KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt pn. „*Wzmocnienie potencjału dydaktycznego UMK w Toruniu w dziedzinach matematyczno-przyrodniczych*”
realizowany w ramach Poddziałania 4.1.1 Programu Operacyjnego Kapitał Ludzki

Wstęp do matematyki

Piotr Jędrzejewicz

UMK Toruń 2014

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Spis treści

Wstęp

Materiały obejmują skrypt wykładu „Wstęp do matematyki" prowadzonego przez autora na Wydziale Matematyki i Informatyki Uniwersytetu Mikołaja Kopernika w Toruniu. Wykład jest prowadzony w wymiarze 30 godzin na I roku studiów I stopnia matematyki i ekonomii, nauczania matematyki oraz nauczania matematyki i informatyki w zakresie zajęć komputerowych. Do skryptu dołączone są listy zadań przeznaczone na ćwiczenia do tego wykładu, również w wymiarze 30 godzin.

Cel przedmiotu

Przedmiot „Wstęp do matematyki" odgrywa ważną rolę w przygotowaniu do studiowania pozostałych przedmiotów matematycznych. Można wyróżnić trzy aspekty tej roli. Po pierwsze, wprowadza się podstawowe pojęcia dotyczące zbiorów, funkcji i relacji oraz zagadnienia z teorii mocy. Po drugie, wykształca się u studentów podstawowe umiejętności operowania obiektami matematycznymi, posługiwania się językiem matematycznym i przeprowadzania rozumowań matematycznych. Po trzecie, przedstawia się, w jaki sposób jest zbudowana współczesna matematyka (konstrukcje zbiorów liczbowych, aksjomatyka Peana, informacja o aksjomatyce teorii zbiorów, a także definicja pary w sensie Kuratowskiego oraz definicja funkcji). Te trzy aspekty wzajemnie się przenikają i stanowią o specyfice tego przedmiotu.

Pierwszy etap realizacji przedmiotu stanowią elementy logiki – rachunek zdań, rachunek kwantyfikatorów oraz metody dowodzenia twierdzeń. Szczególną wagę przywiązuje się do praktycznego posługiwania się symboliką logiczną, poprawnego zapisywania zdań matematycznych oraz interpretacji takich zapisów. Rozbudowane zostały zagadnienia dotyczące metod dowodzenia twierdzeń. Podstawowym celem jest tu nauczenie studentów (w miarę możliwości) poprawnego przeprowadzania prostych rozumowań matematycznych oraz formułowania dowodów.

Kolejne rozdziały to zbiory i odwzorowania, gdzie szczególnie ważne są ogólne pojęcia dotyczące funkcji, które będą przydatne na różnych przedmiotach w dalszym toku studiów. Opieramy się tu na intuicyjnym pojęciu zbioru i szkolnej definicji funkcji. Jest to zabieg celowy, sprzyjający łatwiejszemu opanowaniu praktycznemu zagadnień dotyczących zbiorów i funkcji. Następny rozdział stanowią relacje, w tym definicja funkcji jako relacji, relacje porządkujące i relacje równoważności. Tu szczególnie trudnym pojęciem jest zbiór ilorazowy, więc ważne jest, aby student poznał różne przykłady (zbiór reszt modulo m, wektory swobodne). Kolejny rozdział stanowi teoria mocy z informacjami o aksjomatach teorii mnogości. Ostatni rozdział to konstrukcje zbiorów liczbowych z aksjomatyką zbioru liczb naturalnych.

Tematy wykładów i ćwiczeń

Tabela przedstawia tematykę kolejnych wykładów i ćwiczeń.

tydzień	wykład	ćwiczenia
1.	Wstępne uwagi o matematyce Spójniki logiczne i kwantyfikatory	Przykłady zdań w matematyce
2.	Rachunek zdań	Rachunek zdań
3.	Rachunek kwantyfikatorów	Rachunek zdań
4.	Twierdzenia i dowody	Rachunek kwantyfikatorów
5.	Twierdzenia i dowody	Twierdzenia i dowody
6.	Indukcja matematyczna	Twierdzenia i dowody
7.	Zbiory	Indukcja matematyczna
8.	Zbiory	Kolokwium Zbiory
9.	Funkcje	Zbiory
10.	Funkcje	Funkcje
11.	Relacje	Funkcje
12.	Relacje	Relacje
13.	Teoria mocy	Relacje
14.	Teoria mocy	Teoria mocy
15.	Konstrukcje zbiorów liczbowych	Teoria mocy Kolokwium

Z uwagi na to, że w danym tygodniu zajęć ćwiczenia mogą odbywać się przed wykładem, lista zadań do wykładu nr n jest przewidziana do realizacji w tygodniu nr $n+1$.

1 Wstępne uwagi o matematyce

Nazwa przedmiotu zobowiązuje do tego, aby na początku udzielić kilku wskazówek pomagających szukać odpowiedzi na pytanie czym jest matematyka.

1.1 Hasło „matematyka" w słownikach i encyklopediach

W wydaniu internetowym Słownika Języka Polskiego PWN ([18]) rzeczownik *matematyka* ma trzy znaczenia. Pierwsze z nich to:

> *nauka posługująca się metodą dedukcji, zajmująca się badaniem zbiorów liczb, punktów i innych elementów abstrakcyjnych.*

Pod pojęciem „innych elementów abstrakcyjnych" kryje się ogromna różnorodność obiektów matematycznych, są to m.in. funkcje, relacje, zbiory z różnymi strukturami. Jakie są pozostałe dwa znaczenia słowa *matematyka*? Proszę to sprawdzić pod adresem `http://sjp.pwn.pl/szukaj/matematyka`.

Podobne określenie znajdziemy w internetowym wydaniu Oksfordzkiego Słownika Języka Angielskiego ([17]) na stronie `http://www.oxforddictionaries.com/definition/english/mathematics`:

> *The abstract science of number, quantity, and space, either as abstract concepts (pure mathematics), or as applied to other disciplines such as physics and engineering (applied mathematics).*

W internetowym wydaniu Encyklopedii PWN ([15]) matematyka jest określona jako *nauka dedukcyjna, gałąź wiedzy, której cel można określić jako badanie konsekwencji przyjętych założeń.* Warto zapoznać się z całym artykułem zamieszczonym na stronie `http://encyklopedia.pwn.pl/haslo/3938552/matematyka.html`. Matematyka jest tam przedstawiona w zwięzły sposób w ujęciu historycznym. Odnotujmy ostatnie zdanie tego artykułu:

> *Matematykę współczesną charakteryzuje z jednej strony duża abstrakcyjność i sformalizowanie, a z drugiej – szybko rosnący zasięg zastosowań, obejmujących nie tylko nauki techniczne i przyrodnicze, ale też ekonomię i niektóre działy nauk humanistycznych.*

Z artykułu poświęconego matematyce w Wikipedii ([20]) na stronie `http://pl.wikipedia.org/wiki/Matematyka` dowiemy się m.in., że

> *matematyka teoretyczna, nazywana czasami matematyką czystą, jest często rozwijana bez wyraźnego związku z konkretnymi zastosowaniami. (...) Szkolne rozumienie matematyki, jako nauki wyłącznie o liczbach i pojęciach geometrycznych, zdezaktualizowało się już w XIX wieku wraz z postępami algebry i teorii mnogości.*

Znajdziemy tam również cytaty definicji i wizji matematyki różnych autorów, przegląd działów matematyki według klasyfikacji Amerykańskiego Towarzystwa Matematycznego MSC 2010 ([16]) oraz dokładniejsze wyjaśnienie struktury formalnej teorii matematycznych. Przy okazji warto również przejrzeć artykuł o matematyce w angielskiej wersji Wikipedii ([19]) na stronie `http://en.wikipedia.org/wiki/Mathematics`.

1.2 Co to jest matematyka?

Szukając odpowiedzi na postawione pytanie warto sięgnąć po książkę pod takim właśnie tytułem autorstwa Richarda Couranta i Herberta Robbinsa ([13]):

> *Matematyka, jako wyraz myśli ludzkiej, odzwierciedla czynną wolę, kontemplacyjny rozum i dążenie do doskonałości estetycznej. Jej podstawowymi elementami są: logika i intuicja, analiza i konstrukcja, uogólnianie i indywidualizowanie. Różne tradycje podkreślały różne spośród tych aspektów, jednak tylko gra przeciwstawnych sił, walka o ich syntezę stanowi o żywotności, użyteczności i ogromnym znaczeniu matematyki.*

W Przedmowie do drugiego wydania wspomnianej książki autor uzupełnień Ian Stewart deklaruje([13]):

> *Jednym z celów (tej książki) jest obalenie przesądu, „matematyka jest tylko systemem wniosków wyprowadzonym z definicji i postulatów, które muszą być niesprzeczne, ale zależą tylko od swobodnego uznania matematyków." (. . .) Matematyka jest zawieszona pomiędzy rzeczywistością a nierzeczywistością; jej sens nie tkwi ani w formalnej abstrakcji, ani w świecie fizycznym. (. . .) Matematyka wiąże abstrakcyjny świat pojęć umysłu ze światem fizycznym, nie będąc częścią żadnego z nich.*

Ciekawą dyskusję różnych aspektów specyfiki doświadczenia matematycznego odnajdziemy w książce Philipa J. Davisa i Reubena Hersha pt. „Świat matematyki". W przedmowie autor przywołuje podstawowe pytania:

> *Co to jest liczba? Co to jest zbiór? Co to jest dowód? Co wiemy o matematyce? I jak to wiemy? Co to jest „ścisłość matematyczna"? Co to jest „intuicja matematyczna"?*
>
> *Kiedy sformułowałem te pytania, zdałem sobie sprawę, że nie znam na nie odpowiedzi. (. . .) Co gorsza, nie miałem podstawy czy kryterium, które pozwoliłoby mi mierzyć różne opinie, bronić lub atakować jakiś pogląd. Nawiązałem rozmowy z innymi matematykami na temat dowodu, wiedzy, matematycznej rzeczywistości i okazało się, że mój stan mglistej niepewności był typowy.*

2 Spójniki logiczne i kwantyfikatory

2.1 Przykłady zdań w matematyce

Oznaczenia zbiorów:

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$ – zbiór liczb naturalnych z zerem,

$\mathbb{N}_1 = \{1, 2, 3, \dots\}$ – zbiór liczb naturalnych bez zera,

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ – zbiór liczb całkowitych,

$\mathbb{Q}$ – zbiór liczb wymiernych,

$\mathbb{R}$ – zbiór liczb rzeczywistych.

Przykład 1. Zdania prawdziwe:

(a) „$\frac{1}{3} + \frac{1}{6} = \frac{1}{2}$”,

(b) „$3|6$”,

(c) „$\sqrt{2} \notin \mathbb{Q}$”,

(d) „Jeśli $x = 1$, to $x^2 = 1$”, gdzie x oznacza daną liczbę rzeczywistą,

(e) „Jeśli $a^2+b^2 = c^2$, to trójkąt jest prostokątny”, gdzie a, b, c oznaczają długości boków danego trójkąta.

Przykład 2. Zdania fałszywe:

(a) „$2 + 2 = 5$”,

(b) „$\sqrt{2} \in \mathbb{Q}$”,

(c) „$\mathbb{Q} \subset \mathbb{Z}$”.

Pytanie 1. *Czy prawdziwe jest zdanie:*

„Jeśli trójkąt jest prostokątny, to $a^2 + b^2 = c^2$”

(a, b, c – długości boków danego trójkąta)?

Zdanie posiadające jedną z dwóch wartości logicznych: „prawda” lub „fałsz”, nazywamy **zdaniem logicznym**. Zdania logiczne oznaczamy literami p, q, r, ...

Wartość logiczną „fałsz” oznaczamy symbolem 0, a wartość logiczną „prawda” symbolem 1. Jeśli zdanie p jest fałszywe, to piszemy $v(p) = 0$, a jeśli jest prawdziwe, to piszemy $v(p) = 1$.

Złożone zdania logiczne są zbudowane z innych zdań logicznych za pomocą **spójników logicznych**: jednoargumentowego $\sim$ i dwuargumentowych $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$, $\underline{\vee}$.

2.2 Spójniki logiczne

Negacja zdania p:

$$\sim p - \text{„nie } p\text{”, „nieprawda, że } p\text{”.}$$

Przykład 3. „1 nie jest liczbą pierwszą”,
dokładniej: „nieprawda, że 1 jest liczbą pierwszą”.
Zdanie $\sim p$ jest negacją zdania p: „1 jest liczbą pierwszą”.

Zdanie $\sim p$ jest:

– prawdziwe, gdy p jest fałszywe,

– fałszywe, gdy p jest prawdziwe.

$v(p)$	$v(\sim p)$
0	1
1	0

Koniunkcja zdań p i q:

$$p \wedge q - \text{„}p \text{ i } q\text{”.}$$

Przykład 4. „2 jest liczbą pierwszą i parzystą”, dokładniej: „2 jest liczbą pierwszą i 2 jest liczbą parzystą”. Jest to koniunkcja $p \wedge q$, gdzie p oznacza zdanie „2 jest liczbą pierwszą”, a q oznacza zdanie „2 jest liczbą parzystą”.

Zdanie $p \wedge q$ jest:

– prawdziwe, gdy oba zdania p i q są prawdziwe,

– fałszywe, gdy co najmniej jedno ze zdań p i q jest fałszywe.

$v(p)$	$v(q)$	$v(p \wedge q)$
0	0	0
0	1	0
1	0	0
1	1	1

Alternatywa zdań p i q:

$$p \vee q - \text{„}p \text{ lub } q\text{”.}$$

Przykład 5. Wybierzmy pewną liczbę całkowitą x i rozważmy zdanie: „$x < 1$ lub $x > -1$”. Jest to alternatywa $p \vee q$, gdzie p oznacza zdanie „$x < 1$”, a q oznacza zdanie „$x > -1$”. W przypadku $x = 0$ oba zdania są prawdziwe i alternatywa też jest zdaniem prawdziwym.

Zdanie $p \vee q$ jest:

– prawdziwe, gdy co najmniej jedno ze zdań p i q jest prawdziwe,

– fałszywe, gdy oba zdania p i q są fałszywe.

$v(p)$	$v(q)$	$v(p \vee q)$
0	0	0
0	1	1
1	0	1
1	1	1

Alternatywa rozłączna zdań p i q:

$$p \veebar q - \text{„}p \text{ albo } q\text{”}.$$

Przykład 6. Rozważmy dwie (różne) proste na płaszczyźnie. Mówimy: „Dane proste się przecinają albo są równoległe”. Jest to alternatywa rozłączna $p \veebar q$, gdzie p oznacza zdanie „Dane proste się przecinają”, a q oznacza zdanie „Dane proste są równoległe”.

Zdanie $p \veebar q$ jest:

– prawdziwe, gdy jedno ze zdań p, q jest prawdziwe, a drugie fałszywe,

– fałszywe, gdy oba zdania p i q są jednocześnie prawdziwe lub jednocześnie fałszywe.

$v(p)$	$v(q)$	$v(p \veebar q)$
0	0	0
0	1	1
1	0	1
1	1	0

Alternatywy rozłącznej (w zdaniu prawdziwym) używamy, gdy chcemy podkreślić, że oba zdania nie mogą jednocześnie być prawdziwe.

Uwaga 1. Jeśli zdanie $p \veebar q$ jest prawdziwe, to zdanie $p \vee q$ też jest prawdziwe, np.: „Dane proste się przecinają lub są równoległe”. Jeśli zdanie $p \vee q$ jest prawdziwe, to zdanie $p \veebar q$ nie musi być prawdziwe, np.: „$0 < 1$ albo $0 > -1$”.

Równoważność zdań p i q:

$$p \Leftrightarrow q - \text{„}p \text{ wtedy i tylko wtedy, gdy } q\text{”}, \text{ „}p \text{ dokładnie wtedy, gdy } q\text{”}.$$

Przykład 7. Rozważmy czworokąt wypukły $ABCD$. Zdanie: „Czworokąt $ABCD$ jest opisany na okręgu wtedy i tylko wtedy, gdy $AB + CD = AD + BC$” jest równoważnością zdań p: „Czworokąt $ABCD$ jest opisany na okręgu” i q: „$AB + CD = AD + BC$”.

Zdanie $p \Leftrightarrow q$ jest:

– prawdziwe, gdy oba zdania p i q są jednocześnie prawdziwe lub jednocześnie fałszywe,

– fałszywe, gdy jedno ze zdań p, q jest prawdziwe, a drugie fałszywe.

$v(p)$	$v(q)$	$v(p \Leftrightarrow q)$
0	0	1
0	1	0
1	0	0
1	1	1

Implikacja o poprzedniku p i następniku q:

$$p \Rightarrow q \text{ – „jeśli } p\text{, to } q\text{”, „}p \text{ implikuje } q\text{”.}$$

Jak określamy wartość logiczną implikacji?

Przykład 8. Zdanie „$x = 1 \Rightarrow x^2 = 1$” jest prawdziwe dla każdej liczby rzeczywistej x. Zwróćmy uwagę na wartość logiczną poprzednika oraz następnika tej implikacji dla poszczególnych wartości x.

	„$x = 1$”	„$x^2 = 1$”
dla $x = 1$	prawda	prawda
dla $x = 0$	fałsz	fałsz
dla $x = -1$	fałsz	prawda

Prawdziwość implikacji oznacza, że jeśli zdanie p jest prawdziwe, to zdanie q też musi być prawdziwe (a jeśli p nie jest prawdziwe, to q może być jakiekolwiek).

Zdanie $p \Rightarrow q$ jest:

– prawdziwe, gdy oba zdania są prawdziwe, gdy oba zdania są fałszywe oraz gdy zdanie p jest fałszywe, a zdanie q jest prawdziwe,

– fałszywe, gdy zdanie p jest prawdziwe, a zdanie q jest fałszywe.

$v(p)$	$v(q)$	$v(p \Rightarrow q)$
0	0	1
0	1	1
1	0	0
1	1	1

Przy zapisywaniu bardziej skomplikowanych zdań logicznych używamy nawiasów, np.:

$$\sim (\sim p), \quad (p \wedge q) \vee r, \quad (p \Rightarrow q) \wedge \sim (q \Rightarrow r), \quad \sim (\sim (p \wedge q) \wedge (p \vee q)) \Rightarrow (p \Rightarrow q).$$

2.3 Kwantyfikatory

Zdanie

$$\text{„Dla każdego } x \in X \text{ (zachodzi) } \varphi(x)\text{”}$$

zapisujemy symbolicznie

$$\forall_{x \in X}\ \varphi(x).$$

Zdanie

$$\text{„Istnieje } x \in X \text{ takie, że } \varphi(x)\text{”},$$

zapisujemy

$$\exists_{x \in X}\ \varphi(x).$$

Zdanie $\exists_{x \in X}\ \varphi(x)$ jest prawdziwe dokładnie wtedy, gdy $\varphi(x)$ jest zdaniem prawdziwym dla co najmniej jednego $x \in X$.

Symbol $\forall$ nazywamy kwantyfikatorem ogólnym, a symbol $\exists$ nazywamy kwantyfikatorem szczegółowym.

$$\forall \text{ – for All} \qquad \exists \text{ – Exists}$$

W matematyce elementarnej popularne są polskie symbole kwantyfikatorów:

$\bigwedge$ – kwantyfikator ogólny (zamiast $\forall$),

$\bigvee$ – kwantyfikator szczegółowy (zamiast $\exists$).

Przykład 9. **Przykłady zdań z kwantyfikatorami:**

(a) $\forall_{x \in \mathbb{R}}\ x^2 < 1$ – zdanie fałszywe,

(b) $\exists_{x \in \mathbb{R}}\ x^2 < 1$ – zdanie prawdziwe,

(c) $\forall_{x \in \mathbb{R}}\ x^2 \geqslant 0$ – zdanie prawdziwe,

(d) $\exists_{x \in \mathbb{R}}\ x^2 \geqslant 0$ – zdanie prawdziwe,

(e) $\forall_{n \in \mathbb{N}_1}\ n \mid 6$ – zdanie fałszywe,

(f) $\exists_{n \in \mathbb{N}_1}\ n \mid 6$ – zdanie prawdziwe,

(g) $\forall_{n \in \mathbb{Z}}\ n = n + 1$ – zdanie fałszywe,

(h) $\exists_{n \in \mathbb{Z}}\ n = n + 1$ – zdanie fałszywe.

2.4 Wielokrotne użycie spójników

Zdania $(p \vee q) \vee r$ i $p \vee (q \vee r)$ mają zawsze tę samą wartość logiczną (dlaczego?), więc nawiasy możemy opuścić: $p \vee q \vee r$. Podobnie otrzymujemy zdanie $p \wedge q \wedge r$.

Zdanie $p_1 \wedge p_2 \wedge \ldots \wedge p_n$ jest:

– prawdziwe, gdy każde ze zdań $p_1, p_2, \ldots, p_n$ jest prawdziwe,

– fałszywe, gdy co najmniej jedno ze zdań $p_1, p_2, \ldots, p_n$ jest fałszywe.

Przykład 10. Niech $x_1, x_2, \ldots, x_n$ będą dowolnymi liczbami rzeczywistymi. Wówczas:

$$x_1^2 + x_2^2 + \ldots + x_n^2 = 0 \Leftrightarrow (x_1 = 0 \wedge x_2 = 0 \wedge \ldots \wedge x_n = 0).$$

Zdanie $p_1 \vee p_2 \vee \ldots \vee p_n$ jest:

– prawdziwe, gdy co najmniej jedno ze zdań $p_1, p_2, \ldots, p_n$ jest prawdziwe,

– fałszywe, gdy każde ze zdań $p_1, p_2, \ldots, p_n$ jest fałszywe.

Przykład 11. Niech $x_1, x_2, \ldots, x_n$ będą dowolnymi liczbami rzeczywistymi. Wówczas dla dowolnej liczby rzeczywistej x mamy:

$$(x - x_1)(x - x_2)\ldots(x - x_n) = 0 \Leftrightarrow (x = x_1 \vee x = x_2 \vee \ldots \vee x = x_n).$$

Zdania $(p \Leftrightarrow q) \Leftrightarrow r$ i $p \Leftrightarrow (q \Leftrightarrow r)$ mają zawsze tę samą wartość logiczną (sprawdź!), ale wartość logiczną zdania $p \Leftrightarrow q \Leftrightarrow r$ określamy inaczej.

Przykład 12. Dla dowolnych liczb dodatnich a, b zachodzą równoważności:

$$\frac{a+b}{2} \geqslant \sqrt{ab} \Leftrightarrow a + b \geqslant 2\sqrt{ab} \Leftrightarrow a + b - 2\sqrt{ab} \geqslant 0 \Leftrightarrow (\sqrt{a} - \sqrt{b})^2 \geqslant 0.$$

Zdanie $p_1 \Leftrightarrow p_2 \Leftrightarrow \ldots \Leftrightarrow p_n$ definiujemy jako koniunkcję kolejnych równoważności:

$$(p_1 \Leftrightarrow p_2) \wedge (p_2 \Leftrightarrow p_3) \wedge \ldots \wedge (p_{n-2} \Leftrightarrow p_{n-1}) \wedge (p_{n-1} \Leftrightarrow p_n).$$

Zdanie $p_1 \Leftrightarrow p_2 \Leftrightarrow \ldots \Leftrightarrow p_n$ jest:

– prawdziwe, gdy wszystkie zdania $p_1, p_2, \ldots, p_n$ są jednocześnie prawdziwe lub jednocześnie fałszywe,

– fałszywe, gdy wśród zdań $p_1, p_2, \ldots, p_n$ są zdania prawdziwe i zdania fałszywe.

Jak można określić prawdziwość zdania

$$p_1 \Rightarrow p_2 \Rightarrow \ldots \Rightarrow p_n?$$

Zdanie $p_1 \Rightarrow p_2 \Rightarrow \ldots \Rightarrow p_n$ definiujemy jako koniunkcję kolejnych implikacji:

$$(p_1 \Rightarrow p_2) \wedge (p_2 \Rightarrow p_3) \wedge \ldots \wedge (p_{n-2} \Rightarrow p_{n-1}) \wedge (p_{n-1} \Rightarrow p_n).$$

Zdanie $p_1 \Rightarrow p_2 \Rightarrow \ldots \Rightarrow p_n$ jest:

– prawdziwe, gdy wszystkie zdania $p_1, p_2, \ldots, p_n$ są jednocześnie prawdziwe lub jednocześnie fałszywe, lub dla pewnego k zdania p_1, p_2, …, p_k są fałszywe, a p_{k+1}, …, p_n są prawdziwe,

– fałszywe, gdy dla pewnych $i < j$ zdanie p_i jest prawdziwe, a zdanie p_j jest fałszywe.

3 Rachunek zdań

3.1 Wyrażenia rachunku zdań

Ważną własnością spójników logicznych jest to, że wartość logiczna zdania złożonego zależy jedynie od sposobu, w jaki jest ono zbudowane i od wartości logicznych jego zdań składowych. Wartość logiczna zdania złożonego nie zależy od konkretnej postaci (treści) zdań składowych.

Dlatego możemy rozważać wyrażenia rachunku zdań utworzone poprawnie (za pomocą spójników logicznych i nawiasów) z symboli p, q, r, itp. Symbole te nazywamy zmiennymi zdaniowymi. Gdy w takim wyrażeniu podstawimy za zmienne zdaniowe konkretne zdania logiczne, to otrzymamy złożone zdanie logiczne.

Uwaga 2. Jeśli to nie prowadzi do nieporozumień, to zmienne zdaniowe i wyrażenia z nich utworzone możemy nazywać krótko zdaniami.

3.2 Metoda zero-jedynkowa

Wartość logiczną zdania złożonego

$$((p \Rightarrow q) \wedge (q \Rightarrow p)) \Rightarrow (p \wedge q)$$

dla poszczególnych wartościowań zdań prostych możemy obliczyć następująco:

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$p \wedge q$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$	$((p \Rightarrow q) \wedge (q \Rightarrow p)) \Rightarrow (p \wedge q)$
0	0	1	1	0	1	0
0	1	1	0	0	0	1
1	0	0	1	0	0	1
1	1	1	1	1	1	1

Szybszy sposób polega na tym, że nie wypisujemy poszczególnych zdań składowych w oddzielnych kolumnach (np. $p \Rightarrow q$, $q \Rightarrow p$ i $p \wedge q$), piszemy tylko całe zdanie złożone, a wartości logiczne poszczególnych zdań składowych wypisujemy pod tymi zdaniami (dokładniej: pod ich spójnikami logicznymi). Gdy wypiszemy np. wartości logiczne zdań $p \Rightarrow q$ i $q \Rightarrow p$, to wartości logiczne zdania $(p \Rightarrow q) \wedge (q \Rightarrow p)$ wypisujemy pod spójnikiem „$\wedge$”.

p	q	$((p$	$\Rightarrow$	$q)$	$\wedge$	$(q$	$\Rightarrow$	$p))$	$\Rightarrow$	$(p$	$\wedge$	$q)$
0	0		1		1		1		0		0	
0	1		1		0		0		1		0	
1	0		0		0		1		1		0	
1	1		1		1		1		1		1	

3.3 Wyrażenia logicznie równoważne

Przykład 13. Wyrażenia

$$(p \vee q) \wedge r \quad \text{i} \quad (p \wedge r) \vee (q \wedge r)$$

mają równe wartości logiczne dla dowolnych wartości logicznych zmiennych zdaniowych.

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

Definicja 1. *Wyrażenia rachunku zdań nazywamy* **logicznie równoważnymi**, *gdy mają równe wartości logiczne dla dowolnych wartości logicznych zmiennych zdaniowych.*

Przykład 14. (a) Wyrażenia p i $\sim (\sim p)$ są logicznie równoważne.

(b) Wyrażenia

$$p \Rightarrow q, \quad \sim q \Rightarrow \sim p, \quad (\sim p) \vee q \quad \text{i} \quad \sim (p \wedge \sim q)$$

są logicznie równoważne.

Przykład 15. (a) Wyrażenia $(p \vee q) \wedge r$ i $(p \wedge r) \vee (q \wedge r)$ są logicznie równoważne.

(b) Wyrażenia $(p \wedge q) \vee r$ i $(p \vee r) \wedge (q \vee r)$ są logicznie równoważne.

Czasami można uzasadnić logiczną równoważność wyrażeń bez korzystania z tabelki. Na przykład, zdanie $\sim (p \wedge q)$ jest fałszywe tylko w przypadku, gdy zdanie $p \wedge q$ jest prawdziwe, czyli gdy oba zdania p i q są prawdziwe. Zdanie $\sim p \vee \sim q$ jest fałszywe tylko w przypadku, gdy oba zdania $\sim p$, $\sim q$ są fałszywe, czyli też tylko, gdy oba zdania p i q są prawdziwe. Zatem zdania

$$\sim (p \wedge q) \quad \text{i} \quad \sim p \vee \sim q$$

są logicznie równoważne.

Analogicznie możemy uzasadnić, że zdania

$$\sim (p \vee q) \quad \text{i} \quad \sim p \wedge \sim q$$

są logicznie równoważne.

3.4 Tautologie

Przykład 16. Wyrażenie

$$(p \Rightarrow q) \vee (q \Rightarrow p)$$

ma wartość logiczną „prawda” dla dowolnych wartości logicznych zdań prostych.

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \vee (q \Rightarrow p)$
0	0	1	1	1
0	1	1	0	1
1	0	0	1	1
1	1	1	1	1

Definicja 2. Tautologią *nazywamy wyrażenie rachunku zdań, które ma wartość logiczną „prawda” dla dowolnych wartości logicznych zmiennych zdaniowych.*

Przykład 17. **Przykłady tautologii:**

(a) $p \Rightarrow p$,

(b) $p \vee \sim p$,

(c) $\sim (p \wedge \sim p)$,

(d) $(\sim p \Rightarrow p) \Rightarrow p$,

(e) $(p \wedge q) \Rightarrow p$,

(f) $p \Rightarrow (p \vee q)$,

(g) $\sim p \Rightarrow (p \Rightarrow q)$,

(h) $((p \Rightarrow q) \wedge (q \Rightarrow p)) \Rightarrow (p \Leftrightarrow q)$,

(i) $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$.

Wyrażenie postaci $P \Leftrightarrow Q$ jest tautologią dokładnie wtedy, gdy wyrażenia P i Q są logicznie równoważne.

Przykład 18. **Przykłady tautologii w postaci równoważności:**

(a) Prawo podwójnego przeczenia:

$$p \Leftrightarrow \sim (\sim p).$$

(b) Prawa de Morgana:

$$\sim (p \wedge q) \Leftrightarrow (\sim p \vee \sim q),$$
$$\sim (p \vee q) \Leftrightarrow (\sim p \wedge \sim q).$$

(c) Metoda dowodu „nie wprost” jest oparta na tautologii

$$(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p).$$

(d) Metoda dowodu „przez sprzeczność” jest oparta na tautologii

$$(p \Rightarrow q) \Leftrightarrow \sim (p \wedge \sim q).$$

(e) Rozdzielność koniunkcji względem alternatywy:

$$(p \vee q) \wedge r \Leftrightarrow (p \wedge r) \vee (q \wedge r).$$

(f) Rozdzielność alternatywy względem koniunkcji:

$$(p \wedge q) \vee r \Leftrightarrow (p \vee r) \wedge (q \vee r).$$

3.5 Reguły dowodzenia

Rozważmy wyrażenia rachunku zdań $P_1, \ldots, P_n, Q$. Jeśli wyrażenie

$$P_1 \wedge \ldots \wedge P_n \Rightarrow Q$$

jest tautologią, to schemat

$$\frac{\begin{array}{c} P_1 \\ \vdots \\ P_n \end{array}}{Q}$$

nazywamy regułą dowodzenia. Reguła dowodzenia oznacza, że z prawdziwości zdań $P_1, \ldots, P_n$ wynika prawdziwość zdania Q.

Przykład 19. **Przykłady reguł dowodzenia**

$$\frac{p \wedge q}{p} \qquad \frac{p}{p \vee q} \qquad \frac{q}{p \Rightarrow q} \qquad \frac{\sim p}{p \Rightarrow q}$$

$$\frac{\begin{array}{c} p \\ q \end{array}}{p \wedge q} \qquad \frac{\begin{array}{c} p \\ p \Leftrightarrow q \end{array}}{q} \qquad \frac{\begin{array}{c} p \Rightarrow q \\ q \Rightarrow r \end{array}}{p \Rightarrow r} \qquad \frac{\begin{array}{c} p \Rightarrow q \\ q \Rightarrow p \end{array}}{p \Leftrightarrow q}$$

Możemy patrzeć na reguły dowodzenia jak na inny zapis pewnych tautologii, ale faktycznie ich rola jest znacznie ważniejsza. W teoriach formalnych reguły dowodzenia określają sposób uzyskiwania twierdzeń danej teorii wychodząc od aksjomatów. Szczególnie ważna jest reguła odrywania (modus ponens)

$$\frac{\begin{array}{c} p \\ p \Rightarrow q \end{array}}{q}$$

która oznacza, że jeśli zdanie p jest twierdzeniem danej teorii i udowodnimy, że z p wynika q, to q też jest twierdzeniem.

4 Rachunek kwantyfikatorów

4.1 Formy zdaniowe

Forma zdaniowa $\varphi(x)$ określona w zbiorze X to wyrażenie, które jest zdaniem, jeśli za x wstawimy dowolny element zbioru X. Zbiór X nazywamy zakresem formy zdaniowej $\varphi(x)$.

Przykład 20. (a) $\varphi(x) =$ „$x^2 < 1$”, gdzie $x \in \mathbb{R}$,
$\varphi(x)$ jest zdaniem:

- prawdziwym dla $x \in (-1, 1)$,
- fałszywym dla $x \in (-\infty, -1] \cup [1, +\infty)$,

(b) $\varphi(x) =$ „$x^2 \geqslant 0$”, gdzie $x \in \mathbb{R}$,
$\varphi(x)$ jest zdaniem prawdziwym dla wszystkich $x \in \mathbb{R}$,

(c) $\varphi(n) =$ „$n \mid 6$” (n dzieli 6), gdzie $n \in \mathbb{N}_1$,
$\varphi(n)$ jest zdaniem:

- prawdziwym dla $n = 1, 2, 3, 6$
- fałszywym dla pozostałych n,

(d) $\varphi(n) =$ „$n = n + 1$”, gdzie $n \in \mathbb{Z}$,
$\varphi(n)$ jest zdaniem fałszywym dla każdego $n \in \mathbb{Z}$.

Uwaga 3. Forma zdaniowa określona w zbiorze X pozwala każdemu elementowi tego zbioru przyporządkować zdanie. Możemy więc ją nazwać funkcją zdaniową.

Pytanie 2. *Co jest dziedziną tej funkcji?*

4.2 Kwantyfikatory

Jeśli $\varphi(x)$ jest formą zdaniową określoną w zbiorze X, to możemy utworzyć następujące dwa zdania logiczne.

1. Zdanie

„Dla każdego $x \in X$ (zachodzi) $\varphi(x)$”,

które zapisujemy:

$$\forall_{x \in X}\ \varphi(x).$$

2. Zdanie

„Istnieje $x \in X$ takie, że $\varphi(x)$”,

które zapisujemy:

$$\exists_{x \in X}\ \varphi(x).$$

Zauważmy, że:

– jeśli $\varphi(x)$ jest zdaniem prawdziwym dla wszystkich $x \in X$, to zdania $\forall_{x\in X}\ \varphi(x)$ i $\exists_{x\in X}\ \varphi(x)$ są prawdziwe,

– jeśli $\varphi(x)$ jest zdaniem fałszywym dla wszystkich $x \in X$, to zdania $\forall_{x\in X}\ \varphi(x)$ i $\exists_{x\in X}\ \varphi(x)$ są fałszywe,

– jeśli $\varphi(x)$ jest zdaniem prawdziwym dla pewnych elementów zbioru X, a fałszywym dla innych elementów tego zbioru, to zdanie $\forall_{x\in X}\ \varphi(x)$ jest fałszywe, a zdanie $\exists_{x\in X}\ \varphi(x)$ jest prawdziwe.

Definicja 3. Zbiorem spełniania *formy zdaniowej $\varphi(x)$, określonej w zbiorze X, nazywamy zbiór wszystkich elementów $x \in X$, dla których $\varphi(x)$ jest zdaniem prawdziwym.*

Zauważmy, że:

– zdanie $\forall_{x\in X}\ \varphi(x)$ jest prawdziwe wtedy i tylko wtedy, gdy zbiorem spełniania formy $\varphi(x)$ jest cały zbiór X,

– zdanie $\exists_{x\in X}\ \varphi(x)$ jest prawdziwe wtedy i tylko wtedy, gdy zbiór spełniania formy $\varphi(x)$ jest niepusty.

Pytanie 3. *Jak należy określić wartość logiczną zdań $\forall_{x\in X}\ \varphi(x)$ i $\exists_{x\in X}\ \varphi(x)$ w przypadku, gdy X jest zbiorem pustym?*

Jeśli zakres formy zdaniowej (zbiór X) jest jasno określony, to zamiast $\forall_{x\in X}\ \varphi(x)$ i $\exists_{x\in X}\ \varphi(x)$ możemy pisać: $\forall_x\ \varphi(x)$, $\exists_x\ \varphi(x)$.

4.3 Formy zdaniowe wielu zmiennych

Możemy rozważać formy zdaniowe większej liczby zmiennych, np. $\varphi(x, y, z)$, gdzie $x \in X$, $y \in Y$, $z \in Z$ lub $\varphi(x, y)$, gdzie $x, y \in X$. Ogólniej, rozważamy formy zdaniowe postaci $\varphi(x_1, \ldots, x_n)$, gdzie $x_1, \ldots, x_n \in X$ lub $x_1 \in X_1$, $\ldots$, $x_n \in X_n$.

Przykład 21. **Przykłady form zdaniowych:**

(a) „$x < y$”, gdzie $x, y \in \mathbb{N}$,

(b) „$x \cdot y = 0$”, gdzie $x \in \mathbb{Z}$, $y \in \mathbb{R}$,

(c) „$A \in k$”, gdzie A należy do zbioru punktów na płaszczyźnie, k należy do zbioru prostych na płaszczyźnie,

(d) „Punkt A leży między punktami B i C”, gdzie A, B, C należą do zbioru punktów na płaszczyźnie.

Rozważmy formę zdaniową $\varphi(x, y)$ zmiennych $x, y \in X$. Zdanie

$$\forall_{x\in X}\ \forall_{y\in X}\ \varphi(x, y)$$

oznacza, że dla każdego $x \in X$ zachodzi to, że dla każdego $y \in X$ zachodzi $\varphi(x, y)$. Prościej:

„dla dowolnych $x, y \in X$ zachodzi $\varphi(x, y)$”,

co zapisujemy używając jednego symbolu kwantyfikatora:

$$\forall_{x,y\in X}\ \varphi(x, y).$$

Zdanie

$$\exists_{x\in X}\ \exists_{y\in X}\ \varphi(x, y)$$

oznacza, że istnieje $x \in X$, dla którego istnieje $y \in X$ taki, że zachodzi $\varphi(x, y)$. Prościej:

„istnieją $x, y \in X$ takie, że $\varphi(x, y)$”,

co też zapisujemy używając jednego symbolu kwantyfikatora:

$$\exists_{x,y\in X}\ \varphi(x, y).$$

Niech teraz $\varphi(x_1, \ldots, x_n)$ będzie formą zdaniową zmiennych x_1, …, x_n, gdzie $x_1 \in X_1$, …, $x_n \in X_n$. Zdanie

„Dla dowolnych $x_1 \in X_1$, …, $x_n \in X_n$ (zachodzi) $\varphi(x_1, \ldots, x_n)$”

zapisujemy

$$\forall_{x_1\in X_1,\ldots,x_n\in X_n}\ \varphi(x_1, \ldots, x_n).$$

Zdanie

„Istnieją $x_1 \in X_1$, …, $x_n \in X_n$ takie, że $\varphi(x_1, \ldots, x_n)$”,

zapisujemy

$$\exists_{x_1\in X_1,\ldots,x_n\in X_n}\ \varphi(x_1, \ldots, x_n).$$

Zadanie 1. *Które z następujących zdań są prawdziwe, a które fałszywe:*

$$\forall_{x,y\in\mathbb{Z}}\ x < y, \qquad \forall_{x,y\in\mathbb{R}}\ x \cdot y = y \cdot x, \qquad \exists_{x\in\mathbb{N}}\ \exists_{y\in\mathbb{Z}}\ x < y?$$

Niech $\varphi(x, y)$ będzie formą zdaniową zmiennych $x \in X$, $y \in Y$.

Zdanie

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

oznacza, że istnieje $x \in X$ takie, że $\varphi(x, y)$ zachodzi dla każdego $y \in Y$.

Zdanie

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

oznacza, że dla każdego $x \in X$ istnieje takie $y \in Y$, że zachodzi $\varphi(x, y)$.

Zadanie 2. *Które z następujących zdań są prawdziwe, a które fałszywe:*

$$\forall_{x\in\mathbb{Z}}\ \exists_{y\in\mathbb{Z}}\ x < y, \qquad \exists_{x\in\mathbb{Z}}\ \forall_{y\in\mathbb{Z}}\ x < y, \qquad \exists_{x\in\mathbb{Z}}\ \forall_{y\in\mathbb{Z}}\ x \cdot y = 0?$$

Zadanie 3. *Utwórz kilka ciekawych zdań z użyciem kwantyfikatorów $\forall$, $\exists$ i form zdaniowych:*

$$x < y, \quad x \leqslant y, \quad x \cdot y = 0, \quad x \cdot y = 1,$$

gdzie x, y przebiegają zbiory: $\mathbb{N}$, $\mathbb{N}_1$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$. Określ prawdziwość utworzonych zdań.

Jeśli $\varphi(x, y)$ jest formą zdaniową zmiennych x, y, gdzie $x \in X$, $y \in Y$, to

$$\forall_{y \in Y}\ \varphi(x, y) \quad \text{i} \quad \exists_{y \in Y}\ \varphi(x, y)$$

są formami zdaniowymi zmiennej x. Mówimy, że w tych wyrażeniach x jest zmienną wolną, a y jest zmienną związaną. Natomiast w wyrażeniach

$$\forall_{x \in X}\ \forall_{y \in Y}\ \varphi(x, y), \quad \exists_{x \in X}\ \forall_{y \in Y}\ \varphi(x, y),$$

$$\forall_{x \in X}\ \exists_{y \in Y}\ \varphi(x, y) \quad \text{i} \quad \exists_{x \in X}\ \exists_{y \in Y}\ \varphi(x, y)$$

zmienne x i y są obie zmiennymi związanymi.

Zadanie 4. *Rozważmy następujące funkcje zdaniowe zmiennej $x \in \mathbb{Z}$:*

$$1)\ \forall_{y \in \mathbb{N}}\ x < y, \quad 2)\ \exists_{y \in \mathbb{N}}\ x < y, \quad 3)\ \forall_{y \in \mathbb{R}}\ x \cdot y = 0, \quad 4)\ \exists_{y \in \mathbb{Z}}\ x \cdot y = 1.$$

Dla jakich wartości $x \in \mathbb{Z}$ są to zdania prawdziwe?

Odpowiedź:
1) dla wszystkich $x < 0$,
2) dla wszystkich $x \in \mathbb{Z}$,
3) dla $x = 0$,
4) dla $x \in \{1, -1\}$.

4.4 Przykłady użycia kwantyfikatorów

Przykład 22. Przykłady definicji zapisanych za pomocą kwantyfikatorów.

(a) Dla $a \in \mathbb{Z}$ zdanie „a jest liczbą parzystą”:

$$\exists_{k \in \mathbb{Z}}\ a = 2k.$$

(b) Dla $a, b \in \mathbb{Z}$ zdanie „a jest podzielne przez b”:

$$\exists_{k \in \mathbb{Z}}\ a = k \cdot b.$$

(c) Dla $p \in \mathbb{N}_1$ zdanie „p jest liczbą pierwszą”:

$$(p \neq 1) \wedge \forall_{a \in \mathbb{N}_1}\ (a \mid p \Rightarrow a = 1 \vee a = p).$$

(d) Dla $b \in \mathbb{R}$ i $A \subset \mathbb{R}$ zdanie „b jest ograniczeniem z góry zbioru A”:

$$\forall_{a \in A}\ a \leqslant b.$$

Przykład 23. (a) Między dowolnymi dwiema różnymi liczbami rzeczywistymi istnieje liczba wymierna:

$$\forall_{x\in\mathbb{R}}\,\forall_{y\in\mathbb{R}}\,(x\neq y\Rightarrow\exists_{w\in\mathbb{Q}}\,((x<w\wedge w<y)\vee(y<w\wedge w<x)))$$

lub krócej:

$$\forall_{x,y\in\mathbb{R}}\,(x<y\Rightarrow\exists_{w\in\mathbb{Q}}\,x<w<y).$$

(b) Od pewnego miejsca wszystkie wyrazy ciągu (x_n) są dodatnie:

$$\exists_N\forall_{n>N}\,x_n>0.$$

(c) Zasada indukcji matematycznej:

$$(T(0)\wedge\forall_{n\in\mathbb{N}}\,(T(n)\Rightarrow T(n+1)))\Rightarrow\forall_{n\in\mathbb{N}}\,T(n).$$

4.5 Prawa rachunku kwantyfikatorów

Prawo rachunku kwantyfikatorów to wyrażenie utworzone poprawnie z symboli kwantyfikatorów $\forall$, $\exists$, symboli form zdaniowych, np. $\varphi(x)$, $\psi(x,y)$, oraz spójników logicznych, które jest zdaniem prawdziwym dla dowolnej formy zdaniowej i dowolnych wartości zmiennych.

Prawa de Morgana dla kwantyfikatorów:

$$\sim(\forall_{x\in X}\,\varphi(x))\Leftrightarrow\exists_{x\in X}\,(\sim\varphi(x)),$$

$$\sim(\exists_{x\in X}\,\varphi(x))\Leftrightarrow\forall_{x\in X}\,(\sim\varphi(x)).$$

Przykład 24. (a) Liczba b nie jest ograniczeniem z góry zbioru A:

$$\sim(\forall_{a\in A}\,a\leqslant b)\Leftrightarrow\exists_{a\in A}\ \sim(a\leqslant b)\Leftrightarrow\exists_{a\in A}\,a>b.$$

(b) W zbiorze $\mathbb{N}$ nie ma liczby największej:

$$\sim(\exists_{m\in\mathbb{N}}\,\forall_{n\in\mathbb{N}}\,m\geqslant n)\Leftrightarrow\forall_{m\in\mathbb{N}}\ \sim(\forall_{n\in\mathbb{N}}\,m\geqslant n)$$

$$\Leftrightarrow\forall_{m\in\mathbb{N}}\,\exists_{n\in\mathbb{N}}\ \sim(m\geqslant n)\Leftrightarrow\forall_{m\in\mathbb{N}}\,\exists_{n\in\mathbb{N}}\,m<n.$$

Inne ważne prawa rachunku kwantyfikatorów:

$$(\forall_{x\in X}\,\varphi(x))\ \Rightarrow\ (\exists_{x\in X}\,\varphi(x)),$$

$$(\exists_{x\in X}\,\forall_{y\in Y}\,\varphi(x,y))\ \Rightarrow\ (\forall_{y\in Y}\,\exists_{x\in X}\,\varphi(x,y)).$$

Dla danego elementu $x_0\in X$ mamy prawa:

$$(\forall_{x\in X}\,\varphi(x))\ \Rightarrow\ \varphi(x_0),$$

$$\varphi(x_0)\ \Rightarrow\ (\exists_{x\in X}\,\varphi(x)).$$

5 Twierdzenia i dowody

5.1 Twierdzenia

Twierdzenie to prawdziwe zdanie logiczne dotyczące obiektów danej teorii. Przykład:

„$\sqrt{2}$ jest liczbą niewymierną".

Twierdzenia na ogół mają postać implikacji

$$p \Rightarrow q,$$

a dokładniej:

$$\forall_{x \in X}(p(x) \Rightarrow q(x)),$$

gdzie $p(x)$ i $q(x)$ to formy zdaniowe określone w pewnym zbiorze X. Zdanie p nazywamy założeniem, a zdanie q – tezą twierdzenia. Mówimy też, że p jest warunkiem wystarczającym (dostatecznym) dla q, a q jest warunkiem koniecznym dla p.

Pytanie 4. *Warunkiem wystarczającym na podzielność liczby naturalnej przez* 9 *jest to, by suma cyfr jej zapis dziesiętnego była równa* 9*. Czy jest to warunek konieczny?*

Pytanie 5. *Warunkiem koniecznym na to, by czworokąt był kwadratem jest posiadanie wszystkich kątów prostych. Czy jest to warunek wystarczający?*

Twierdzenie $q \Rightarrow p$ nazywamy odwrotnym do twierdzenia $p \Rightarrow q$.

Przykład 25. **Twierdzenie:**

„Dla dowolnego trójkąta ABC, jeśli $|\sphericalangle BAC| = 90°$, to $|AB|^2 + |AC|^2 = |BC|^2$."

Twierdzenie odwrotne:

„Dla dowolnego trójkąta ABC, jeśli $|AB|^2 + |AC|^2 = |BC|^2$, to $|\sphericalangle BAC| = 90°$."

Niektóre twierdzenia mają postać zamkniętego układu implikacji

$$\begin{cases} p_1 \Rightarrow q_1 \\ p_2 \Rightarrow q_2 \\ \quad \vdots \\ p_n \Rightarrow q_n, \end{cases}$$

gdzie dla każdego x dokładnie jedno ze zdań $p_1(x)$, $p_2(x)$, …, $p_n(x)$ jest prawdziwe.

Przykład 26. Dla dowolnego trójkąta ABC:

$$\begin{cases} |\sphericalangle BAC| < 90° \Rightarrow |AB|^2 + |AC|^2 > |BC|^2, \\ |\sphericalangle BAC| = 90° \Rightarrow |AB|^2 + |AC|^2 = |BC|^2, \\ |\sphericalangle BAC| > 90° \Rightarrow |AB|^2 + |AC|^2 < |BC|^2. \end{cases}$$

5.2 Dowody dedukcyjne i redukcyjne

Podstawową metodą dowodzenia twierdzeń postaci

$$p \Rightarrow q$$

jest dowód dedukcyjny będący w najprostszym przypadku ciągiem implikacji wychodzących od założenia i kończących się tezą:

$$p \Rightarrow p_1 \Rightarrow \ldots \Rightarrow p_k \Rightarrow q.$$

Przykład 27. Jeśli a, b, c $(a \neq 0)$ są takimi liczbami całkowitymi, że $a \mid b$ i $a \mid c$, to $a \mid b + c$.

Dowód. Niech a, b, c $(a \neq 0)$ będą takimi liczbami całkowitymi, że $a \mid b$ i $a \mid c$. Skoro $a \mid b$, to istnieje $k \in \mathbb{Z}$, takie że $b = ka$. Skoro $a \mid c$, to istnieje $k \in \mathbb{Z}$, takie że $c = la$. Zatem $b + c = ka + la = (k + l)a$, co oznacza, że $a \mid b + c$. □

Ciąg implikacji

$$p \Rightarrow p_1 \Rightarrow \ldots \Rightarrow p_k \Rightarrow q$$

czasami konstruujemy od końca, nazywamy to metodą redukcyjną.

Przykład 28. Jeśli liczby rzeczywiste a, b są dodatnie, to

$$\frac{a+b}{2} \geqslant \sqrt{ab}.$$

Dowód redukcyjny powyższej nierówności został uzyskany w Przykładzie 12, str. 13.

W praktyce często stosujemy metodę mieszaną, łączącą elementy obu metod.

5.3 Metoda „nie wprost”

Metoda dowodu „nie wprost” jest oparta na tautologii

$$(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p).$$

Zadanie 5. *Dane są liczby całkowite a i b. Wykaż, że jeśli $a \cdot b$ jest liczbą parzystą, to a jest parzyste lub b jest parzyste.*

Dowód. Załóżmy, wbrew tezie, że a i b nie są parzyste, czyli $a = 2k + 1$, $b = 2l + 1$, gdzie k i l są liczbami całkowitymi. Wówczas iloczyn

$$a \cdot b = (2k + 1)(2l + 1) = 4kl + 2k + 2l + 1 = 2(2kl + k + l) + 1$$

nie jest liczbą parzystą. □

Zadanie 6. *Dane są liczby naturalne k_1, k_2, …, $k_n > 0$. Wykaż, że jeśli*

$$(*) \qquad \frac{1}{k_1} + \ldots + \frac{1}{k_n} > \frac{n}{2},$$

to $k_i = 1$ dla pewnego i.

Dowód. Załóżmy, wbrew tezie, że $k_i \neq 1$ dla każdego i. Zatem $k_1, \ldots, k_n \geqslant 2$, skąd

$$\frac{1}{k_1} + \ldots + \frac{1}{k_n} \leqslant \underbrace{\frac{1}{2} + \ldots + \frac{1}{2}}_{n} = \frac{n}{2},$$

co oznacza, że nierówność $(*)$ nie zachodzi. □

5.4 Metoda „przez sprzeczność"

Metoda dowodu zdania p „przez sprzeczność" polega na przyjęciu założenia $\sim p$ i wywnioskowaniu z niego „sprzeczności": zdania fałszywego lub dwóch zdań wzajemnie sprzecznych.

Zadanie 7. *Udowodnij, że liczba $\sqrt{2}$ jest niewymierna.*

Dowód. Przypuśćmy, że $\sqrt{2}$ jest liczbą wymierną: $\sqrt{2} = \frac{m}{n}$, gdzie m i n są liczbami całkowitymi, $n \neq 0$, przy czym możemy założyć, że $\mathrm{NWD}\,(m, n) = 1$.

Wówczas $\frac{m^2}{n^2} = 2$, skąd $m^2 = 2n^2$, więc m^2 jest liczbą parzystą. Zatem m jest liczbą parzystą: $m = 2k$, gdzie k jest liczbą całkowitą. Otrzymujemy: $(2k)^2 = 2n^2$, czyli $2k^2 = n^2$. Tak więc n też jest liczbą parzystą, a to oznacza, że $\mathrm{NWD}\,(m, n) \neq 1$ – sprzeczność. □

Metoda dowodu implikacji

$$p \Rightarrow q$$

„przez sprzeczność" jest oparta na tautologii

$$(p \Rightarrow q) \Leftrightarrow \sim (p \wedge \sim q).$$

Zadanie 8. *Dane są liczby rzeczywiste x, y. Udowodnij, że jeżeli $x^2 + y^2 < 1$, to $x + y < \sqrt{2}$.*

Dowód. Przypuśćmy, że nierówność $x^2 + y^2 < 1$ zachodzi, a nierówność $x + y < \sqrt{2}$ nie zachodzi, czyli zachodzi nierówność $x+y \geqslant \sqrt{2}$. Podnosząc tę ostatnią nierówność obustronnie do kwadratu, otrzymujemy:

$$x^2 + y^2 + 2xy \geqslant 2.$$

Z nierówności $x^2 + y^2 < 1$ wynika, że $2x^2 + 2y^2 < 2$. Zatem

$$2x^2 + 2y^2 < x^2 + y^2 + 2xy,$$

skąd po przekształceniach dostajemy:

$$(x - y)^2 < 0.$$

Otrzymana sprzeczność kończy dowód. □

5.5 Przegląd metod dowodzenia twierdzeń

Tabela na następnej stronie zawiera zestawienie podstawowych technik dowodowych. Założenie twierdzenia jest oznaczone przez A, teza przez B. Tabela została zaczerpnięta z rozprawy Clausa Zinna pt. „Understanding informal mathematical discourse" ([24], str. 40), oryginalnie pochodzi z książki Daniela Solowa „How to read and do proofs" ([23]).

Technika dowodu	Kiedy używamy?	Co zakładamy?	Co mamy uzyskać?	Jak to wykonujemy?
dedukcyjno – redukcyjna	Jako pierwsza próba oraz gdy B nie ma rozpoznawalnej postaci.	A	B	Wyciągamy kolejne wnioski z A, budujemy przesłanki, z których wynika B.
nie wprost	Gdy w B jest słowo „nie”.	nie B	nie A	Wyciągamy kolejne wnioski z „nie B”, budujemy przesłanki, z których wynika „nie A”.
przez sprzeczność	Gdy w B jest słowo „nie” oraz gdy pierwsze dwie metody zawodzą.	A i „nie B”	Jakąś sprzeczność	Wyciągamy wnioski z A i „nie B”, aż uzyskamy sprzeczność.
konstrukcja	Gdy w B jest zwrot „istnieje”, „jest”, „dla pewnego” lub podobny.	A	Istnieje szukany obiekt.	Odgadujemy lub konstruujemy szukany obiekt. Następnie pokazujemy, że ten obiekt ma wymaganą własność.
wybór	Gdy w B jest zwrot „dla dowolnego”, „dla każdego” lub podobny.	A, i wybieramy obiekt mający daną własność.	Zachodzi pewien warunek.	Wyciągamy wnioski z A i z tego, że ten obiekt ma daną własność. Również budujemy przesłanki, z których wynika, że zachodzi rozważany warunek.
indukcja	Gdy B ma zachodzić dla każdej liczby naturalnej, począwszy od pewnej liczby, np. n_0.	Twierdzenie zachodzi dla n.	Twierdzenie zachodzi dla $n+1$. Trzeba też sprawdzić, że twierdzenie zachodzi dla n_0.	Najpierw podstawiamy n_0 za n i pokazujemy, że twierdzenie jest prawdziwe. Następnie przyjmujemy założenie, że twierdzenie zachodzi dla n i dowodzimy go dla $n+1$.
przypadek szczególny	Gdy w B jest zwrot „istnieje”, „dla wszystkich”, „dla każdego” lub podobny.	A	B	Wyciągamy wnioski przez zastosowanie A do jednego konkretnego obiektu mającego daną własność.
bezpośrednia jednoznaczność	Gdy w B jest zwrot „dokładnie jeden” lub „jednoznacznie określony”.	Są dwa (niekoniecznie różne) takie obiekty i zachodzi A.	Te dwa obiekty są równe.	Wyciągamy wnioski wykorzystując A oraz własności danych obiektów. Również budujemy przesłanki, z których wynika, że te obiekty są równe.
pośrednia jednoznaczność	Gdy w B jest zwrot „dokładnie jeden” lub „jednoznacznie określony”.	Są dwa różne takie obiekty i zachodzi A.	Jakąś sprzeczność.	Wyciągamy wnioski z A wykorzystując własności danych obiektów oraz fakt, że są różne.
przez eliminację	Gdy B ma postać „C lub D”	A i „nie C”	D	Wyciągamy wnioski z A i „nie C”, a także budujemy przesłanki, z których wynika D.
przez przypadki	Gdy A ma postać „C lub D”	Przypadek 1: C Przypadek 2: D	B B	Najpierw dowodzimy, że z C wynika B, następnie dowodzimy, że z D wynika B.
max/min 1	Gdy B ma postać „$\max S \leqslant x$” lub „$\min S \geqslant x$”	Wybieramy element s w zbiorze S i zakładamy A.	$s \leqslant x$ lub $s \geqslant x$	Wyciągamy wnioski z A oraz z faktu, że s należy do S. Również budujemy przesłanki, z których wynika B.
max/min 2	Gdy B ma postać „$\max S \geqslant x$” lub „$\min S \leqslant x$”	A	Konstrukcję elementu s zbioru S, takiego że $s \geqslant x$ lub $s \leqslant x$	Wykorzystujemy A oraz sposób konstrukcji do stworzenia szukanego elementu s zbioru S.

6 Indukcja matematyczna

6.1 Dyskusja

Przykład 29. Oblicz sumę $1 + 3 + 5 + \ldots + (2n - 1)$, gdzie n jest liczbą naturalną.

Dyskusja. Wprowadźmy oznaczenie:

$$S_n = 1 + 3 + 5 + \ldots + (2n - 1).$$

Widzimy, że dla $n = 1$ ostatnim składnikiem powyższej sumy jest $2n - 1 = 1$, czyli suma składa się tylko z jednego składnika: $S_1 = 1$. Mamy: $S_2 = 1 + 3 = 4$, $S_3 = 1 + 3 + 5 = 9$, $S_4 = 1 + 3 + 5 + 7 = 16$, $S_5 = 25$, $S_6 = 36$. Widzimy, że powinno być $S_n = n^2$. Czy można to jakoś uzasadnić? Trzeba się przyjrzeć, w jaki sposób otrzymujemy kolejne S_n.

Na przykład, jeśli mamy już obliczone

$$S_6 = 1 + 3 + 5 + 7 + 9 + 11 = 36,$$

to sumy

$$S_7 = 1 + 3 + 5 + 7 + 9 + 11 + 13$$

nie będziemy liczyli od początku, tylko skorzystamy z tego, że $S_7 = S_6 + 13 = 49$, $S_8 = S_7 + 15 = 64$ i tak dalej. Zwróćmy uwagę na to, co należy dodać do S_n, żeby otrzymać S_{n+1}. Otóż:

$$S_7 = S_6 + (2 \cdot 7 - 1) = 6^2 + 2 \cdot 6 + 1 = (6 + 1)^2 = 7^2$$

oraz

$$S_8 = S_7 + (2 \cdot 8 - 1) = 7^2 + 2 \cdot 7 + 1 = (7 + 1)^2 = 8^2.$$

Dopiero teraz mamy pewność, że te przekształcenia można kontynuować i zawsze będzie $S_n = n^2$. Nasza pewność bierze się stąd, że jeśli $S_n = n^2$, to

$$S_{n+1} = S_n + (2 \cdot (n + 1) - 1) = n^2 + 2n + 1 = (n + 1)^2.$$

Ten ostatni rachunek pokazuje, że dla każdego n zachodzi implikacja:

$$S_n = n^2 \Rightarrow S_{n+1} = (n + 1)^2.$$

Oznacza to, że prawdziwe są następujące implikacje:

$$S_1 = 1^2 \Rightarrow S_2 = 2^2, \quad S_2 = 2^2 \Rightarrow S_3 = 3^2, \quad S_3 = 3^2 \Rightarrow S_4 = 4^2, \quad \ldots$$

Jeśli zatem sprawdzimy, że $S_1 = 1^2$, to z tego będzie wynikała równość $S_2 = 2^2$, a z tego z kolei będzie wynikało, że $S_3 = 3^2$, i tak dalej dla kolejnych liczb naturalnych.

Podsumujmy nasze obserwacje. Jeśli chcemy udowodnić równość $S_n = n^2$ dla dowolnego naturalnego $n \geqslant 1$, to wystarczy sprawdzić, że:
I. $S_1 = 1^2$,
II. dla każdego naturalnego $n \geqslant 1$ zachodzi implikacja $S_n = n^2 \Rightarrow S_{n+1} = (n + 1)^2$.

6.2 Ogólny schemat metody indukcji

Jeśli $T(n)$ jest formą zdaniową określoną w zbiorze liczb naturalnych, to prawdziwe jest zdanie

$$(T(0) \wedge \forall_{n\in\mathbb{N}} (T(n) \Rightarrow T(n+1))) \Rightarrow \forall_{n\in\mathbb{N}} T(n).$$

W przypadku formy zdaniowej określonej w zbiorze $\mathbb{N}_1 = \{1, 2, 3, \dots\}$, rozważamy zdanie

$$(T(1) \wedge \forall_{n\in\mathbb{N}_1} (T(n) \Rightarrow T(n+1))) \Rightarrow \forall_{n\in\mathbb{N}_1} T(n).$$

6.3 Przykłady dowodów indukcyjnych

Zadanie 9. *Dowieść, że dla dowolnej liczby naturalnej n*

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \ldots + n \cdot (n+1) = \frac{n \cdot (n+1) \cdot (n+2)}{3}.$$

Rozwiązanie. I. Baza indukcji.
Dla $n = 1$ równość jest oczywista:

$$1 \cdot 2 = \frac{1 \cdot 2 \cdot 3}{3}.$$

II. Krok indukcyjny.
Niech n będzie dowolną liczbą naturalną. Załóżmy, że dana w zadaniu równość zachodzi dla n:

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

Wówczas dla $n+1$ mamy:

$$1 \cdot 2 + \ldots + n \cdot (n+1) + (n+1) \cdot (n+2) = \frac{n \cdot (n+1) \cdot (n+2)}{3} + (n+1) \cdot (n+2) =$$

$$= (n+1) \cdot (n+2) \cdot \left(\frac{n}{3} + 1\right) = \frac{(n+1) \cdot (n+2) \cdot (n+3)}{3},$$

czyli dla $n+1$ równość jest prawdziwa.

Na mocy zasady indukcji matematycznej równość

$$1 \cdot 2 + 2 \cdot 3 + \ldots + n \cdot (n+1) = \frac{n \cdot (n+1) \cdot (n+2)}{3}$$

zachodzi dla dowolnego naturalnego $n \geqslant 1$. □

Czasami twierdzenie ma sens i jest prawdziwe również dla $n = 0$. Wówczas za bazę indukcji możemy przyjąć $n = 0$, ale wtedy krok indukcyjny trzeba udowodnić dla dowolnego naturalnego $n \geqslant 0$. Schemat dowodu wygląda więc następująco:
I. Baza indukcji: $T(0)$.
II. Krok indukcyjny: $\forall_{n\geqslant 0}(T(n) \Rightarrow T(n+1))$.

Zadanie 10. *Dowieść, że dla dowolnego* $n \geqslant 0$ *liczba* $2^{2n+1} + 3n + 7$ *jest podzielna przez* 9.

Rozwiązanie. Dla $n = 0$ mamy liczbę $2^{2\cdot 0+1} + 3 \cdot 0 + 7 = 9$, która jest, oczywiście, podzielna przez 9.

Niech n będzie dowolną liczbą naturalną. Załóżmy, że dla n twierdzenie jest prawdziwe, czyli liczba $2^{2n+1} + 3n + 7$ jest podzielna przez 9. Wówczas

$$2^{2(n+1)+1} + 3(n+1) + 7 = 2^{2n+3} + 3n + 3 + 7 =$$

$$= 4 \cdot 2^{2n+1} + 3n + 10 = 4 \cdot (2^{2n+1} + 3n + 7) - 9n - 18.$$

Liczby $9n$ i 18 są podzielne przez 9, liczba $2^{2n+1} + 3n + 7$ też (z założenia indukcyjnego), więc liczba $2^{2(n+1)+1} + 3(n+1) + 7$ również jest podzielna przez 9, czyli dla $n + 1$ twierdzenie jest prawdziwe.

Na mocy indukcji matematycznej liczba $2^{2n+1} + 3n + 7$ jest podzielna przez 9 dla dowolnego naturalnego n. □

6.4 Inne warianty metody indukcji

Rozważmy następującą sytuację. Pewne twierdzenie $T(n)$ jest prawdziwe dla $n = 0$ i $n = 1$. Ponadto, dla dowolnego naturalnego n, z prawdziwości twierdzeń $T(n)$ i $T(n+1)$ wynika prawdziwość twierdzenia $T(n+2)$. Wówczas twierdzenie jest prawdziwe dla dowolnego naturalnego n.

Według takiego schematu będzie przebiegał dowód indukcyjny w następnym zadaniu. Zapiszmy ten schemat symbolicznie.

I. Baza indukcji: $T(0) \wedge T(1)$.

II. Krok indukcyjny: $\forall_{n \geqslant 0}(T(n) \wedge T(n+1) \Rightarrow T(n+2))$.

Dowód indukcyjny w następnym zadaniu będzie przebiegał według schematu:

I. Baza indukcji: $T(0) \wedge T(1) \wedge T(2)$.

II. Krok indukcyjny: $T(k) \wedge T(k+1) \wedge T(k+2) \Rightarrow T(k+3)$ dla dowolnego $k \geqslant 0$.

Zadanie 11. *Ciąg* (a_n) *określają następujące warunki:*

$$a_0 = 2,\ a_1 = 3,\ a_2 = 6,$$

$$a_n = (n+4)a_{n-1} - 4na_{n-2} + 4(n-2)a_{n-3},\ \textit{dla}\ n \geqslant 3.$$

Udowodnij, że dla każdego n

$$a_n = n! + 2^n.$$

Rozwiązanie. Mamy

$$a_0 = 0! + 2^0, \quad a_1 = 1! + 2^1, \quad a_2 = 2! + 2^2,$$

więc dla $n = 0, 1, 2$ twierdzenie jest prawdziwe.

Niech n będzie dowolną liczbą naturalną. Załóżmy, że

$$a_n = n! + 2^n, \quad a_{n+1} = (n+1)! + 2^{n+1} \quad \text{i} \quad a_{n+2} = (n+2)! + 2^{n+2}.$$

Wówczas dla $n+3$ mamy

$$\begin{aligned} a_{n+3} &= (n+7)a_{n+2} - 4(n+3)a_{n+1} + 4(n+1)a_n \\ &= (n+7)((n+2)! + 2^{n+2}) - 4(n+3)((n+1)! + 2^{n+1}) + 4(n+1)(n! + 2^n) \\ &= \text{tu jest trochę rachunków} = (n+3)! + 2^{n+3}, \end{aligned}$$

czyli dla $n+3$ twierdzenie jest prawdziwe.

Na mocy indukcji wzór $a_n = n! + 2^n$ zachodzi dla dowolnego naturalnego n. □

Przykładem „mocnej" wersji indukcji jest dowód następującego twierdzenia.

Twierdzenie 1. *Dowolną liczbę naturalną większą od* 1 *można przedstawić w postaci iloczynu liczb pierwszych.*

Uwaga 4. Jeśli n jest liczbą pierwszą, to iloczyn ten składa się tylko z jednego czynnika.

Dowód. Liczba $n = 2$ jest liczbą pierwszą, czyli iloczynem jednej liczby pierwszej.

Niech n będzie dowolną liczbą naturalną większą od 2. Załóżmy, że każdą liczbę naturalną mniejszą od n można przedstawić w postaci iloczynu liczb pierwszych. Pokażemy, że n też można przedstawić w postaci iloczynu liczb pierwszych.

Jeśli n jest liczbą pierwszą, to teza dla n zachodzi. Jeśli n jest liczbą złożoną, to można ją przedstawić w postaci iloczynu dwóch liczb od niej mniejszych: $n = k \cdot l$, $k, l < n$. Na mocy założenia zarówno k, jak i l, jest iloczynem liczb pierwszych: $k = p_1 \cdot \ldots \cdot p_i$, $l = q_1 \cdot \ldots \cdot q_j$, zatem $n = k \cdot l$ też, oczywiście można tak przedstawić: $n = p_1 \cdot \ldots \cdot p_i \cdot q_1 \cdot \ldots \cdot q_j$, co kończy dowód kroku indukcyjnego. □

Schemat powyższego dowodu:

I. Baza: T(2).

II. Krok: $\forall_{n>2}[T(2) \wedge \ldots \wedge T(n-1) \Rightarrow T(n)]$.

Pytanie 6. *Dlaczego w punkcie* (II) *jest „$n > 2$", a nie „$n \geqslant 2$"?*

7 Zbiory

7.1 Sposoby określania zbiorów

Można wyróżnić trzy podstawowe sposoby określania zbiorów:

1) Zbiór wszystkich elementów postaci $f(t)$, gdzie t przebiega zbiór T:

$$\{f(t),\ t \in T\}.$$

2) Zbiór wszystkich elementów x zbioru X spełniających warunek $\varphi(x)$:

$$\{x \in X :\ \varphi(x)\}.$$

3) Zbiór skończony możemy określić przez wypisanie jego elementów, np.

$$\{n \in \mathbb{N}_1 :\ n \mid 6\} = \{1, 2, 3, 6\}.$$

Przykład 30. (a) Zbiór liczb parzystych możemy określić na dwa sposoby:

$$\{2k;\ k \in \mathbb{Z}\} = \{n \in \mathbb{Z} :\ 2 \mid n\}.$$

(b) Prostą o równaniu $y = ax + b$ możemy określić jako zbiór punktów o współrzędnych $(x, ax + b)$, gdzie $x \in \mathbb{R}$:

$$\{(x, ax + b);\ x \in \mathbb{R}\}$$

lub jako zbiór tych punktów o współrzędnych (x, y), które spełniają warunek $y = ax + b$:

$$\{(x, y) \in \mathbb{R}^2 :\ y = ax + b\}.$$

(c) Wykres funkcji $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = \sin x$, możemy określić jako zbiór punktów postaci $(x, \sin x)$, gdzie $x \in \mathbb{R}$:

$$\{(x, \sin x),\ x \in \mathbb{R}\}.$$

(d) Okrąg o środku (a, b) i promieniu r możemy określić jako zbiór rozwiązań równania $(x - a)^2 + (y - b)^2 = r^2$:

$$\{(x, y) \in \mathbb{R}^2 :\ (x - a)^2 + (y - b)^2 = r^2\}.$$

Przykład 31. Przedziały osi liczbowej:

$$(a, b) = \{x \in \mathbb{R} :\ x > a \wedge x < b\},$$

$$[a, b) = \{x \in \mathbb{R} :\ x \geqslant a \wedge x < b\},$$

$$(-\infty, a) = \{x \in \mathbb{R} :\ x < a\}.$$

Zaznaczmy, że zbiory A i B są równe dokładnie wtedy, gdy mają te same elementy, czyli dla dowolnego elementu x prawdziwe jest zdanie

$$(x \in A) \Leftrightarrow (x \in B).$$

7.2 Inkluzja zbiorów

Definicja 4. *Mówimy, że zbiór A jest zawarty w zbiorze B, co zapisujemy $A \subset B$, jeśli wszystkie elementy zbioru A należą do zbioru B, czyli dla dowolnego elementu x prawdziwe jest zdanie*

$$(x \in A) \Rightarrow (x \in B).$$

Jeśli $A \subset B$, to zbiór A nazywamy podzbiorem zbioru B.

Przykład 32. (a) $\{0\} \subset [0,1) \subset (-1,1) \subset [-1,1] \subset (-\infty, 1]$,

(b) $\mathbb{N}_1 \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Następujące twierdzenie wyrażą dwie podstawowe własności inkluzji.

Twierdzenie 2. (a) *Dla dowolnych zbiorów A, B, jeżeli $A \subset B$ i $B \subset A$, to $A = B$.*

(b) *Dla dowolnych zbiorów A, B, C, jeżeli $A \subset B$ i $B \subset C$, to $A \subset C$.*

Dowód. (a) Jeżeli $A \subset B$ i $B \subset A$, to dla dowolnego elementu x prawdziwe jest zdanie

$$(x \in A \Rightarrow x \in B) \ \wedge \ (x \in B \Rightarrow x \in A),$$

więc prawdziwe jest również zdanie

$$x \in A \Leftrightarrow x \in B.$$

Zatem $A = B$.

(b) Jeżeli $A \subset B$ i $B \subset C$, to dla dowolnego elementu x mamy:

$$(x \in A \Rightarrow x \in B) \ \wedge \ (x \in B \Rightarrow x \in C),$$

więc mamy również:

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

Zatem $A \subset C$. □

Zbiór pusty to zbiór posiadający 0 elementów, oznaczamy go symbolem $\varnothing$. Zbiór pusty jest zawarty w każdym zbiorze:

$$\varnothing \subset A.$$

7.3 Działania na zbiorach

Definicja 5. *Rozważmy dowolne dwa zbiory A i B.*

(a) **Suma** $A \cup B$ *składa się z wszystkich elementów, które należą do zbioru A lub do zbioru B:*

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

(b) **Część wspólna** *(przekrój)* $A \cap B$ *składa się z wszystkich elementów, które należą jednocześnie do zbioru* A *i do zbioru* B*:*

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

(c) **Różnica** $A \setminus B$ *składa się z wszystkich elementów, które należą do zbioru* A*, ale nie należą do zbioru* B*:*

$$(x \in A \setminus B) \Leftrightarrow (x \in A \wedge x \notin B).$$

Uwaga 5. $(x \notin A) \Leftrightarrow \sim (x \in A)$

Definicja 6. Różnica symetryczna $A \div B$ *składa się z wszystkich elementów, które należą do zbioru* A*, a nie należą do* B*, oraz tych, które należą do* B*, a nie należą do* A*:*

$$(x \in A \div B) \Leftrightarrow (x \in A \veebar x \in B).$$

Uwaga 6. $A \div B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$

Przykład 33. Przykłady działań na przedziałach:

(a) $[0, 2) \cup [1, 3) = [0, 3)$,

(b) $[0, 2) \cap [1, 3) = [1, 2)$,

(c) $[0, 2) \setminus [1, 3) = [0, 1)$,

(d) $[0, 2) \cup \{2\} = [0, 2]$,

(e) $(-1, +\infty) \cap (-\infty, 1) = (-1, 1)$,

(f) $[-1, 1] \setminus \{-1, 1\} = (-1, 1)$,

(g) $[-1, 1] \setminus \{0\} = [-1, 0) \cup (0, 1]$.

Przykład 34. Wspólne dzielniki liczb 12 i 18 to są dokładnie dzielniki liczby 6:

$$\{n \in \mathbb{N}_1 : \ n \mid 12\} \cap \{n \in \mathbb{N}_1 : \ n \mid 18\} = \{n \in \mathbb{N}_1 : \ n \mid 6\}.$$

Następujące twierdzenie wyraża dwie własności działań związane z inkluzją.

Twierdzenie 3. *Niech* A*,* B*,* C *będą dowolnymi zbiorami.*

(a) *Jeżeli* $A \subset C$ *i* $B \subset C$*, to* $A \cup B \subset C$.

(b) *Jeżeli* $A \subset B$ *i* $A \subset C$*, to* $A \subset B \cap C$.

Dowód. (a) Załóżmy, że $A \subset C$ i $B \subset C$. Rozważmy dowolny element $x \in A \cup B$. Wówczas $x \in A$ lub $x \in B$. Jeśli $x \in A$, to $x \in C$ na mocy inkluzji $A \subset C$. Jeśli $x \in B$, to $x \in C$ na mocy inkluzji $B \subset C$. Zatem w obu przypadkach $x \in C$. Wykazaliśmy, że dowolny element zbioru $A \cup B$ należy do zbioru C, czyli $A \cup B \subset C$.

(b) Załóżmy, że $A \subset B$ i $A \subset C$. Rozważmy dowolny element $x \in A$. Skoro $A \subset B$ i $x \in A$, to $x \in B$. Skoro $A \subset C$ i $x \in A$, to $x \in C$. Zatem $x \in B$ i $x \in C$, czyli $x \in B \cap C$. □

Zadanie 12. *Wykaż, że dla dowolnych zbiorów A, B i C zachodzą następujące równoważności:*

$$A \subset B \Leftrightarrow A \setminus B = \varnothing \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B.$$

Przykład 35. Działania ze zbiorem pustym:

(a) $A \cup \varnothing = A$,

(b) $A \cap \varnothing = \varnothing$,

(c) $A \setminus \varnothing = A$,

(d) $\varnothing \setminus A = \varnothing$.

7.4 Własności działań na zbiorach

Twierdzenie 4. *Dla dowolnych zbiorów A, B i C zachodzą następujące równości:*

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

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

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

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

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

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

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

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

Takich równości można dowodzić dwiema metodami – rachunku zdań (bardziej formalna) i diagramów Venne'a (bardziej obrazowa). Dla przykładu udowodnimy równości (a) i (h) metodą rachunku zdań.

Dowód. (a) Dla dowolnego elementu x mamy:
$x \in (A \cup B) \cap C \Leftrightarrow x \in (A \cup B) \wedge x \in C \Leftrightarrow (x \in A \vee x \in B) \wedge x \in C \Leftrightarrow (x \in A \wedge x \in C) \vee (x \in B \wedge x \in C) \Leftrightarrow (x \in A \cap C) \vee (x \in B \cap C) \Leftrightarrow x \in (A \cap C) \cup (B \cap C)$.

Skorzystaliśmy z definicji sumy i przekroju zbiorów oraz z tautologii $(p \vee q) \wedge r \Leftrightarrow (p \wedge r) \vee (q \wedge r)$.

(h) Dla dowolnego elementu x mamy:
$x \in A \setminus (B \setminus C) \Leftrightarrow x \in A \wedge x \notin (B \setminus C) \Leftrightarrow x \in A \wedge \sim (x \in B \setminus C) \Leftrightarrow x \in A \wedge \sim (x \in B \wedge x \notin C) \Leftrightarrow x \in A \wedge (x \notin B \vee x \in C) \Leftrightarrow (x \in A \wedge x \notin B) \vee (x \in A \wedge x \in C) \Leftrightarrow x \in A \setminus B \vee x \in A \cap C \Leftrightarrow x \in (A \setminus B) \cup (A \cap C)$. □

Ciekawy przykład zastosowania diagramów Venne'a ([21], zad. 90, str. 13).

Zadanie 13. *Załóżmy, że prawdziwe są następujące stwierdzenia:*

(a) *wśród ludzi posiadających telewizory są tacy, którzy nie są malarzami,*

(b) *ludzie, którzy codziennie pływają w basenie, a nie są malarzami, nie mają telewizorów.*

Czy wynika stąd, że prawdziwe jest następujące stwierdzenie:

(c) *nie wszyscy posiadacze telewizorów pływają codziennie w basenie?*

7.5 Algebra podzbiorów danego zbioru

Niech X będzie dowolnym zbiorem. Zbiór podzbiorów zbioru X oznaczamy symbolem 2^X. Dokładniej, 2^X jest zbiorem, którego elementami są wszystkie podzbiory zbioru X:

$$A \in 2^X \Leftrightarrow A \subset X.$$

Przykład 36. (a) Jeśli $X = \{a, b\}$, to

$$2^X = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}.$$

(b) Jeśli $X = \{1, 2, 3\}$, to

$$2^X = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

(c) Jeśli $X = \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$, to

$$\begin{aligned} 2^X \;=\; & \{\emptyset, \{\clubsuit\}, \{\diamondsuit\}, \{\heartsuit\}, \{\spadesuit\}, \{\clubsuit, \diamondsuit\}, \{\clubsuit, \heartsuit\}, \{\clubsuit, \spadesuit\}, \{\diamondsuit, \heartsuit\}, \{\diamondsuit, \spadesuit\}, \\ & \{\heartsuit, \spadesuit\}, \{\clubsuit, \diamondsuit, \heartsuit\}, \{\clubsuit, \diamondsuit, \spadesuit\}, \{\clubsuit, \heartsuit, \spadesuit\}, \{\diamondsuit, \heartsuit, \spadesuit\}, \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}\}. \end{aligned}$$

Twierdzenie 5. *Jeśli zbiór X ma n elementów, to zbiór 2^X ma 2^n elementów.*

Powyższe twierdzenie posiada proste uzasadnienie kombinatoryczne. Otóż, jeśli chcemy utworzyć podzbiór zbioru $X = \{x_1, x_2, \ldots, x_n\}$, to powinniśmy kolejno zdecydować: czy element x_1 ma należeć do tego podzbioru, czy nie, czy element x_2 ma należeć do tego podzbioru, czy nie, i tak dalej, aż do elementu x_n. Za każdym razem mamy dwie możliwości, więc wszystkich możliwości utworzenia podzbioru jest

$$\underbrace{2 \cdot 2 \cdot \ldots \cdot 2}_{n} = 2^n.$$

Jeśli mamy ustalony zbiór X i rozważamy tylko jego podzbiory, to zbiór X nazywamy **przestrzenią** lub **uniwersum.**

Definicja 7. Dopełnieniem zbioru A *w przestrzeni* X *nazywamy zbiór*

$$A' = X \setminus A.$$

Dla każdego elementu $x \in X$ prawdziwe jest zdanie

$$x \in A' \Leftrightarrow \sim (x \in A).$$

Ponadto, zachodzą następujące zależności:

$$A \cap A' = \varnothing, \quad A \cup A' = X, \quad (A')' = A, \quad \varnothing' = X, \quad X' = \varnothing.$$

Odnotujmy **prawa de Morgana dla zbiorów**.

Twierdzenie 6. *Dla dowolnych zbiorów $A, B \subset X$ zachodzą następujące równości:*

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

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

Dowód. 1) Dla dowolnego elementu $x \in X$ mamy:
$x \in (A \cup B)' \Leftrightarrow \sim (x \in A \cup B) \Leftrightarrow \sim (x \in A \vee x \in B) \Leftrightarrow \sim (x \in A) \wedge \sim (x \in B) \Leftrightarrow x \in A' \wedge x \in B'$.

Skorzystaliśmy z tautologii $\sim (p \vee q) \Leftrightarrow \sim p \wedge \sim q)$.

2) Analogicznie. Z jakiej tautologii należy tu skorzystać? □

Podobne zależności zachodzą dla większej liczby zbiorów, na przykład:

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

$$(A \cap B \cap C \cap D)' = A' \cup B' \cup C' \cup D'.$$

7.6 Iloczyn kartezjański zbiorów

Rozważmy dwa zbiory A i B. Z dowolnych elementów $a \in A$ i $b \in B$ możemy utworzyć parę (a, b). Zbiór wszystkich takich par oznaczamy symbolem $A \times B$ i nazywamy **iloczynem kartezjańskim** zbiorów A i B:

$$A \times B = \{(a, b);\ a \in A,\ b \in B\},$$

przy czym

$$(a, b) = (a', b') \Leftrightarrow (a = a') \wedge (b = b').$$

Uwaga 7. Parę uporządkowaną można zdefiniować jako zbiór

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

(definicja Kuratowskiego).

Twierdzenie 7. *Jeśli zbiory A i B są skończone i zbiór A ma m elementów, a zbiór B ma n elementów, to zbiór $A \times B$ ma $m \cdot n$ elementów.*

Powyższy fakt najłatwiej uzasadnić ustawiając elementy zbioru $A \times B$ w tablicy $m \times n$:

$$\begin{array}{ccccc} (a_1,b_1) & (a_1,b_2) & (a_1,b_3) & \cdots & (a_1,b_n) \\ (a_2,b_1) & (a_2,b_2) & (a_2,b_3) & \cdots & (a_2,b_n) \\ (a_3,b_1) & (a_3,b_2) & (a_3,b_3) & \cdots & (a_3,b_n) \\ \vdots & \vdots & \vdots & & \vdots \\ (a_m,b_1) & (a_m,b_2) & (a_m,b_3) & \cdots & (a_m,b_n), \end{array}$$

gdzie $A = \{a_1, a_2, \ldots, a_m\}$, $B = \{b_1, b_2, \ldots, b_n\}$.

Kwadratem kartezjańskim zbioru A nazywamy zbiór $A^2 = A \times A$.

Przykład 37. $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ – płaszczyzna (z układem współrzędnych),

$$[0,3) \times (1,2] \subset \mathbb{R}^2,$$

$$[0,3) \times (1,2] = \{(x,y);\ x \in [0,3),\ y \in (1,2]\}.$$

Analogicznie określamy iloczyn kartezjański większej liczby zbiorów, na przykład

$$A \times B \times C = \{(a,b,c);\ a \in A,\ b \in B,\ c \in C\},$$

przy czym

$$(a,b,c) = (a',b',c') \Leftrightarrow (a = a') \wedge (b = b') \wedge (c = c').$$

Uwaga 8. Formalnie iloczyn kartezjański trzech zbiorów $A \times B \times C$ definiujemy za pomocą iloczynu kartezjańskiego dwóch zbiorów:

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

Wówczas trójka (a,b,c) jest zdefiniowana jako para $((a,b),c)$.

Zbiór

$$A^n = \underbrace{A \times A \times \ldots \times A}_{n} =$$

$$= \{(a_1, a_2, \ldots, a_n);\ a_1, a_2, \ldots, a_n \in A\}$$

nazywamy n-tą potęgą kartezjańską zbioru A, na przykład $\mathbb{R}^3$ to przestrzeń trójwymiarowa (z układem współrzędnych) i ogólnie $\mathbb{R}^n$ to przestrzeń n-wymiarowa.

7.7 Działania uogólnione na zbiorach

Jeśli T jest zbiorem i dla każdego $t \in T$ jest określony pewien zbiór A_t, to mówimy, że jest określona rodzina zbiorów

$$\{A_t,\ t \in T\}.$$

Przykład 38. (a) $\{[t,+\infty),\ t \in \mathbb{R}\}$,

(b) $\{(-t,t),\ t > 1\} = \{(-t,t),\ t \in (1,+\infty)\}$,

(c) $\{\{0,1,\ldots,n\},\ n\in\mathbb{N}\}$,

(d) $\{\{0,n\},\ n=1,2,3\}=\{\{0,n\},\ n\in\{1,2,3\}\}$.

Definicja 8. Suma $\bigcup\limits_{t\in T} A_t$ *zbiorów rodziny* $\{A_t,\ t\in T\}$ *składa się z wszystkich elementów, które należą do co najmniej jednego z tych zbiorów:*

$$x\in\bigcup_{t\in T} A_t \Leftrightarrow \exists_{t\in T} x\in A_t.$$

Przypadek szczególny:

$$\bigcup_{k=1}^{n} A_k = A_1\cup A_2\cup\ldots\cup A_n$$

$$x\in\bigcup_{k=1}^{n} A_k \Leftrightarrow x\in A_1\vee x\in A_2\vee\ldots\vee x\in A_n.$$

Przykład 39.

$$x\in\bigcup_{t\in\mathbb{R}}[t,+\infty)\Leftrightarrow\exists_{t\in\mathbb{R}}x\in[t,+\infty)\Leftrightarrow\exists_{t\in\mathbb{R}}x\geqslant t$$

Otrzymane zdanie jest prawdziwe dla każdego $x\in\mathbb{R}$, więc

$$\bigcup_{t\in\mathbb{R}}[t,+\infty)=\mathbb{R}.$$

Przykład 40. (a) $\bigcup_{t\in(1,+\infty)}(-t,t)=\mathbb{R}$

(b) $\bigcup_{n\in\mathbb{N}}\{0,1,\ldots,n\}=\mathbb{N}$

Definicja 9. Część wspólna *(przekrój)* $\bigcap\limits_{t\in T} A_t$ *zbiorów rodziny* $\{A_t,\ t\in T\}$ *składa się z wszystkich elementów, które należą do każdego z tych zbiorów:*

$$x\in\bigcap_{t\in T} A_t \Leftrightarrow \forall_{t\in T} x\in A_t.$$

Przypadek szczególny:

$$\bigcap_{k=1}^{n} A_k = A_1\cap A_2\cap\ldots\cap A_n$$

$$x\in\bigcap_{k=1}^{n} A_k \Leftrightarrow x\in A_1\wedge x\in A_2\wedge\ldots\wedge x\in A_n.$$

Przykład 41. (a) $x\in\bigcap_{t\in\mathbb{R}}[t,+\infty)\Leftrightarrow\forall_{t\in\mathbb{R}}x\in[t,+\infty)\Leftrightarrow\forall_{t\in\mathbb{R}}x\geqslant t.$
Otrzymane zdanie jest fałszywe dla każdego $x\in\mathbb{R}$, więc

$$\bigcap_{t\in\mathbb{R}}[t,+\infty)=\varnothing.$$

(b) $x\in\bigcap_{t\in(1,+\infty)}(-t,t)\Leftrightarrow\forall_{t\in(1,+\infty)}x\in(-t,t)\Leftrightarrow\forall_{t>1}-t<x<t.$
Otrzymane zdanie jest prawdziwe dokładnie wtedy, gdy $x\in[-1,1]$, więc

$$\bigcap_{t\in(1,+\infty)}(-t,t)=[-1,1].$$

7.8 Zbiór słów nad alfabetem

Jako alfabet możemy obrać dowolny zbiór A (zazwyczaj zakładamy, że jest to zbiór skończony). Elementy zbioru A nazywamy literami. Słowami nad alfabetem A nazywamy ciągi elementów z A. Jeśli elementy zbioru A oznaczamy pojedynczymi symbolami, to litery słowa piszemy (bez odstępów i przecinków) jedna za drugą. Liczbę liter danego słowa nazywamy jego długością.

Przykład 42. $A = \{a, b, c\}$

(a) słowa jednoliterowe (długości 1): a, b, c,

(b) słowa dwuliterowe (długości 2): aa, ab, ac, ba, bb, bc, ca, cb, cc,

(c) słowa trzyliterowe (długości 3): aaa, aab, ...

Przykład 43. $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, słowami są na przykład:

(a) 000 – długości 3,

(b) 1234 – długości 4,

(c) 5 – długości 1,

(d) 100 000 000 – długości 9,
007 – długości 3.

Jeśli słowo w ma długość m, a słowo v ma długość n, to możemy utworzyć słowo wv, które ma długość $m + n$.

Przyjmujemy, że jest jedno słowo puste ε złożone z 0 liter. Dla dowolnego słowa w mamy $\varepsilon w = w\varepsilon = w$.

Bardziej formalnie, zbiorem słów długości n nad alfabetem A nazywamy zbiór A^n. Ponadto przyjmujemy $A^0 = \{\varepsilon\}$. Zbiór wszystkich słów oznaczamy symbolem A^*:

$$A^* = A^0 \cup A^1 \cup A^2 \cup \ldots = \bigcup_{n=0}^{\infty} A^n.$$

8 Funkcje

8.1 Pojęcie funkcji

Przypomnijmy nieformalną definicję funkcji.

> „Jeżeli mamy dwa zbiory X i Y, i każdemu elementowi zbioru X przyporządkujemy jeden i tylko jeden element zbioru Y, to takie przyporządkowanie nazywamy **funkcją**."

Zbiór X nazywamy **dziedziną** tej funkcji, a zbiór Y jej **przeciwdziedziną**. Jeśli f jest taką funkcją, to piszemy $f\colon X \to Y$.

Przykład 44. (a) $f\colon \mathbb{N} \to \mathbb{N}$, $f(n) = n + 1$,

(b) $g_i\colon \mathbb{R} \to \mathbb{R}$, $g_1(x) = ax + b$, $g_2(x) = \sin x$, $g_3(x) = 2^x$, $g_4(x) = a_n x^n + \ldots + a_1 x + a_0$,

(c) $E(x) = [x]$, np. $E\colon \mathbb{R} \to \mathbb{R}$ lub $E\colon \mathbb{R} \to \mathbb{Z}$,

(d) $f\colon \mathbb{N}_1 \times \mathbb{N}_1 \to \mathbb{N}_1$, $f(m, n) = \mathrm{NWD}(m, n)$,

(e) $g\colon \mathbb{R}^3 \to \mathbb{R}$, $g(x, y, z) = xy + yz + zx$,

(f) $h\colon \mathbb{R} \to \mathbb{R}^2$, $h(t) = (\cos t, \sin t)$,

(g) $F\colon \mathbb{R}^2 \to \mathbb{R}^2$, $F(x, y) = (x^2 + y^2, xy)$.

Przykład 45. Funkcje określone w dowolnym zbiorze X:

(a) $\mathrm{Id}_X\colon X \to X$, $\mathrm{Id}_X(x) = x$ – funkcja identycznościowa,

(b) $A \subset X$, $\chi_A\colon X \to \{0, 1\}$, $\chi_A(x) = \begin{cases} 1, & \text{jeśli } x \in A, \\ 0, & \text{jeśli } x \notin A \end{cases}$ – funkcja charakterystyczna podzbioru A,

(c) $f\colon X \to 2^X$, $f(x) = \{x\}$.

Przykład 46. Jeśli A jest dowolnym alfabetem, to mamy funkcje:

length$\colon X^* \to \mathbb{N}$, length$(w)$ – długość słowa w,

head$\colon X^* \setminus \{\epsilon\} \to X$, head$(w)$ – pierwsza litera słowa w,

tail$\colon X^* \setminus \{\epsilon\} \to X$, tail$(w)$ – ostatnia litera słowa w,

rev$\colon X^* \to X^*$, rev(w) – słowo z odwróconą kolejnością liter.

Przykład 47. Nieskończony ciąg $a_1, a_2, a_3, \ldots$ elementów dowolnego zbioru A wyznacza funkcję $f\colon \mathbb{N}_1 \to A$, $f(n) = a_n$.

Uwaga 9. W zasadzie w ten sposób definiujemy pojęcie ciągu nieskończonego.

Przykład 48. Pole jest funkcją określoną w odpowiednim zbiorze figur, np. T – zbiór trójkątów na płaszczyźnie, $P\colon T \to \mathbb{R}$, $P(ABC)$ – pole trójkąta ABC.

Definicja 10. *Wykresem funkcji* $f\colon X \to Y$ *nazywamy zbiór*

$$W_f = \{(x, f(x));\ x \in X\} = \{(x, y) \in X \times Y :\ \exists_{x \in X} y = f(x)\}.$$

Przykład 49. Wykresem funkcji $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, jest zbiór

$$\{(x, x^2);\ x \in \mathbb{R}\}.$$

Zauważmy, że każda funkcja jest jednoznacznie określona przez swój wykres.

Pytanie 7. *Kiedy zbiór* $R \subset X \times Y$ *jest wykresem jakiejś funkcji ze zbioru* X *do* Y*?*

8.2 Zbiór wartości funkcji

Definicja 11. Zbiorem wartości *funkcji* $f\colon X \to Y$ *nazywamy zbiór*

$$f(X) = \{f(x);\ x \in X\} = \{y \in Y :\ \exists_{x \in X}\ y = f(x)\}.$$

Przykład 50. (a) $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^n$, gdzie $n \in \mathbb{N}_1$,

$$f(\mathbb{R}) = \begin{cases} [0, +\infty), & \text{jeśli } n \text{ jest parzyste,} \\ \mathbb{R}, & \text{jeśli } n \text{ jest nieparzyste.} \end{cases}$$

(b) $g\colon \mathbb{R} \to \mathbb{R}$, $g(x) = ax + b$, gdzie $a, b \in \mathbb{R}$,

$$g(\mathbb{R}) = \begin{cases} \mathbb{R}, & \text{jeśli } a \neq 0, \\ \{b\}, & \text{jeśli } a = 0. \end{cases}$$

(c) $E\colon \mathbb{R} \to \mathbb{R}$, $f(x) = [x]$, $E(\mathbb{R}) = \mathbb{Z}$

(d) $h\colon \mathbb{R} \to \mathbb{R}^2$, $h(t) = (\cos t, \sin t)$, $h(\mathbb{R}) =?$

Uwaga 10. Zbiór wartości jest *podzbiorem* przeciwdziedziny:

$$f(X) \subset Y,$$

nie musi być równy całej przeciwdziedzinie! Należy odróżniać pojęcia przeciwdziedziny i zbioru wartości.

8.3 Funkcja różnowartościowa

Definicja 12. *Funkcję* $f\colon X \to Y$ *nazywamy* **różnowartościową** *lub* **iniekcją**, *jeśli różnym elementom zbioru* X *przyporządkowuje różne elementy zbioru* Y*:*

$$\forall_{x_1, x_2 \in X}\ x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2).$$

Warunek równoważny, który lepiej się nadaje do sprawdzania różnowartościowości konkretnych funkcji:

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

Pytanie 8. *Dlaczego te dwa warunki są równoważne?*

Uwaga 11. Każda funkcja spełnia warunek

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

Przykład 51. **Przykłady iniekcji:**

(a) $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = ax + b$, gdzie $a \neq 0$,

(b) $g\colon [-\frac{\pi}{2}, \frac{\pi}{2}] \to \mathbb{R}$, $g(x) = \sin x$,

(c) dowolna funkcja rosnąca $f\colon \mathbb{R} \to \mathbb{R}$,

(d) $f\colon X \to 2^X$, $f(x) = \{x\}$, gdzie X – dowolny zbiór.

Zadanie 14. *Dla jakich n funkcja* $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^n$ *jest iniekcją?*

8.4 Funkcja „na"

Definicja 13. *Funkcję* $f\colon X \to Y$ *nazywamy* **funkcją „na"** *lub* **suriekcją**, *jeśli każdy element zbioru* Y *jest przyporządkowany jakiemuś elementowi zbioru* X*:*

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

Możemy to zapisać równoważnie: $\forall_{y\in Y} y \in f(X)$, czyli $Y \subset f(X)$, co oznacza, że $f(X) = Y$ (gdyż $f(X) \subset Y$). Zatem funkcja jest „na", gdy jej przeciwdziedzina jest zbiorem wartości: $f(X) = Y$.

Przykład 52. **Przykłady suriekcji:**

(a) $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = ax + b$, gdzie $a \neq 0$,

(b) $f\colon \mathbb{R} \to [-1, 1]$, $f(x) = \sin x$,

(c) $f\colon \mathbb{R} \to \mathbb{Z}$, $f(x) = [x]$.

Zadanie 15. *Dla jakich n funkcja* $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^n$ *jest suriekcją?*

8.5 Funkcja wzajemnie jednoznaczna

Definicja 14. *Funkcję* $f\colon X \to Y$ *nazywamy* **wzajemnie jednoznaczną** *lub* **bijekcją**, *jeśli jest różnowartościowa i „na" (czyli jest iniekcją i suriekcją).*

Przykład 53. **Przykłady bijekcji:**

(a) $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = ax + b$, gdzie $a \neq 0$,

(b) $f\colon \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\}$, $f(x) = \frac{1}{x}$,

(c) $f\colon [-\frac{\pi}{2}, \frac{\pi}{2}] \to [-1, 1]$, $f(x) = \sin x$,

(d) $f\colon \mathbb{R} \to \mathbb{R}_+$, $f(x) = a^x$, gdzie $a > 0$ i $a \neq 1$.

Zadanie 16. *Dla jakich n funkcja* $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^n$ *jest bijekcją?*

8.6 Składanie funkcji

Rozważmy dwie funkcje $f\colon X \to Y$ i $g\colon Y \to Z$. Dla danego elementu $x \in X$ mamy element $y = f(x) \in Y$, więc mamy również element $g(y) = g(f(x)) \in Z$. W ten sposób otrzymujemy funkcję ze zbioru X do zbioru Z.

Definicja 15. Złożeniem *funkcji* $f\colon X \to Y$ *i* $g\colon Y \to Z$ *nazywamy funkcję*

$$g \circ f\colon X \to Z$$

określoną następująco:

$$(g \circ f)(x) = g(f(x)) \text{ dla } x \in X.$$

Uwaga 12. Kolejność w zapisie $g \circ f$ odpowiada temu, że na element x najpierw „działa" funkcja f, a dopiero potem funkcja g.

Przykład 54. $f, g\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x + 1$, $g(x) = x^2$, $f(g(x)) = x^2 + 1$, $g(f(x)) = (x + 1)^2$.

Twierdzenie 8. *Złożenie dwóch funkcji różnowartościowych jest funkcją różnowartościową.*

Dowód. Rozważmy funkcje różnowartościowe $f\colon X \to Y$ i $g\colon Y \to Z$. Niech $x_1, x_2 \in X$, $x_1 \neq x_2$. Z różnowartościowości funkcji f mamy: $f(x_1) \neq f(x_2)$, a wówczas z różnowartościowości funkcji g wnioskujemy, że $g(f(x_1)) \neq g(f(x_2))$.

Wykazaliśmy, że dla dowolnych $x_1, x_2 \in X$, jeśli $x_1 \neq x_2$, to $(g \circ f)(x_1) \neq (g \circ f)(x_2)$. Zatem funkcja $g \circ f$ jest różnowartościowa. □

Twierdzenie 9. *Złożenie dwóch funkcji „na" jest funkcją „na".*

Dowód. Załóżmy, że funkcje $f\colon X \to Y$ i $g\colon Y \to Z$ są „na". Udowodnimy, że dla dowolnego $z \in Z$ istnieje $x \in X$, taki że $z = (g \circ f)(x)$.

Rozważmy dowolny element $z_0 \in Z$. Funkcja g jest „na", więc istnieje element $y_0 \in Y$, taki że $z_0 = g(y_0)$. Funkcja f jest „na", więc istnieje element $x_0 \in X$, taki że $y_0 = f(x_0)$. Zatem

$$z_0 = g(y_0) = g(f(x_0)) = (g \circ f)(x_0).$$

□

Zadanie 17. *Wykaż, że dowolną funkcję* $f\colon X \to Y$ *można przedstawić w postaci złożenia dwóch funkcji* $g\colon X \to Z$ *i* $h\colon Z \to Y$ (*gdzie* Z *jest pewnym zbiorem*) *takich, że* g *jest „na", a* h *jest różnowartościowa.*

Wskazówka. Spróbuj możliwie najprościej przedstawić w szukany sposób funkcję $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = \sin x$.

8.7 Funkcja odwrotna

Rozważmy dowolną funkcję $f\colon X \to Y$. Funkcja f jest „na" dokładnie wtedy, gdy każdy element $y \in Y$ jest przyporządkowany co najmniej jednemu elementowi $x \in X$. Z kolei różnowartościowość funkcji f jest równoważna temu, że każdy element $y \in Y$ jest przyporządkowany co najwyżej jednemu elementowi $x \in X$.

Funkcja $f\colon X \to Y$ jest bijekcją wtedy i tylko wtedy, gdy każdy element $y \in Y$ jest przyporządkowany dokładnie jednemu elementowi $x \in X$. Wówczas istnieje funkcja $g\colon Y \to X$ taka, że

$$g(y) = x \Leftrightarrow y = f(x) \quad \text{dla} \quad x \in X, y \in Y.$$

Funkcja g spełnia warunki:

$$\forall_{x\in X}\ g(f(x)) = x \quad \text{i} \quad \forall_{y\in Y}\ f(g(y)) = y,$$

czyli

$$g \circ f = \mathrm{Id}_X \quad \text{i} \quad f \circ g = \mathrm{Id}_Y.$$

Funkcję g nazywamy **funkcją odwrotną** do funkcji f i oznaczamy symbolem f^{-1}.

Przykład 55. **Przykłady funkcji odwrotnych:**

(a) $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = ax + b$, gdzie $a \neq 0$,
$f^{-1}\colon \mathbb{R} \to \mathbb{R}$, $f^{-1}(x) = \frac{x-b}{a}$,

(b) $g\colon [0, +\infty) \to [0, +\infty)$, $g(x) = x^n$, gdzie $n \in \mathbb{N}$, $n \geqslant 2$
$g^{-1}\colon [0, +\infty) \to [0, +\infty)$, $g^{-1}(x) = \sqrt[n]{x}$,

(c) $h\colon \mathbb{R} \to (0, +\infty)$, $h(x) = a^x$, gdzie $a > 0$, $a \neq 1$,
$h^{-1}\colon (0, +\infty) \to \mathbb{R}$, $h(x) = \log_a(x)$.

8.8 Obraz i przeciwobraz zbioru

Rozważmy funkcję $f\colon X \to Y$.

Definicja 16. (a) **Obrazem** *zbioru $A \subset X$ nazywamy zbiór*

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

(b) **Przeciwobrazem** *zbioru $B \subset Y$ nazywamy zbiór*

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

Przykład 56. (a) $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 + x + 1$,
$f([-1, 2]) = [\frac{3}{4}, 7]$, $f^{-1}((\frac{3}{4}, 1)) = (-1, -\frac{1}{2}) \cup (-\frac{1}{2}, 0)$

(b) $g\colon \mathbb{R} \to \mathbb{R}$, $g(x) = \sin 3x$,
$g((0, \frac{\pi}{3})) = (0, 1]$, $g^{-1}([-1, 0)) =$
$= \ldots \cup (-\frac{\pi}{3}, 0) \cup (\frac{\pi}{3}, \frac{2\pi}{3}) \cup (\pi, \frac{4\pi}{3}) \cup \ldots = \bigcup_{k\in\mathbb{Z}} (\frac{(2k-1)\pi}{3}, \frac{2k\pi}{3})$

(c) $E\colon \mathbb{R} \to \mathbb{R}$, $E(x) = [x]$,
$E((-\sqrt{2}, \sqrt{2})) = \{-2, -1, 0, 1\}$, $E^{-1}((-\sqrt{2}, \sqrt{2})) = [-1, 2)$.

Zadanie 18. *Rozważmy funkcję* $f\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $f(x, y) = xy$.

(a) *Znajdź obrazy zbiorów:* $\{1, 10, 100, 1000\} \times \{1, 10, 100, 1000\}$, $2\mathbb{Z} \times 2\mathbb{Z}$, $\{2^n : n \in \mathbb{N}\} \times \{2k + 1 : k \in \mathbb{N}\}$.

(b) *Znajdź przeciwobrazy zbiorów:* $\{1, 2, 3\}$, $2\mathbb{Z}$, $2\mathbb{Z} + 1$.

Przykład 57. Dla dowolnej funkcji $g\colon \mathbb{R}^2 \to \mathbb{R}$ zbiór rozwiązań równania $g(x, y) = 0$ jest przeciwobrazem zbioru $\{0\}$:

$$\{(x, y) \in \mathbb{R}^2 : g(x, y) = 0\} = g^{-1}(\{0\}).$$

Twierdzenie 10. *Niech* $f\colon X \to Y$ *będzie dowolną funkcją.*

(a) *Dla dowolnych zbiorów* $A, B \subset X$, *jeśli* $A \subset B$, *to* $f(A) \subset f(B)$.

(b) *Dla dowolnych zbiorów* $C, D \subset Y$, *jeśli* $C \subset D$, *to* $f^{-1}(C) \subset f^{-1}(D)$.

Dowód. (a) Załóżmy, że zbiory $A, B \subset X$ spełniają warunek $A \subset B$. Weźmy dowolny element $y_0 \in f(A)$, czyli $y_0 = f(x_0)$, gdzie $x_0 \in A$. Wówczas $x_0 \in B$, ponieważ $A \subset B$. Mamy: $y_0 = f(x_0)$ i $x_0 \in B$, więc $y_0 \in f(B)$.

(b) Rozważmy teraz zbiory $C, D \subset Y$, takie że $C \subset D$. Jeśli $x_0 \in f^{-1}(C)$, to $f(x_0) \in C$, a zatem $f(x_0) \in D$, co oznacza, że $x_0 \in f^{-1}(D)$. □

Twierdzenie 11. *Niech* $f\colon X \to Y$ *będzie dowolną funkcją. Wówczas dla dowolnych zbiorów* $A, B \subset X$ *zachodzą następujące zależności:*

(a) $f(A \cup B) = f(A) \cup f(B)$,

(b) $f(A \cap B) \subset f(A) \cap f(B)$,

(c) $f(A) \setminus f(B) \subset f(A \setminus B)$.

Dowód. (a) Stosując Twierdzenie 10 (a) do inkluzji $A \subset A \cup B$ i $B \subset A \cup B$ otrzymujemy inkluzje $f(A) \subset f(A \cup B)$ i $f(B) \subset f(A \cup B)$. Zatem $f(A) \cup f(B) \subset f(A \cup B)$.

Pozostaje do udowodnienia inkluzja $f(A \cup B) \subset f(A) \cup f(B)$. Weźmy dowolny element $y_0 \in f(A \cup B)$. Istnieje $x_0 \in A \cup B$, takie że $y_0 = f(x_0)$. Jeśli $x_0 \in A$, to $y_0 \in f(A)$, a jeśli $x_0 \in B$, to $y_0 \in f(B)$. Ostatecznie, $y_0 \in f(A) \cup f(B)$, co kończy dowód.

(b) Wystarczy zastosować Twierdzenie 10 (a) do inkluzji $A \cap B \subset A$ i $A \cap B \subset B$. □

Twierdzenie 12. *Niech* $f\colon X \to Y$ *będzie dowolną funkcją. Wówczas dla dowolnych zbiorów* $C, D \subset Y$ *zachodzą równości:*

(a) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$,

(b) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$,

(c) $f^{-1}(C \setminus D) = f^{-1}(C) \setminus f^{-1}(D)$.

Dowód. (a) Dla dowolnego $x \in X$ mamy:

$$x \in f^{-1}(C \cup D) \Leftrightarrow f(x) \in C \cup D \Leftrightarrow (f(x) \in C \vee f(x) \in D) \Leftrightarrow (x \in f^{-1}(C) \vee x \in f^{-1}(D)) \Leftrightarrow x \in f^{-1}(C$$

(b) Analogicznie do (a). □

8.9 Cztery abstrakcyjne zadania o funkcjach

Zadanie 19. *Udowodnij, że funkcja $f\colon X \to Y$ jest różnowartościowa dokładnie wtedy, gdy dla dowolnych podzbiorów $A, B \subset X$ zachodzi implikacja:*

$$A \subsetneqq B \quad \Rightarrow \quad f(A) \subsetneqq f(B).$$

Zadanie 20. *Udowodnij, że funkcja $f\colon X \to Y$ jest „na" dokładnie wtedy, gdy dla dowolnych podzbiorów $C, D \subset Y$ zachodzi implikacja:*

$$C \subsetneqq D \quad \Rightarrow \quad f^{-1}(C) \subsetneqq f^{-1}(D).$$

Zadanie 21. *Udowodnij, że funkcja $f\colon X \to Y$ jest różnowartościowa wtedy i tylko wtedy, gdy dla dowolnego zbioru Z i dowolnych funkcji $g_1, g_2\colon Z \to X$ zachodzi implikacja:*

$$f \circ g_1 = f \circ g_2 \quad \Rightarrow \quad g_1 = g_2.$$

Zadanie 22. *Udowodnij, że funkcja $f\colon X \to Y$ jest „na" wtedy i tylko wtedy, gdy dla dowolnego zbioru Z i dowolnych funkcji $h_1, h_2\colon Y \to Z$ zachodzi implikacja:*

$$h_1 \circ f = h_2 \circ f \quad \Rightarrow \quad h_1 = h_2.$$

Rozwiązanie. ($\Rightarrow$) Załóżmy, że funkcja $f\colon X \to Y$ jest „na" i rozważmy dowolne funkcje $h_1, h_2\colon Y \to Z$, takie że

$$(*) \qquad h_1 \circ f = h_2 \circ f.$$

Pokażemy, że $h_1 = h_2$.

Dla dowolnego $y \in Y$ istnieje $x \in X$, taki że $y = f(x)$ (f jest „na"). Zatem, z równości $(*)$ dla $y \in Y$ otrzymujemy

$$h_1(y) = h_1(f(x)) = h_2(f(x)) = h_2(y),$$

co oznacza, że $h_1 = h_2$.

($\Leftarrow$) Pokażemy, że jeśli funkcja $f\colon X \to Y$ nie jest „na", to istnieje zbiór Z i funkcje $h_1, h_2\colon Y \to Z$, dla których nie jest prawdziwa implikacja

$$h_1 \circ f = h_2 \circ f \Rightarrow h_1 = h_2,$$

czyli $h_1 \circ f = h_2 \circ f$ i $h_1 \neq h_2$.

Zauważmy, że wystarczy rozważyć dwuelementowy zbiór $Z = \{a, b\}$, funkcję $h_1 \colon Y \to Z$ określić wzorem $h_1(y) = a$ dla każdego $y \in Y$, a funkcję $h_2 \colon Y \to Z$ określić następująco:

$$h_2(y) = \begin{cases} a, \text{ jeśli } y \in f(X), \\ b, \text{ jeśli } y \in Y \setminus f(X). \end{cases}$$

Funkcje h_1 i h_2 są różne, gdyż zbiór $Y \setminus f(X)$ jest niepusty (f nie jest „na"). Natomiast dla każdego $x \in X$ oczywiście $f(x) \in f(X)$, więc $h_2(f(x)) = a = h_1(f(x))$. $\square$

9 Relacje

9.1 Pojęcie relacji

Definicja 17. Relacją *n-argumentową zachodzącą między elementami zbiorów* X_1, X_2, ..., X_n *nazywamy podzbiór*

$$\varrho \subset X_1 \times X_2 \times \ldots \times X_n.$$

Jeśli $\varrho \subset X \times Y$ jest relacją dwuargumentową (binarną), to zamiast $(x, y) \in \varrho$ piszemy $x \varrho y$.

Definicja 18. *Relacją binarną określoną w zbiorze* X *nazywamy podzbiór* $\varrho \subset X \times X$.

9.2 Funkcja jako relacja

Uwaga 13. Wykres funkcji $f\colon X \to Y$, jako podzbiór iloczynu kartezjańskiego $X \times Y$, jest relacją binarną zachodzącą między elementami zbiorów X i Y. Funkcję zdefiniowaliśmy nieformalnie jako przyporządkowanie, natomiast wykres jest z formalnego punktu widzenia „porządnym" obiektem matematycznym. I ten właśnie obiekt oficjalnie definiujemy jako funkcję.

Definicja 19. Funkcją *nazywamy relację binarną* $R \subset X \times Y$, *taką że dla każdego elementu* $x \in X$ *jest jeden i tylko jeden element* $y \in Y$ *spełniający warunek* $(x, y) \in R$:

$$\forall_{x \in X} \exists!_{y \in Y} (x, y) \in R.$$

Kwantyfikator $\exists!$ oznacza „istnieje dokładnie jeden". Powyższy warunek możemy wyrazić również za pomocą standardowych kwantyfikatorów:

$$(\forall_{x \in X} \exists_{y \in Y} (x, y) \in R) \wedge (\forall_{x \in X} \forall_{y_1, y_2 \in Y} ((x, y_1) \in R \wedge (x, y_2) \in R) \Rightarrow y_1 = y_2).$$

9.3 Własności relacji binarnych

Rozważmy relację binarną ϱ określoną w zbiorze X: $\varrho \subset X \times X$.

Definicja 20. *Mówimy, że relacja* ϱ *jest:*

- **zwrotna**, *jeśli* $\forall_{x \in X} x \varrho x$,
- **przeciwzwrotna**, *jeśli* $\forall_{x \in X} \sim x \varrho x$,
- **symetryczna**, *jeśli* $\forall_{x,y \in X} x \varrho y \Rightarrow y \varrho x$,
- **asymetryczna** *(antysymetryczna), jeśli* $\forall_{x,y \in X} x \varrho y \Rightarrow \sim y \varrho x$,
- **słabo antysymetryczna**, *jeśli* $\forall_{x,y \in X} x \varrho y \wedge y \varrho x \Rightarrow x = y$,
- **spójna**, *jeśli* $\forall_{x,y \in X} x \varrho y \vee y \varrho x \vee x = y$,

– **przechodnia**, *jeśli* $\forall_{x,y,z\in X} x\varrho y \wedge y\varrho z \Rightarrow x\varrho z$.

Przykład 58. Zbadajmy własności następujących relacji binarnych w zbiorze $\mathbb{R}$: „$x < y$”, „$x \leqslant y$”, „$|x| = |y|$”.

relacja w $\mathbb{R}$	$x < y$	$x \leqslant y$	$\lvert x\rvert = \lvert y\rvert$
zwrotność	−	+	+
przeciwzwrotność	+	−	−
symetria	−	−	+
asymetria	+	−	−
słaba antysymetria	+	+	−
spójność	+	+	−
przechodniość	+	+	+

Przykład 59. Zbadajmy własności następujących relacji binarnych w zbiorze $\mathbb{N}_1$: „x i y są tej samej parzystości”, „$y = x^2$”, „$x \mid y$”.

relacja w $\mathbb{N}_1$	x i y stsp	$y = x^2$	$x \mid y$
zwrotność	+	−	+
przeciwzwrotność	−	−	−
symetria	+	−	−
asymetria	−	−	−
słaba antysymetria	−	+	+
spójność	−	−	−
przechodniość	+	−	+

Uwaga 14. Jeśli relacja jest asymetryczna, to jest też słabo antysymetryczna.

9.4 Grafy i macierze relacji binarnych

Rozważmy relację binarną ϱ określoną w zbiorze skończonym X. Możemy narysować graf, którego wierzchołki są oznaczone elementami tego zbioru. Krawędź grafu o początku x i końcu y (strzałkę prowadzącą z x do y) rysujemy wtedy i tylko wtedy, gdy $x\varrho y$.

Własności danej relacji można odczytać z grafu.

zwrotność	Przy każdym wierzchołku jest pętla.
przeciwzwrotność	Przy żadnym wierzchołku nie ma pętli.
symetria	Na każdej krawędzi są strzałki w obie strony.
asymetria	Na każdej krawędzi jest strzałka tylko w jedną stronę. Nie ma pętli.
słaba antysymetria	Na każdej krawędzi jest strzałka tylko w jedną stronę. (Mogą być pętle.)
spójność	Każde dwa (różne) wierzchołki są połączone krawędzią.

Macierz relacji ϱ tworzymy w ten sposób, że wiersze i kolumny oznaczamy elementami zbioru X. Na przecięciu wiersza oznaczonego elementem x i kolumny oznaczonej elementem y stawiamy 1, jeśli $x\varrho y$, a 0 w przeciwnym wypadku.

Przykład 60. Niech $X = \{1, 2, 3, 4, 5\}$.

$x < y$

$x\backslash y$	1	2	3	4	5
1	0	1	1	1	1
2	0	0	1	1	1
3	0	0	0	1	1
4	0	0	0	0	1
5	0	0	0	0	0

$x \mid y$

$x\backslash y$	1	2	3	4	5
1	1	1	1	1	1
2	0	1	0	1	0
3	0	0	1	0	0
4	0	0	0	1	0
5	0	0	0	0	1

$y = x^2$

$x\backslash y$	1	2	3	4	5
1	1	0	0	0	0
2	0	0	0	1	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0

x i y stsp

$x\backslash y$	1	2	3	4	5
1	1	0	1	0	1
2	0	1	0	1	0
3	1	0	1	0	1
4	0	1	0	1	0
5	1	0	1	0	1

Własności danej relacji można odczytać z macierzy.

zwrotność	Na głównej przekątnej są same jedynki.
przeciwzwrotność	Na głównej przekątnej są same zera.
symetria	Macierz jest symetryczna (względem głównej przekątnej).
asymetria	Na miejscach symetrycznych (względem głównej przekątnej) nie ma dwóch jedynek. Na głównej przekątnej są same zera.
słaba antysymetria	Na miejscach symetrycznych (względem głównej przekątnej) nie ma dwóch jedynek.
spójność	Na miejscach symetrycznych (względem głównej przekątnej) nie ma dwóch zer.

Zadanie 23. (a) *Narysować dowolny graf relacji. Zbadać własności tej relacji. Utworzyć jej macierz.*

(b) *Napisać dowolną macierz relacji. Zbadać własności tej relacji. Narysować jej graf.*

9.5 Relacje porządkujące

Definicja 21. *Relację binarną ϱ określoną w zbiorze X nazywamy relacją częściowego porządku (lub relacją porządkującą), jeśli jest zwrotna, słabo antysymetryczna i przechodnia. Zbiór X z określoną w nim relacją porządkującą nazywamy zbiorem częściowo uporządkowanym.*

Relację porządkującą oznaczamy zazwyczaj symbolem „$\preccurlyeq$”. Mówimy wówczas, że $(X, \preccurlyeq)$ jest zbiorem częściowo uporządkowanym. Mamy zatem warunki:

$$\forall_{x\in X} x \preccurlyeq x, \quad \forall_{x,y\in X} x \preccurlyeq y \wedge y \preccurlyeq x \Rightarrow x = y,$$

$$\forall_{x,y,z\in X} x \preccurlyeq y \wedge y \preccurlyeq z \Rightarrow x \preccurlyeq z.$$

Jeśli „$\preccurlyeq$” jest relacją częściowego porządku, to możemy określić relację „$\prec$” następująco:

$$x \prec y \Leftrightarrow x \preccurlyeq y \wedge x \neq y.$$

Jeśli $x \prec y$, to mówimy, że element x jest mniejszy od y (w sensie relacji), a y jest większy od x. Jeśli $x \preccurlyeq y$, to mówimy, że element x jest mniejszy lub równy y (w sensie relacji), a y jest większy lub równy x.

9.6 Elementy ekstremalne

Definicja 22. *Niech $(X, \preccurlyeq)$ będzie zbiorem częściowo uporządkowanym. Element $x \in X$ nazywamy:*

– **najmniejszym,** *jeśli jest mniejszy od pozostałych elementów:*

$$\forall_{y\in X} x \preccurlyeq y,$$

– **największym,** *jeśli jest większy od pozostałych elementów:*

$$\forall_{y\in X} y \preccurlyeq x,$$

– **minimalnym,** *jeśli nie ma elementów od niego mniejszych:*

$$\forall_{y\in X} y \preccurlyeq x \Rightarrow y = x,$$

– **maksymalnym,** *jeśli nie ma elementów od niego większych:*

$$\forall_{y\in X} x \preccurlyeq y \Rightarrow y = x.$$

Przykład 61. Elementy ekstremalne.

zbiór częściowo uporządkowany	elementy minimalne	elementy maksymalne
$(\{1,2,3,4,5\}, \leqslant)$	1 – najmniejszy	5 – największy
$(\{1,2,3,4,5\}, \mid)$	1 – najmniejszy	$3, 4, 5$
$(\mathbb{N}_1, \mid)$	1 – najmniejszy	nie ma
$(\mathbb{N}_2, \mid)$	liczby pierwsze	nie ma
$(2^{\{a,b,c\}}, \subset)$	$\emptyset$	$\{a,b,c\}$
$(2^{\{a,b,c\}} \setminus \{\emptyset, \{a,b,c\}\}, \subset)$	$\{a\}, \{b\}, \{c\}$	$\{a,b\}, \{a,c\}, \{b,c\}$

Zadanie 24. *Narysuj kilka diagramów zbiorów częściowo uporządkowanych, wskaż elementy minimalne, maksymalne, najmniejsze, największe.*

Uwaga 15. Element najmniejszy (jeśli istnieje) jest jedynym elementem minimalnym. Analogicznie, element największy jest jedynym maksymalnym. Jedyny element minimalny nie musi być elementem najmniejszym (chyba, że zbiór jest skończony).

9.7 Porządek liniowy

Definicja 23. *Relację porządkującą, która jest spójna, nazywamy relacją porządku liniowego. Oznacza to, że spełniony jest warunek*

$$\forall_{x,y\in X} x \preccurlyeq y \vee y \preccurlyeq x.$$

Przykład 62. Zbiory liniowo uporządkowane: $(\mathbb{R}, \leqslant)$, $(\{1,2,4,8\}, |)$, $(\{\{a\},\{a,b\},\{a,b,c\}\}, \subset)$.

W zbiorze liniowo uporządkowanym istnieje co najwyżej jeden element minimalny. Jeśli taki element istnieje, to jest elementem najmniejszym. Analogiczna własność zachodzi oczywiście dla elementów maksymalnych.

Porządek leksykograficzny

Niech $(A, \preccurlyeq)$ będzie zbiorem liniowo uporządkowanym. W zbiorze słów nad alfabetem A określamy relację porządku leksykograficznego „$\preccurlyeq_{lex}$" w sposób następujący:

$$a_1a_2\ldots a_m \preccurlyeq_{lex} b_1b_2\ldots b_n \Leftrightarrow \begin{cases} a_1 \prec b_1 \\ \vee \\ a_1 = b_1, \ldots, a_{k-1} = b_{k-1}, a_k \prec b_k \\ \vee \\ a_1 = b_1, \ldots, a_m = b_m, m \leqslant n. \end{cases}$$

Relacja „$\preccurlyeq_{lex}$" jest porządkiem liniowym w zbiorze A^*.

Porządek gęsty

Definicja 24. *Porządek liniowy „$\preccurlyeq$" w zbiorze X nazywamy gęstym, jeśli dla dowolnych dwóch elementów $a, b \in X$ spełniających warunek $a \prec b$ istnieje element $c \in X$ taki, że $a \prec c$ i $c \prec b$.*

Przykład 63. Przykłady zbiorów uporządkowanych gęsto: $\mathbb{Q}$, $\mathbb{R}$ ze „zwykłą" relacją $x \leqslant y$.

Przykład 64. Przykład zbioru z porządkiem liniowym, który nie jest gęsty: $(\mathbb{Z}, \leqslant)$.

Twierdzenie 13. *Jeśli $(X, \preccurlyeq)$ jest zbiorem uporządkowanym gęsto, to dla dowolnych dwóch elementów $a, b \in X$ spełniających warunek $a \prec b$ istnieje nieskończenie wiele elementów $c \in X$ takich, że $a \prec c$ i $c \prec b$.*

Dowód. Jeśli elementy $a, b \in X$ spełniają warunek $a \prec b$, to istnieje element $b_1 \in X$, taki że $a \prec b_1$ i $b_1 \prec b$. A skoro $a \prec b_1$, to istnieje element $b_2 \in X$, taki że $a \prec b_2$ i $b_2 \prec b_1$ (z czego wynika, że $b_2 \prec b$). Następnie, istnieje element $b_3 \in X$, taki że $a \prec b_3$ i $b_3 \prec b_2$ (skąd mamy: $b_3 \prec b$).

W ten sposób konstruujemy nieskończony ciąg elementów b_1, b_2, b_3, ..., spełniających dla każdego n warunki:

$$a \prec b_n \prec b_{n-1} \prec \ldots \prec b_2 \prec b_1 \prec b.$$

□

Porządek ciągły

Definicja 25. *Porządek gęsty „$\preccurlyeq$” w zbiorze X nazywamy ciągłym, jeśli dla dowolnych dwóch niepustych podzbiorów $A, B \subset X$ spełniających warunek*

$$\forall_{a\in A}\forall_{b\in B}\ a \preccurlyeq b$$

istnieje element $c \in X$ taki, że

$$\Big(\forall_{a\in A}\ a \preccurlyeq c\Big) \wedge \Big(\forall_{b\in B}\ c \preccurlyeq b\Big).$$

Przykład 65. Przykład zbioru z porządkiem ciągłym: $(\mathbb{R}, \leqslant)$.

Przykład 66. Przykłady zbiorów z porządkiem liniowym, który nie jest ciągły: $\mathbb{Z}$, $\mathbb{Q}$ z relacją „$\leqslant$”.

Porządek dobry

Definicja 26. *Porządek liniowy „$\preccurlyeq$” w zbiorze X nazywamy dobrym, jeśli w każdym niepustym podzbiorze $A \subset X$ istnieje element najmniejszy.*

Przykład 67. Przykłady zbiorów uporządkowanych w sposób dobry:

- dowolny zbiór skończony liniowo uporządkowany,
- $\mathbb{N}$ z relacją „$\leqslant$”,
- $\mathbb{N} \times \mathbb{N}$ z porządkiem leksykograficznym wyznaczonym przez relację „$\leqslant$” w zbiorze $\mathbb{N}$.

Przykład 68. Przykłady podzbiorów zbioru $\mathbb{R}$ z relacją „$\leqslant$”, które są uporządkowane w sposób dobry:

- $\{-\frac{1}{n}, n \in \mathbb{N} \setminus \{0\}\}$,
- $\{-\frac{1}{n}, n \in \mathbb{N} \setminus \{0\}\} \cup \{0\}$,
- $\{-\frac{1}{n}, n \in \mathbb{N} \setminus \{0\}\} \cup \{1 - \frac{1}{n}, n \in \mathbb{N} \setminus \{0\}\}$,
- $\{m - \frac{1}{n}, m \in \mathbb{N}, n \in \mathbb{N} \setminus \{0\}\}$.

Przykład 69. Przykłady zbiorów z porządkiem liniowym, który nie jest dobry: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{R}_+$, $[0, +\infty)$ z relacją „$\leqslant$”.

Twierdzenie Zermela. *Każdy zbiór można dobrze uporządkować.*

Dowód tego twierdzenia można znaleźć w [11], str. 157 oraz w [7], str. 153.

9.8 Relacje równoważności

Definicja 27. *Relację binarną ϱ określoną w zbiorze X nazywamy* **relacją równoważności**, *jeśli jest zwrotna, symetryczna i przechodnia:*

$$\forall_{x\in X}\ x\varrho x, \qquad \forall_{x,y\in X}\ x\varrho y \Rightarrow y\varrho x, \qquad \forall_{x,y,z\in X}\ x\varrho y \wedge y\varrho z \Rightarrow x\varrho z.$$

Niech m będzie liczbą naturalną, $m > 1$. W zbiorze $\mathbb{Z}$ określmy relację

$$x \equiv y \pmod m \Leftrightarrow m \mid x - y.$$

Zapis $x \equiv y \pmod m$ czytamy „x przystaje do y modulo m".

Przystawanie modulo m jest relacją równoważności w zbiorze $\mathbb{Z}$ (sprawdź!). Zauważmy, że $x \equiv y \pmod m$ dokładnie wtedy, gdy x i y dają tę samą resztę przy dzieleniu przez m.

Przykład 70. Tabela liczb całkowitych dających odpowiednie reszty przy dzieleniu przez 5.

reszta	liczby
0	$\ldots, -10, -5, 0, 5, 10, \ldots$
1	$\ldots, -9, -4, 1, 6, 11, \ldots$
2	$\ldots, -8, -3, 2, 7, 12, \ldots$
3	$\ldots, -7, -2, 3, 8, 13, \ldots$
4	$\ldots, -6, -1, 4, 9, 14, \ldots$

Widzimy, że liczby znajdujące się w jednym wierszu są ze sobą w relacji, a liczby znajdujące się w różnych wierszach nie są ze sobą w relacji, na przykład:

$$-10 \equiv 5 \pmod 5, \qquad 11 \equiv -4 \pmod 5, \qquad 2014 \equiv 4 \pmod 5,$$

$$3 \equiv 13 \pmod 5, \qquad -9 \not\equiv 7 \pmod 5, \qquad -2 \not\equiv 2 \pmod 5.$$

9.9 Klasy abstrakcji

Definicja 28. *Niech ϱ będzie relacją binarną w zbiorze X. Dla każdego elementu $x \in X$ określamy zbiór*

$$[x]_\varrho = \{y \in X :\ x\varrho y\} \subset X.$$

Jeśli ϱ jest relacją równoważności, to zbiór $[x]_\varrho$ nazywamy **klasą abstrakcji** *(lub klasą równoważności) elementu x.*

Przykład 71. Dla relacji przystawania modulo 5 mamy np.:

$$[0]_\varrho = \{\ldots, -5, 0, 5, 10, \ldots\},$$

$$[7]_\varrho = [2]_\varrho = \{\ldots, -3, 2, 7, 12, \ldots\},$$
$$[2014]_\varrho = [4]_\varrho = \{\ldots, -6, -1, 4, 9, 14, \ldots\}.$$

Zauważmy, że zbiory $[0]_\varrho$, $[1]_\varrho$, $[2]_\varrho$, $[3]_\varrho$, $[4]_\varrho$ są parami rozłączne oraz

$$[0]_\varrho \cup [1]_\varrho \cup [2]_\varrho \cup [3]_\varrho \cup [4]_\varrho = \mathbb{Z}.$$

Jeśli ϱ jest relacją równoważności w zbiorze X, to

$$[x]_\varrho = \{y \in X : \ x \varrho y\} = \{y \in X : \ y \varrho x\}.$$

Twierdzenie 14. *Jeśli ϱ jest relacją równoważności w zbiorze X, to:*

(a) $\forall_{x \in X} \ x \in [x]_\varrho$,

(b) $\forall_{x,y \in X} \ x \varrho y \Leftrightarrow [x]_\varrho = [y]_\varrho$,

(c) $\forall_{x,y \in X} \ [x]_\varrho = [y]_\varrho \vee [x]_\varrho \cap [y]_\varrho = \emptyset$.

Dowód. (a) Dla dowolnego $x \in X$ mamy: $x \varrho x$, więc $x \in [x]_\varrho$.

(b) ($\Rightarrow$) Załóżmy, że $x, y \in X$ spełniają warunek $x \varrho y$. Udowodnimy równość zbiorów $[x]_\varrho = [y]_\varrho$. Dla dowolnego $z \in X$ mamy:

- jeśli $z \in [x]_\varrho$, to $x \varrho z$, a skoro (z symetrii) $y \varrho x$, to (z przechodniości) $y \varrho z$, co oznacza, że $z \in [y]_\varrho$,
- jeśli $z \in [y]_\varrho$, to $y \varrho z$, a ponieważ $x \varrho y$, więc (z przechodniości) $x \varrho z$, co oznacza, że $z \in [x]_\varrho$.

($\Leftarrow$) Załóżmy, że dla pewnych elementów $x, y \in X$ zachodzi równość $[x]_\varrho = [y]_\varrho$. Z punktu (a) wiemy, że $y \in [y]_\varrho$, zatem $y \in [x]_\varrho$, a to oznacza, że $x \varrho y$.

(c) Rozważmy dowolne elementy $x, y \in X$. W punkcie (b) wykazaliśmy, że jeśli $x \varrho y$, to $[x]_\varrho = [y]_\varrho$. Udowodnimy teraz, że jeśli $\sim (x \varrho y)$, to $[x]_\varrho \cap [y]_\varrho = \emptyset$.

Zastosujemy metodę „nie wprost", tzn. wykażemy, że jeśli $[x]_\varrho \cap [y]_\varrho \neq \emptyset$, to $x \varrho y$. Załóżmy, że $[x]_\varrho \cap [y]_\varrho \neq \emptyset$, czyli istnieje pewien element $z \in [x]_\varrho \cap [y]_\varrho$. Skoro $z \in [x]_\varrho$, to $x \varrho z$, a skoro $z \in [y]_\varrho$, to $y \varrho z$, więc (z symetrii) również $z \varrho y$. Otrzymaliśmy: $x \varrho z$ oraz $z \varrho y$, więc (z przechodniości) $x \varrho y$.

□

Wniosek 1. *Jeśli ϱ jest relacją równoważności w zbiorze X, to jej klasy abstrakcji są niepuste, parami rozłączne i ich sumą jest cały zbiór X.*

Mówimy, że klasy abstrakcji określają podział zbioru X. Okazuje się, że zachodzi też zależność odwrotna.

Twierdzenie 15. *Jeśli zbiór X jest podzielony na niepuste, parami rozłączne podzbiory:*

$$X = \bigcup_{i \in I} X_i, \quad X_i \neq \emptyset, \quad X_i \cap X_j = \emptyset \ \textit{dla} \ i \neq j,$$

to możemy określić relację ϱ odpowiadającą temu podziałowi, taką że elementy x, y są w relacji, gdy należą do tej samej części podziału:

$$x \varrho y \Leftrightarrow \exists_{i \in I} x, y \in X_i.$$

Wówczas ϱ jest relacją równoważności, a jej klasami abstrakcji są części podziału zbioru X.

Dowód. Skoro $X = \bigcup_{i \in I} X_i$, to każdy element $x \in X$ należy do pewnego zbioru X_i, a wówczas $x \varrho x$. Jeśli elementy $x, y \in X$ spełniają warunek $x \varrho y$, to $x, y \in X_i$ dla pewnego i, więc również $y \varrho x$. Jeśli dla $x, y, z \in X$ mamy: $x \varrho y$ i $y \varrho z$, to $x, y \in X_i$ dla pewnego i oraz $y, z \in X_j$ dla pewnego j. Wówczas $X_i \cap X_j \neq \emptyset$, więc $i = j$, a zatem $x \varrho z$. Udowodniliśmy, że ϱ jest relacją równoważności.

Rozważmy teraz dowolny element $x \in X$. Element x należy do dokładnie jednego zbioru X_i. Zatem dla dowolnego $y \in X$ mamy:

$$x \varrho y \Leftrightarrow y \in X_i,$$

więc

$$[x]_\varrho = \{y \in X : \ x \varrho y\} = X_i.$$

□

Przykład 72. (a) podział $X = \{A, B, C, D\} \cup \{E, F\} \cup \{G, H\} \cup \{I\}$ określa relację $\sim$ taką, że np. $A \sim A$, $A \sim B$, $A \sim C$, $A \sim D$, $A \not\sim E$, $A \not\sim F$, $A \not\sim G$, $A \not\sim H$, $A \not\sim I$,

(b) podział $\{1, 2, 3, 4, 5\} = \{1, 3, 5\} \cup \{2, 4\}$ określa relację $\sim$ taką, że $x \sim y \Leftrightarrow x$ i y są tej samej parzystości.

Zbiór ilorazowy

Definicja 29. *Jeśli ϱ jest relacją typu równoważności w zbiorze X, to zbiór jej klas abstrakcji nazywamy* **zbiorem ilorazowym** *i oznaczamy symbolem X/ϱ.*

Przykład 73. Dla przystawania modulo 5 mamy

$$\mathbb{Z}/\varrho = \{[0]_\varrho, [1]_\varrho, [2]_\varrho, [3]_\varrho, [4]_\varrho\}.$$

10 Teoria mocy

10.1 Zbiory przeliczalne

Definicja 30. *Zbiór, którego elementy można ustawić w ciąg (skończony lub nieskończony), nazywamy przeliczalnym.*

W myśl powyższej definicji wszystkie zbiory skończone oraz zbiór liczb naturalnych są zbiorami przeliczalnymi.

Przykład 74. $\mathbb{Z}$ jest zbiorem przeliczalnym. Przykład ustawienia wszystkich liczb całkowitych w ciąg:

$$0,\ 1,\ -1,\ 2,\ -2,\ 3,\ -3,\ 4,\ -4,\ \ldots$$

Zadanie 25. *Podaj jawny wzór powyższego ciągu.*

Twierdzenie 16. *Podzbiór zbioru przeliczalnego jest zbiorem przeliczalnym.*

Dowód. Oczywiście podzbiór zbioru skończonego jest zbiorem skończonym, a więc przeliczalnym. Rozważmy teraz dowolny nieskończony zbiór przeliczalny:

$$A = \{a_1,\ a_2,\ a_3,\ \ldots\}.$$

Każdy skończony podzbiór zbioru A jest zbiorem przeliczalnym. Niech B będzie dowolnym nieskończonym podzbiorem zbioru A. Elementy zbioru B stanowią podciąg ciągu elementów zbioru A:

$$B = \{a_{i_1},\ a_{i_2},\ a_{i_3},\ \ldots\},$$

gdzie $i_1 < i_2 < i_3 < \ldots$, zatem B jest zbiorem przeliczalnym. □

Twierdzenie 17. *Suma dwóch zbiorów przeliczalnych jest zbiorem przeliczalnym.*

Dowód. Rozważmy dowolne dwa zbiory przeliczalne A i B. Jeśli A i B są zbiorami skończonymi, to ich suma też jest zbiorem skończonym, a więc przeliczalnym. Załóżmy teraz, że A jest zbiorem nieskończonym:

$$A = \{a_1,\ a_2,\ a_3,\ \ldots\}.$$

Jeśli zbiór $B \setminus A$ jest skończony:

$$B \setminus A = \{b_1,\ b_2,\ \ldots,\ b_n\},$$

to wszystkie elementy zbioru $A \cup B$ możemy ustawić w ciąg następująco:

$$b_1,\ b_2,\ \ldots,\ b_n,\ a_1,\ a_2,\ a_3,\ \ldots$$

Jeśli natomiast zbiór $B \setminus A$ jest nieskończony:

$$B \setminus A = \{b_1,\ b_2,\ b_3,\ \ldots\},$$

to wszystkie elementy zbioru $A \cup B$ możemy ustawić w ciąg następująco:

$$a_1,\ b_1,\ a_2,\ b_2,\ a_3,\ b_3,\ \ldots$$

□

W powyższym dowodzie rozważaliśmy elementy zbioru $B \setminus A$ zamiast B po to, aby otrzymać ciąg, w którym wyrazy się nie powtarzają. Zauważmy, że taki zabieg wcale nie jest konieczny do udowodnienia przeliczalności zbioru.

Uwaga 16. Dla dowolnego ciągu

$$a_1,\, a_2,\, a_3,\, \ldots$$

(którego wyrazy mogą się powtarzać) zbiór jego wyrazów

$$A = \{a_1,\, a_2,\, a_3,\, \ldots\}$$

jest przeliczalny.

Możemy to uzasadnić używając analogicznego argumentu jak w dowodzie Twierdzenia 16. Dzięki powyższej uwadze łatwiej udowodnimy następujące twierdzenie, będące uogólnieniem Twierdzenia 17.

Twierdzenie 18. a) *Suma przeliczalnej rodziny zbiorów przeliczalnych jest zbiorem przeliczalnym.*

b) *Iloczyn kartezjański skończonej liczby zbiorów przeliczalnych jest zbiorem przeliczalnym.*

Dowód. **a)** Rozważmy rodzinę zbiorów

$$\mathcal{A} = \{A_t,\ t \in T\},$$

gdzie T jest zbiorem przeliczalnym, taką że dla każdego $t \in T$ zbiór A_t jest przeliczalny.

Jeśli wśród zbiorów rodziny $\mathcal{A}$ są zbiory skończone, to przez T_0 oznaczamy zbiór wszystkich tych $t \in T$, dla których A_t jest zbiorem skończonym. Jeśli ponadto T_0 jest zbiorem skończonym, to suma

$$\bigcup_{t \in T_0} A_t$$

jest zbiorem skończonym, jako skończona suma zbiorów skończonych. Jeśli zaś T_0 jest zbiorem nieskończonym, to jego elementy można ustawić w ciąg nieskończony:

$$T_0 = \{t_1,\, t_2,\, t_3,\, \ldots\},$$

gdyż jest przeliczalny jako podzbiór zbioru T. Wówczas elementy kolejnych zbiorów skończonych:

$$\begin{aligned} A_{t_1} &= \{a_1^{(1)},\, a_2^{(1)},\, \ldots,\, a_{n_1}^{(1)}\},\\ A_{t_2} &= \{a_1^{(2)},\, a_2^{(2)},\, \ldots,\, a_{n_2}^{(2)}\},\\ A_{t_3} &= \{a_1^{(3)},\, a_2^{(3)},\, \ldots,\, a_{n_3}^{(3)}\},\\ &\vdots \end{aligned}$$

możemy ustawić w jeden ciąg

$$a_1^{(1)},\, a_2^{(1)},\, \ldots,\, a_{n_1}^{(1)},\, a_1^{(2)},\, a_2^{(2)},\, \ldots,\, a_{n_2}^{(2)},\, a_1^{(3)},\, a_2^{(3)},\, \ldots,\, a_{n_3}^{(3)},\, \ldots$$

Zbiór wyrazów tego ciągu, czyli

$$\bigcup_{t\in T_0} A_t$$

jest zatem zbiorem przeliczalnym.

Załóżmy teraz, że wśród zbiorów rodziny $\mathcal{A}$ są zbiory nieskończone (przeliczalne) i oznaczmy przez T_1 zbiór wszystkich tych $t \in T$, dla których A_t jest zbiorem nieskończonym. Jeśli T_1 jest zbiorem skończonym: $T_1 = \{t'_1, t'_2, \ldots, t'_m\}$, to przeliczalność zbioru

$$\bigcup_{t\in T_1} A_t = A_{t'_1} \cup \cdots \cup A_{t'_m}$$

uzasadniamy prostą indukcją: dla $m = 1$ oczywiste z założenia, że $A_{t'_1}$ jest przeliczalny, w kroku indukcyjnym, jeśli zbiór $A_{t'_1} \cup \cdots \cup A_{t'_m}$ jest przeliczalny, to zbiór $(A_{t'_1} \cup \cdots \cup A_{t'_m}) \cup A_{t'_{m+1}}$ też jest przeliczalny, na mocy Twierdzenia 17. Niech teraz T_1 będzie zbiorem nieskończonym (przeliczalnym): $T_1 = \{t'_1, t'_2, t'_3 \ldots\}$. Elementy kolejnych zbiorów:

$$\begin{aligned}
A_{t'_1} &= \{a_1^{(1)},\, a_2^{(1)},\, a_3^{(1)},\, a_4^{(1)},\, \ldots\},\\
A_{t'_2} &= \{a_1^{(2)},\, a_2^{(2)},\, a_3^{(2)},\, a_4^{(2)},\, \ldots\},\\
A_{t'_3} &= \{a_1^{(3)},\, a_2^{(3)},\, a_3^{(3)},\, a_4^{(3)},\, \ldots\},\\
A_{t'_4} &= \{a_1^{(4)},\, a_2^{(4)},\, a_3^{(4)},\, a_4^{(4)},\, \ldots\},\\
&\vdots
\end{aligned}$$

możemy ustawić w jeden ciąg np. tak:

$$a_1^{(1)},\, a_1^{(2)},\, a_2^{(1)},\, a_1^{(3)},\, a_2^{(2)},\, a_3^{(1)},\, a_1^{(4)},\, a_2^{(3)},\, a_3^{(2)},\, a_4^{(1)},\, \ldots$$

Zbiór wyrazów tego ciągu, czyli

$$\bigcup_{t\in T_1} A_t$$

jest wówczas zbiorem przeliczalnym.

Ostatecznie, zbiór

$$\bigcup_{t\in T} A_t = \Big(\bigcup_{t\in T_0} A_t\Big) \cup \Big(\bigcup_{t\in T_1} A_t\Big)$$

jest przeliczalny jako suma dwóch zbiorów przeliczalnych, na mocy Twierdzenia 17.

b) Udowodnimy najpierw, że iloczyn kartezjański dwóch zbiorów przeliczalnych jest zbiorem przeliczalnym.

Jeśli zbiory A i B są skończone, to zbiór $A \times B$ jest skończony, a więc przeliczalny. Jeśli zbiór A jest skończony:

$$A = \{a_1,\, a_2,\, \ldots,\, a_n\},$$

a zbiór B jest nieskończony (przeliczalny):

$$B = \{b_1,\, b_2,\, b_3,\, \dots\},$$

to elementy zbioru $A \times B$ możemy ustawić w ciąg

$$(a_1, b_1),\ (a_2, b_1),\ \dots,\ (a_n, b_1),\ (a_1, b_2),\ (a_2, b_2),\ \dots,\ (a_n, b_2),\ (a_1, b_3),\ (a_2, b_3),\ \dots,\ (a_n, b_3),\ \dots$$

Jeśli zbiór A jest nieskończony (przeliczalny), a zbiór B jest skończony, to postępujemy analogicznie.

Załóżmy teraz, że oba zbiory A i B są nieskończone (przeliczalne):

$$A = \{a_1,\, a_2,\, a_3,\, a_4,\, \dots\},$$

$$B = \{b_1,\, b_2,\, b_3,\, b_4,\, \dots\},$$

Wówczas elementy zbioru $A \times B$ możemy ustawić w ciąg w sposób następujący:

$$(a_1, b_1),\ (a_2, b_1),\ (a_1, b_2),\ (a_3, b_1),\ (a_2, b_2),\ (a_1, b_3),\ (a_4, b_1),\ (a_3, b_2),\ (a_2, b_3),\ (a_1, b_4),\ \dots$$

Niech teraz $A_1,\, A_2,\, \dots,\, A_n$ będą zbiorami przeliczalnymi. Wówczas zbiór

$$A_1 \times A_2 \times \cdots \times A_n$$

jest przeliczany na mocy prostej indukcji. Przypadek $n = 2$ został rozpatrzony powyżej. Jeśli teza zachodzi dla pewnego $n \geqslant 2$ oraz zbiory $A_1,\, A_2,\, \dots,\, A_n,\, A_{n+1}$ są przeliczalne, to zbiór $A_1 \times A_2 \times \cdots \times A_n$ jest przeliczalny na mocy założenia indukcyjnego, a wówczas zbiór

$$(A_1 \times A_2 \times \cdots \times A_n) \times A_{n+1}$$

jest przeliczalny jako iloczyn kartezjański dwóch zbiorów przeliczalnych. □

Wniosek 2. *$\mathbb{Z} \times \mathbb{Z}$ jest zbiorem przeliczalnym.*

Przykład 75. $\mathbb{Q}$ jest zbiorem przeliczalnym.

Dowód. Każdą liczbę wymierną można jednoznacznie przedstawić w postaci $\frac{a}{b}$, gdzie a i b są liczbami całkowitymi, $b > 0$ oraz $\mathrm{NWD}(a, b) = 1$. Wystarczy teraz zauważyć, że zbiór par

$$\{(a, b) \in \mathbb{Z} \times \mathbb{Z} :\ b > 0,\ \mathrm{NWD}(a, b) = 1\}$$

jest przeliczalny, jako podzbiór zbioru $\mathbb{Z} \times \mathbb{Z}$. □

Twierdzenie 19. *Jeśli X jest zbiorem przeliczalnym, to zbiór wszystkich ciągów skończonych o wyrazach z X też jest zbiorem przeliczalnym.*

Dowód. Zbiór ciągów długości n o wyrazach z X, czyli zbiór X^n, jest przeliczalny na mocy Twierdzenia 18 b). Wówczas zbiór wszystkich ciągów skończonych o wyrazach z X, czyli zbiór

$$X \cup X^2 \cup X^3 \cup \ldots = \bigcup_{n=1}^{\infty} X^n$$

jest przeliczalny na mocy Twierdzenia 18 a). □

Wniosek 3. *Zbiór wszystkich słów nad przeliczalnym alfabetem jest przeliczalny.*

Wniosek 4. *Zbiór wielomianów jednej zmiennej o współczynnikach wymiernych jest zbiorem przeliczalnym.*

Dowód. Wielomian $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, gdzie $a_n \neq 0$, jest jednoznacznie określony przez ciąg jego współczynników $(a_n,\ a_{n-1},\ \ldots,\ a_1,\ a_0)$. Wystarczy więc zauważyć, że zbiór takich ciągów

$$\{(a_n,\ a_{n-1},\ \ldots,\ a_1,\ a_0),\ n \in \mathbb{N} \setminus \{0\},\ a_n,\ a_{n-1},\ \ldots,\ a_1,\ a_0 \in \mathbb{Q} :\ a_n \neq 0\}$$

jest przeliczalny, jako podzbiór zbioru wszystkich ciągów skończonych o wyrazach z $\mathbb{Q}$. □

Liczba $\sqrt{2}$ nie jest wymierna, ale jest pierwiastkiem wielomianu $x^2 - 2$ o współczynnikach wymiernych. Liczbę będącą pierwiastkiem niezerowego wielomianu o współczynnikach wymiernych nazywamy liczbą algebraiczną.

Wniosek 5. *Zbiór liczb algebraicznych jest zbiorem przeliczalnym.*

Dowód. Skoro zbiór niezerowych wielomianów jednej zmiennej o współczynnikach wymiernych jest przeliczalny, a każdy taki wielomian ma skończoną liczbę pierwiastków, to zbiór tych pierwiastków jest przeliczalny jako suma przeliczalnej rodziny zbiorów skończonych. Dokładniej, zbiór wielomianów jednej zmiennej o współczynnikach wymiernych oznaczmy przez $\mathbb{Q}[x]$, zbiór pierwiastków wielomianu P oznaczmy przez $V(P)$. Wówczas dla każdego $P \in \mathbb{Q}[x] \setminus \{0\}$ zbiór $V(P)$ jest skończony, więc zbiór

$$\bigcup_{P \in \mathbb{Q}[x] \setminus \{0\}} V(P)$$

jest przeliczalny na mocy Twierdzenia 18 a). □

10.2 Zbiory nieprzeliczalne

Twierdzenie 20. *Zbiór zawierający zbiór nieprzeliczalny jest zbiorem nieprzeliczalnym.*

Dowód. Rozważmy dwa zbiory X i Y, takie że $X \subset Y$. W oparciu o metodę „nie wprost" wystarczy udowodnić, że jeśli Y jest przeliczalny, to X jest przeliczalny, a to jest teza Twierdzenia 16. □

Twierdzenie 21. *Jeśli zbiór X ma więcej niż jeden element, to zbiór wszystkich ciągów nieskończonych o wyrazach z X jest zbiorem nieprzeliczalnym.*

Dowód. Niech zbiór X ma co najmniej dwa elementy, oznaczmy je przez a i b. Przypuśćmy, że zbiór wszystkich ciągów nieskończonych o wyrazach z X jest przeliczalny. Rozważmy ustawienie w ciąg wszystkich takich ciągów:

$$\begin{aligned}
x^{(1)} &= (x_1^{(1)},\ x_2^{(1)},\ x_3^{(1)},\ x_4^{(1)},\ \ldots),\\
x^{(2)} &= (x_1^{(2)},\ x_2^{(2)},\ x_3^{(2)},\ x_4^{(2)},\ \ldots),\\
x^{(3)} &= (x_1^{(3)},\ x_2^{(3)},\ x_3^{(3)},\ x_4^{(3)},\ \ldots),\\
x^{(4)} &= (x_1^{(4)},\ x_2^{(4)},\ x_3^{(4)},\ x_4^{(4)},\ \ldots),\\
&\vdots
\end{aligned}$$

Rozważmy ciąg

$$x^{(0)} = (x_1^{(0)}, x_2^{(0)}, x_3^{(0)}, x_4^{(0)}, \dots)$$

określony następująco:

$$x_n^{(0)} = \begin{cases} a, & \text{jeśli } x_n^{(n)} \neq a, \\ b, & \text{jeśli } x_n^{(n)} = a, \end{cases}$$

$n = 1, 2, 3, \dots$ Zauważmy, że n-ty wyraz ciągu $x^{(0)}$ jest różny od n-tego wyrazu ciągu $x^{(n)}$, więc ciąg $x^{(0)}$ jest różny od każdego z ciągów $x^{(1)}$, $x^{(2)}$, $x^{(3)}$, $\dots$ Otrzymaliśmy sprzeczność z założeniem, że zbiór wszystkich ciągów nieskończonych o wyrazach z X jest przeliczalny. □

Przykład 76. $\mathbb{R}$ jest zbiorem nieprzeliczalnym.

Dowód. Skoro zbiór wszystkich ciągów nieskończonych o wyrazach ze zbioru $\{0, 1\}$ jest nieprzeliczalny, to zbiór wszystkich liczb rzeczywistych o zapisie dziesiętnym postaci $0, c_1c_2c_3 \dots$, gdzie $c_1, c_2, c_3, \dots \in \{0, 1\}$, też jest nieprzeliczalny. Zatem zbiór $\mathbb{R}$ zawiera zbiór nieprzeliczalny, więc też jest nieprzeliczalny. □

Twierdzenie 22. *Różnica $A \setminus B$ zbioru nieprzeliczalnego A i zbioru przeliczalnego B, jest zbiorem nieprzeliczalnym.*

Dowód. Rozważmy zbiór nieprzeliczalny A i zbioru przeliczalny B. Gdyby zbiór $A \setminus B$ był przeliczalny, to zbiór

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

też byłby przeliczalny (Twierdzenie 17) – sprzeczność. Zatem zbiór $A \setminus B$ jest nieprzeliczalny. □

Wniosek 6. *Zbiór liczb niewymiernych jest zbiorem nieprzeliczalnym.*

10.3 Równoliczność zbiorów

Definicja 31. *Zbiory A i B nazywamy równolicznymi, jeśli istnieje bijekcja $f\colon A \to B$.*

Twierdzenie 23. *Dwa zbiory skończone są równoliczne dokładnie wtedy, gdy mają tę samą liczbę elementów.*

Dowód. ($\Rightarrow$) Załóżmy, że zbiory A i B są równoliczne, czyli istnieje bijekcja $f\colon A \to B$. Niech zbiór A ma n elementów: $A = \{a_1, a_2, \dots, a_n\}$. Skoro funkcja f jest różnowartościowa, to elementy $f(a_1)$, $f(a_2)$, $\dots$, $f(a_n)$ są parami różne. Ponadto, każdy element zbioru B jest postaci $f(a_i)$ dla pewnego i, ponieważ funkcja f jest „na". Zatem $f(a_1), f(a_2), \dots, f(a_n)$ są wszystkimi elementami zbioru B, co oznacza, że zbiór B ma n elementów.

($\Leftarrow$) Jeśli zbiory A i B mają po n elementów:

$$A = \{a_1, a_2, \dots, a_n\}, \quad B = \{b_1, b_2, \dots, b_n\},$$

to funkcja $f\colon A \to B$, taka że $f(a_i) = b_i$ dla $i = 1, 2, \dots, n$, jest bijekcją. □

Twierdzenie 24. *Dowolne dwa nieskończone zbiory przeliczalne są równoliczne.*

Dowód. Rozważmy dwa dowolne nieskończone zbiory przeliczalne A i B:

$$A = \{a_1, a_2, a_3, \dots\}, \quad B = \{b_1, b_2, b_3, \dots\},$$

gdzie możemy założyć, że $a_i \neq a_j$ oraz $b_i \neq b_j$ dla $i \neq j$. Wówczas funkcja $f\colon A \to B$, taka że $f(a_i) = b_i$ dla $i = 1, 2, 3, \dots$, jest bijekcją. □

Przykład 77. Dowolne dwa spośród następujących zbiorów są równoliczne:

$$\mathbb{R},\ \mathbb{R} \setminus \{0\},\ \mathbb{R}_+,\ \mathbb{R}_+ \cup \{0\},\ (0,1),\ (0,1],\ [0,1].$$

Przykład 78. Jeśli $a < b$ i $c < d$, to przedziały (a, b) i (c, d) są równoliczne.

Twierdzenie 25. *Jeżeli zbiór A jest nieskończony, to dla dowolnego podzbioru skończonego $B \subseteq A$, zbiory A i $A \setminus B$ są równoliczne.*

Dowód. Rozważmy zbiór nieskończony A i dowolny skończony podzbiór B zbioru A:

$$B = \{b_1, b_2, \dots, b_k\}.$$

Zbiór $A \setminus B$ jest nieskończony, więc możemy wybrać ciąg nieskończony utworzony z elementów zbioru $A \setminus B$:

$$a_1, a_2, a_3, \dots,$$

którego elementy są parami różne. Niech $C = \{a_1, a_2, a_3, \dots\}$. (Oczywiście, w tym ciągu nie muszą występować wszystkie elementy zbioru $A \setminus B$.)

Określmy funkcję $f\colon A \to A \setminus B$ następująco:

$$f(x) = \begin{cases} a_i, & \text{jeśli } x \in B,\ x = b_i,\ i \in \{1, \dots, k\}, \\ a_{k+i}, & \text{jeśli } x \in C,\ x = a_i,\ i \in \{1, 2, 3, \dots\}, \\ x, & \text{jeśli } x \in A \setminus (B \cup C). \end{cases}$$

Wykażemy, że funkcja f jest bijekcją. Zauważmy najpierw, że f jest „na”: dla $y \in C$, $y = a_i$ mamy: $y = f(b_i)$, jeśli $i \leqslant k$ oraz $y = f(a_{i-k})$, jeśli $i > k$, zaś dla $y \in (A \setminus B) \setminus C$ mamy $y = f(y)$.

Uzasadnimy teraz różnowartościowość funkcji f. Niech $x_1, x_2 \in A$, $x_1 \neq x_2$. Jeśli $x_1, x_2 \in A \setminus (B \cup C)$, to $f(x_1) = x_1$ i $f(x_2) = x_2$, więc $f(x_1) \neq f(x_2)$. Jeśli $x_1 \in (B \cup C)$, $x_2 \in A \setminus (B \cup C)$, to $f(x_1) \in C$, zaś $f(x_2) = x_2 \in A \setminus (B \cup C)$, więc $f(x_1) \neq f(x_2)$.

Niech teraz $x_1, x_2 \in (B \cup C)$. Jeśli $x_1, x_2 \in B$, $x_1 = b_i$, $x_2 = b_j$, $i \neq j$, to $f(x_1) = a_i$, $f(x_2) = a_j$, więc $f(x_1) \neq f(x_2)$. Analogicznie, jeśli $x_1, x_2 \in C$, $x_1 = a_i$, $x_2 = a_j$, $i \neq j$, to $f(x_1) = a_{k+i}$, $f(x_2) = a_{k+j}$, i również $f(x_1) \neq f(x_2)$. Pozostał przypadek $x_1 \in B$, $x_2 \in C$. Wówczas $x_1 = b_i$, $i \leqslant k$, $x_2 = a_j$, $j \geqslant 1$, więc $f(x_1) = a_i$, $f(x_2) = a_{k+j}$, przy czym $a_i \neq a_{k+j}$, ponieważ $i < k + j$. □

Twierdzenie 26. *Jeżeli zbiór A jest nieprzeliczalny, to dla dowolnego podzbioru przeliczalnego $B \subseteq A$, zbiory A i $A \setminus B$ są równoliczne.*

Dowód. Niech A będzie zbiorem nieprzeliczalnym, niech B będzie przeliczalnym podzbiorem zbioru A. Jeśli zbiór B jest skończony, to równoliczność zbiorów A i $A\setminus B$ wynika z poprzedniego twierdzenia. Niech zatem B będzie zbiorem nieskończonym:

$$B = \{b_1, b_2, b_3, \dots\},$$

gdzie $b_i \neq b_j$ dla $i \neq j$.

Zbiór $A \setminus B$ jest nieskończony (Twierdzenie 22), więc, podobnie jak w dowodzie poprzedniego twierdzenia, wybieramy ciąg nieskończony utworzony z elementów zbioru $A \setminus B$:

$$a_1, a_2, a_3, \dots,$$

gdzie $a_i \neq a_j$ dla $i \neq j$, i wprowadzamy oznaczenie $C = \{a_1, a_2, a_3, \dots\}$.

Rozważamy następującą funkcję $f\colon A \to A \setminus B$:

$$f(x) = \begin{cases} a_{2i}, & \text{jeśli } x \in B,\ x = b_i,\ i \in \{1,2,3,\dots\}, \\ a_{2i-1}, & \text{jeśli } x \in C,\ x = a_i,\ i \in \{1,2,3,\dots\}, \\ x, & \text{jeśli } x \in A \setminus (B \cup C). \end{cases}$$

Analogicznie, jak w dowodzie poprzedniego twierdzenia, uzasadniamy, że funkcja f jest bijekcją. □

Wniosek 7. *Zbiór $\mathbb{R} \setminus \mathbb{Q}$ jest równoliczny z $\mathbb{R}$.*

Twierdzenie 27. *Dla dowolnego zbioru X zbiór 2^X jest równoliczny ze zbiorem wszystkich funkcji ze zbioru X do zbioru $\{0,1\}$.*

Dowód. Zbiór wszystkich funkcji ze zbioru X do zbioru $\{0,1\}$ oznaczmy przez $\mathcal{F}$. Istnieje naturalna bijekcja między zbiorem 2^X a zbiorem $\mathcal{F}$, w której podzbiorowi $A \subset X$ odpowiada funkcja charakterystyczna $\chi_A\colon X \to \{0,1\}$,

$$\chi_A(x) = \begin{cases} 1, & \text{jeśli } x \in A, \\ 0, & \text{jeśli } x \notin A, \end{cases}$$

zaś funkcji $f\colon X \to \{0,1\}$ odpowiada podzbiór $A_f = \{x \in X :\ f(x) = 1\}$. □

Zbiory skończone i zbiory nieskończone

Dysponując pojęciem równoliczności zbiorów możemy zdefiniować pojęcie zbioru nieskończonego. Wyjaśnijmy najpierw specyfikę zbiorów skończonych.

Zadanie 26. *Niech A będzie zbiorem skończonym. Udowodnij, że dla dowolnej funkcji $f\colon A \to A$ następujące warunki są równoważne:*

(a) *funkcja f jest różnowartościowa,*

(b) *funkcja f jest „na”,*

(c) *funkcja f jest bijekcją.*

Zadanie 27. *Wykaż, że dla dowolnego zbioru A następujące warunki są równoważne.*

(a) *Zbiór A jest nieskończony.*

(b) *Istnieje funkcja różnowartościowa $f\colon A \to A$, która nie jest „na".*

(c) *Istnieje podzbiór $B \subsetneq A$ oraz bijekcja $f\colon A \leftrightarrows B$.*

Powyższych własności dowodzimy operując intuicyjnym pojęciem zbioru skończonego i zbioru nieskończonego. Własność wyrażoną w powyższym zadaniu możemy jednak przyjąć jako formalną definicję zbioru nieskończonego.

Definicja 32. *Zbiór nazywamy nieskończonym, jeśli jest równoliczny z pewnym swoim podzbiorem właściwym. Zbiór, który nie jest nieskończonym, nazywamy skończonym.*

Zadanie 28. *Niech zbiór B będzie podzbiorem zbioru A. W oparciu o powyższą definicję, uzasadnij, że:*

– *jeśli zbiór B jest nieskończony, to zbiór A też jest nieskończony,*

– *jeśli zbiór A jest skończony, to zbiór B też jest skończony.*

10.4 Liczby kardynalne

Każdemu zbiorowi odpowiada liczba kardynalna nazywana mocą tego zbioru. Moc zbioru A oznaczamy symbolem $|A|$. Stosowane są również oznaczenia: $\overline{\overline{A}}$, $\#A$. Moc zbioru skończonego to liczba naturalna będąca liczbą jego elementów.

Zbiory A i B są równoliczne dokładnie wtedy, gdy ich moce są równe:

$$|A| = |B|.$$

Moc zbioru liczb naturalnych oznaczamy symbolem „alef zero":

$$|\mathbb{N}| = \aleph_0.$$

Przykład 79. Każdy nieskończony podzbiór zbioru $\mathbb{N}$ jest jest mocy $\aleph_0$.

Moc zbioru liczb rzeczywistych oznaczamy symbolem „continuum":

$$|\mathbb{R}| = \mathfrak{C}.$$

Zbiorami mocy continuum są zbiory wymienione w Przykładzie 77. Przykład 78 pokazuje, jak poszerzyć tę listę.

Przykład 80. Przykłady zbiorów mocy continuum:

$$(a, b),\ [a, b],\ [a, +\infty),\ \mathbb{R} \setminus \mathbb{Q},$$

gdzie $a, b \in \mathbb{R}$, $a < b$.

Nierówności między liczbami kardynalnymi

Definicja 33. *Mówimy, że moc zbioru A nie przekracza mocy zbioru B, jeśli istnieje funkcja różnowartościowa $f\colon A \to B$. Oznaczenie: $|A| \leqslant |B|$.*

Definicja 34. *Mówimy, że moc zbioru A jest mniejsza od mocy zbioru B (co zapisujemy: $|A| < |B|$), jeśli $|A| \leqslant |B|$ i $|A| \neq |B|$.*

Twierdzenie 28 (Cantor – Bernstein)**.** *Jeśli $|A| \leqslant |B|$ i $|B| \leqslant |A|$, to $|A| = |B|$.*

Dowód tego twierdzenia można znaleźć w [11], str. 102 oraz w [7], str. 152.

Wniosek 8. *Jeśli $|A| \leqslant |B|$, $|B| \leqslant |C|$ i $|A| = |C|$, to $|A| = |B| = |C|$.*

Zadanie 29. *Wykaż, że następujące zbiory są mocy continuum:*

(a) *zbiór $\mathbb{C}$ liczb zespolonych,*

(b) *zbiór $2^{\mathbb{N}}$,*

(c) *zbiór ciągów nieskończonych o wyrazach naturalnych.*

Wskazówki: (a) Skonstruuj funkcję różnowartościową $f\colon \mathbb{R}_+ \times \mathbb{R}_+ \to \mathbb{R}_+$.
(b) Skonstruuj funkcję różnowartościową $f\colon \mathbb{R} \to 2^{\mathbb{Q}}$ oraz funkcję różnowartościową ze zbioru ciągów nieskończonych o wyrazach 0, 1 do zbioru $\mathbb{R}$.
(c) Skonstruuj funkcję różnowartościową ze zbioru ciągów nieskończonych o wyrazach naturalnych do zbioru $2^{\mathbb{N}\times\mathbb{N}}$.

Twierdzenie 29 (Cantor)**.** *Dla dowolnego zbioru A zachodzi nierówność $|2^A| > |A|$.*

Dowód. Funkcja $f\colon A \to 2^A$, $f(a) = \{a\}$, jest różnowartościowa, więc $|A| \leqslant |2^A|$. Wykażemy, że $|A| \neq |2^A|$.

Przypuśćmy, że $|A| = |2^A|$, czyli istnieje bijekcja $g\colon A \to 2^A$. Każdemu elementowi $a \in A$ jest wówczas przyporządkowany pewien zbiór $f(a) = B_a \subset A$.

Rozważmy zbiór

$$C = \{a \in A :\ a \notin B_a\}.$$

Zauważmy, że dla dowolnego elementu $a \in A$ mamy:

$$a \in C \Leftrightarrow a \notin B_a.$$

Funkcja f jest „na” oraz $C \in 2^A$, więc $C = f(a_0) = B_{a_0}$ dla pewnego $a_0 \in A$. Wówczas

$$a_0 \notin B_{a_0} \Leftrightarrow a_0 \in C \Leftrightarrow a_0 \notin B_{a_0}$$

– sprzeczność. □

Paradoks Cantora. Oznaczmy przez Ω zbiór, którego elementami są wszystkie zbiory. Wówczas elementami zbioru 2^Ω są wszystkie podzbiory zbioru Ω. Każdy element zbioru 2^Ω jest zbiorem, więc jest elementem zbioru Ω. W takim razie $2^\Omega \subset \Omega$, więc $|2^\Omega| \leqslant |\Omega|$.

Z drugiej strony, z twierdzenia Cantora mamy: $|2^\Omega| > |\Omega|$, co stanowi sprzeczność na mocy twierdzenia Cantora – Bernsteina.

Tego typu paradoksy powstały w związku ze zbyt dowolnym operowaniem intuicyjnym pojęciem zbioru i doprowadziły do konieczności oparcia teorii zbiorów na ścisłych podstawach aksjomatycznych. Odnotujmy jeszcze paradoks Russella.

Paradoks Russella. Oznaczmy przez X zbiór wszystkich zbiorów, które nie są swoimi elementami:

$$X = \{A,\ A \text{ – zbiór},\ A \notin A\}.$$

Zatem dla dowolnego zbioru A mamy:

$$A \in X \Leftrightarrow A \notin A.$$

Zastanówmy się, czy zbiór X jest swoim elementem:

$$X \in X \Leftrightarrow X \notin X$$

– sprzeczność.

10.5 Aksjomaty teorii mnogości

Pewnik wyboru. Dla każdej rodziny zbiorów niepustych i parami rozłącznych istnieje zbiór, który z każdym ze zbiorów tej rodziny ma dokładnie jeden element wspólny.

Dzięki pewnikowi wyboru można udowodnić wiele podstawowych twierdzeń. Jednych z nich jest lemat Kuratowskiego – Zorna, za pomocą którego dowodzi się istnienia różnych maksymalnych obiektów, np. bazy dowolnej przestrzeni liniowej.

Niech $(X, \preccurlyeq)$ będzie zbiorem częściowo uporządkowanym. Niech $A \subset X$ będzie dowolnym podzbiorem. Element $b \in X$ nazywamy ograniczeniem górnym zbioru A, jeśli

$$\forall_{a \in A}\ a \preccurlyeq b.$$

Lemat Kuratowskiego – Zorna. Jeśli w zbiorze częściowo uporządkowanym $(X, \preccurlyeq)$ każdy podzbiór liniowo uporządkowany posiada ograniczenie górne, to w zbiorze X istnieje element maksymalny.

Dowód można znaleźć w [11], str. 158.

Okazuje się, że lemat Kuratowskiego – Zorna i twierdzenie Zermela o tym, że każdy zbiór można dobrze uporządkować (str. 54) są równoważne pewnikowi wyboru, każde z nich może zastąpić pewnik wyboru w zestawie aksjomatów i wówczas będzie można pewnik wyboru udowodnić jako twierdzenie.

Hipoteza continuum. Dowolny nieskończony podzbiór zbioru $\mathbb{R}$ ma moc $\aleph_0$ lub $\mathfrak{c}$.

Gödel udowodnił, że pewnik wyboru i hipoteza continuum są (względnie) niesprzeczne z pozostałymi aksjomatami teorii mnogości, tzn. jeśli nie uzyskamy sprzeczności z pozostałych aksjomatów, to nie uzyskamy jej też dołączając do aksjomatów pewnik wyboru lub hipotezę continuum. Cohen wykazał, że pewnik wyboru i hipoteza continuum są (logicznie) niezależne od pozostałych aksjomatów teorii mnogości, tzn. z nich nie wynikają, więc do aksjomatów można dołączyć zarówno pewnik wyboru lub hipotezę continuum, jak i ich negacje. Dokładniejszą dyskusję tych zagadnień można znaleźć w [9], str. 136, 137.

Aksjomaty Zermelo – Fraenkla teorii mnogości ([9], str. 176 – 178 [22], str. 175, 176).

1. Aksjomat ekstensjonalności. Jeśli dwa zbiory x, y mają te same elementy, to są równe:

$$\forall x\, \forall y\, [\, \forall z\, (z \in x \Leftrightarrow z \in y) \Rightarrow x = y\,].$$

2. Aksjomat pary. Dla dowolnych zbiorów x, y istnieje zbiór $z = \{x, y\}$:

$$\forall x\, \forall y\, \exists z\, \forall u\, (u \in z \Leftrightarrow u = x \vee u = y).$$

3. Aksjomat sumy. Dla dowolnej rodziny zbiorów x istnieje zbiór y będący sumą zbiorów tej rodziny:

$$\forall x\, \exists y\, \forall z\, [\, z \in y \Leftrightarrow \exists u\, (z \in u \wedge u \in x)\,].$$

4. Aksjomat zbioru potęgowego. Dla dowolnego zbioru x istnieje zbiór y, którego elementami są wszystkie podzbiory zbioru x:

$$\forall x\, \exists y\, \forall z\, [\, z \in y \Leftrightarrow \forall u\, (u \in z \Rightarrow u \in x)\,].$$

5 – 8. Aksjomaty:

– wyróżniania – dla dowolnych zbiorów $x_1, \ldots, x_n$ i dowolnego zbioru y istnieje zbiór z, którego elementami są wszystkie elementy zbioru y spełniające warunek $\varphi(x_1, \ldots, x_n)$,

– nieskończoności – istnieje zbiór x, którego elementem jest zbiór pusty, taki że dla dowolnego elementu y zbioru x zbiór $\{y\}$ też jest elementem zbioru x,

– zastępowania – dla dowolnego zbioru u i dla dowolnej relacji $\varphi(x, y)$ określającej funkcję w zbiorze u istnieje zbiór będący zbiorem wartości tej funkcji,

– ufundowania – dla dowolnego zbioru niepustego x istnieje zbiór y będący elementem zbioru x, którego żaden element nie jest elementem zbioru x.

Aksjomat (pewnik) wyboru w zapisie formalnym:

$$\forall x\, \{\, [\, \forall y\, (y \in x \Rightarrow \exists z\, (z \in y)) \wedge$$

$$\wedge\, \forall y\, \forall u\, (y \in x \wedge u \in x \Rightarrow y = u \vee \sim \exists v\, (v \in y \wedge v \in u))\,] \Rightarrow$$

$$\Rightarrow \exists w\, \{\, \forall y\, [\, y \in x \Rightarrow \exists z\, (z \in y \wedge z \in w \wedge \forall v\, (v \in y \wedge v \in w \Rightarrow v = z))\,]\,\}\,\}.$$

11 Konstrukcje zbiorów liczbowych

11.1 Zbiór liczb naturalnych

Zbiór liczb naturalnych określamy aksjomatycznie:

$\mathbb{N}$ – zbiór,

$*\colon \mathbb{N} \to \mathbb{N}$, $n \mapsto n^*$ – funkcja następnika,

$0 \in \mathbb{N}$ – wyróżniony element (zero).

Aksjomaty Peana:

1. Liczba 0 nie jest następnikiem żadnej liczby naturalnej:

$$\forall_{n\in\mathbb{N}}\ n^* \neq 0.$$

2. Funkcja następnika jest różnowartościowa:

$$\forall_{m,n\in\mathbb{N}}\ m^* = n^* \Rightarrow m = n.$$

3. Aksjomat indukcji matematycznej. Dla dowolnego podzbioru $A \subset \mathbb{N}$ mamy:

$$(0 \in A \wedge \forall_{n\in\mathbb{N}}\ (n \in A \Rightarrow n^* \in A)) \Rightarrow A = \mathbb{N}.$$

Istnienie zbioru spełniającego powyższe warunki wynika z aksjomatów teorii mnogości.

Dodawanie liczb naturalnych określamy indukcyjnie (schemat rekursji):

$m + 0 = m$ dla $m \in \mathbb{N}$,

$m + n^* = (m + n)^*$ dla $m, n \in \mathbb{N}$.

Mnożenie liczb naturalnych:

$m \cdot 0 = 0$ dla $m \in \mathbb{N}$,

$m \cdot n^* = m \cdot n + m$ dla $m, n \in \mathbb{N}$.

Określamy: $1 = 0^*$, $2 = 1^*$, $3 = 2^*$, $4 = 3^*$, ...

Przykład 81. $n + 1 = n^*$

Dowód. $n + 1 = n + 0^* = (n + 0)^* = n^*$ □

Przykład 82. $2 + 2 = 4$

Dowód. $2 + 2 = 2 + 1^* = (2 + 1)^* = (2^*)^* = 3^* = 4$ □

Przykład 83. $2 \cdot 2 = 4$

Dowód. $2 \cdot 2 = 2 \cdot 1^* = (2 \cdot 1) + 2 = (2 \cdot 0^*) + 2 = ((2 \cdot 0) + 2) + 2 = (0 + 2) + 2 = (0 + 1^*) + 2 = (0 + 1)^* + 2 = (0^*)^* + 2 = 1^* + 2 = 2 + 2 = 4$ □

11.2 Zbiór liczb całkowitych

Mając dany zbiór liczb naturalnych $\mathbb{N}$ konstruujemy zbiór liczb całkowitych $\mathbb{Z}$ jako zbiór ilorazowy pewnej relacji równoważności.

Rozważmy zbiór

$$X = \mathbb{N} \times \mathbb{N} = \{(a, b);\ a, b \in \mathbb{N}\}.$$

W zbiorze X określamy relację binarną

$$(a, b)\varrho(c, d) \Leftrightarrow a + d = b + c.$$

Relacja ϱ jest relacją równoważności.

Definicja 35. $\mathbb{Z} = X/\varrho = \{[x]_\varrho,\ x \in X\}$.

Przykład 84. Liczbę całkowitą -1 definiujemy jako klasę abstrakcji pary $(0, 1)$. Mamy $(0, 1)\varrho(a, b) \Leftrightarrow 0 + b = 1 + a$, więc

$$[(0, 1)]_\varrho = \{(a, b) \in X :\ b = a + 1\} = \{(0, 1), (1, 2), (2, 3), (3, 4), \dots\}$$

Działania w zbiorze $\mathbb{Z}$ określamy następująco:

$$[(a, b)]_\varrho + [(c, d)]_\varrho = [(a + c, b + d)]_\varrho,$$

$$[(a, b)]_\varrho \cdot [(c, d)]_\varrho = [(ac + bd, ad + bc)]_\varrho,$$

i sprawdzamy poprawność definicji: jeśli $(a, b)\varrho(a', b')$ i $(c, d)\varrho(c', d')$, to $(a + c, b + d)\varrho(a' + c', b' + d')$ i $(ac + bd, ad + bc)\varrho(a'c' + b'd', a'd' + b'c')$.

11.3 Zbiór liczb wymiernych

Rozważmy zbiór

$$X = \mathbb{Z} \times \mathbb{Z} \setminus \{0\} = \{(a, b);\ a, b \in \mathbb{Z},\ b \neq 0\}.$$

W zbiorze X określamy relację binarną

$$(a, b)\varrho(c, d) \Leftrightarrow ad = bc.$$

Relacja ϱ jest relacją równoważności.

Definicja 36. $\mathbb{Q} = X/\varrho = \{[x]_\varrho,\ x \in X\}$.

Przykład 85. Liczbę wymierną $\frac{1}{2}$ definiujemy jako klasę abstrakcji pary $(1, 2)$. Mamy

$$(1, 2)\varrho(a, b) \Leftrightarrow 1 \cdot b = 2 \cdot a,$$

więc

$$[(1, 2)]_\varrho = \{(a, b) \in X :\ b = 2a\} =$$
$$= \{(1, 2), (-1, -2), (2, 4), (-2, -4), (3, 6), (-3, -6), \dots\}$$

Działania w zbiorze $\mathbb{Q}$ określamy następująco:

$$[(a,b)]_\varrho + [(c,d)]_\varrho = [(ad+bc, bd)]_\varrho,$$
$$[(a,b)]_\varrho \cdot [(c,d)]_\varrho = [(ac, bd)]_\varrho.$$

Definicje te są poprawne, tzn. nie zależą od wyboru reprezentantów klas abstrakcji: jeśli $(a,b)\varrho(a',b')$ i $(c,d)\varrho(c',d')$,
to $(ad+bc, bd)\varrho(a'd'+b'c', b'd')$ i $(ac, bd)\varrho(a'c', b'd')$.

11.4 Zbiór liczb rzeczywistych

Zbiór liczb rzeczywistych można skonstruować na dwa sposoby.

Sposób I. Przekroje Dedekinda. Rozważamy podziały zbioru liczb wymiernych na dwa niepuste podzbiory A, B spełniające warunek

$$\forall_{a\in A}\forall_{b\in B}\ a < b.$$

Przekrój Dedekinda (A,B) określający liczbę $\sqrt{2}$:

$$A = \mathbb{Q} \cap (-\infty, \sqrt{2}) = \{x \in \mathbb{Q} :\ x < 0 \vee x^2 < 2\},$$
$$B = \mathbb{Q} \cap (\sqrt{2}, +\infty) = \{x \in \mathbb{Q} :\ x > 0 \wedge x^2 > 2\}.$$

Jeśli w jest liczbą wymierną to mamy dwa przekroje:

$$A_1 = \{x \in \mathbb{Q} :\ x \leqslant w\}, \quad B_1 = \{x \in \mathbb{Q} :\ x > w\},$$
$$A_2 = \{x \in \mathbb{Q} :\ x < w\}, \quad B_2 = \{x \in \mathbb{Q} :\ x \geqslant w\},$$

które należy utożsamić.

Sposób II. Rozważamy ciągi Cauchy'ego liczb wymiernych, czyli wszystkie ciągi liczb wymiernych, które okażą się zbieżne w zbiorze liczb rzeczywistych. Za pomocą relacji równoważności "sklejamy" ciągi zbieżne do tej samej liczby rzeczywistej.

11.5 Zbiór liczb zespolonych

Zbiór liczb zespolonych. Definicja: $\mathbb{C} = \mathbb{R} \times \mathbb{R}$.

Działania w $\mathbb{C}$:

$$(a,b) + (c,d) = (a+c, b+d),$$
$$(a,b) \cdot (c,d) = (ac-bd, ad+bc).$$

Para $(a,0)$ odpowiada liczbie rzeczywistej a:

$$(a,0) + (c,0) = (a+c, 0), \quad (a,0)\cdot(c,0) = (ac, 0).$$

Przyjmując $i = (0,1)$ mamy:

$$a + bi = (a,0) + (b,0)\cdot(0,1) = (a,0) + (0,b) = (a,b),$$
$$i^2 = (0,1)\cdot(0,1) = (-1,0) = -1.$$

Literatura

Podręczniki i zbiory zadań

[1] Bond Robert, Keane William, *An Introduction to Abstract Mathematics*, Waveland Press 2007.

[2] Chartrand Gary, Polimeni Albert, Zhang Ping, *Mathematical Proofs: A Transition to Advanced Mathematics*, Pearson 2012.

[3] Cichoń Jacek, *Wykłady ze wstępu do matematyki*, DWE 2003.

[4] Guzicki Wojciech, Zakrzewski Piotr, *Wykłady ze wstępu do matematyki*, PWN 2005.

[5] Guzicki Wojciech, Zakrzewski Piotr, *Wstęp do matematyki: zbiór zadań*, PWN 2005.

[6] Hammack Richard, *Book of proof*, Virginia Commonwealth University, http://www.people.vcu.edu/~rhammack/BookOfProof/BookOfProof.pdf

[7] Kraszewski Jan, *Wstęp do matematyki*, WNT 2007.

[8] Marek Wiktor, Onyszkiewicz Janusz, *Elementy logiki i teorii mnogości w zadaniach*, PWN 2005.

[9] Murawski Roman, Świrydowicz Kazimierz, *Wstęp do teorii mnogości*, UAM 2006.

[10] Musielak Julian, *Wstęp do matematyki*, PWN 1970.

[11] Rasiowa Helena, *Wstęp do matematyki współczesnej*, PWN 2005.

[12] Ross Kenneth, Wright Charles, *Matematyka dyskretna*, PWN 2005.

Literatura do rozdziału 1

[13] Courant Richard, Robbins Herbert, *Co to jest matematyka?*.

[14] Davis Philip, Hersh Reuben, *Świat matematyki*.

[15] Encyklopedia PWN, wydanie internetowe, `http://encyklopedia.pwn.pl/`.

[16] Mathematics Subject Classification, American Mathematical Society, `http://www.ams.org/msc/msc2010.html`.

[17] Oxford Dictionaries, Oxford University Press, wydanie internetowe, `http://www.oxforddictionaries.com/`.

[18] Słownik Języka Polskiego PWN, wydanie internetowe, `http://sjp.pwn.pl/`.

[19] Wikipedia, wersja angielska, `http://en.wikipedia.org/wiki/`.

[20] Wikipedia, wersja polska, `http://pl.wikipedia.org/wiki/`.

Pozostała literatura

[21] Babinskaja Irina L., *Zadaczi matematiczeskich olimpiad*, Nauka, Moskwa 1975, `http://ilib.mccme.ru/djvu/olimp/babinska.htm`

[22] Murawski Roman, *Filozofia matematyki. Zarys dziejów*, PWN, Warszawa 1995.

[23] Solow Daniel, *How to read and do proofs*, Wiley 1982.

[24] Zinn Claus, *Understanding informal mathematical discourse*, Erlangen 2004.