leftrightarrow q) \wedge s$, $\neg\neg p$, $p \vee q \vee r$. Nie są nimi natomiast żadne z następujących: $\neg \wedge p$, $p \neg q$, $(p \rightarrow q)$.

Oznaczmy prawdę symbolem **1**, natomiast fałsz symbolem **0**.

Definicja 1.7 (Wartościowanie formuł). Definiujemy *wartościowanie zmiennej zdaniowej* p w następujący sposób:

$$v(p) := \begin{cases} \mathbf{1}, & \text{gdy zdanie } p \text{ jest prawdziwe} \\ \mathbf{0}, & \text{gdy zdanie } p \text{ jest fałszywe} \end{cases}.$$

Pojęcie wartościowania rozszerzamy na zbiór wszystkich formuł zdaniowych w następujący sposób:

- (i) Negacja $\neg p$ jest zdaniem prawdziwym wtedy i tylko wtedy, gdy p jest zdaniem fałszywym.
- (ii) Implikacja $p \rightarrow q$ jest zdaniem fałszywym wtedy i tylko wtedy, gdy p jest zdaniem prawdziwym oraz q jest zdaniem fałszywym.
- (iii) Koniunkcja $p \wedge q$ jest zdaniem prawdziwym wtedy i tylko wtedy, gdy p oraz q są zdaniem prawdziwymi.
- (iv) Alternatywa $p \vee q$ jest zdaniem prawdziwym wtedy i tylko wtedy, gdy przynajmniej ze zdań p i q jest zdaniem prawdziwym.
- (v) Równoważność $p \leftrightarrow q$ jest zdaniem prawdziwym wtedy i tylko wtedy, gdy p oraz q mają taką samą wartość logiczną.

Powyższe stwierdzenia możemy zapisać za pomocą następujących tabel:

p	$\neg p$	$\rightarrow$	0	1	$\wedge$	0	1	$\vee$	0	1	$\leftrightarrow$	0	1
0	1	0	1	1	0	0	0	0	0	1	0	1	0
1	0	1	0	1	1	0	1	1	1	1	1	0	1

Przykład 1.8. Rozważmy zdanie (c) z Przykładu 1.3. Wówczas jego wartość logiczną możemy wyznaczyć w następujący sposób:

$$\begin{aligned} v(p) &= \mathbf{1}, & v(q) &= \mathbf{0}, & v(r) &= \mathbf{0}, \\ v(p \wedge r) &= \mathbf{0}, \\ v((p \wedge r) \rightarrow q) &= \mathbf{1}. \end{aligned}$$

Definicja 1.9 (Formuły równoważne). Mówimy, że formuły p oraz q są *równoważne* (piszemy $p \equiv q$) wtedy i tylko wtedy, gdy dla każdego wartościowania formuła p ma taką samą wartość logiczną co formuła q .

Przykład 1.10. Formuły $p \rightarrow (q \rightarrow r)$ oraz $(p \wedge q) \rightarrow r$ są równoważne. Możemy to pokazać za pomocą następującej tabelki:

p	q	r	$p \rightarrow (q \rightarrow r)$	$(p \wedge q) \rightarrow r$
0	0	0	1	1
0	0	1	1	1
0	1	0	1	1
0	1	1	1	1
1	0	0	1	1
1	0	1	1	1
1	1	0	0	0
1	1	1	1	1

Definicja 1.11 (Tautologia). Formuła, która dla dowolnego wartościowania zmiennych zdaniowych zawsze przyjmuje wartość **1** nazywa się *tautologią*.

Dwie podstawowe metody sprawdzania, czy zadana formuła jest tautologią to:

1. metoda zero-jedynkowa (tabelkowa),
2. metoda skrócona (nie wprost).

Twierdzenie 1.12 (Podstawowe tautologie klasycznego rachunku zdań). *Następujące formuły zdaniowe są tautologiami:*

1. $p \rightarrow p$,
2. $p \vee \neg p$ (prawo wyłączonego środka),
3. $\neg(p \wedge \neg p)$ (prawo sprzeczności),
4. $\neg\neg p \leftrightarrow p$ (prawo podwójnego przeczenia),
5. $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$ (prawo de Morgana),
6. $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$ (prawo de Morgana),
7. $(p \leftrightarrow q) \leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$ (prawo eliminacji równoważności),
8. $p \wedge q \rightarrow p$,
9. $p \rightarrow p \vee q$,
10. $p \wedge q \leftrightarrow q \wedge p$,
11. $p \vee q \leftrightarrow q \vee p$,
12. $(p \rightarrow q) \rightarrow ((q \rightarrow r) \rightarrow (p \rightarrow r))$,
13. $p \rightarrow (q \rightarrow p)$,
14. $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$ (prawo transpozycji),
15. $p \wedge (p \rightarrow q) \rightarrow q$ (prawo odrywania; *Modus Ponens*),
16. $p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$ (prawo rozdzielności koniunkcji względem alternatywy),
17. $p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$ (prawo rozdzielności alternatywy względem koniunkcji),
18. $(p \rightarrow q) \leftrightarrow (\neg p \vee q)$ (prawo eliminacji implikacji).

Dowód. Dla przykładu udowodnimy prawo 13.

Sposób 1. Metoda tabelkowa (zero-jedynkowa)

p	q	$q \rightarrow p$	$p \rightarrow (q \rightarrow p)$
0	0	1	1
0	1	0	1
1	0	1	1
1	1	1	1

W ostatniej kolumnie znajdują się same jedynki, a zatem formuła jest prawdziwa niezależnie od wartościowania zmiennych, czyli jest tautologią.

Sposób 2. Metoda skrócona

Założmy nie wprost, że formuła $p \rightarrow (q \rightarrow p)$ nie jest tautologią. Oznacza to, że istnieje wartościowanie zmiennych p i q , przy którym cała formuła jest fałszywa. Ponieważ rozważana formuła jest w postaci implikacji, zatem aby była fałszywa poprzednik musi być prawdziwy, a wniosek fałszywy, czyli musi zachodzić $v(p) = 1$ oraz $v(q \rightarrow p) = 0$. Drugie równanie mówi, że implikacja $q \rightarrow p$ jest fałszywa, skąd wynika, że $v(q) = 1$ oraz $v(p) = 0$. W tym momencie otrzymuje sprzeczność, ponieważ p nie może być

równocześnie prawdziwe i fałszywe. Oznacza to, że nie istnieje wartościowanie, dla którego $p \rightarrow (q \rightarrow p)$ jest fałszywe, a zatem jest to tautologia. $\square$

Obie metody, zero-jedynkowa i skrócona, mogą być wykorzystane do sprawdzenia poprawności wnioskowania. Powiemy, że schemat rozumowania jest niezawodny, jeśli z prawdziwych przesłanek nie wynika fałszywy wniosek.

Przykład 1.13. Rozważmy następujące wnioskowanie:

„Jeśli Jan uczy się logiki, to jeśli jego poglądy są wewnętrznie sprzeczne, to je zmienia. Jeśli jednak zmienia poglądy, to straci autorytet. Zatem jeśli jego poglądy są wewnętrznie sprzeczne, lecz Jan nie uczy się logiki, to nie straci autorytetu.”

Oznaczmy składowe powyższego rozumowania w następujący sposób:

p — „Jan uczy się logiki.”

q — „Poglądy Jana są wewnętrznie sprzeczne.”

r — „Jan zmienia poglądy”.

s — „Jan straci autorytet”.

Wówczas schemat powyższego rozumowania ma postać

$$[(p \rightarrow (q \rightarrow r)) \wedge (r \rightarrow s)] \rightarrow ((q \wedge \neg p) \rightarrow \neg s).$$

Implikacja ta jest tautologią, zatem schemat rozumowania jest niezawodny, czyli wnioskowanie jest poprawne.

Zadanie 1.14. Sprawdzić metodą skróconą i zero-jedynkową, że powyższa implikacja rzeczywiście jest tautologią.

Definicja 1.15 (Formuły spełnialne i kontrtautologie). Powiemy, że formuła p jest *spełnialna*, jeżeli istnieje takie wartościowanie zmiennych zdaniowych, przy którym formuła p jest prawdziwa. Jeśli takie wartościowanie nie istnieje, to powiemy, że formuła p jest *niespełnialna* lub że jest *kontrtautologią*.

Twierdzenie 1.16. *Formuła p jest tautologią wtedy i tylko wtedy, gdy formuła $\neg p$ nie jest spełnialna.*

Dowód. Przypuśćmy, że formuła p jest tautologią. Wtedy dla każdego wartościowania v mamy $v(p) = \mathbf{1}$. Stąd otrzymujemy, że dla każdego wartościowania v mamy $v(\neg p) = \mathbf{0}$, a więc nie istnieje wartościowanie, które spełnia $\neg p$, czyli formuła ta nie jest spełnialna.

Przypuśćmy, że formuła $\neg p$ nie jest spełnialna, czyli nie istnieje wartościowanie v takie, że $v(\neg p) = \mathbf{0}$. Wynika stąd, że dla każdego wartościowania v mamy $v(p) = \mathbf{1}$, a więc p jest tautologią. $\square$

Do tej pory pojawiły się cztery funktory dwuargumentowe ($\rightarrow$, $\wedge$, $\vee$, $\leftrightarrow$), pozwalające z dwóch formuł tworzyć nową formułę, oraz jeden funktor jednoargumentowy ($\neg$), pozwalający z jednej formuły tworzyć nową formułę. Mają one tę własność, że wartość logiczna nowych zdań zależy tylko od wartości logicznej zdań składowych, a nie od ich sensu. Stąd też powyższe funktory nazywa się *ekstensjonalnymi*. Nie są to jednak wszystkie ekstensjonalne funktory jedno- i dwuargumentowe.

Ile jest funktorów jednoargumentowych (unarnych)? Każdej wartości logicznej ($\mathbf{0}$ i $\mathbf{1}$) argumentu funktora przyporządkowujemy jedną z wartości logicznych $\mathbf{0}$ lub $\mathbf{1}$. Zatem funktorów unarnych jest $2^2 = 4$.

p	$f_1(p)$	$f_2(p)$	$f_3(p)$	$f_4(p)$
0	0	0	1	1
1	0	1	0	1
	F	id	$\neg$	T

Zadanie 1.17. Ile jest funktorów dwuargumentowych (binarnych)? Zrobić tabelkę analogiczną do powyższej dla funktorów binarnych.

Zadanie 1.18. Ile jest funktorów n -argumentowych?

Wyróżnijmy jeszcze dwa funktory binarne.

Definicja 1.19 (NOR i NAND).

- (i) *Kreskę Sheffera* (inaczej NOR) oznaczamy przez $|$ i definiujemy w następujący sposób:
 $p|q$ jest zdaniem prawdziwym wtedy i tylko wtedy, gdy oba zdania p i q są fałszywe;
- (ii) *Strzałkę Peirce'a* (inaczej NAND) oznaczamy przez $\downarrow$ i definiujemy w następujący sposób:
 $p \downarrow q$ jest zdaniem prawdziwym wtedy i tylko wtedy, gdy oba zdania p i q są prawdziwe.

Definicja 1.20 (Układy funkcjonalnie pełne). Układ funktorów nazwiemy *funkcjonalnie pełnym*, jeżeli wszystkie funktory jedno- i dwuargumentowe można wyprowadzić za pomocą funktorów z tego układu.

Twierdzenie 1.21. *Układami funkcjonalnie pełnymi są:*

- (a) $\{\neg, \rightarrow, \wedge, \vee, \leftrightarrow\}$,
- (b) $\{\wedge, \neg\}$ oraz $\{\vee, \neg\}$,
- (c) $\{\downarrow\}$,
- (d) $\{|\}$.

Dowód punktów (a) i (b) pominiemy.

Zadanie 1.22. Korzystając z (b), udowodnij (c) i (d).

Zadanie 1.23. Pokaż, że $\{\wedge, \vee\}$ nie jest funkcjonalnie pełny.

Definicja 1.24 (Koniunkcyjna postać normalna). *Literałem* nazywamy zmienną zdaniową lub jej zaprzeczenie. Powiemy, że formuła jest w koniunkcyjnej postaci normalnej (CNF), jeśli jest koniunkcją formuł będących alternatywą literalów. Innymi słowy, formuła jest w CNF gdy ma postać

$$\varphi_1 \wedge \dots \wedge \varphi_n,$$

gdzie każda z formuł φ_i , dla $i \in \{1, \dots, n\}$, jest postaci

$$\psi_1^i \vee \dots \vee \psi_{k_i}^i,$$

dla pewnych literalów $\psi_1^i, \dots, \psi_{k_i}^i$.

Przykład 1.25. Formułami w postaci CNF są na przykład:

1. $(p \vee q \vee r) \wedge (\neg p \vee \neg r) \wedge (r \vee \neg q)$,
2. $p \wedge q$,
3. $p \vee q \vee r \vee \neg s$,
4. p .

Twierdzenie 1.26. *Dla każdej formuły istnieje równoważna formuła w koniunkcyjnej postaci normalnej.*

Szkic dowodu (nieobowiązkowy). Mając daną formułę stosujemy kolejno prawo eliminacji równoważności (7) i prawo eliminacji implikacji (18). Następnie przekształcamy formułę korzystając z praw de Morgana, podwójnego przeczenia, łączności, przemienności i rozdzielności alternatywy względem koniunkcji i koniunkcji względem alternatywy. $\square$

Przykład 1.27.

$$\begin{aligned} & ((p \rightarrow q) \wedge p) \rightarrow q \\ \equiv & ((\neg p \vee q) \wedge p) \rightarrow q \\ \equiv & \neg((\neg p \vee q) \wedge p) \vee q \\ \equiv & (\neg(\neg p \vee q) \vee \neg p) \vee q \\ \equiv & (p \wedge \neg q) \vee \neg p \vee q \\ \equiv & (p \wedge \neg q) \vee (\neg p \vee q) \\ \equiv & (p \vee (\neg p \vee q)) \wedge (\neg q \vee (\neg p \vee q)) \\ \equiv & (p \vee \neg p \vee q) \wedge (\neg q \vee \neg p \vee q). \end{aligned}$$

Definicja 1.28 (Forma zdaniowa). *Formą zdaniową* nazywamy wyrażenie zawierające zmienne, które po wstawieniu w miejsce tych zmiennych konkretnych obiektów staje się zdaniem logicznym.

Zbiór obiektów, które możemy wstawić w miejsce zmiennej w formie zdaniowej nazywa się *zakresem* tej zmiennej.

Przykład 1.29.

1. „ $x+2=4$ ” — forma zdaniowa jednej zmiennej, której zakresem jest zbiór liczb rzeczywistych.
2. „ x jest studentem I roku matematyki na PW” — forma zdaniowa jednej zmiennej, której zakresem jest zbiór ludzi.
3. „ $x^2+y^2<3$ ” — forma zdaniowa dwóch zmiennych x i y , których zakresem jest zbiór liczb rzeczywistych.
4. „ x ma y lat” — forma zdaniowa dwóch zmiennych, w której zakresem x jest zbiór ludzi, a zakresem y jest zbiór liczb dodatnich.

Formy zdaniowe o jednej zmiennej będziemy oznaczać przez $p(x), q(x), \dots$, formy o dwóch zmiennych przez $p(x, y), q(x, y), \dots$. Symbole $p, q, \dots$ nazywamy *predykatami*.

Zauważmy, że podstawiając w miejsce zmiennych konkretne wartości z odpowiedniego zakresu (w powyższych przykładach liczby lub osoby), formy zdaniowe stają się (prawdziwymi lub fałszywymi) formułami logicznymi.

Definicja 1.30 (Spełnialność i prawdziwość form zdaniowych). Niech $p(x)$ będzie formą zdaniową zmiennej x o zakresie X .

- (i) Element $a \in X$ *spełnia formę zdaniową* $p(x)$ wtedy i tylko wtedy, gdy $p(a)$ jest zdaniem prawdziwym.
- (ii) Formę zdaniową nazywamy *prawdziwą* wtedy i tylko wtedy, gdy jest spełniona przez wszystkie obiekty z zakresu jej zmiennych.
- (iii) Formę zdaniową nazywamy *fałszywą* wtedy i tylko wtedy, gdy nie jest spełniona przez żaden obiekt z zakresu jej zmiennych.

Przykład 1.31. Rozważmy formę $p(x) \equiv x+2=4$. Wtedy jeśli za zakres zmiennej x weźmiemy zbiór liczb rzeczywistych, to 2 spełnia tę formę zdaniową, natomiast 3 nie. Jeśli natomiast za zakres weźmiemy zbiór liczb nieparzystych, to $p(x)$ będzie fałszywa. Gdy zakresem będzie singleton $\{2\}$, forma będzie prawdziwa.

Z prostych form zdaniowych oraz spójników możemy tworzyć bardziej złożone formy zdaniowe. Niech $p(x)$ i $q(x)$ będą formami jednej zmiennej o zakresie X . Wtedy element $a \in X$ spełnia formę $p(x) \wedge q(x)$ wtedy i tylko wtedy, gdy zdanie $p(a) \wedge q(a)$ jest prawdziwe, czyli gdy a spełnia $p(x)$ oraz $q(x)$.

Rozważmy następujące zdanie:

„Jeśli n jest liczbą pierwszą, to n jest liczbą nieparzystą lub n jest równe 2.”

Możemy je opisać formułą $p \rightarrow (q \vee r)$, gdzie p, q, r oznaczają odpowiednio zdania:

- p : n jest liczbą pierwszą,
- q : n jest liczbą nieparzystą,
- r : n jest równe 2.

Podstawiając p w miejsce zdania „ n jest liczbą pierwszą” ukrywamy jednak część informacji. Zdanie to mówi przecież o pewnej liczbie n , co więcej, zdania p i q dotyczą tej samej liczby n . Zapiszmy więc $p(n)$ zamiast p aby podkreślić, że prawdziwość p zależy od tego jaką konkretną wartość przypiszemy zmiennej n . Zdanie $p(n)$ będzie prawdziwe, jeśli za n podstawimy jakąś liczbę pierwszą i fałszywe w przeciwnym przypadku. Zgodnie z tą konwencją nasze zdanie przyjmie postać $p(n) \rightarrow (q(n) \vee r(n))$.

Zwróćmy jednak uwagę, że trudno ocenić prawdziwość zdania p dopóki nie podstawimy w miejsce n jakiejś konkretnej liczby. Z drugiej strony wartość logiczna całego zdania $p(n) \rightarrow (q(n) \vee r(n))$ nie zależy od wyboru liczby n — jest ono prawdziwe dla każdej liczby naturalnej.

Aby móc formalnie zapisywać zdania takie jak powyższe wprowadzimy *kwantyfikatory* $\forall$ który będzie oznaczał „dla każdego” oraz $\exists$ który będzie oznaczał „istnieje”. Każde wystąpienie kwantyfikatora będzie dotyczyło pewnej zmiennej. W naszym przykładzie napiszemy

$$\forall_n p(n) \rightarrow (q(n) \vee r(n)),$$

gdzie zakresem zmiennej n jest zbiór liczb naturalnych $\mathbb{N}$.

Definicja 1.32 (Zasięg kwantyfikatora). *Zasięgiem* kwantyfikatora nazywamy część wyrażenia ujętą w nawiasy, przy czym lewy nawias występuje bezpośrednio po tym kwantyfikatorze. Gdy bezpośrednio po kwantyfikatorze nie występuje nawias, to zasięgiem kwantyfikatora jest następująca po nim forma zdaniowa.

Mówimy, że x jest zmienną *wolną* w danym wyrażeniu wtedy i tylko wtedy, gdy nie występuje w zasięgu żadnego kwantyfikatora o indeksie x . W przeciwnym razie mówimy, że x jest zmienną *związaną*.

Przykład 1.33. W wyrażeniu $\exists_x(p(x) \vee q(x))$ w zasięgu kwantyfikatora $\forall_x$ znajduje się cała alternatywa, natomiast w wyrażeniu $\exists_x p(x) \vee q(x)$ tylko forma zdaniowa $p(x)$.

W wyrażeniu $\forall_x(x + y = 3 \rightarrow \exists_y x \cdot y < 2)$ oba wystąpienia zmiennej x są związane, podobnie jak drugie wystąpienie zmiennej y . Natomiast pierwsze wystąpienie zmiennej y jest wolne.

Definicja 1.34 (Formuła rachunku kwantyfikatorów). Formuły rachunku predykatów definiujemy w następujący sposób.

- (i) Formy zdaniowe są formułami.
- (ii) Jeśli P jest formułą i x jest zmienną wolną w P lub nie ma wystąpienia w P , to $\forall_x P$ jest formułą.
- (iii) Jeśli P jest formułą i x jest zmienną wolną w P lub nie ma wystąpienia w P , to $\exists_x P$ jest formułą.

Niech $p(x)$ będzie formą zdaniową jednej zmiennej x , natomiast X zakresem zmiennej x . Wstawienie przed $p(x)$ dowolnego kwantyfikatora o indeksie x zmienia tę formę zdaniową w zdanie logiczne. Zdanie $\forall_x p(x)$ jest prawdziwe wtedy i tylko wtedy, gdy każdy element z zakresu zmiennej x spełnia formę zdaniową $p(x)$. Zdanie $\exists_x p(x)$ jest prawdziwe wtedy i tylko wtedy, gdy istnieje co najmniej jeden element z zakresu zmiennej x spełniający formę zdaniową $p(x)$.

Przykład 1.35. Niech $p(x) \equiv x + 1 > 0$ oraz niech zakresem zmiennej x będzie $\mathbb{R}$. Wtedy zdanie $\exists_x x + 1 > 0$ jest zdaniem prawdziwym, natomiast zdanie $\forall_x x + 1 > 0$ jest zdaniem fałszywym.

Definicja 1.36 (Podstawienie). Wyrażenie matematyczne jest *podstawieniem* formuły rachunku kwantyfikatorów wtedy i tylko wtedy, gdy powstaje z niej przez zastąpienie wszystkich występujących w niej zmiennych zdaniowych i symboli predykatywnych zdaniami logicznymi i formami zdaniowymi.

Przykład 1.37. Wyrażenie

$$\forall_x x^2 \geq 0 \rightarrow \exists_x x^2 \geq 0$$

jest podstawieniem formuły

$$\forall_x p(x) \rightarrow \exists_x p(x).$$

Definicja 1.38. Formuły, których prawdziwość wynika tylko z ich struktury i nie zależy od znaczenia wyrażeń atomowych w nich występujących, nazywamy *tautologiami rachunku kwantyfikatorów*.

Twierdzenie 1.39 (Prawa rachunku kwantyfikatorów).

1. $\forall_x p(x) \rightarrow p(x)$,
2. $p(x) \rightarrow \exists_x p(x)$,
3. $\forall_x p(x) \rightarrow \exists_x p(x)$,
4. $\neg \forall_x p(x) \leftrightarrow \exists_x \neg p(x)$,

5. $\neg \exists x p(x) \leftrightarrow \forall x \neg p(x)$,
6. $\forall x (p(x) \vee q) \leftrightarrow \forall x p(x) \vee q$, *gdy x jest zmienną wolną w q* ,
7. $\exists x (p(x) \vee q) \leftrightarrow \exists x p(x) \vee q$, *gdy x jest zmienną wolną w q* ,
8. $\forall x (p(x) \wedge q(x)) \leftrightarrow \forall x p(x) \wedge \forall x q(x)$,
9. $\exists x (p(x) \vee q(x)) \leftrightarrow \exists x p(x) \vee \exists x q(x)$,
10. $\forall x p(x) \vee \forall x q(x) \rightarrow \forall x (p(x) \vee q(x))$,
11. $\exists x p(x) \wedge \exists x q(x) \rightarrow \exists x (p(x) \wedge q(x))$,
12. $\forall x (p(x) \rightarrow q(x)) \rightarrow (\forall x p(x) \rightarrow \forall x q(x))$,
13. $\forall x (p(x) \rightarrow q(x)) \rightarrow (\exists x p(x) \rightarrow \exists x q(x))$,
14. $\forall x p(x) \leftrightarrow \forall y p(y)$,
15. $\exists x p(x) \leftrightarrow \exists y p(y)$,
16. $\forall x \forall y p(x, y) \leftrightarrow \forall y \forall x p(x, y)$,
17. $\exists x \exists y p(x, y) \leftrightarrow \exists y \exists x p(x, y)$,
18. $\exists x \forall y p(x, y) \rightarrow \forall y \exists x p(x, y)$,

Często chcemy wyrazić, że Ψ jest prawdą dla każdego lub dla jakiegoś x spełniającego warunek Φ . Będziemy używać w tym celu *kwantyfikatorów ograniczonych*.

Definicja 1.40 (Kwantyfikatory ograniczone).

$$\begin{aligned}\forall_{x:\Phi} \Psi &\equiv \forall x (\Phi \rightarrow \Psi), \\ \exists_{x:\Phi} \Psi &\equiv \exists x (\Phi \wedge \Psi).\end{aligned}$$

Przykład 1.41. Mamy świat wszystkich ludzi i osłów, stałą **Joe** oraz predykaty:

$\text{Osioł}(x)$ — x jest osłem,

$\text{Ma}(x, y)$ — x ma y (y należy do x),

$\text{Bije}(x, y)$ — x bije y .

Zdanie „Jeśli Joe ma osła, to go bije” ma postać

$$\forall x (\text{Osioł}(x) \wedge \text{Ma}(\text{Joe}, x) \rightarrow \text{Bije}(\text{Joe}, x)).$$

Często chcemy wyrazić, że $p(x)$ jest prawdą dla dokładnie jednego x . Będziemy używać w tym celu *kwantyfikatora jednostkowego*.

Definicja 1.42 (Kwantyfikator jednostkowy).

$$\exists!_x p(x) \equiv \exists x (p(x) \wedge \forall y (p(y) \rightarrow x = y))$$

Część 2. Elementy teorii zbiorów

Teoria zbiorów (inaczej teoria mnogości) oparta jest o rachunek predykatów posługujący się jedynym symbolem predykatowym. Symbol ten jest dwuargumentowy i oznaczamy go przez $\in$.

Predykat ten jest najczęściej interpretowany w modelu jako symbol przynależności do zbioru. Obiekt, który jest wartością zmiennej po lewej stronie symbolu $\in$ jest elementem zbioru, który jest wartością zmiennej występującej po stronie prawej.

Dla ułatwienia posługiwania się formalizmem związanym z aksjomatyczną teorią mnogości używamy wielu skrótów pozwalających na bardziej zwięzłe zapisywanie formuł. Często używany symbol $\notin$ jest skrótem mówiącym, że dwa elementy nie są ze sobą w relacji $\in$, to znaczy $x \notin X \equiv \neg x \in X$.

Kolejny skrót oznaczamy przez $=$ i definiujemy go w następujący sposób:

$$X = Y \equiv \forall z (z \in X \leftrightarrow z \in Y).$$

Skrót ten definiuje dwa zbiory jako *równe* jeżeli o każdym elemencie z możemy powiedzieć, że należy do zbioru X wtedy i tylko wtedy, gdy należy do zbioru Y . Innymi słowy dwa zbiory są równe jeśli posiadają dokładnie te same elementy.

Podobnie do równości definiujemy *zawieranie (inkluzję)* zbiorów:

$$X \subseteq Y \equiv \forall z (z \in X \rightarrow z \in Y).$$

Zbiór niezawierający żadnego elementu nazywamy *zbiorem pustym* i oznaczamy przez $\emptyset$.

Zbiór skończony (o skończenie wielu elementach) możemy zdefiniować przez wypisanie jego elementów.

Przykład 2.1.

1. $A = \{1, 2, 3\}$, $1 \in A$, $4 \notin A$, $\{2, 3\} \subseteq A$,
2. $B = \{\text{kot}, \text{pies}\}$, $\text{kot} \in B$, $\text{koala} \notin B$, $3 \notin B$,
3. $C = \{\emptyset\}$, $\emptyset \in C$, $\emptyset \subseteq C$,
4. $D = \emptyset$, $\emptyset \notin D$, $\emptyset \subseteq D$.

Zbiór możemy także zdefiniować za pomocą warunku, który musi być spełniony przez wszystkie elementy tego zbioru.

Przykład 2.2.

1. X jest zbiorem studentów pierwszego roku PW,
2. $Y = \{n \in \mathbb{N} : n^2 < 68 \wedge n \text{ jest liczbą pierwszą}\}$,
3. $Z = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 4\}$.

W ogólnym przypadku piszemy $A = \{x \in X : p(x)\}$, gdzie $p(x)$ jest formą zdaniową zmiennej x o zakresie X . Wtedy

$$a \in A \leftrightarrow p(a) \text{ jest zdaniem prawdziwym.}$$

Oznaczenia dla najczęściej spotykanych zbiorów liczbowych:

$\mathbb{N}$	zbiór liczb naturalnych
$\mathbb{Z}$	zbiór liczb całkowitych
$\mathbb{Q}$	zbiór liczb wymiernych
$\mathbb{R}$	zbiór liczb rzeczywistych
$\mathbb{R} \setminus \mathbb{Q}$	zbiór liczb rzeczywistych niewymiernych
$\mathbb{C}$	zbiór liczb zespolonych

Twierdzenie 2.3. Dla dowolnych zbiorów A , B , C zachodzi:

- (i) $\emptyset \subseteq A$,
- (ii) $A \subseteq A$,
- (iii) jeżeli $(A \subseteq B \wedge B \subseteq C)$ to $A \subseteq C$,
- (iv) $(A \subseteq B \wedge B \subseteq A)$ wtedy i tylko wtedy, gdy $A = B$,
- (v) jeżeli $A \neq B$ to $A \not\subseteq B \vee B \not\subseteq A$.

Aby zilustrować zależności między zbiorami, będziemy posługiwać się *diagramami Venna*. W tym schemacie zbiory reprezentowane są przez elipsy lub inne figury geometryczne. Czasem obrazuje się również przestrzeń, umieszczając elipsy wewnątrz prostokąta. Figurom nadaje się różne tekstury i kolory, co znacznie ułatwia dostrzeżenie relacji pomiędzy zbiorami (inkluzja, suma, iloczyn, itp.).

2.1. PODSTAWOWE DZIAŁANIA NA ZBIORACH

2.1.1. Suma zbiorów.

Definicja 2.4 (Suma zbiorów). Sumą zbiorów A i B (ozn. $A \cup B$) nazywamy zbiór tych elementów, które należą do zbioru A lub do zbioru B . Innymi słowy $x \in A \cup B$ wtedy i tylko wtedy, gdy $x \in A \vee x \in B$.

Twierdzenie 2.5. Dla dowolnych zbiorów A , B , C , D zachodzi:

- (i) $A \cup B = B \cup A$,
- (ii) $(A \cup B) \cup C = A \cup (B \cup C)$,
- (iii) $\emptyset \cup A = A$,
- (iv) $A \cup A = A$,
- (v) $A \subseteq A \cup B$,
- (vi) $B \subseteq A \cup B$,

- (vii) jeżeli $A \subseteq C$ i $B \subseteq C$, to $A \cup B \subseteq C$,
- (viii) jeżeli $A \subseteq B$ i $C \subseteq D$, to $A \cup C \subseteq B \cup D$,
- (ix) $A \subseteq B$ wtedy i tylko wtedy, gdy $A \cup B = B$.

Dowód. Dla przykładu udowodnimy punkt (vii). Załóżmy, że zachodzą inkluzje $A \subseteq C$ i $B \subseteq C$. Chcemy pokazać, że wtedy $A \cup B \subseteq C$. Niech $x \in A \cup B$. Oznacza to, że $x \in A$ lub $x \in B$. Jeżeli $x \in A$, to z pierwszej założonej inkluzji wynika, że $x \in C$. Jeżeli $x \in B$, to z drugiej założonej inkluzji wynika, że $x \in C$. Pokazaliśmy zatem, że jeśli $x \in A \cup B$, to $x \in C$. $\square$

2.1.2. Iloczyn zbiorów.

Definicja 2.6 (Iloczyn zbiorów). *Iloczynem (częścią wspólną) zbiorów A i B (ozn. $A \cap B$) nazywamy zbiór tych elementów, które należą do zbioru A i do zbioru B . Innymi słowy $x \in A \cap B$ wtedy i tylko wtedy, gdy $x \in A \wedge x \in B$.*

Twierdzenie 2.7. *Dla dowolnych zbiorów A, B, C, D zachodzi:*

- (i) $A \cap B = B \cap A$,
- (ii) $(A \cap B) \cap C = A \cap (B \cap C)$,
- (iii) $\emptyset \cap A = \emptyset$,
- (iv) $A \cap A = A$,
- (v) $A \cap B \subseteq A$,
- (vi) $A \cap B \subseteq B$,
- (vii) jeżeli $A \subseteq B$ i $A \subseteq C$, to $A \subseteq B \cap C$,
- (viii) jeżeli $A \subseteq B$ i $C \subseteq D$, to $A \cap C \subseteq B \cap D$,
- (ix) $A \subseteq B$ wtedy i tylko wtedy, gdy $A \cap B = A$.

Dowód. Dla przykładu udowodnimy punkt (ii).

$$\begin{aligned} x \in (A \cap B) \cap C &\leftrightarrow x \in (A \cap B) \wedge x \in C \leftrightarrow (x \in A \wedge x \in B) \wedge x \in C \\ &\leftrightarrow x \in A \wedge (x \in B \wedge x \in C) \leftrightarrow x \in A \wedge x \in (B \cap C) \\ &\leftrightarrow x \in A \cap (B \cap C). \end{aligned}$$

$\square$

Definicja 2.8 (Zbiory rozłączne). O dwóch zbiorach mówimy, że są *rozłączne*, gdy $A \cap B = \emptyset$.

Twierdzenie 2.9 (Prawa dla sum i iloczynów zbiorów). *Dla dowolnych zbiorów A, B, C , zachodzi:*

- (i) $A \cap (A \cup B) = A$,
- (ii) $(A \cap B) \cup B = B$,
- (iii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
- (iv) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

2.1.3. Różnica zbiorów.

Definicja 2.10 (Różnica zbiorów). *Różnicą zbiorów A i B (ozn. $A \setminus B$) nazywamy zbiór tych elementów, które należą do A , a nie należą do B . Innymi słowy, $x \in A \setminus B$ wtedy i tylko wtedy, gdy $x \in A \wedge x \notin B$.*

Twierdzenie 2.11. *Dla dowolnych zbiorów A, B, C, D zachodzi:*

- (i) $A \setminus B \subseteq A$,
- (ii) jeżeli $A \subseteq B$ i $C \subseteq D$, to $A \setminus D \subseteq B \setminus C$,
- (iii) jeżeli $C \subseteq D$, to $A \setminus D \subseteq A \setminus C$,
- (iv) $A \subseteq B$ wtedy i tylko wtedy, gdy $A \setminus B = \emptyset$,
- (v) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$,
- (vi) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$,
- (vii) $A \cup (B \setminus A) = A \cup B$,
- (viii) jeżeli $A \subseteq B$, to $A \cup (B \setminus A) = B$,
- (ix) $A \setminus (A \setminus B) = A \cap B$,
- (x) $A \setminus (B \cup C) = (A \setminus B) \setminus C$.

Dowód. Dla przykładu udowodnimy punkt (x).

$$\begin{aligned}
x \in A \setminus (B \cup C) &\leftrightarrow x \in A \wedge \neg(x \in (B \cup C)) \leftrightarrow x \in A \wedge \neg(x \in B \vee x \in C) \\
&\leftrightarrow x \in A \wedge (\neg x \in B \wedge \neg x \in C) \leftrightarrow (x \in A \wedge \neg x \in B) \wedge \neg x \in C \\
&\leftrightarrow x \in (A \setminus B) \wedge \neg x \in C \leftrightarrow x \in (A \setminus B) \setminus C.
\end{aligned}$$

□

2.1.4. Dopełnienie zbioru. Zazwyczaj ograniczamy się do zbiorów, które są podzbiórmi pewnego ustalonego zbioru, zwanego *przestrzenią*.

Definicja 2.12 (Dopełnienie zbioru). *Dopełnieniem* zbioru A (ozn. A') w przestrzeni X nazywamy zbiór tych elementów z przestrzeni, które nie należą do A . Innymi słowy, $x \in A'$ wtedy i tylko wtedy, gdy $x \in X \setminus A$.

Twierdzenie 2.13. *Dla dowolnych podzbiorów A i B przestrzeni X zachodzi:*

- (i) $X \cap A = A$,
- (ii) $X \cup A = X$,
- (iii) $X' = \emptyset$,
- (iv) $\emptyset' = X$,
- (v) $(A')' = A$,
- (vi) $A \subseteq B$ wtedy i tylko wtedy, gdy $B' \subseteq A'$,
- (vii) $A \cup A' = X$,
- (viii) $A \cap A' = \emptyset$,
- (ix) $(A \cup B)' = A' \cap B'$,
- (x) $(A \cap B)' = A' \cup B'$,
- (xi) $A \setminus B = A \cap B'$,
- (xii) $A \setminus B = (A' \cup B)'$,
- (xiii) $A \subseteq B$ wtedy i tylko wtedy, gdy $A \cap B' = \emptyset$,
- (xiv) $A \subseteq B$ wtedy i tylko wtedy, gdy $A' \cup B = X$.

2.1.5. Różnica symetryczna.

Definicja 2.14 (Różnica symetryczna). *Różnicą symetryczną* zbiorów A i B (ozn. $A \div B$) nazywamy sumę zbioru elementów, które należą do A i nie należą do B i zbioru elementów, które należą do B i nie należą do A . Innymi słowy, $x \in A \div B$ wtedy i tylko wtedy, gdy $x \in (A \setminus B) \cup (B \setminus A)$.

Twierdzenie 2.15. *Dla dowolnych zbiorów A , B i C zachodzi:*

- (i) $A \div B = \emptyset$ wtedy i tylko wtedy, gdy $A = B$,
- (ii) $A \div B = B \div A$,
- (iii) $(A \div B) \div C = A \div (B \div C)$,
- (iv) $A \cap (B \div C) = (A \cap B) \div (A \cap C)$,
- (v) $A \div \emptyset = A$.

Przykład 2.16. Niech $X = \{1, 2, 3, 4, 5, \{1, 2\}, \emptyset\}$ będzie przestrzenią oraz niech

$$\begin{aligned}
A &= \{1, 2, 3, 4\}, \\
B &= \{3, 4, 5\}, \\
C &= \{\{1, 2\}, 3, 2\}, \\
D &= \{\emptyset, 2\}, \\
E &= \emptyset.
\end{aligned}$$

Wtedy

$$\begin{array}{lll}
A \cup B = \{1, 2, 3, 4, 5\} & A \cup C = \{1, 2, 3, \{1, 2\}\} & A \cup D = \{1, 2, 3, 4, \{\emptyset\}\} \\
A \cap B = \{3\} & A \cap C = \{2, 3\} & A \cup E = \{1, 2, 3, 4\} \\
A \setminus B = \{1, 2\} & A \setminus C = \{1, 4\} & C \cap D = \{2\} \\
B \setminus A = \{5\} & C \setminus A = \{\{1, 2\}\} & C \cap E = \emptyset \\
A \div B = \{1, 2, 5\} & A \div C = \{1, 4, \{1, 2\}\} & C \setminus D = \{\{1, 2\}, 3\} \\
A' = \{5, \{1, 2\}, \emptyset\} & (A \cup B)' = \{\{1, 2\}, \emptyset\} & \\
E \in D & A \cup B \cup C = X \setminus \{\emptyset\} &
\end{array}$$

2.1.6. Zbiór potęgowy. Często rozważamy zbiory, których elementy również są zbiorami. Takie zbiory nazywamy *rodzinami* zbiorów. W szczególności wyróżniamy rodzinę wszystkich podzbiorów danego zbioru.

Definicja 2.17 (Zbiór potęgowy). Dla zbioru X definiujemy jego *zbiór potęgowy* $\mathcal{P}(X)$ jako zbiór wszystkich podzbiorów x . Innymi słowy, $A \in \mathcal{P}(X)$ wtedy i tylko wtedy, gdy $A \subseteq X$.

Przykład 2.18. Zbiór $A = \{a, b, c\}$ ma 8 podzbiorów:

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A\},$$

natomiast zbiór $B = \{\emptyset, \{\emptyset\}\}$ ma 4 podzbiory:

$$\mathcal{P}(B) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, B\}.$$

Twierdzenie 2.19. Dla dowolnych zbiorów X, Y zachodzi:

- (i) $\mathcal{P}(X) \neq \emptyset$,
- (ii) jeżeli $X \subseteq Y$, to $\mathcal{P}(X) \subseteq \mathcal{P}(Y)$,
- (iii) jeżeli $A, B \in \mathcal{P}(X)$, to $A \cup B, A \cap B, A \setminus B, A \div B \in \mathcal{P}(X)$.

Twierdzenie 2.20. Jeżeli zbiór X ma n elementów, to wtedy zbiór $\mathcal{P}(X)$ ma 2^n elementów.

Dowód. Niech $X = \{a_1, a_2, \dots, a_n\}$. Niech A będzie podzbiorem zbioru X . Dla zbioru A definiujemy ciąg $e^A = (e_1^A, \dots, e_n^A)$ w następujący sposób:

$$e_i^A = \begin{cases} 1 & \text{gdy } a_i \in A \\ 0 & \text{gdy } a_i \notin A \end{cases}.$$

Każdemu podzbiorem zbioru X odpowiada dokładnie jeden ciąg zero-jedynkowy o długości n . Zatem wszystkich podzbiorów zbioru n -elementowego jest dokładnie tyle, ile ciągów zero-jedynkowych o długości n , czyli 2^n . $\square$

2.1.7. Iloczyn kartezjański.

Definicja 2.21 (Para). Mając dane dwa elementy a i b definiujemy *parę uporządkowaną* (a, b) w następujący sposób:

$$(a, b) := \{\{a\}, \{a, b\}\}.$$

Podobnie definiujemy *uporządkowaną trójkę* (a, b, c) :

$$(a, b, c) := (a, (b, c)).$$

W ogólności, dla każdego $n \in \mathbb{N}_+$, definiujemy *uporządkowaną n -tkę*:

$$(a_1, a_2, \dots, a_n) := (a_1, (a_2, \dots, a_{n-1}, a_n)).$$

Twierdzenie 2.22. Niech dane będą dwie pary (a, b) oraz (c, d) . Wtedy

$$(a, b) = (c, d) \text{ wtedy i tylko wtedy, gdy } a = c \text{ oraz } b = d$$

Dowód. Zgodnie z definicją pary, $(a, b) = (c, d)$ wtedy i tylko wtedy, gdy $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. Rozważmy dwa przypadki.

- a) Niech $a = b$. Wtedy $\{\{a\}, \{a, b\}\} = \{\{a\}\}$. Zatem $\{c\} = \{a\}$ oraz $\{c, d\} = \{a\}$. Wtedy $c = a$ oraz $d = c = a$. Zatem $(a, b) = (a, a) = (c, d)$.
- b) Niech $a \neq b$. Wtedy mamy dwie możliwości.

- (i) $\{c\} = \{a, b\}$ i $\{a\} = \{c, d\}$. Ponieważ jednak $a \neq b$, zatem zbiór $\{a, b\}$ ma dwa różne elementy, a zbiór $\{c\}$ jeden element. Sprzeczność.
- (ii) $\{c\} = \{a\}$ i $\{a, b\} = \{c, d\}$. Wtedy $a = c$. Czyli $\{a, b\} = \{a, d\}$. Ponieważ $a \neq b$ oraz zbiór $\{a, b\}$ ma dwa różne elementy, zatem $a \neq d$. Z definicji równości zbioru dostajemy, że $b = d$. $\square$

Definicja 2.23 (Iloczyn kartezjański). *Iloczynem (produktem) kartezjańskim* zbiorów A i B (ozn. $A \times B$) nazywamy zbiór uporządkowanych par (a, b) takich, że $a \in A$ oraz $b \in B$. Innymi słowy, $(a, b) \in A \times B$ wtedy i tylko wtedy, gdy $a \in A$ i $b \in B$.

Iloczyn kartezjański możemy uogólnić na dowolne $n \in \mathbb{N}_+$ zbiorów:

$$A_1 \times A_2 \times \dots \times A_n := \{(a_1, a_2, \dots, a_n) : a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n\}.$$

Przykład 2.24.

- (a) Zbiór liczb zespolonych $\mathbb{C}$ jest iloczynem kartezjańskim $\mathbb{R} \times \mathbb{R}$.
- (b) Niech $A = \{1, 2, 3\}$ oraz $B = \{a, b\}$. Wtedy

$$\begin{aligned} A \times B &= \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\} \\ &\neq \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\} = B \times A. \end{aligned}$$

- (c) Walec to iloczyn kartezjański koła (podstawy) i odcinka (wysokości).
- (d) Powierzchnia torusa jest iloczynem kartezjańskim dwóch okręgów.

Twierdzenie 2.25. (i) $A \times (B \cup C) = (A \times B) \cup (A \times C)$,

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

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

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

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

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

(vii) jeżeli $C \neq \emptyset$, to $A \subseteq B \Leftrightarrow (A \times C) \subseteq (B \times C)$,

(viii) jeżeli $C \neq \emptyset$, to $A \subseteq B \Leftrightarrow (C \times A) \subseteq (C \times B)$.

Przykład 2.26. Z faktu, że $(A \times C) \subseteq (B \times C)$ nie musi wynikać, że $A \subseteq B$. Gdy $C = \emptyset$, to $A \times C = B \times C = \emptyset$ dla dowolnych dwóch zbiorów A i B . Zatem i dla takich, dla których $A \not\subseteq B$.

Co więcej, nie jest prawdą, że $C \times A = C \times B$ implikuje równość zbiorów A i B . Znowu biorąc za C zbiór pusty dostajemy pierwszą z równości, druga natomiast nie jest prawdziwa.

Twierdzenie 2.27. Jeżeli zbiór A ma n elementów i zbiór B ma m elementów, to zbiór $A \times B$ ma $n \cdot m$ elementów.

Dowód. Niech m będzie dowolną liczbą naturalną oraz $Y = \{y_1, \dots, y_m\}$. Udowodnimy twierdzenie za pomocą indukcji matematycznej ze względu na n .

Niech $n = 0$. Wtedy $X = \emptyset$, a zatem $\emptyset \times Y = \emptyset$. Zbiór pusty nie ma elementów, czyli rzeczywiście składa się z $0 \cdot m = 0$ elementów. Niech $n = 1$. Wtedy $X = \{x_1\}$ i iloczyn kartezjański zbiorów X i Y ma postać $\{(x_1, y_1), \dots, (x_1, y_m)\}$, czyli rzeczywiście składa się z $1 \cdot m = m$ elementów.

Założmy, że dla pewnego $n \in \mathbb{N}$ jeżeli zbiór X składa się z n elementów, to $X \times Y$ składa się z $n \cdot m$ elementów. Rozważmy zbiór $X = \{x_1, \dots, x_n, x_{n+1}\}$. Tworzymy iloczyn $X \times Y$. Powstały zbiór możemy podzielić na dwa rozłączne podzbiory takie, że do pierwszego z nich należą pary (x_i, y_j) dla $i \leq n$, $j \leq m$, natomiast do drugiego należą pary (x_{n+1}, y_j) dla $j \leq m$. Na mocy założenia indukcyjnego pierwszy z tych zbiorów składa się z $n \cdot m$ elementów, drugi natomiast ma m elementów. Zatem cały iloczyn $X \times Y$ składa się z $n \cdot m + m = (n+1) \cdot m$ elementów. $\square$

2.2. UOGÓLNIONE DZIAŁANIA NA ZBIORACH

Definicja 2.28 (Indeksowana rodzina zbiorów). Niech X, T będą niepustymi zbiorami. Indeksowaną rodziną podzbiorów zbioru X o indeksach ze zbioru T nazywamy dowolną funkcję $f: T \rightarrow \mathcal{P}(X)$.

Funkcja f przyporządkowuje indeksowi t ze zbioru T pewien podzbiór zbioru X , który będziemy oznaczać przez X_t . Innymi słowy, $f(t) = X_t$ dla $t \in T$. Rodzinę indeksowaną będziemy oznaczać przez $(X_t)_{t \in T}$.

Przykład 2.29.

- (i) Niech $T = \mathbb{N}_+$, $X_n = \{x \in \mathbb{R} : 1 \leq x \leq 1 + \frac{1}{n}\}$.
- (ii) Niech $T = \mathbb{R}$, $Y_t = \{y \in \mathbb{R} : y^2 > t^2\}$.

Definicja 2.30 (Suma indeksowana). Sumą indeksowaną rodziny $(X_t)_{t \in T}$ nazywamy zbiór tych elementów, które należą do któregoś ze zbiorów X_t . Innymi słowy,

$$x \in \bigcup_{t \in T} X_t \text{ wtedy i tylko wtedy, gdy istnieje } t \in T \text{ takie, że } x \in X_t.$$

Przykład 2.31.

- (a) $\bigcup_{n \in \mathbb{N}_+} \{x \in \mathbb{R} : 1 \leq x \leq 1 + \frac{1}{n}\} = [1, 2]$,
- (b) $\bigcup_{t \in \mathbb{R}} \{y \in \mathbb{R} : y^2 > t^2\} = \mathbb{R} \setminus \{0\}$.

Definicja 2.32 (Iloczyn indeksowany). Iloczynem indeksowanym rodziny $(X_t)_{t \in T}$ nazywamy zbiór tych elementów, które należą do każdego ze zbiorów X_t . Innymi słowy,

$$x \in \bigcap_{t \in T} X_t \text{ wtedy i tylko wtedy, gdy dla każdego } t \in T \text{ zachodzi } x \in X_t.$$

Przykład 2.33.

- (a) $\bigcap_{n \in \mathbb{N}_+} \{x \in \mathbb{R} : 1 \leq x \leq 1 + \frac{1}{n}\} = \{1\}$,
- (b) $\bigcap_{t \in \mathbb{R}} \{y \in \mathbb{R} : y^2 > t^2\} = \emptyset$.

Twierdzenie 2.34. Dla dowolnej rodziny indeksowanej $(A_t)_{t \in T}$ zachodzi:

- (a) $\bigcap_{t \in T} A_t \subseteq A_t \subseteq \bigcup_{t \in T} A_t$ dla każdego $t \in T$,
- (b) jeżeli dla każdego $t \in T$ zachodzi inkluzja $A_t \subseteq A$, to $\bigcup_{t \in T} A_t \subseteq A$,
- (c) jeżeli dla każdego $t \in T$ zachodzi inkluzja $A \subseteq A_t$, to $A \subseteq \bigcap_{t \in T} A_t$.

Twierdzenie 2.35. Dla dowolnych rodzin indeksowanych $(A_t)_{t \in T}$ oraz $(B_t)_{t \in T}$ takich, że $A_t \subseteq B_t$ dla każdego $t \in T$ zachodzi:

- (a) $\bigcup_{t \in T} A_t \subseteq \bigcup_{t \in T} B_t$,
- (b) $\bigcap_{t \in T} A_t \subseteq \bigcap_{t \in T} B_t$.

Twierdzenie 2.36. Dla dowolnego zbioru A i rodzin indeksowanych $(A_t)_{t \in T}$, $(B_t)_{t \in T}$ zachodzi:

- (a) $A \cup \bigcup_{t \in T} A_t = \bigcup_{t \in T} (A \cup A_t)$,
- (b) $A \cup \bigcap_{t \in T} A_t = \bigcap_{t \in T} (A \cup A_t)$,
- (c) $A \cap \bigcup_{t \in T} A_t = \bigcup_{t \in T} (A \cap A_t)$,
- (d) $A \cap \bigcap_{t \in T} A_t = \bigcap_{t \in T} (A \cap A_t)$,
- (e) $\bigcup_{t \in T} A_t \cup \bigcup_{t \in T} B_t = \bigcup_{t \in T} (A_t \cup B_t)$,
- (f) $\bigcap_{t \in T} A_t \cap \bigcap_{t \in T} B_t = \bigcap_{t \in T} (A_t \cap B_t)$,
- (g) $\bigcup_{t \in T} A_t \cap \bigcup_{t \in T} B_t \supseteq \bigcup_{t \in T} (A_t \cap B_t)$,
- (h) $\bigcap_{t \in T} A_t \cup \bigcap_{t \in T} B_t \subseteq \bigcap_{t \in T} (A_t \cup B_t)$,
- (i) $A \setminus \bigcup_{t \in T} A_t = \bigcap_{t \in T} (A \setminus A_t)$,
- (j) $A \setminus \bigcap_{t \in T} A_t = \bigcup_{t \in T} (A \setminus A_t)$.

Uwaga 2.37. Kontrprzykład na równość w punktach (g) i (h).

Niech $A_n = \{x \in \mathbb{R} : x < n\}$ oraz $B_n = \{x \in \mathbb{R} : x \geq n\}$. Wtedy $\bigcup_{n \in \mathbb{N}} (A_n \cap B_n) = \emptyset$, natomiast $\bigcup_{n \in \mathbb{N}} A_n = \bigcup_{n \in \mathbb{N}} B_n = \mathbb{R}$. Z drugiej strony, $\bigcap_{n \in \mathbb{N}} A_n = \bigcap_{n \in \mathbb{N}} B_n = \emptyset$, ale $\bigcap_{n \in \mathbb{N}} (A_n \cup B_n) = \mathbb{R}$.

Definicja 2.38 (Suma uogólniona). Sumą uogólnioną rodziny zbiorów $\mathcal{A}$ nazywamy zbiór $\bigcup \mathcal{A}$ tych elementów, które należą do co najmniej jednego ze zbiorów z rodziny $\mathcal{A}$. Innymi słowy,

$$a \in \bigcup \mathcal{A} \leftrightarrow \exists_A (A \in \mathcal{A} \wedge a \in A).$$

Definicja 2.39 (Iloczyn uogólniony). *Iloczynem uogólnionym* rodziny zbiorów $\mathcal{A}$ nazywamy zbiór $\bigcap \mathcal{A}$ tych elementów, które należą do każdego ze zbiorów z rodziny $\mathcal{A}$. Innymi słowy,

$$a \in \bigcap \mathcal{A} \leftrightarrow \forall_A (A \in \mathcal{A} \rightarrow a \in A).$$

Przykład 2.40. Niech $\mathcal{A} = \{\{1, 2\}, \{2, 3\}, \{2, 4, 5\}\}$. Wtedy

$$\bigcup \mathcal{A} = \{1, 2, 3, 4, 5\}, \quad \bigcap \mathcal{A} = \{2\}.$$

Przykład 2.41. Dla każdego zbioru A zachodzi równość $A = \bigcup \mathcal{P}(A)$.

„ $\supseteq$ ”

$$a \in \bigcup \mathcal{P}(A) \leftrightarrow \exists_B (B \in \mathcal{P}(A) \wedge a \in B) \leftrightarrow \exists_B (B \subseteq A \wedge a \in B) \rightarrow \exists_B (a \in A) \leftrightarrow a \in A.$$

„ $\subseteq$ ”

$$a \in A \leftrightarrow \{a\} \subseteq A \leftrightarrow \{a\} \in \mathcal{P}(A) \rightarrow \exists_B (B \in \mathcal{P}(A) \wedge a \in B) \leftrightarrow a \in \bigcup \mathcal{P}(A).$$

Przykład 2.42. Pokażemy, że $\bigcap \bigcap (a, b) = a$. Przypomnijmy, że $(a, b) = \{\{a\}, \{a, b\}\}$. Zatem

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

Definicja 2.43. Niech $(A_t)_{t \in T}$ będzie rodziną indeksowaną podzbiorów przestrzeni X . *Produkt uogólniony* zbiorów rodziny $(A_t)_{t \in T}$ nazywamy zbiór wszystkich funkcji $f: T \rightarrow \bigcup_{t \in T} A_t$ takich, że $f(t) \in A_t$ dla każdego $t \in T$. Zbiór ten oznaczamy przez $\prod_{t \in T} A_t$.

W szczególności, jeżeli dla każdego $t \in T$ mamy $A_t = A \subseteq X$, to produkt $\prod_{t \in T} A_t$ jest zbiorem wszystkich funkcji $f: T \rightarrow A$. Zamiast $\prod_{t \in T} A_t$ piszemy wtedy po prostu A^T .

Jeżeli $T = \mathbb{N}$, to produkt uogólniony będziemy oznaczać przez $\prod_{n=0}^{\infty} A_n$.

Przykład 2.44.

1. Niech $T = \mathbb{R}$. Zdefiniujmy $A_t = \{x \in \mathbb{Z} : x > t\}$. Wtedy $\bigcup_{t \in T} A_t = \mathbb{Z}$. Zgodnie z definicją mamy

$$\prod_{t \in T} A_t = \{f \in \mathbb{Z}^{\mathbb{R}} : \forall t \in T \ f(t) \in A_t\}.$$

Do powyższego zbioru należy na przykład funkcja $f(t) = \lfloor t \rfloor + 3$: dla każdego $t \in T$ zachodzi nierówność $\lfloor t \rfloor + 1 > t$, czyli $f(t) \in A_t$. Jeżeli natomiast za każde A_t przyjmiemy $\mathbb{Z}$, to wtedy $\prod_{t \in T} A_t = \mathbb{Z}^{\mathbb{R}}$ jest zbiorem wszystkich funkcji $f: \mathbb{R} \rightarrow \mathbb{Z}$.

2. Niech $(A_n)_{n \in \mathbb{N}}$ będzie indeksowaną rodziną zbiorów takich, że $A_n = \{0, \dots, n\}$ dla każdego $n \in \mathbb{N}$. Wtedy produkt $\prod_{n=0}^{\infty} A_n$ jest zbiorem ciągów $(a_n)_{n \in \mathbb{N}}$ takich, że dla każdego $n \in \mathbb{N}$ zachodzi $a_n \leq n$.

3. Niech $(A_n)_{n \in \mathbb{N}}$ będzie indeksowaną rodziną zbiorów takich, że $A_n = \{0, 1\}$. Wtedy $\prod_{n=0}^{\infty} A_n = \{0, 1\}^{\mathbb{N}}$, czyli produkt jest zbiorem nieskończonych ciągów zero-jedynkowych.

Część 3. Relacje

Definicja 3.1. Niech dane będą dwa zbiory X i Y . Dowolny podzbiór $R \subseteq X \times Y$ nazywamy *relacją* określoną na iloczynie kartezjańskim $X \times Y$.

Często zamiast pisać $(x, y) \in R$ będziemy używać oznaczenia xRy , co odczytujemy jako „ x jest w relacji R z y ”. Relacje definiujemy najczęściej podając formę zdaniową dwóch zmiennych $p(x, y)$ określającą zbiór R , czyli $xRy \leftrightarrow p(x, y)$.

Przykład 3.2.

(a) Niech $X = \{1, 3, 6, 17\}$, $Y = \{3, 5\}$. Wtedy $R = \{(1, 3), (1, 5), (3, 5), (17, 3)\}$ jest relacją na $X \times Y$.

- (b) Niech $X = Y$ będzie zbiorem ludzi. Wprowadzamy relację R w następujący sposób: xRy wtedy i tylko wtedy, gdy x jest wyższy od y .
- (c) Niech $X = Y = \mathbb{R}$. Wtedy $R = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ jest relacją.
- (d) Niech $X = Y = \mathbb{N}$. Wprowadzamy na $\mathbb{N}^2$ relację podzielności: xRy wtedy i tylko wtedy, gdy x jest dzielnikiem y .
- (e) Dla zbioru X definiujemy relację $1_X \subseteq X^2$ w następujący sposób: $1_X = \{(x, x) : x \in X\}$.
- (f) Dla dowolnego zbioru X zbiór X^2 jest relacją.

3.1. DZIEDZINA, PRZECIWDZIEDZINA I OPERACJE NA RELACJACH

Definicja 3.3. Dziedzina $D(R)$ relacji $R \subseteq X \times Y$ nazywamy zbiór poprzedników par uporządkowanych należących do tej relacji, czyli $D(R) = \{x \in X : \exists y \in Y \ xRy\}$.

Przeciwdziedzina $D^*(R)$ relacji $R \subseteq X \times Y$ nazywamy zbiór następników par uporządkowanych należących do tej relacji, czyli $D^*(R) = \{y \in Y : \exists x \in X \ xRy\}$.

Przykład 3.4. Dziedzina dla relacji z przykładu 3.2(a) jest zbiór $\{1, 3, 17\}$, natomiast przeciwdziedzina $\{3, 5\}$. W przykładzie 3.2(c) dziedzina i przeciwdziedzina są równe $[-1, 1]$. W przykładzie 3.2(d) dziedzina to $\mathbb{N}_+$, natomiast przeciwdziedzina to $\mathbb{N}$.

Relacje są zbiorami, zatem możemy na nich wykonywać standardowe działania (suma, iloczyn, itd.).

Twierdzenie 3.5. Dla dowolnych relacji $S, T \subseteq X \times Y$ zachodzi:

- (i) $D(S \cup T) = D(S) \cup D(T)$,
- (ii) $D^*(S \cup T) = D^*(S) \cup D^*(T)$,
- (iii) $D(S \cap T) \subseteq D(S) \cap D(T)$,
- (iv) $D^*(S \cap T) \subseteq D^*(S) \cap D^*(T)$.

Dowód.

(i)

$$\begin{aligned}
 x \in D(S \cup T) &\leftrightarrow \exists y \in Y \ x(S \cup T)y \leftrightarrow \exists y (y \in Y \wedge (xSy \vee xTy)) \\
 &\leftrightarrow \exists y ((y \in Y \wedge xSy) \vee (y \in Y \wedge xTy)) \\
 &\leftrightarrow \exists y (y \in Y \wedge xSy) \vee \exists y (y \in Y \wedge xTy) \\
 &\leftrightarrow x \in D(S) \vee x \in D(T) \leftrightarrow x \in D(S) \cup D(T).
 \end{aligned}$$

□

Przykład 3.6. W punktach (iii) i (iv) w Twierdzeniu 3.5 nie możemy zastąpić inkluzji równością. Niech $S = \{(1, 2), (1, 3), (2, 3)\}$ oraz $T = \{(1, 2), (2, 4)\}$. Wtedy $S \cap T = \{(1, 2)\}$. Mamy też $D(S) = \{1, 2\}$ oraz $D(T) = \{1, 2\}$. Zatem $D(S) \cap D(T) = \{1, 2\} \neq \{1\} = D(S \cap T)$.

Definicja 3.7 (Złożenie relacji). Niech $S \subseteq X \times Y$ oraz $T \subseteq Y \times Z$. Wtedy możemy zdefiniować złożenie relacji $T \circ S \subseteq X \times Z$ w następujący sposób:

$$T \circ S = \{(x, z) \in X \times Z : \exists y \in Y ((x, y) \in S \wedge (y, z) \in T)\}.$$

Definicja 3.8 (Relacja odwrotna). Relacją odwrotną do relacji $R \subseteq X \times Y$ nazywamy relację R^{-1} zdefiniowaną w następujący sposób:

$$R^{-1} = \{(y, x) \in Y \times X : (x, y) \in R\}.$$

Przykład 3.9. Niech $A = \{0, 1, 2\}$, $B = \{2, 3, 4\}$ oraz $C = \{3, 4, 5\}$. Zdefiniujmy $R \subseteq A \times B$ oraz $S \subseteq B \times C$ następująco:

$$R = \{(0, 0), (0, 1), (1, 2), (1, 3), (2, 4)\}, \quad S = \{(2, 3), (3, 4), (4, 5), (2, 5)\}.$$

Wtedy

$$A \times C \supseteq S \circ R = \{(1, 3), (1, 5), (1, 4), (2, 5)\},$$

$$B \times A \supseteq R^{-1} = \{(0, 0), (1, 0), (2, 1), (3, 1), (4, 2)\}.$$

Twierdzenie 3.10. Dla dowolnych relacji $R \subseteq X \times Y$, $S, S_1, S_2 \subseteq Y \times Z$ oraz $T \subseteq Z \times U$ zachodzi:

- (i) $T \circ (S \circ R) = (T \circ S) \circ R$,
- (ii) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$,
- (iii) $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$,
- (iv) $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$,
- (v) $(R^{-1})^{-1} = R$,
- (vi) $(S_1 \cup S_2) \circ R = (S_1 \circ R) \cup (S_2 \circ R)$,
- (vii) $(S_1 \cap S_2) \circ R \subseteq (S_1 \circ R) \cap (S_2 \circ R)$.

Dowód. Dla przykładu pokażemy punkt (iv)

$$\begin{aligned} (x, y) \in (R \cap S)^{-1} &\leftrightarrow (y, x) \in R \cap S \leftrightarrow (y, x) \in R \wedge (y, x) \in S \\ &\leftrightarrow (x, y) \in R^{-1} \wedge (x, y) \in S^{-1} \leftrightarrow (x, y) \in R^{-1} \cap S^{-1} \end{aligned}$$

oraz punkt (vii)

$$\begin{aligned} (x, z) \in (S_1 \cap S_2) \circ R &\leftrightarrow \exists_{y \in Y} ((x, y) \in R \wedge (y, z) \in S_1 \cap S_2) \\ &\leftrightarrow \exists_{y \in Y} ((x, y) \in R \wedge (y, z) \in S_1 \wedge (y, z) \in S_2) \\ &\leftrightarrow \exists_{y \in Y} ((x, y) \in R \wedge (y, z) \in S_1 \wedge (x, y) \in R \wedge (y, z) \in S_2) \\ &\rightarrow \exists_{y \in Y} ((x, y) \in R \wedge (y, z) \in S_1) \wedge \exists_{y \in Y} ((x, y) \in R \wedge (y, z) \in S_2) \\ &\leftrightarrow (x, z) \in (S_1 \circ R) \wedge (x, z) \in (S_2 \circ R) \\ &\leftrightarrow (x, z) \in (S_1 \circ R) \cap (S_2 \circ R). \end{aligned} \quad \square$$

Uwaga 3.11. Pokażemy, że nie zawsze zachodzi równość $(S_1 \cap S_2) \circ R = (S_1 \circ R) \cap (S_2 \circ R)$. Niech $S_1 = \{(1, 3)\}$, $S_2 = \{(2, 3)\}$ oraz $R = \{(0, 1), (0, 2)\}$. Wtedy $S_1 \cap S_2 = \emptyset$, czyli $(S_1 \cap S_2) \circ R = \emptyset$. Ale $S_1 \circ R = \{(0, 3)\} = S_2 \circ R$, czyli $(S_1 \circ R) \cap (S_2 \circ R) = \{(0, 3)\} \neq \emptyset$.

3.2. RODZAJE RELACJI

Definicja 3.12. Niech $R \subseteq X \times X$.

1. R jest relacją *zwrotną* wtedy i tylko wtedy, gdy

$$\forall_{x \in X} xRx.$$

2. R jest relacją *antyzwrotną* wtedy i tylko wtedy, gdy

$$\forall_{x \in X} \neg xRx.$$

3. R jest relacją *symetryczną* wtedy i tylko wtedy, gdy

$$\forall_{x, y \in X} (xRy \rightarrow yRx).$$

4. R jest relacją *antysymetryczną* wtedy i tylko wtedy, gdy

$$\forall_{x, y \in X} (xRy \rightarrow \neg yRx).$$

5. R jest relacją *słabo antysymetryczną* wtedy i tylko wtedy, gdy

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

6. R jest relacją *przechodnią* wtedy i tylko wtedy, gdy

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

7. R jest relacją *spójną* wtedy i tylko wtedy, gdy

$$\forall_{x, y \in X} (xRy \vee yRx).$$

8. R jest relacją *słabo spójną* wtedy i tylko wtedy, gdy

$$\forall_{x, y \in X} (xRy \vee yRx \vee x = y).$$

9. R jest relacją *równoważności* wtedy i tylko wtedy, gdy jest zwrotna, symetryczna i przechodnia.
10. R jest relacją *quasi-porządku* (*praporządku*) wtedy i tylko wtedy, gdy jest zwrotna i przechodnia.
11. R jest relacją *częściowego porządku* wtedy i tylko wtedy, gdy jest zwrotna, antysymetryczna i przechodnia.
12. R jest relacją *porządku liniowego* wtedy i tylko wtedy, gdy jest częściowym porządkiem i jest spójna.

Przykład 3.13. Zbadać własności relacji:

- (a) Niech $X = \{1, 3, 6, 17\}$, $Y = \{3, 5\}$ oraz $R = \{(1, 3), (1, 5), (3, 5), (17, 3)\}$.
- (b) Niech $X = Y$ oraz niech xRy wtedy i tylko wtedy, gdy x jest wyższy od y .
- (c) Niech $X = Y = \mathbb{R}$ oraz $R = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$.
- (d) Niech $X = Y = \mathbb{N}$ oraz niech xRy wtedy i tylko wtedy, gdy x jest dzielnikiem y .
- (e) Dla dowolnego zbioru X definiujemy relację $1_X \subseteq X^2$ w następujący sposób: $1_X = \{(x, x) : x \in X\}$.
- (f) Dla dowolnego zbioru X relację pełną jako X^2 .

Relacje na zbiorach skończonych można reprezentować za pomocą tabelki za pomocą grafów skierowanych.

Przykład 3.14. Niech $A = B = \{0, 1, 2, 3\}$. Rozważmy relacje

$$R = \{(0, 0), (1, 1), (2, 2), (3, 3), (0, 2), (2, 0), (1, 3), (3, 1)\},$$

$$S = \{(0, 1), (1, 2), (0, 2), (0, 3), (1, 3)\},$$

$$T = \{(2, 0), (0, 3), (3, 1), (1, 1)\}.$$

Tabelki dla powyższych relacji wyglądają następująco:

R	0	1	2	3	S	0	1	2	3	T	0	1	2	3
0	+		+		0		+	+	+	0				+
1		+		+	1			+	+	1		+		
2	+		+		2					2	+			
3		+		+	3					3		+		

Narysować odpowiednie grafy.

Jeśli relacja jest zwrotna, to każdy element z przekątnej w tabelce musi należeć do relacji. Analogicznie, jeśli relacja jest antyzwrotna, to żaden element z przekątnej nie należy do relacji.

Jeśli relacja jest symetryczna, to tabelka jest symetryczna względem przekątnej. Analogicznie, jeśli relacja jest antysymetryczna, to żadne dwa elementy o współrzędnych (i, j) i (j, i) z tabelki nie mogą równocześnie należeć do relacji.

Twierdzenie 3.15. Niech $R \subseteq X \times X$. Wtedy

- (i) R jest relacją zwrotną wtedy i tylko wtedy, gdy $1_X \subseteq R$,
- (ii) R jest relacją symetryczną wtedy i tylko wtedy, gdy $R \subseteq R^{-1}$,
- (iii) R jest relacją przechodnią wtedy i tylko wtedy, gdy $R \circ R \subseteq R$.

Dowód.

- (i) Z definicji R jest relacją zwrotną wtedy i tylko wtedy, gdy dla każdego $x \in X$ para (x, x) należy do R . A to jest równoważne temu, że $1_X \subseteq R$.
- (ii) Z definicji R jest relacją symetryczną wtedy i tylko wtedy, gdy dla dowolnych dwóch elementów $x, y \in X$ jeżeli $(x, y) \in R$, to również $(y, x) \in R$. Ponieważ $(y, x) \in R$ jest równoważne temu, że $(x, y) \in R^{-1}$, zatem rzeczywiście dowolna para (x, y) z relacji R należy również do relacji R^{-1} , czyli $R \subseteq R^{-1}$.
- (iii) Z definicji R jest relacją przechodnią wtedy i tylko wtedy, gdy dla dowolnych trzech elementów $x, y, z \in X$ jeżeli $(x, y) \in R$ oraz $(y, z) \in R$, to również $(x, z) \in R$. Niech zatem $(x, y) \in R$ oraz $(y, z) \in R$. Oznacza to, że istnieje taki „pośrednik” pomiędzy x i z (jest nim y), że $(x, z) \in R \circ R$. Zatem $R \circ R \subseteq R$.

□

Wniosek 3.16. Relacja $R \subseteq X^2$ jest relacją równoważności wtedy i tylko wtedy, gdy $R = R \circ R^{-1} \cup 1_X$.

Dowód.

„ $\rightarrow$ ”: Niech R będzie relacją równoważności. Chcemy pokazać dwie inkluzje.

$\subseteq$: Niech $(x, y) \in R$. Ponieważ R jest symetryczna, to $(x, x) \in R^{-1}$. Czyli istnieje element pośredni pomiędzy x i y (jest nim x) taki, że $(x, y) \in R^{-1} \circ R$. Zatem $x \in R \circ R^{-1} \cup 1_X$.

$\supseteq$: Niech $(x, y) \in R \circ R^{-1} \cup 1_X$. Wtedy $(x, y) \in R \circ R^{-1}$ lub $(x, y) \in 1_X$. W drugim przypadku x musi być równe y , czyli $(x, y) = (x, x)$, a ta para należy do relacji R ze zwrotności R . Niech zatem $(x, y) \in R \circ R^{-1}$. Wtedy istnieje $z \in X$ taki, że $(x, z) \in R^{-1}$ oraz $(z, y) \in R$. Z symetrii relacji R mamy, że jest to równoważne temu, że istnieje $z \in X$ taki, że $(x, z) \in R$ oraz $(z, y) \in R$. Z przechodniości R dostajemy więc, że $(x, y) \in R$.

„ $\leftarrow$ ”: Niech $R = R \circ R^{-1} \cup 1_X$. Wtedy relacja R jest zwrotna, ponieważ $1_X \subseteq R$. Niech $(x, y) \in R$. Wtedy $(y, x) \in R^{-1}$. Ze zwrotności relacji R mamy, że $(x, x) \in R$. Zatem z tego, że $(y, x) \in R \circ R^{-1}$, czyli $(y, x) \in R$, co dowodzi symetrii relacji R . Ponieważ R jest symetryczna, zatem $R = R^{-1}$. W związku z tym $R \circ R = R \circ R^{-1} \subseteq R$, czyli R jest przechodnia. □

3.3. RELACJA RÓWNOWAŻNOŚCI I KLASA ABSTRAKCJI

Definicja 3.17. Niech $R \subseteq X$ będzie relacją równoważności. Definiujemy *klasę równoważności* (*abstrakcji*) elementu $x \in X$ w następujący sposób:

$$[x]_R = \{y \in X : xRy\}.$$

Element x nazywamy *reprezentantem* klasy $[x]_R$.

Zbiór klas równoważności relacji R nazywamy *zbiorem ilorazowym* i oznaczamy przez X/R . Czyli

$$X/R = \{[x]_R : x \in X\}.$$

Przykład 3.18.

1. Relacja $R \subseteq \mathbb{N}^2$ zdefiniowana następująco: $nRm \leftrightarrow 2|(n+m)$ jest relacją równoważności. Ma dwie klasy abstrakcji:

$$[0]_R = \{2k : k \in \mathbb{N}\} \text{ oraz } [1]_R = \{2k+1 : k \in \mathbb{N}\}.$$

2. Relacja $R \subseteq \mathbb{N}^2$ zdefiniowana następująco: $nRm \leftrightarrow 3|(n-m)$ jest relacją równoważności. Ma trzy klasy abstrakcji:

$$[0]_R = \{3k : k \in \mathbb{N}\}, [1]_R = \{3k+1 : k \in \mathbb{N}\} \text{ oraz } [2]_R = \{3k+2 : k \in \mathbb{N}\}.$$

3. Relacja $R \subseteq \mathbb{N}^2$ zdefiniowana następująco: $nRm \leftrightarrow 3|(n+m)$ nie jest relacją równoważności. Niech $n=1, m=2, k=1$. Wtedy nRm oraz mRk , ale nie jest prawdą, że nRk , zatem relacja nie jest przechodnia.
4. Niech $X = \{ax+b : a, b \in \mathbb{R}\}$, czyli X jest zbiorem prostych na płaszczyźnie $\mathbb{R}^2$. Relacja równoległości $\parallel$ określona na X^2 jest relacją równoważności. Relacja ta ma nieskończenie wiele klas abstrakcji, każda z nich jest postaci

$$[ax]_{\parallel} = \{ax+b : x \in \mathbb{R}\}.$$

5. Dla dowolnego zbioru X relacja 1_X jest relacją równoważności. Relacja ta ma tyle klas abstrakcji ile elementów jest w zbiorze X , ponieważ dla dowolnego elementu $x \in X$ mamy

$$[x]_{1_x} = \{x\}.$$

6. Dla dowolnego zbioru X relacja X^2 jest relacją równoważności. Relacja ta ma tylko jedną klasę abstrakcji, ponieważ wszystkie elementy są ze sobą w relacji: dla każdego elementu $x \in X$ mamy

$$[x]_{X^2} = X^2.$$

Uwaga 3.19. Dla dowolnej relacji $R \subseteq X^2$ i dowolnego elementu $x \in X$ klasa $[x]_R$ jest niepusta, ponieważ ze zwrotności R mamy, że $x \in [x]_R$. Zatem żadna klasa równoważności nie może być pusta.

Twierdzenie 3.20. Niech $R \subseteq X^2$ będzie relacją równoważności. Następujące warunki są równoważne:

- (i) $[x]_R \cap [y]_R \neq \emptyset$,
- (ii) $[x]_R = [y]_R$,
- (iii) xRy .

Dowód.

- (i) $\rightarrow$ (ii) Niech $[x]_R \cap [y]_R \neq \emptyset$. Istnieje wtedy taki element $z \in X$, że $z \in [x]_R \cap [y]_R$. Zatem xRz oraz yRz . Niech a będzie dowolnym elementem ze zbioru $[x]_R$. Wtedy

$$\begin{aligned} a \in [x]_R &\leftrightarrow xRa \leftrightarrow xRa \wedge xRz \wedge yRz \\ &\leftrightarrow aRx \wedge xRz \wedge zRy \leftrightarrow aRy \rightarrow a \in [y]_R. \end{aligned}$$

- (ii) $\rightarrow$ (iii) Niech $[x]_R = [y]_R$. Wiemy, że $x \in [x]_R$ oraz $y \in [y]_R$. Zatem x i y należą do tej samej klasy abstrakcji, a zatem xRy .
- (iii) $\rightarrow$ (i) Niech xRy . Wtedy $y \in [x]_R$. Ponadto wiemy, że $y \in [y]_R$, czyli $y \in [x]_R \cap [y]_R$, a zatem rzeczywiście $[x]_R \cap [y]_R \neq \emptyset$. □

Definicja 3.21. Niech $X \neq \emptyset$. Rodzinę $P \subseteq \mathcal{P}(\mathcal{P}(X))$ nazywamy rozkładem zbioru X , gdy:

1. $\forall A \in P \ A \neq \emptyset$,
2. $\bigcup P = X$,
3. $\forall A \in P \forall B \in P \ (A \neq B \rightarrow A \cap B = \emptyset)$.

Twierdzenie 3.22. Niech P będzie rozkładem zbioru X . Definiujemy relację R_P następująco:

$$xR_P y \leftrightarrow \exists A \in P \ (x \in A \wedge y \in A).$$

Wtedy:

- (i) relacja R_P jest relacją równoważności,
- (ii) $X/R_P = P$.

Dowód.

- (i) Relacja R_P jest zwrotna, ponieważ dla każdego elementu x musi istnieć zbiór $A \in P$, do którego x należy. Relacja R_P jest symetryczna, ponieważ koniunkcja jest przemienna. Pozostaje pokazać przechodniość relacji R_P . Niech $xR_P y$ oraz $yR_P z$. Wtedy istnieje zbiór $A \in P$, do którego należą x i y , oraz istnieje zbiór $B \in P$, do którego należą y i z . Zatem zbiór $A \cap B$ jest niepusty, co oznacza, że $A = B$. Zatem istnieje zbiór z podziału, do którego należą x i z .
- (ii) „ $\subseteq$ ”: Niech $A \in X/R_P$. Wtedy istnieje element $x \in X$ taki, że $A = [x]_{R_P}$. Niech B będzie zbiorem z rozkładu P takim, że $x \in B$. Ponieważ x należy do dokładnie jednego zbioru z podziału, więc $A = B$. Stąd $A \in P$.
- „ $\supseteq$ ”: Niech $A \in P$. Wtedy A jest zbiorem niepustym. Niech x będzie elementem z A . Wówczas $A = [x]_{R_P}$. □

Część 4. Funkcje

Definicja 4.1. Funkcją częściową prowadzącą ze zbioru X w zbiór Y nazywamy relację $f \subseteq X \times Y$ spełniającą warunek:

$$(1) \quad \forall x \in X \ \forall y, z \in Y \ ((x, y) \in f \wedge (x, z) \in f \rightarrow y = z).$$

Funkcją prowadzącą ze zbioru X w zbiór Y nazywamy funkcję częściową $f \subseteq X \times Y$ spełniającą warunek:

$$(2) \quad \forall x \in X \quad \exists y \in Y \quad (x, y) \in f.$$

Gdy $f \subseteq X \times Y$ jest funkcją częściową, to piszemy $f: X \dashrightarrow Y$, natomiast gdy f jest funkcją używamy zapisu $f: X \rightarrow Y$. Gdy f jest funkcją częściową i para (x, y) należy do f , to piszemy $f(x) = y$ i mówimy, że y jest wartością funkcji f dla argumentu x .

Przykład 4.2.

1. $R \subseteq \mathbb{R} \times \mathbb{R}$ taka, że $(x, y) \in R \leftrightarrow x^2 = y^2$ nie jest funkcją częściową.
2. $R \subseteq \mathbb{R}^+ \times \mathbb{R}^+$ taka, że $(x, y) \in R \leftrightarrow x^2 = y^2$ jest funkcją.
3. $R \subseteq \mathbb{N} \times \mathbb{Z}$ taka, że $(x, y) \in R \leftrightarrow x^2 = y^3$ jest funkcją częściową, ale nie jest funkcją.
4. $R \subseteq \mathbb{N} \times \mathbb{Z}$ taka, że $(x, y) \in R \leftrightarrow x^3 = y^2$ nie jest funkcją częściową.

Definicja 4.3 (Dziedzina i przeciwdziedzina funkcji). Niech dana będzie funkcja częściowa $f: X \dashrightarrow Y$. Dziedziną f nazywamy zbiór

$$\text{Dom}(f) = \{x \in X : \exists y \in Y \quad f(x) = y\}.$$

Gdy f jest funkcją, to oczywiście $\text{Dom}(f) = X$. Przeciwdziedziną lub zbiorem wartości f nazywamy zbiór

$$\text{Rg}(f) = \{y \in Y : \exists x \in X \quad f(x) = y\}.$$

Przykład 4.4.

1. Dla funkcji $f: \mathbb{N} \rightarrow \mathbb{N}$ takiej, że $f(n) = -2n - 2$ mamy $\text{Dom}(f) = \mathbb{N}$ oraz $\text{Rg}(f) = \{2k : k \in \mathbb{Z}_-\}$.
2. Dla funkcji częściowej $f: \mathbb{R} \rightarrow \mathbb{R}$ takiej, że $f(x) = |\tan x|$ mamy $\text{Dom}(f) = \mathbb{R} \setminus \{\frac{\pi}{2} + k\pi : k \in \mathbb{Z}\}$ oraz $\text{Rg}(f) = \mathbb{R}_+ \cup \{0\}$.

Definicja 4.5 (Obcięcie funkcji). Niech dana będzie funkcja $f: X \rightarrow Y$. Obcięciem funkcji f do zbioru $Z \subseteq X$ nazywamy funkcję $f|_Z: Z \rightarrow Y$ taką, że dla każdego $z \in Z$ zachodzi równość $f(x) = f|_Z(x)$.

Przykład 4.6. Niech $f: \mathbb{R} \rightarrow \mathbb{R}$ będzie zadana wzorem $f(x) = \lfloor x \rfloor$. Wtedy obcięcie funkcji f do zbioru liczb naturalnych $f|_{\mathbb{N}}: \mathbb{N} \rightarrow \mathbb{R}$ jest po prostu funkcją identycznościową $f|_{\mathbb{N}}(x) = 1_{\mathbb{N}} = x$.

Funkcje są relacjami, więc możemy zdefiniować operację złożenia funkcji.

Lemat 4.7. Złożenie funkcji $f: X \rightarrow Y$ oraz $g: Y \rightarrow Z$ jest funkcją ze zbioru X w zbiór Z .

Przykład 4.8.

1. $f: \mathbb{R} \ni x \mapsto \sin x \in [-1, 1]$, $g: [-1, 1] \ni x \mapsto \log_3 |x + 2| \in [0, 1]$, $g \circ f(x) = \dots$
2. $f: \mathbb{R} \ni x \mapsto e^x \in \mathbb{R}_+$, $g: \mathbb{R}_+ \ni x \mapsto \ln x \in \mathbb{R}$, ...

Definicja 4.9 (Obraz i przeciwobraz). Niech dana będzie funkcja $f: X \rightarrow Y$ oraz niech $A \subseteq X$ i $B \subseteq Y$.

1. Obrazem zbioru A przez funkcję f nazywamy zbiór

$$\vec{f}(A) = \{y \in Y : \exists x \in A \quad f(x) = y\}.$$

2. Przeciwobrazem zbioru B przez funkcję f nazywamy zbiór

$$\vec{f}^{-1}(B) = \{x \in X : \exists y \in B \quad f(x) = y\}.$$

Przykład 4.10. 1. Niech $f: \mathbb{R} \rightarrow \mathbb{R}$ będzie zadana wzorem $f(x) = x^2 - 7x + 10$. Wyznaczyć obraz zbiorów $\{1, 2, 3\}$, $[0, \infty)$ oraz $[-10, 0]$. Wyznaczyć przeciwobraz zbiorów $\{0, 10\}$, $\mathbb{Z}_-$ oraz $(-\infty, 0]$.

2. Niech $g: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ będzie zadana wzorem $g(x, y) = (2x + y, x - 2y)$. Wyznaczyć obraz prostej $2x + y - 3 = 0$. Wyznaczyć przeciwobraz okręgu $x^2 + y^2 = 1$.

Twierdzenie 4.11. Niech dana będzie funkcja $f: X \rightarrow Y$. Dla dowolnych zbiorów $A, B \subseteq X$ oraz $C, D \subseteq Y$ zachodzi:

- (i) $\vec{f}(A \cup B) = \vec{f}(A) \cup \vec{f}(B)$,
- (ii) $\vec{f}(A \cap B) \subseteq \vec{f}(A) \cap \vec{f}(B)$,
- (iii) $\vec{f}^{-1}(A \cup B) = \vec{f}^{-1}(A) \cup \vec{f}^{-1}(B)$,
- (iv) $\vec{f}^{-1}(A \cap B) = \vec{f}^{-1}(A) \cap \vec{f}^{-1}(B)$.

Uwaga 4.12. W punkcie (ii) inkluzji nie można zastąpić równością. Rozważmy funkcję $f: \{0, 1\} \ni x \mapsto 7 \in \mathbb{N}$ oraz zbiory $A = \{0\}$ i $B = \{1\}$. Wtedy $\vec{f}(A) = \vec{f}(B) = \{7\}$, ale $A \cap B = \emptyset$, więc $\vec{f}(A \cap B) = \emptyset$.

Twierdzenie 4.13. Niech dana będzie funkcja $f: X \rightarrow Y$. Dla dowolnych zbiorów $A \subseteq X$ oraz $B \subseteq \vec{f}(X)$ zachodzi:

- (i) $A \subseteq \vec{f}^{-1}(\vec{f}(A))$,
- (ii) $B = \vec{f}(\vec{f}^{-1}(B))$,
- (iii) jeżeli f jest iniekcją, to $A = \vec{f}^{-1}(\vec{f}(A))$.

Przykład 4.14. Jeśli funkcja f z powyższego twierdzenia nie jest iniekcją, to w punkcie (i) nie możemy zastąpić inkluzji równością. Niech bowiem x_1 i x_2 będą różnymi elementami zbioru X takimi, że $f(x_1) = f(x_2)$. Rozważmy zbiór $A = \{x_1\}$. Wtedy $\vec{f}(A) = \{f(x_1)\}$. Ale wtedy $\vec{f}^{-1}(\vec{f}(A)) = \vec{f}^{-1}(\{f(x_1)\}) \supseteq \{x_1, x_2\} \neq A$.

Definicja 4.15. Niech dana będzie funkcja $f: X \rightarrow Y$.

1. Jeżeli spełniony jest warunek

$$\forall_{x_1, x_2 \in X} (f(x_1) = f(x_2) \rightarrow x_1 = x_2),$$

to funkcję f nazywamy *iniekcją* lub funkcją *różnowartościową*. Piszemy wtedy $f: X \hookrightarrow Y$.

2. Jeżeli spełniony jest warunek

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

to funkcję f nazywamy *suriekcją* lub funkcją *na*. Piszemy wtedy $f: X \twoheadrightarrow Y$.

3. Jeżeli funkcja f jest iniekcją i suriekcją, to f nazywamy *bijekcją*.

Przykład 4.16. Sprawdzić, czy podane funkcje są iniekcjami, suriekcjami, bijekcjami. Wyznaczyć zbiór wartości. Jeśli funkcja jest bijekcją, wyznaczyć funkcję odwrotną.

- 1. Niech $f: \mathbb{R} \ni x \mapsto 3x + 2 \in \mathbb{R}$.
- 2. Niech $f: \mathbb{R} \ni x \mapsto \frac{x}{1+x^2} \in \mathbb{R}$.
- 3. Niech $f: \mathbb{N} \ni n \mapsto (-2)^n \in \mathbb{Z}$.
- 4. Niech $f: \mathbb{C} \ni z \mapsto \bar{z} \in \mathbb{C}$.
- 5. Niech $f: \mathbb{R} \ni x \mapsto 3^x - 2^x \in \mathbb{R}$.

Twierdzenie 4.17. Jeżeli funkcja jest bijekcją, to istnieje do niej funkcja odwrotna. Funkcja odwrotna do bijekcji jest bijekcją.

Twierdzenie 4.18. Złożenie iniekcji jest iniekcją. Złożenie suriekcji jest suriekcją. Złożenie bijekcji jest bijekcją.

Definicja 4.19 (Jądro odwzorowania). Dla dowolnej funkcji $f: X \rightarrow Y$ definiujemy relację $\text{Ker}(f) \subseteq X^2$, zwaną *jądrem* odwzorowania f w następujący sposób:

$$(x_1, x_2) \in \text{Ker}(f) \leftrightarrow f(x_1) = f(x_2).$$

Lemat 4.20. Dla dowolnej funkcji f relacja $\text{Ker}(f)$ jest relacją równoważności.

Dowód. Niech $f: X \rightarrow Y$. Dla dowolnego elementu $x \in X$ para (x, x) należy do $\text{Ker}(f)$, bo $f(x) = f(x)$. Niech $(x_1, x_2) \in \text{Ker}(f)$, czyli $f(x_1) = f(x_2)$. Wtedy oczywiście również $(x_2, x_1) \in \text{Ker}(f)$. Niech $(x_1, x_2), (x_2, x_3) \in \text{Ker}(f)$. Wtedy $f(x_1) = f(x_2)$ oraz $f(x_2) = f(x_3)$, czyli $f(x_1) = f(x_3)$, a zatem $(x_1, x_3) \in \text{Ker}(f)$. Relacja $\text{Ker}(f)$ jest więc zwrotna, symetryczna i przechodnia, a zatem jest relacją równoważności. $\square$

Twierdzenie 4.21 (O faktoryzacji). *Dla każdej funkcji $f: X \rightarrow Y$ istnieje zbiór Z oraz suriekcja $g: X \rightarrow Z$ i iniekcja $h: Z \rightarrow Y$ takie, że $f = h \circ g$.*

Dowód. Niech Z będzie zbiorem klas abstrakcji relacji $\text{Ker}(f)$. Definiujemy funkcję $g: X \rightarrow X/\text{Ker}(f)$ jako $g(x) = [x]_{\text{Ker}(f)}$, czyli każdemu elementowi x ze zbioru X funkcja g przyporządkowuje klasę abstrakcji $[x]_{\text{Ker}(f)}$. Tak zdefiniowana funkcja g jest suriekcją, ponieważ żadna klasa abstrakcji nie jest pusta, czyli każdy element ze zbioru $X/\text{Ker}(f)$ jest wartością funkcji g .

Definiujemy teraz $h: X/\text{Ker}(f) \rightarrow Y$ jako funkcję przyporządkowującą każdej klasie abstrakcji $[x]_{\text{Ker}(f)}$ jeden z jej elementów, czyli

$$h = \{(u, y) \in X/\text{Ker}(f) \times Y : \exists x \in X \ u = [x]_{\text{Ker}(f)} \wedge f(x) = y\}$$

Tak zdefiniowana funkcja h jest funkcją, gdyż zgodnie z definicją relacji $\text{Ker}(f)$ funkcja f przypisuje wszystkim elementom danej klasy abstrakcji te same wartości.

Pokażemy teraz, że h jest iniekcją. Niech $u_1, u_2 \in Z$ będą takie, że $h(u_1) = h(u_2)$. Istnieją wtedy takie elementy $x_1, x_2 \in X$, że $[x_1]_{\text{Ker}(f)} = u_1$ oraz $[x_2]_{\text{Ker}(f)} = u_2$. Z definicji funkcji h mamy $h(u_1) = f(x_1)$ oraz $h(u_2) = f(x_2)$. Ponieważ $h(u_1) = h(u_2)$, zatem $f(x_1) = f(x_2)$. Wynika stąd, że $(x_1, x_2) \in \text{Ker}(f)$, czyli $[x_1]_{\text{Ker}(f)} = [x_2]_{\text{Ker}(f)}$. Oznacza to, że $u_1 = u_2$, czyli h rzeczywiście jest iniekcją.

Pokażemy teraz, że $f = h \circ g$. Ustalmy $x \in X$. Wtedy $g(x) = [x]_{\text{Ker}(f)}$ oraz $h([x]_{\text{Ker}(f)}) = f(x)$. Zatem $h \circ g(x) = f(x)$ dla każdego elementu $x \in X$. $\square$

Przykład 4.22. Niech X będzie zbiorem kwadratów na płaszczyźnie. Rozważmy funkcję $f: X \rightarrow \mathbb{N}_+$ przypisującą każdemu kwadratowi długość jego boku. Wtedy $\text{Ker}(f)$ wyznacza podział zbioru kwadratów na rodziny kwadratów o takich samych długościach boków. Funkcja h z Twierdzenia o faktoryzacji przypisuje każdej takiej rodzinie kwadratów liczbę naturalną będącą długością boku tych kwadratów.

Część 5. Teoria mocy

Definicja 5.1. Powiemy, że dwa zbiory X i Y są *równoliczne* wtedy i tylko wtedy, gdy istnieje bijekcja między nimi. Piszemy wtedy $X \sim Y$.

Przykład 5.2. 1. Dwa zbiory skończone są równoliczne, jeżeli mają tyle samo elementów. Na przykład zbiory $\{1, 2, 3, 4\}$ oraz $\{x \in \mathbb{R} : x^4 - 3x^2 + 1 = 0\}$ są równoliczne: oba mają 4 elementy.
2. Zbiór liczb naturalnych $\mathbb{N}$ jest równoliczny ze zbiorem liczb naturalnych parzystych Par , ponieważ istnieje bijekcja między nimi, na przykład $f: \mathbb{N} \ni n \mapsto 2n \in \text{Par}$.

Drugi z przykładów pokazuje, że zbiór może być równoliczny ze swoim podzbiorem właściwym. Opowieść o Hotelu Hilberta.

Twierdzenie 5.3. *Dla dowolnych zbiorów X, Y oraz X zachodzi:*

1. $X \sim X$,
2. jeżeli $X \sim Y$, to $Y \sim X$,
3. jeżeli $X \sim Y$ oraz $Y \sim Z$, to $X \sim Z$.

Dowód. 1. Jako bijekcję ustalającą równoliczność X z samym sobą wystarczy wziąć 1_X (identyczność na X).

2. Niech $f: X \rightarrow Y$ będzie bijekcją. Wtedy istnieje funkcja odwrotna $f^{-1}: Y \rightarrow X$, która również jest bijekcją.

3. Niech $f: X \rightarrow Y$ oraz $g: Y \rightarrow Z$ będą bijekcjami. Złożenie bijekcji jest bijekcją, a zatem $g \circ f: X \rightarrow Z$ ustala równoliczność X z Z . $\square$

Dzięki powyższemu twierdzeniu widać, że możemy dokonać klasyfikacji zbiorów ze względu na ich liczbę.

Definicja 5.4. Każdemu zbiorowi X przyporządkowujemy jego *liczbę kardynalną* (jego *moc*) oznaczaną przez $|X|$ (lub $\bar{X}$, $\#X$) w taki sposób, że dwóm zbiorom X i Y jest przyporządkowana ta sama liczba kardynalna wtedy i tylko wtedy, gdy zbiory te są równoliczne, czyli $|X| = |Y|$ wtedy i tylko wtedy, gdy $X \sim Y$.

Należy podkreślić, że równoliczność $\sim$ nie jest relacją, określamy ją bowiem dla dowolnych zbiorów, które nie tworzą zbioru.

5.1. ZBIORY PRZELICZALNE

Definicja 5.5. Zbiorem *przeliczalnym* nazywamy każdy zbiór równoliczny ze zbiorem liczb naturalnych $\mathbb{N}$. Moc zbiorów przeliczalnych oznaczamy symbolem $\aleph_0$.

Zbiorem *co najwyżej przeliczalnym* nazywamy każdy zbiór skończony lub przeliczalny.

- Przykład 5.6.**
1. Zbiór pusty jest co najwyżej przeliczalny.
 2. Zbiór $\{1, 3, 6\}$ jest skończony, a więc jest co najwyżej przeliczalny.
 3. Zbiór liczb naturalnych jest przeliczalny, ponieważ $\mathbb{N} \sim \mathbb{N}$.
 4. Zbiór liczb naturalnych parzystych jest przeliczalny, ponieważ $\mathbb{N} \sim \text{Par}$.
 5. Zbiór liczb pierwszych jest przeliczalny, ponieważ $\mathbb{N} \sim \text{Par}$.

Twierdzenie 5.7. *Zbiór liczb całkowitych jest przeliczalny.*

Dowód. Ustalamy bijekcję pomiędzy $\mathbb{Z}$ oraz $\mathbb{N}$ w następujący sposób:

$$f(k) = \begin{cases} 2k & \text{gdy } k \geq 0 \\ -2k - 1 & \text{gdy } k < 0 \end{cases}.$$

$\square$

Intuicyjnie rzecz ujmując, zbiór jest co najwyżej przeliczalny, gdy jego elementy dają się ustawić w (skończony lub nieskończony) ciąg. Innymi słowy, można je „przeliczyć”.

Twierdzenie 5.8. *Zbiór $A \neq \emptyset$ jest co najwyżej przeliczalny wtedy i tylko wtedy, gdy jest on zbiorem wyrazów pewnego ciągu nieskończonego.*

Dowód.

- $\rightarrow$ Niech A będzie zbiorem skończonym $\{a_0, \dots, a_m\}$. Wtedy jest on zbiorem wyrazów pewnego ciągu nieskończonego $(b_n)_{n \in \mathbb{N}}$ określonego w następujący sposób: $b_i = a_i$ dla każdego $i \in \{0, \dots, m\}$ oraz $b_i = a_m$ dla każdego $i > m$. Jeżeli natomiast A jest zbiorem nieskończonym i co najwyżej przeliczalnym, to jest przeliczalny, a zatem istnieje bijekcja $f: \mathbb{N} \rightarrow A$. Wtedy A jest zbiorem wyrazów ciągu nieskończonego $(b_n)_{n \in \mathbb{N}}$ określonego jako $b_n = f(n)$ dla każdego $n \in \mathbb{N}$.
- $\leftarrow$ Niech A będzie zbiorem wyrazów pewnego ciągu nieskończonego $(b_n)_{n \in \mathbb{N}}$. Jeżeli A jest zbiorem skończonym, to z definicji jest zbiorem co najwyżej przeliczalnym. Niech więc A będzie zbiorem nieskończonym. Zdefiniujmy funkcję $f: \mathbb{N} \rightarrow A$ a następujący sposób: $f(0) = b_0$ oraz $f(i)$ jest równe pierwszemu wyrazowi ciągu $(b_n)_{n \in \mathbb{N}}$ różnemu od każdego z wyrazów $b_0, \dots, b_{i-1}$. Tak zdefiniowana funkcja jest bijekcją, a zatem A jest przeliczalny. $\square$

Twierdzenie 5.9. *Podzbiór zbioru co najwyżej przeliczalnego jest co najwyżej przeliczalny.*

Dowód. Niech X będzie zbiorem co najwyżej przeliczalnym oraz niech $Y \subseteq X$. Jeżeli Y jest zbiorem skończonym, to z definicji jest co najwyżej przeliczalny. Jeżeli $Y = X$, to również jest co najwyżej przeliczalny. Załóżmy zatem, że Y jest nieskończony oraz $Y \subsetneq X$. Ponieważ X jest wtedy zbiorem nieskończonym, a zatem zbiorem przeliczalnym, to istnieje bijekcja $f: \mathbb{N} \rightarrow X$. Definiujemy $g: \mathbb{N} \rightarrow Y$ w następujący sposób: $g(0) = f(n_0)$, gdzie $n_0 = \min\{i \in \mathbb{N}: f(i) \in Y\}$

oraz $g(k) = f(n_k)$, gdzie $n_k = \min\{i \in \mathbb{N} : f(i) \in Y \wedge i > n_{k-1}\}$. Tak określona funkcja g jest bijekcją, a zatem Y jest równoliczny z X , czyli jest co najwyżej przeliczalny. $\square$

Twierdzenie 5.10. *Suma dowolnej skończonej liczby zbiorów co najwyżej przeliczalnych jest co najwyżej przeliczalna.*

Dowód. Wystarczy pokazać, że suma dwóch zbiorów co najwyżej przeliczalnych jest co najwyżej przeliczalna. Teza twierdzenia wynika następnie z prostej indukcji. Niech zatem dane będą dwa zbiory co najwyżej przeliczalne X i Y . Jeżeli jeden z nich jest pusty, to teza jest oczywista. Niech oba będą niepuste oraz niech $f: \mathbb{N} \rightarrow X$ oraz $g: \mathbb{N} \rightarrow Y$ przekształcają oba zbiory na $\mathbb{N}$. Definiujemy funkcję $h: \mathbb{N} \rightarrow X \cup Y$ w następujący sposób:

$$h(n) = \begin{cases} f(n) & \text{gdy } n \text{ jest parzyste} \\ g(n) & \text{gdy } n \text{ jest nieparzyste} \end{cases}.$$

Funkcja g przekształca $\mathbb{N}$ na zbiór $X \cup Y$, a zatem jest on co najwyżej przeliczalny. $\square$

Twierdzenie 5.11. *Zbiór $\mathbb{N}$ jest równoliczny z $\mathbb{N}^2$.*

Dowód. (Kodowanie płaszczyzny) Zdefiniujemy funkcję $C: \mathbb{N}^2 \rightarrow \mathbb{N}$ w następujący sposób:

$$C(n, m) = \frac{(n+m)(n+m+1)}{2} + m.$$

Powyższą funkcję nazywamy *funkcją pary Cantora*. Jest ona bijekcją. [wymaga uzupełnienia] $\square$

Wniosek 5.12. *Produkt kartezjański skończenie wielu zbiorów co najwyżej przeliczalnych jest co najwyżej przeliczalny.*

Dowód. Wystarczy pokazać, że produkt kartezjański dwóch zbiorów co najwyżej przeliczalnych jest co najwyżej przeliczalny. Uogólnienie na dowolną skończoną liczbę zbiorów to prosta indukcja.

Niech dane będą dwa zbiory co najwyżej przeliczalne X i Y . Jeżeli jeden z nich jest pusty, to $X \times Y$ jest pusty, czyli co najwyżej przeliczalny. Jeżeli jeden ze zbiorów jest skończony, bez straty ogólności możemy założyć, że jest to X , to iloczyn kartezjański $X \times Y$ jest sumą skończenie wielu zbiorów co najwyżej przeliczalnych. Niech bowiem $X = \{x_1, \dots, x_n\}$. Wtedy $X \times Y = (\{x_1\} \times Y) \cup \dots \cup (\{x_n\} \times Y)$. Każdy ze składników tej sumy ma moc taką jak Y , a zatem cała suma jest co najwyżej przeliczalna.

Założmy więc, że oba zbiory są nieskończone, a zatem przeliczalne. Wtedy istnieją bijekcje $f: X \rightarrow \mathbb{N}$ oraz $g: Y \rightarrow \mathbb{N}$. Rozważmy naturalną bijekcję $f \times g: X \times Y \rightarrow \mathbb{N} \times \mathbb{N}$ zdefiniowaną jako $(f \times g)(n, m) = (f(n), g(m))$. Aby pokazać, że $X \times Y$ jest przeliczalny, wystarczy wziąć złożenie dwóch bijekcji $C \circ (f \times g): X \times Y \rightarrow \mathbb{N}$, które ustanawia równoliczność zbiorów $X \times Y$ oraz $\mathbb{N}$. $\square$

Twierdzenie 5.13. *Suma przeliczalnie wielu zbiorów przeliczalnych jest przeliczalna.*

Dowód. Wiemy, że każdy zbiór przeliczalny jest równoliczny ze zbiorem $\mathbb{N}$ oraz że dla dowolnego $k \in \mathbb{N}_+$ istnieje bijekcja $f_k: \mathbb{N}^k \rightarrow \mathbb{N}$. Pokażemy, że $\bigcup_{k \in \mathbb{N}_+} \mathbb{N}^k$ jest zbiorem przeliczalnym. Elementami zbioru $\bigcup_{k \in \mathbb{N}_+} \mathbb{N}^k$ są skończone ciągi $(a_1, \dots, a_k)$. Każdemu takiemu ciągowi możemy przyporządkować parę $(k, f_k(a_1, \dots, a_k)) \in \mathbb{N}_+ \times \mathbb{N}$. Zauważmy, że takie przyporządkowanie jest bijekcją ze zbioru $\bigcup_{k \in \mathbb{N}_+} \mathbb{N}^k$ na zbiór $\mathbb{N}_+ \times \mathbb{N}$: wynika to natychmiast z bijectywności wszystkich funkcji f_k . Ponieważ zbiór $\mathbb{N}_+ \times \mathbb{N}$ jest przeliczalny, zatem również $\bigcup_{k \in \mathbb{N}_+} \mathbb{N}^k$ musi być przeliczalny. $\square$

Twierdzenie 5.14. *Zbiór liczb wymiernych $\mathbb{Q}$ jest równoliczny z $\mathbb{N}$.*

Dowód. Na mocy powyższych twierdzeń zbiór $\mathbb{Z} \times \mathbb{N}$ jest zbiorem przeliczalnym. Zauważmy teraz, że każda liczba wymierna daje się przedstawić w postaci $\frac{m}{n}$, gdzie $m \in \mathbb{Z}$ oraz $n \in \mathbb{N}$. Zdefiniujemy funkcję $g: \mathbb{Z} \times \mathbb{N} \rightarrow \mathbb{Q}$ jako $g(m, n) = \frac{m}{n}$. Tak określona funkcja przekształca $\mathbb{Z} \times \mathbb{N}$ na $\mathbb{Q}$, a zatem moc $\mathbb{Q}$ jest nie większa niż moc zbioru $\mathbb{Z} \times \mathbb{N}$. Ponieważ $\mathbb{Q}$ jest nieskończony, więc jest przeliczalny. $\square$

Wniosek 5.15. *Zbiór wszystkich ciągów skończonych jest przeliczalny. Zbiór wszystkich wielomianów jest przeliczalny. Zbiór liczb algebraicznych jest przeliczalny.*

5.2. ZBIORY NIEPRZELICZALNE

Istnieją zbiory, których elementy nie sposób ustawić w ciąg. Takie zbiory nazywamy nieprzeliczalnymi.

Definicja 5.16. Zbiory, które nie są co najwyżej przeliczalne nazywamy *nieprzeliczalnymi*.

Lemat 5.17. *Każda liczba rzeczywista z przedziału $(0, 1]$ ma jednoznaczne dziesiętne rozwinięcie nieskończone, które nie jest od pewnego miejsca stale równe 0.*

Twierdzenie 5.18. *Zbiór liczb rzeczywistych z przedziału $(0, 1]$ jest nieprzeliczalny.*

Dowód. Pokażemy, że nie istnieje bijekcja $f: \mathbb{N} \rightarrow (0, 1]$. Dla dowodu nie wprost założmy, że taka bijekcja istnieje. Oznacza to, że każda liczba z przedziału $(0, 1]$ jest wyrazem ciągu $(f(n))_{n \in \mathbb{N}}$. Oznaczmy i -tą cyfrę w rozwinięciu dziesiętnym liczby $f(n)$ przez $f_i(n)$.

Rozważmy teraz liczbę rzeczywistą $a \in (0, 1]$ o reprezentacji dziesiętnej $a = 0, a_0 a_1 a_2 a_3 \dots$ taką, że

$$a_i = (f_i(i) + 1) \bmod 10.$$

Ponieważ f jest bijekcją, zatem istnieje taka liczba naturalna k , dla której $f(k) = a$. Wtedy k -ta cyfra w rozwinięciu dziesiętnym a jest równa $f_k(k)$. Z drugiej strony, z definicji liczby a , k -ta cyfra w rozwinięciu dziesiętnym, czyli a_k , jest równa $f_k(k) + 1$. Dostajemy zatem równość $f_k(k) = f_k(k) + 1$, otrzymując sprzeczność.

Oznacza to, że nie istnieje bijekcja $f: \mathbb{N} \rightarrow (0, 1]$. Ponieważ $(0, 1]$ nie jest zbiorem ani skończonym ani przeliczalnym, zatem jest zbiorem nieprzeliczalnym. $\square$

Twierdzenie 5.19. *Zbiory $(0, 1)$ i $(0, 1]$ są równoliczne.*

Dowód. Równoliczność jest ustanowiona na przykład przez bijekcję $f: (0, 1) \rightarrow [0, 1]$ zdefiniowaną w następujący sposób:

$$f(x) = \begin{cases} 1, & \text{gdy } x = \frac{1}{2} \\ \frac{1}{n+2}, & \text{gdy } x = \frac{1}{n+3} \text{ dla pewnego } n \in \mathbb{N} \\ x, & \text{w przeciwnym przypadku} \end{cases} \quad \square$$

Twierdzenie 5.20. *Zbiór liczb rzeczywistych jest równoliczny ze zbiorem liczb rzeczywistych z przedziału $(0, 1)$.*

Dowód. Wskażemy bijekcję między rozważanymi zbiorami. Pokażemy najpierw, że $(0, 1) \sim (0, \pi)$. Wystarczy wziąć funkcję $f: (0, 1) \ni x \mapsto \pi x \in (0, \pi)$. Równoliczność $(0, \pi) \sim \mathbb{R}$ jest ustanowiona przez funkcję cotangens: $(0, \pi) \ni x \mapsto \operatorname{ctg} x \in \mathbb{R}$ jest bijekcją. $\square$

Definicja 5.21. Moc zbioru liczb rzeczywistych nazywamy *continuum* i oznaczamy przez $\mathfrak{c}$.

Twierdzenie 5.22 (bez dowodu). *Zbiór liczb niewymiernych ma moc $\mathfrak{c}$.*

Twierdzenie 5.23 (bez dowodu). *Zbiór wszystkich podzbiorów $\mathbb{N}$ ma moc $\mathfrak{c}$. Zbiór wszystkich nieskończonych podzbiorów $\mathbb{N}$ ma moc $\mathfrak{c}$. Zbiór wszystkich skończonych podzbiorów $\mathbb{N}$ ma moc $\aleph_0$.*

5.3. TWIERDZENIE CANTORA-BERNSTEINA

Lemat 5.24. *Niech dane będą zbiory A , B i C . Jeżeli $C \subseteq B \subseteq A$ oraz $|A| = |C|$, to $|A| = |B|$.*

Dowód (nieobowiązkowy). Ponieważ zbiory A i C są równoliczne, zatem istnieje bijekcja $f: A \rightarrow C$. W dowodzie skonstruujemy bijekcję $g: A \rightarrow B$. Definiujemy rekurencyjnie ciąg zbiorów:

$$\begin{aligned} Z_0 &= B \setminus C, \\ Z_{n+1} &= \vec{f}(Z_n). \end{aligned}$$

Niech $Z := \bigcup_{n \in \mathbb{N}} Z_n$. Zauważmy, że dla każdego $n \in \mathbb{N}$ zachodzi inkluzja $Z_n \subseteq B$. Stąd wynika, że również $Z \subseteq B$. Definiujemy teraz $g: A \rightarrow B$ w następujący sposób:

$$g(x) = \begin{cases} f(x), & \text{gdy } x \in A \setminus Z \\ x, & \text{gdy } x \in Z \end{cases}.$$

Tak zdefiniowana funkcja jest poprawnie określona. Wystarczy zatem pokazać, że jest bijekcją.

Pokażemy najpierw, że g jest iniekcją. Niech a_1, a_2 będą elementami ze zbioru A takimi, że $a_1 \neq a_2$. Udowodnimy, że w każdym z trzech poniższych przypadków $g(a_1) \neq g(a_2)$.

- (a) Jeżeli $a_1, a_2 \in Z$, to $g(a_1) = a_1 \neq a_2 = g(a_2)$.
- (b) Jeżeli $a_1, a_2 \notin Z$, to $g(a_1) = f(a_1)$ oraz $f(a_2) = g(a_2)$. Ponieważ f była iniekcją, zatem $g(a_1) \neq g(a_2)$.
- (c) Niech $a_1 \in Z$ oraz $a_2 \notin Z$, co oznacza, że $g(a_1) = a_1$ oraz $g(a_2) = f(a_2)$. Załóżmy nie wprost, że $g(a_1) = g(a_2)$. Wtedy $a_1 = f(a_2)$, a stąd $f(a_2) \in Z$. Istnieje zatem $n \in \mathbb{N}$ takie, że $f(a_2) \in Z_n$. Jeżeli $n = 0$, to $f(a_2) \in B \setminus C$, a w szczególności $f(a_2) \notin C$. Jednakże f jest bijekcją na zbiór C , zatem otrzymujemy sprzeczność. Rozważmy przypadek $n > 0$. Wtedy $f(a_2) \in Z_n = \vec{f}(Z_{n-1})$, czyli dla pewnego $z \in Z_{n-1}$ zachodzi $f(z) = f(a_2)$. Z iniektywności funkcji f mamy $z = a_2$, a zatem $a_2 \in Z_{n-1}$. Jest to sprzeczne z założeniem, że $a_2 \notin Z$. Otrzymana sprzeczność dowodzi nierówności $g(a_1) \neq g(a_2)$.

Pozostaje pokazać, że g jest suriekcją, czyli że $\vec{g}(A) = B$. Wiemy, że $Z \subseteq B \subseteq A$. Otrzymujemy stąd

$$\begin{aligned} \vec{g}(A) &= \vec{g}((A \setminus Z) \cup Z) = \vec{g}(A \setminus Z) \cup \vec{g}(Z) \\ &= \vec{f}(A \setminus Z) \cup Z = \vec{f}(A \setminus Z) \cup \bigcup_{n \in \mathbb{N}} Z_n = \vec{f}(A \setminus Z) \cup (B \setminus C) \cup \bigcup_{n \in \mathbb{N}_+} Z_n = \\ &= \vec{f}(A \setminus Z) \cup (B \setminus C) \cup \bigcup_{n \in \mathbb{N}} \vec{f}(Z_n) = \vec{f}(A \setminus Z) \cup (B \setminus C) \cup \vec{f}\left(\bigcup_{n \in \mathbb{N}} Z_n\right) = \\ &= \vec{f}(A \setminus Z) \cup (B \setminus C) \cup \vec{f}(Z) = \vec{f}(A) \cup (B \setminus C) = C \cup (B \setminus C) = B. \end{aligned}$$

Skonstruowana funkcja g jest zatem bijekcją ze zbioru A na zbiór B , co dowodzi równoliczności tych zbiorów. $\square$

Twierdzenie 5.25 (Cantora-Bernsteina). *Niech dane będą zbiory A i B . Jeżeli $|A| \leq |B|$ oraz $|B| \leq |A|$, to $|A| = |B|$.*

Dowód (nieobowiązkowy). Nierówności $|A| \leq |B|$ oraz $|B| \leq |A|$ oznaczają, że zbiór A jest równoliczny z pewnym podzbiorem zbioru B oraz że zbiór B jest równoliczny z pewnym podzbiorem zbioru A . Istnieją zatem dwie iniekcje $f: A \rightarrow B$ oraz $g: B \rightarrow A$. Oznacza to, że zbiory A , $\vec{g}(B)$ i $\vec{g}(\vec{f}(A))$ spełniają założenia Lematu 5.24, tj. $\vec{g}(\vec{f}(A)) \subseteq \vec{g}(B) \subseteq A$. Z iniektywności g zbiory B i $\vec{g}(B)$ są równoliczne, a to oznacza równoliczność zbiorów A i B . $\square$

5.4. TWIERDZENIE CANTORA

Twierdzenie 5.26 (Cantora). *Moc dowolnego zbioru X jest silnie mniejsza od mocy jego zbioru potęgowego $\mathcal{P}(X)$.*

Dowód. Aby pokazać, że moc X jest nie większa od mocy $\mathcal{P}(X)$ wystarczy pokazać, że istnieje iniekcja $f: X \rightarrow \mathcal{P}(X)$. Zauważmy, że taka iniekcja rzeczywiście istnieje — wystarczy zdefiniować f w następujący sposób: $f(x) = \{x\}$.

Aby pokazać, że moc X jest silnie mniejsza od mocy $\mathcal{P}(X)$ należy pokazać, że nie istnieje suriekcja $g: X \rightarrow \mathcal{P}(X)$. Załóżmy dla dowodu nie wprost, że taka suriekcja istnieje. Zdefiniujmy teraz następujący zbiór:

$$B = \{x \in X : x \notin g(x)\}.$$

Tak zdefiniowany zbiór B jest elementem $\mathcal{P}(X)$. Ponieważ g jest suriekcją musi istnieć taki element $b \in X$, dla którego $g(b) = B$. Mamy dwie możliwości:

- jeżeli $b \in B$, to z definicji B mamy $b \notin g(b)$, ale wtedy $b \notin B$ — sprzeczność;
- jeżeli $b \notin B$, to z definicji B mamy $b \in g(b)$, ale wtedy $b \in B$ — sprzeczność.

Oznacza to, że nie istnieje poszukiwana suriekcja. $\square$

Część 6. Teoria porządku

Definicja 6.1. Niech dany będzie zbiór X . Relację $R \subseteq X^2$ nazywamy *relacją częściowego porządku* na X , jeżeli jest zwrotna, słabo antysymetryczna i przechodnia. Najczęściej relację częściowego porządku będziemy oznaczać symbolem $\leq_X$ lub po prostu $\leq$. Parę $(X, \leq)$ nazywamy *częściowym porządkiem*, natomiast o zbiorze X mówimy, że jest *częściowo uporządkowany* przez relację $\leq_X$.

Przykład 6.2.

1. Niech X będzie zbiorem. Wtedy $(\mathcal{P}(X), \subseteq)$ jest częściowym porządkiem.
2. Niech $|$ oznacza relację podzielności w zbiorze liczb naturalnych. Wtedy $(\mathbb{N}_+, |)$ jest częściowym porządkiem.
3. Para $(\mathbb{R}, \leq)$ jest częściowym porządkiem.

Relacje częściowego porządku możemy przedstawiać graficznie za pomocą tak zwanych *diagramów Hassego*.

Definicja 6.3 (Elementy wyróżnione). Niech $(X, \leq)$ będzie częściowym porządkiem.

1. Element $x \in X$ nazywamy elementem *minimalnym*, gdy $\forall_{y \in X} (y \leq x \rightarrow x = y)$.
2. Element $x \in X$ nazywamy elementem *maksymalnym*, gdy $\forall_{y \in X} (x \leq y \rightarrow x = y)$.
3. Element $x \in X$ nazywamy elementem *najmniejszym*, gdy $\forall_{y \in X} x \leq y$.
4. Element $x \in X$ nazywamy elementem *największym*, gdy $\forall_{y \in X} y \leq x$.

Uwaga 6.4. Zauważmy, że elementy wyróżnione nie muszą istnieć. Elementów minimalnych (maksymalnych) może być wiele, natomiast element najmniejszy (największy) może być tylko jeden. Jeżeli w porządku istnieje element najmniejszy (największy), to jest on jedynym elementem minimalnym (maksymalnym).

Przykład 6.5. W częściowym porządku $(\mathbb{Z}, \leq)$ nie ma żadnego elementu wyróżnionego. W porządku $(\mathbb{N}, \leq)$ nie ma elementów maksymalnych ani elementu największego, natomiast 0 jest elementem najmniejszym i minimalnym. W porządku $(X, 1_X)$ dla co najmniej dwuelementowego zbioru X każdy element jest elementem minimalnym i maksymalnym, natomiast nie istnieje ani element największy ani najmniejszy.

Definicja 6.6 (Majoranta, minoranta, supremum, infimum). Niech $(X, \leq)$ będzie częściowym porządkiem oraz niech A będzie podzbiorem X .

1. Element $x \in X$ nazywamy *ograniczeniem górnym* (lub *majorantą* lub *kresem górnym*) zbioru A , gdy każdy element ze zbioru A jest mniejszy lub równy x , czyli gdy

$$\forall_{a \in A} a \leq x.$$

Zbiór ograniczeń górnych danego zbioru A będziemy oznaczać przez $\text{Maj } A$.

2. Element $x \in X$ nazywamy *ograniczeniem dolnym* (lub *minorantą* lub *kresem dolnym*) zbioru A , gdy każdy element ze zbioru A jest większy lub równy x , czyli gdy

$$\forall_{a \in A} x \leq a.$$

Zbiór ograniczeń dolnych danego zbioru A będziemy oznaczać przez $\text{Min } A$.

3. Element $x \in X$ nazywamy *supremum* zbioru A , jeżeli x jest najmniejszym ograniczeniem górnym, czyli zachodzą dwa warunki:

- $\forall_{a \in A} a \leq x$,
- $\forall_{y \in X} ((\forall_{a \in A} a \leq y) \rightarrow x \leq y)$.

Piszemy wtedy $x = \sup A$.

4. Element $x \in X$ nazywamy *infimum* zbioru A , jeżeli x jest największym ograniczeniem dolnym, czyli zachodzą dwa warunki:

- $\forall a \in A \ x \leq a$,
- $\forall y \in X \ ((\forall a \in A \ y \leq a) \rightarrow y \leq x)$.

Piszemy wtedy $x = \inf A$.

Przykład 6.7. Jakies diagramy.

Definicja 6.8 (Liniowy porządek). Niech $(X, \leq)$ będzie częściowym porządkiem. Jeżeli relacja $\leq$ jest spójna, to nazywamy ją *relacją liniowego porządku*. O zbiorze X mówimy wtedy, że jest *liniowo uporządkowany*, natomiast częściowy porządek $(X, \leq)$ nazywamy *liniowym porządkiem*.

Definicja 6.9 (Łańcuch i antyłańcuch). Niech $(X, \leq)$ będzie częściowym porządkiem oraz niech A będzie podzbiorem X .

1. Powiemy, że A jest *łańcuchem*, gdy relacja $\leq$ obcięta do zbioru A porządkuje ten zbiór liniowo. Zatem łańcuchem nazywamy taki podzbiór zbioru częściowo uporządkowanego, w którym dowolne dwa elementy są porównywalne.
2. Powiemy, że A jest *antyłańcuchem*, gdy relacja $\leq$ obcięta do zbioru A jest identycznością. Zatem antyłańcuchem nazywamy taki podzbiór zbioru częściowo uporządkowanego, w którym żadne dwa różne elementy nie są porównywalne.

Definicja 6.10 (Izomorfizm porządków). Niech $(X, \leq_X)$ oraz $(Y, \leq_Y)$ będą dwoma częściowymi porządkami. Powiemy, że porządki te są *izomorficzne (podobne)*, jeżeli istnieje bijekcja $f: X \rightarrow Y$ zachowująca porządek, czyli spełniająca warunek

$$\forall x, y \in X \ (x \leq_X y \leftrightarrow f(x) \leq_Y f(y)).$$

Definicja 6.11 (Porządek gęsty). Poset $(X, \leq)$ jest gęsty, jeżeli spełniony jest warunek

$$\forall x, y \in X \ (x \neq y \wedge x \leq y \rightarrow \exists z \in X \ (z \neq x \wedge z \neq y \wedge x \leq z \leq y)).$$

Przykład 6.12.

1. $(\mathbb{R}, \leq)$ jest gęsty, ponieważ pomiędzy dwiema różnymi liczbami rzeczywistymi istnieje różna od nich liczba rzeczywista.
2. $(\mathbb{Q}, \leq)$ również jest gęsty.
3. Posety $(\mathbb{N}, \leq)$ i $(\mathbb{Z}, \leq)$ nie są gęste.
4. Każdy antyłańcuch jest gęstym posetem.
5. Żaden skończony porządek liniowy o co najmniej dwóch elementach nie jest gęsty.

Twierdzenie 6.13. *Gęstość jest przenoszona przez podobieństwo, tzn. jeżeli $(X, \leq_X)$ jest gęsty i izomorficzny z $(Y, \leq_Y)$, to $(Y, \leq_Y)$ również jest gęsty.*

Dowód. Niech $(X, \leq_X)$ będzie gęstym posetem izomorficznym z posetem $(Y, \leq_Y)$. Istnieje zatem pewien izomorfizm $f: X \rightarrow Y$. Jeżeli żadne dwa różne elementy z Y nie są porównywalne, to Y jest gęsty wprost z definicji. W przeciwnym przypadku wybierzmy dwa różne elementy $y_1, y_2 \in Y$ takie, że $y_1 \leq_Y y_2$. Wtedy $f^{-1}(y_1)$ oraz $f^{-1}(y_2)$ są różnymi elementami zbioru X takimi, że $f^{-1}(y_1) \leq_X f^{-1}(y_2)$. Zbiór X jest gęsto uporządkowany, istnieje więc $x \in X$ różny od $f^{-1}(y_1)$ i $f^{-1}(y_2)$ taki, że $f^{-1}(y_1) \leq_X x \leq_X f^{-1}(y_2)$. Z własności izomorfizmu f dostajemy wtedy, że $y_1 = f(f^{-1}(y_1)) \leq_Y f(x) \leq_Y f(f^{-1}(y_2)) = y_2$. Ponieważ f jest bijekcją, mamy $f(x) \neq y_1$ oraz $f(x) \neq y_2$. Dowodzi to gęstości posetu $(Y, \leq_Y)$. $\square$

Przykład 6.14. Niech $X = [0, 1]$. Rozważmy zbiór X^X , czyli zbiór wszystkich funkcji $f: [0, 1] \rightarrow [0, 1]$. Zadajemy na zbiorze X^X częściowy porządek w następujący sposób:

$$f \sqsubseteq g \text{ wtedy i tylko wtedy, gdy } \forall x \in X \ f(x) \leq g(x).$$

Pokażemy, że posety $(X^X, \sqsubseteq)$ oraz $(\mathcal{P}(X), \subseteq)$ nie są izomorficzne.

Zauważmy najpierw, że poset $(X^X, \sqsubseteq)$ jest gęsty. Niech f i g będą funkcjami ze zbioru X^X oraz niech $f \sqsubseteq g$ i $f \neq g$. Definiujemy funkcję $h \in X^X$ wzorem $h(x) = \frac{f(x)+g(x)}{2}$. Wtedy $f \sqsubseteq h \sqsubseteq g$ oraz $f \neq h \neq g$.

Wystarczy teraz pokazać, że $(\mathcal{P}(X), \subseteq)$ nie jest gęsty. Istotnie, możemy wybrać takie dwa elementy A i B ze zbioru $\mathcal{P}(X)$, dla których nie istnieje zbiór C taki, że $A \subsetneq C \subsetneq B$. Wystarczy wziąć $A = \emptyset$ oraz $B = \{0\}$.

Jeden z posetów jest gęsty, natomiast drugi nie, zatem na mocy poprzedniego twierdzenia posety te nie są izomorficzne.

Definicja 6.15 (Przekrój Dedekinda). Niech $(X, \leq)$ będzie porządkiem liniowym. *Przekrojem Dedekinda* nazywamy parę (X_1, X_2) niepustych podzbiorów zbioru X :

- (i) $X_1 \cup X_2 = X$,
- (ii) $X_1 \cap X_2 = \emptyset$,
- (iii) $\forall x_1 \in X_1 \forall x_2 \in X_2 \ x_1 < x_2$.

Powiemy, że przekrój daje *skok*, jeżeli X_1 ma element największy i X_2 ma element najmniejszy.

Przekrój (X_1, X_2) daje *lukę*, jeżeli X_1 nie ma elementu największego i X_2 nie ma elementu najmniejszego.

Przykład 6.16.

Twierdzenie 6.17. *Liniowy porządek $(X, \leq)$ jest gęsty wtedy i tylko wtedy, gdy żaden przekrój nie daje skoku.*

Dowód. □

Definicja 6.18. Porządek liniowy $(X, \leq)$ nazywamy *ciągłym*, jeżeli żaden przekrój nie daje luki.

Przykład 6.19. Porządki liniowe $(\mathbb{N}, \leq)$ i $(\mathbb{R}, \leq)$ są ciągłe, natomiast $(\mathbb{Q}, \leq)$ i $(\mathbb{R} \setminus \mathbb{Q}, \leq)$ nie są ciągłe.

Twierdzenie 6.20 (bez dowodu). *Ciągłość jest przenoszona przez podobieństwo, tzn. jeżeli $(X, \leq_X)$ jest ciągły i izomorficzny z $(Y, \leq_Y)$, to $(Y, \leq_Y)$ również jest ciągły.*

Wniosek 6.21. *Porządki $(\mathbb{R}, \leq)$ i $(\mathbb{R} \setminus \mathbb{Q}, \leq)$ nie są izomorficzne.*

Definicja 6.22. Porządek liniowy $(X, \leq)$ nazywamy *dobrym*, jeżeli każdy niepusty podzbiór zbioru X ma element najmniejszy.

Uwaga 6.23. *Żaden porządek gęsty o co najmniej dwóch elementach nie jest dobry.*

Przykład 6.24. Porządek $(\mathbb{N}, \leq)$ jest dobry. Porządek $(\mathbb{Z}, \leq)$ nie jest dobry, ponieważ cały zbiór $\mathbb{Z}$ nie ma elementu najmniejszego. Porządek $(\mathbb{N}, |)$ nie jest dobry, bo nie jest liniowy. Porządek $(\mathbb{Q}_+ \cup \{0\}, \leq)$ nie jest dobry, bo np. zbiór $\{x \in \mathbb{Q}_+ \cup \{0\} : x < \sqrt{2}\}$ nie ma elementu najmniejszego.

Część 7. Aksjomat wyboru i równoważne twierdzenia

Aksjomat Wyboru. *Jeżeli $\mathcal{A}$ jest rodziną niepustych i parami rozłącznych zbiorów, to istnieje zbiór mający z każdym elementem A dokładnie jeden element wspólny. Formalnie:*

$$\begin{aligned} & \forall \mathcal{A} \left(\emptyset \notin \mathcal{A} \wedge \forall_X \forall_Y (X \in \mathcal{A} \wedge Y \in \mathcal{A} \rightarrow X \neq Y \wedge X \cap Y = \emptyset) \right. \\ & \quad \left. \rightarrow \exists_Z \forall_V (V \in \mathcal{A} \rightarrow \exists_v V \cap Z = \{v\}) \right). \end{aligned}$$

Poniższe twierdzenia są podane bez dowodów. Znajomość dowodów nie będzie wymagana na egzaminie.

Twierdzenie 7.1 (o funkcji wyboru). *Jeżeli $\mathcal{A}$ jest rodziną niepustych, to istnieje funkcja, która każdemu zbiorowi z rodziny $\mathcal{A}$ przyporządkowuje któryś z jego elementów. Formalnie:*

$$\forall \mathcal{A} \left(\emptyset \notin \mathcal{A} \rightarrow \exists_f (f: \mathcal{A} \rightarrow \bigcup \mathcal{A} \wedge \forall_A (A \in \mathcal{A} \rightarrow f(A) \in A)) \right).$$

Twierdzenie 7.2 (o suriekcji i iniekcji). *Niech X i Y będą zbiorami oraz niech $f: X \rightarrow Y$ będzie suriekcją. Wtedy istnieje iniekcja $g: Y \rightarrow X$ taka, że $f \circ g$ jest funkcją identycznościową na Y .*

Lemat 7.3 (Kuratowskiego–Zorna). *Niech $(P, \leq)$ będzie niepustym częściowym porządkiem. Jeżeli każdy niepusty łańcuch ma majorantę, to w $(P, \leq)$ istnieje element maksymalny.*

Twierdzenie 7.4 (Hausdorffa o łańcuchu maksymalnym). *W każdym niepustym zbiorze częściowo uporządkowanym istnieje łańcuch maksymalny ze względu na relację inkluzję.*

Twierdzenie 7.5 (Zermelo). *Dla każdego niepustego zbioru X istnieje relacja $R \subseteq X^2$ taka, że (X, R) jest dobrym porządkiem.*

Twierdzenie 7.6. *Twierdzenia 7.1–7.5 są równoważne Aksjomatowi Wyboru.*