

Roman Murawski
Kazimierz Świrydowicz

Podstawy logiki i teorii mnogości



WYDAWNICTWO NAUKOWE UAM

PODSTAWY LOGIKI
I TEORII MNOGOŚCI

*Pani Doktor habilitowanej
Beacie Begier-Krasińskiej*

UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU

Roman Murawski
Kazimierz Świrydowicz

PODSTAWY LOGIKI I TEORII MNOGOŚCI



POZNAŃ 2016

Roman Murawski, Kazimierz Świrydowicz
Wydział Matematyki i Informatyki
Uniwersytet im. Adama Mickiewicza w Poznaniu

Recenzent: prof. dr hab. Marian Nowak

Podręcznik dla studentów matematyki i informatyki

© Roman Murawski and Kazimierz Świrydowicz 2016

This edition © Uniwersytet im. Adama Mickiewicza w Poznaniu,
Wydawnictwo Naukowe UAM, Poznań 2016

Projekt okładki: Sylwia Rząsa
Redakcja: Aleksandra Ratajczak
Redakcja techniczna: Elżbieta Rygielska

ISBN 978-83-232-3055-7

WYDAWNICTWO NAUKOWE UNIwersYTETU IM. ADAMA MICKIEWICZA W POZNANIU
61-701 POZNAŃ, UL. FREDRY 10

www.press.amu.edu.pl

Sekretariat: tel. 61 829 46 46, faks 61 829 46 47, e-mail: wyd nauk@amu.edu.pl

Dział sprzedaży: tel. 61 829 46 40, e-mail: press@amu.edu.pl

Wydanie II poprawione. Ark. wyd. 13,50. Ark. druk. 10,25.

DRUK I OPRAWA: EXPOL, WŁOCŁAWEK, UL. BRZESKA 4

Spis treści

Przedmowa	7
Rozdział 1. Elementy klasycznego rachunku zdań	9
1.1. Wprowadzenie	9
1.2. Język rachunku zdań; tautologie	13
1.3. Schematy wnioskowań. Wnioskowania niezawodne	16
1.4. Tautologie rachunku zdań	20
1.5. Warunek dostateczny i konieczny	23
1.6. Symbolika beznawiasowa	24
Zadania	25
Rozdział 2. Funkcje logiczne	27
2.1. Funkcje logiczne – podstawowe definicje	27
2.2. Koniunkcyjna i alternatywna postać normalna	30
2.3. Zupełne układy funkcji	33
Zadania	36
Rozdział 3. System aksjomatyczny logiki klasycznej	38
3.1. Logika klasyczna: syntaktyka	38
3.2. Podstawowe twierdzenia logiki klasycznej	42
Zadania	52
Rozdział 4. Elementy rachunku predykatów	53
4.1. Wprowadzenie	53
4.2. Język rachunku predykatów	54
4.3. Formułowanie wypowiedzi w języku rachunku predykatów	58
4.4. Przykłady tautologii rachunku predykatów	61
4.5. Kwantyfikatory o ograniczonym zakresie	62
4.6. Kwantyfikatory ilościowe	64
4.7. System aksjomatyczny rachunku predykatów	66
Zadania	69

Rozdział 5. Podstawy teorii zbiorów	72
5.1. Uwagi wstępne	72
5.2. Zasada ekstensjonalności	74
5.3. Relacja inkluzji. Zbiór pusty i zbiór potęgowy	76
5.4. Działania na zbiorach	79
5.5. Algebry Boole'a	86
Zadania	90
Rozdział 6. Relacje	93
6.1. Wprowadzenie. Definicja relacji	93
6.2. Relacje binarne i ich własności. Działania na relacjach binarnych	95
6.3. Relacje równoważności	99
Zadania	102
Rozdział 7. Funkcje	106
7.1. Definicja funkcji. Rodzaje funkcji	106
7.2. Operacje na funkcjach	108
7.3. Obrazy i przeciwobrazy oraz ich własności	111
Zadania	114
Rozdział 8. Relacje porządkujące	117
8.1. Rodzaje relacji porządkujących	117
8.2. Zbiory częściowo uporządkowane	120
8.3. Zbiory dobrze uporządkowane	127
Zadania	132
Rozdział 9. Teoria mocy	135
9.1. Wprowadzenie	135
9.2. Liczby kardynalne. Twierdzenie Cantora–Bernsteina	137
9.3. Zbiory przeliczalne	139
9.4. Zbiory nieprzeliczalne	141
Zadania	145
Dodatek. Uwagi historyczne	147
Literatura	152
Skorowidz symboli	154
Skorowidz terminów	157
Skorowidz nazwisk	161

Przedmowa

Książka ta powstała na podstawie wykładów i ćwiczeń z logiki matematycznej i teorii mnogości dla zaocznych studentów informatyki (kurs licencjacki). Jej celem jest przedstawienie elementów obu tych dziedzin, które są niezbędne w dalszym studium informatyki i które stanowią nieodzowny fundament wykształcenia każdego matematyka i informatyka.

Książka składa się z dwóch części. Część pierwszą stanowią rozdziały 1–4 poświęcone wykładowi elementów rachunku zdań i rachunku predykatów oraz funkcjom logicznym i aksjomatycznemu ujęciu logiki klasycznej. Druga część książki, tzn. rozdziały 5–9, poświęcona jest wykładowi tzw. naiwnej teorii mnogości, czyli teorii mnogości w ujęciu nieaksjomatycznym. Omawiamy tu po kolei pojęcie zbioru, algebrę zbiorów, relacje, w tym relacje równoważności, relacje częściowo porządkujące i relacje dobrze porządkujące, dalej funkcje, a wreszcie zagadnienia związane z teorią mocy (a więc pojęcie równoliczności, zbiory przeliczalne i nieprzeliczalne, liczby kardynalne). Do książki dołączono dodatek zawierający uwagi historyczne o rozwoju logiki i teorii mnogości. Na końcu poszczególnych rozdziałów podano zadania mające pomóc w przyswojeniu sobie studiowanego materiału. Nie mają one oczywiście zastąpić zbiorów zadań z logiki i teorii mnogości, korzystanie z których jest niezbędne, by dobrze opanować odpowiednie zagadnienia.

Definicje i twierdzenia posiadają potrójną numerację: pierwsza liczba oznacza numer rozdziału, druga — numer paragrafu w ramach danego rozdziału, a trzecia — numer bieżącej definicji czy twierdzenia w ramach danego paragrafu. Tak więc na przykład „definicja 7.3.4” oznacza definicję 4 umieszczoną w paragrafie 3 rozdziału 7. Koniec dowodu oznaczamy literami Q.E.D. (będącymi skrótem łacińskiego *quod erat demonstrandum* — czego należało dowieść).

Autorstwo poszczególnych rozdziałów jest następujące: R. Murawski napisał rozdział 2 oraz rozdziały 5–9 (bez paragrafów 8.1 i 8.2), K. Świrydowicz zaś rozdziały 1, 3, 4 i paragrafy 8.1 i 8.2 oraz przygotował zadania. Obaj autorzy wspólnie napisali Dodatek. Rysunki i diagramy, które zamieszczono w książce wykonała Pani dr Izabela Bondecka-Krykowska, której w tym miejscu serdecznie dziękujemy. Dziękujemy też Panu drowi Michałowi Kozakowi, który pomagał nam w przygotowaniu wersji *camera ready* tekstu.

Książkę tę pragniemy zadedykować Pani Doktor habilitowanej Beacie Begier-Krasińskiej ze Szpitala Klinicznego „Przemienienia Pańskiego” Uniwersytetu Medycznego im. Karola Marcinkowskiego w Poznaniu z wyrazami wdzięczności za opiekę.

Roman Murawski
Kazimierz Świrydowicz

Poznań, w maju 2016

Rozdział 1

Elementy klasycznego rachunku zdań

1.1. Wprowadzenie

Język nauki składa się ze zdań. W logice zdanie rozumie się jako wyrażenie, które coś stwierdza. Za zdania w sensie logicznym uważa się takie wyrażenia oznajmujące, które są na tyle jednoznaczne, by móc o nich orzekać, że są prawdziwe albo fałszywe. Tak więc za zdania uznamy nie tylko wyrażenia, takie jak „ $2 + 2 = 4$ ”, ale i „ciąg ten jest monotoniczny”, gdy wiadomo, o jakim ciągu mowa. Za zdania w logice nie są uznawane więc ani zdania pytające („Byłże on prawdziwym prorokiem, czy też był tylko zwyczajnie nawiedzony?”), rozkazujące („Pasażerom LOT-u zabrania się wysiadać z samolotów w czasie lotu!”), ani też wypowiedzi oznajmujące mętne czy niedostatecznie sprecyzowane, o których przez to nie można orzec, czy są prawdziwe, czy też fałszywe („Prawdziwe piękno polega na jedności w wielości”). Od tego miejsca, mówiąc o zdaniach, mamy na myśli wyłącznie zdania w sensie logicznym.

Prawdziwość i fałszywość nazywamy wartościami logicznymi. W logice klasycznej, a tylko taką logiką będziemy się tu zajmować, uważa się, że istnieją tylko te dwie wartości logiczne. W logikach wielowartościowych i innych logikach nieklasycznych¹ dopuszcza się więcej wartości logicznych.

¹ Współczesne badania logik wielowartościowych zostały zainaugurowane w 1920 roku przez polskiego logika Jana Łukasiewicza (1878–1956) i przez amerykańskiego logika Emila Posta (1897–1954; nb. urodzonego w Augustowie); logiki takie są próbą formalnego, matematycznego scharakteryzowania fenomenu wielowartościowości. Por. G. Malinowski, *Logiki wielowartościowe*, Państwowe Wydawnictwo Naukowe, Warszawa 1990. Inne logiki nieklasyczne są także faktycznie wielowartościowe, por. np. K. Świrydowicz, *Podstawy logiki modalnej*, Wydawnictwo Naukowe UAM, Poznań 2004. Doniosłość badań nad tymi logikami bierze się także stąd, że znajdują one dziś zastosowanie w informatyce.

Obok zdań w klasycznej logice rozważa się także tak zwane funkcje zdaniowe. Funkcją zdaniową nazywamy takie wyrażenie oznajmujące, które zawiera zmienne, a staje się zdaniem, gdy dokona się w nim podstawień za wszystkie występujące w nim zmienne lub skwantyfikuje się te zmienne. Funkcjami logicznymi będą więc wyrażenia takie, jak „ x jest miastem wojewódzkim”, „ a jest starszym bratem geniusza” czy „ $x \leq y$ ”. Funkcje zdaniowe nie są więc zdaniami; z podanych przykładowo funkcji można otrzymać na przykład zdania: „Kraków jest miastem wojewódzkim”, „Kutno jest miastem wojewódzkim” czy „dla każdej liczby x istnieje taka liczba y , że $x \leq y$ ”.

Wśród zdań wyróżniamy zdania proste, które nie zawierają części będącej osobnym zdaniem, i zdania złożone, zawierające części będące zdaniami. Tak więc zgodnie z tą definicją złożone jest nie tylko zdanie „2 jest liczbą pierwszą, a 4 nie jest liczbą pierwszą”, ale i zdanie „Zaiste, człowiek jest stworzeniem rozumnym”, ponieważ zawiera część, będącą osobnym zdaniem („człowiek jest stworzeniem rozumnym”).

Zdania złożone buduje się ze zdań prostych przez łączenie ich spójnikami. Spośród licznych spójników międzyzdaniowych mowy potocznej logikę interesuje tylko pewien ich podzbiór. Przedmiotem zainteresowania logiki są zasadniczo następujące spójniki dwuargumentowe:

*i (oraz, a, a ponadto),
lub (względnie, bądź),
jeżeli ..., to ...
wtedy i tylko wtedy, gdy (zawsze i tylko, gdy)*

oraz spójnik jednoargumentowy

nie jest tak, że.

Spójniki mowy potocznej wymienione w jednym wierszu uważane są za praktycznie jednoznaczne. Zamiast „nie jest tak, że” używa się często spójnika „nieprawda, że”, choć ściśle biorąc, zaprzecza on nie tyle treści zdania, co jego wartości logicznej.

Język logiki jest językiem sztucznym, powstałym z uproszczenia mowy potocznej. Jego składnikami są zdaniowe symbole elementarne (oznaczane przez p, q, r, p_1 itd.) oraz spójniki dwuargumentowe: koniunkcji \wedge , alternatywy \vee , równoważności \leftrightarrow i implikacji \rightarrow oraz jednoargumentowy spójnik negacji \neg . Sens tych spójników wyznaczany jest przez następujące tabelki, w których symbol 1 reprezentuje „zdanie prawdziwe”, a 0 „zdanie fałszywe”:

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

Sens spójnika negacji określa następująca tabelka:

p	$\neg p$
1	0
0	1

Ustalona w logice terminologia nakazuje pierwszy człon zdania będącego implikacją nazywać poprzednikiem tej implikacji, a drugi człon – jej następnikiem. Mówi się też o składnikach alternatywy i o czynnikach koniunkcji. Terminologia logiczna nakazuje ponadto nazywać koniunkcją, alternatywą, itd. zdanie, w którym głównym spójnikiem jest spójnik koniunkcji, alternatywy itd. Gdy nie ma obawy nieporozumienia, nazw: „implikacja”, „alternatywa” itd. używa się też często w odniesieniu do spójników logicznych; w niniejszym podręczniku również będziemy używać niekiedy tych samych nazw w odniesieniu i do spójników, i do zdań złożonych.

Związek pomiędzy językiem logiki a mową potoczną czy jej fragmentem (językiem matematyki) ustala się następująco:

- spójnik koniunkcji \wedge wiąże się ze słowem „i” („oraz”, „a”, „a ponadto”),
- spójnik alternatywy \vee z „lub” („względnie”, „bądź”),
- spójnik równoważności \leftrightarrow z „wtedy i tylko wtedy, gdy” („zawsze i tylko gdy”),
- spójnik implikacji \rightarrow z „jeżeli... to...”,
- spójnik negacji \neg z „nie jest tak, że” („nieprawda, że”)².

² Do zapisu spójników logicznych używa się innych jeszcze symboli:

Negacja	Koniunkcja	Alternatywa	Implikacja	Równoważność
$\neg\phi$	$\phi \cap \psi$	$\phi \cup \psi$	$\phi \Rightarrow \psi$	$\phi \Leftrightarrow \psi$
ϕ	$\phi \& \psi$	$\phi \vee \psi$	$\phi \rightarrow \psi$	$\phi \sim \psi$
$N\phi$	$K\phi\psi$	$A\phi\psi$	$C\phi\psi$	$E\phi\psi$
$\sim\phi$	$\phi \cdot \psi$	$\phi \vee \psi$	$\phi \supset \psi$	$\phi \equiv \psi$
ϕ'	$\phi \cdot \psi$	$\phi + \psi$	$\phi \rightarrow \psi$	$\phi \equiv \psi$

Symbolika z pierwszego wiersza używana jest przede wszystkim przez matematyków związanych z teorią krat i algebraami Boole’a. Druga używana była przez Davida Hilberta. Trzecia to symbolika beznawiasowa, czyli symbolika polska, pochodząca od polskiego logika Jana Łukasiewicza. Czwarta symbolika pochodzi od Bertanda Russella i Giu-

Trzeba jednak zdecydowanie podkreślić, że język logiki jest uproszczeniem, a nie formalną rekonstrukcją fragmentu mowy potocznej. Jest to konsekwencja następujących faktów.

Po pierwsze, spójniki mowy potocznej nakładają ograniczenia na możliwe połączenia zdań. Na przykład, o ile koniunkcja dwóch zdań prawdziwych powinna być zdaniem prawdziwym, to zawahamy się przed uznaniem za prawdziwe następującego zdania: „trawa jest zielona i pierwiastek kwadratowy z 2 jest liczbą niewymierną”. Podobnie, jakkolwiek implikacja o fałszywym poprzedniku zawsze jest prawdziwa, wątpliwe jednak jest, czy za prawdziwe uznać zdanie: „jeśli $2+2 = 5$, to Warszawa jest stolicą Polski”. Spójniki mowy potocznej wymagają bowiem jakiegoś związku treściowego pomiędzy łączonymi przez nie zdaniami.

Po drugie, spójniki mowy potocznej nadają niekiedy dodatkowy sens zdaniu złożonemu. I tak na przykład w języku logiki koniunkcja jest przemienne: dla ustalenia wartości logicznej kolejność zdań łączych spójnikiem koniunkcji jest obojętna. Tymczasem w języku potocznym słowo „i” wskazuje często kolejność czasową i nie zawsze wolno zmieniać kolejność jego argumentów bez zmiany sensu zdania. Co innego, dajmy na to, zakochać się i się ożenić, a co innego ożenić się i się zakochać. Podobnie, co innego ożenić się i mieć dzieci, a co innego mieć dzieci i się ożenić. W obu tych przypadkach zmiana kolejności zdań może spowodować, że zdanie z prawdziwego zmieni się w fałszywe. Tym dodatkowym sensem w przypadku spójnika „jeżeli... to...” jest okoliczność, że w mowie potocznej jest on używany dla zaznaczenia, że między argumentami tego spójnika zachodzi **w y n i k a n i e**.

W logice mówi się, że spójniki logiczne są **e k s t e n s j o n a l n e**, to znaczy wartość logiczna zdania złożonego jest jednoznacznie wyznaczona przez wartość logiczną jego argumentów, a spójniki mowy potocznej są **i n t e n s j o n a l n e**, to znaczy na wartość logiczną zdania złożonego z mowy potocznej mają wpływ nie tylko występujące w nim spójniki, ale także treść łączych przez nie zdań.

Nie należy więc utożsamiać spójników mowy potocznej z odpowiednimi spójnikami logicznymi. Łatwo jednak zauważyć, że gdy przechodzimy od mowy potocznej czy języka matematyki do języka logiki, to zwykle związki między prawdziwością czy fałszywością argumentów spójnika „i”

seppe Peana. Ostatnia wreszcie to symbolika Ernsta Schrödera i Charlesa Peirce'a. Por. R. Murawski, *Rozwój symboliki logicznej*, Wydawnictwo Naukowe UAM, Poznań 1988.

będą takie same jak między członami koniunkcji, i podobnie dla pozostałych spójników.

Uwzględniając powyższe uwagi i zastrzeżenia, będziemy na ogół traktować spójniki logiczne tak, jakby to były spójniki międzyzdaniowe mowy potocznej.

DEFINICJA 1.1.1. Schematem zdania wyrażonym w języku rachunku zdań nazywamy formułę powstającą ze zdania przez konsekwentne zastąpienie zdań prostych zmiennymi zdaniowymi, a spójników międzyzdaniowych — odpowiednimi spójnikami logicznymi.

„Konsekwentne zastąpienie” oznacza, że te same zdania proste zastępuje się tymi samymi zmiennymi zdaniowymi, a różne zdania proste — różnymi zmiennymi.

Na przykład schematem zdania: „Jestem matematykiem lub nie jestem matematykiem” jest formuła $p \vee \neg p$, a schematem zdania: „Jeśli ktoś kradnie drewno w lesie lub poluje na zwierzynę łowną w okresie ochronnym, to podlega karze” będzie formuła $(p \vee q) \rightarrow r$.

Na koniec uściślimy pojęcie sprzeczności.

DEFINICJA 1.1.2. Para zdań jest parą zdań sprzecznych, jeśli jedno z nich jest negacją drugiego lub jest logicznie równoważne negacji drugiego.

Tak więc parą zdań sprzecznych³ jest w szczególności każda para postaci p i $\neg p$.

1.2. Język rachunku zdań; tautologie

Język rachunku zdań omówiliśmy wstępnie w poprzednim paragrafie; teraz podamy precyzyjną definicję.

DEFINICJA 1.2.1. Następujące znaki nazywamy znakami języka rachunku zdań:

$$p_1, p_2, p_3, \dots$$

$$\neg, \wedge, \vee, \leftrightarrow, \rightarrow$$

$$), ($$

³ Nie każda para zdań, z których każde jest w logicznym konflikcie z drugim, to para zdań sprzecznych, na przykład zdaniami sprzecznymi nie są: „Każdy człowiek pali papierosy” i „Żaden człowiek nie pali papierosów”. Podane tu przykładowo zdania nazywamy przeciwnymi; choć nigdy nie są one jednocześnie prawdziwe, to bywają jednak jednocześnie fałszywe.

Znaki wymienione w pierwszym wierszu to zmienne zdaniowe, w drugim – spójniki logiczne, w trzecim – nawiasy⁴. Dla uproszczenia zamiast p_1 będziemy pisać niekiedy po prostu p , zamiast $p_2 - q$, zamiast $p_3 - r$, a zamiast $p_4 - s$.

Nie każdy ciąg znaków języka rachunku zdań jest poprawnie („gramatycznie”) zbudowaną formułą. Zdefiniujemy teraz pojęcie poprawnie zbudowanej formuły zdaniowej języka rachunku zdań. Formuły poprawnie zbudowane będziemy nazywać po prostu formułami.

DEFINICJA 1.2.2. (i) *Każda zmienna zdaniowa jest formułą języka rachunku zdań.*

(ii) *Jeśli ϕ , ψ są formułami języka rachunku zdań, to napisy $\neg(\phi)$, $(\phi) \wedge (\psi)$, $(\phi) \vee (\psi)$, $(\phi) \leftrightarrow (\psi)$ i $(\phi) \rightarrow (\psi)$ są formułami języka rachunku zdań.*

(iii) *Nie ma innych formuł języka rachunku zdań poza zmiennymi zdaniowymi i takimi formułami, które powstają dzięki zastosowaniu reguły (ii).*

Aby ułatwić rozważania, obok zmiennych zdaniowych użyliśmy tu liter ϕ i ψ ; litery te (i ewentualnie χ , $\phi_1, \psi_1, \chi_1 \dots$) będą dalej reprezentować dowolne formuły języka rachunku zdań.

Powyższa definicja to przykład definicji indukcyjnej przez indukcję strukturalną: w definicji takiej podaje się listę obiektów elementarnych oraz reguły tworzenia z nich obiektów bardziej złożonych, zastrzegając, że wszelki obiekt definiowanego zbioru musi być albo elementarny, albo uzyskany z obiektów elementarnych przez zastosowanie podanych reguł.

Dla wygody przyjmuje się pewne konwencje dotyczące używania nawiasów. W szczególności:

- pojedynczej zmiennej nie bierze się w nawiasy,
- nie dodaje się nawiasu, gdy umieszcza się znak negacji przed formułą już poprzedzoną znakiem negacji (tak więc zamiast $\neg(\neg(\phi))$ pisze się $\neg\neg(\phi)$),
- nie dodaje się nowego nawiasu, dodając nowy człon alternatywy do formuły będącej alternatywą i nowy składnik koniunkcji do formuły, która jest koniunkcją; tak więc np. pisze się $(\phi) \wedge (\psi) \wedge (\chi)$ zamiast $((\phi) \wedge (\psi)) \wedge (\chi)$ i zamiast $(\phi) \wedge ((\psi) \wedge (\chi))$ ⁵.

⁴ Nawiasy nie są konieczne dla zapisu formuł rachunku zdań; o symbolice beznawiasowej będzie mowa niżej – por. paragraf 1.6.

⁵ Por. listę tautologii podaną w paragrafie 1.4; na opuszczanie nawiasów pozwalają prawa łączności dla alternatywy i koniunkcji.

Przyjmujemy, że, wzorem arytmetyki, najsilniej wiąże znak \neg , potem znaki \wedge i \vee , a następnie znaki \rightarrow i \leftrightarrow . Tak więc zamiast np. $(p \vee q) \rightarrow (r \wedge s)$ wolno pisać $p \vee q \rightarrow r \wedge s$.

Warto zauważyć, że każda formuła rachunku zdań może być potraktowana jako schemat zdania, a ściśle biorąc, nawet nie jednego zdania, lecz całej klasy zdań. Niektóre z takich zdań są prawdziwe z uwagi na swą budowę, jak to na przykład zachodzi w przypadku zdań: „Jeśli piękno polega na proporcji części, to polega na proporcji części”, „ciąg a_n jest monotoniczny lub nie jest monotoniczny”, „nieprawda, że zarazem wątpię i nie wątpię”. Prowadzi nas to do pojęcia tautologii.

DEFINICJA 1.2.3. Tautologią rachunku zdań albo prawem logicznym rachunku zdań jest formuła języka rachunku zdań, która przy dowolnej interpretacji zmiennych zdaniowych zmienia się w zdanie prawdziwe.

Przykładami tautologii są formuły $p \rightarrow p$, $p \vee \neg p$ czy $\neg(p \wedge \neg p)$; formuły te odpowiadają podanym wyżej przykładom.

Aby sprawdzić, czy jakaś formuła jest tautologią, nie wystarczy dokonywać kolejnych podstawień za zmienne – dla każdej formuły przykładów podstawień jest bowiem nieskończenie wiele. Wystarczy jednak spostrzec, że każda zmienna zdaniowa występująca w formule zdaniowej może uzyskać albo wartość 0, albo wartość 1, a wartość całej formuły jest jednoznacznie wyznaczona przez wartości przypisane zmiennym. Uwaga ta stanowi podstawę dla tak zwanej metody zero-jedynkowej rozstrzygania, czy dana formuła jest tautologią.

Rozpatrzmy mianowicie – dla zilustrowania metody – formułę

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

Ponieważ ma ona dwie zmienne, wystarczy sprawdzić, czy będzie prawdziwa w następujących czterech przypadkach: gdy obie zmienne uzyskują wartość 1, pierwsza ma wartość 1, druga 0, pierwsza ma wartość 0, a druga 1 oraz gdy obie mają wartość 0, to jest, gdy obie zmienne reprezentują zdanie prawdziwe, pierwsza reprezentuje zdanie prawdziwe, a druga fałszywe itd. Wyniki analizy tych przypadków zapiszemy skrótowo w następującej tabelce:

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

Ponieważ rozważana formuła uzyskuje tylko wartość 1 (patrz: ostatnia kolumna), więc jest ona tautologią. A oto drugi przykład:

$$(p \rightarrow q) \rightarrow (\neg p \rightarrow \neg q).$$

Wyniki analizy ujmijemy w następującej tabelce:

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

Formuła ta nie jest tautologią, ponieważ jeśli zmienna p uzyska wartość 0, a q wartość 1, to formuła ta uzyska wartość 0 (patrz: trzeci wiersz tabelki).

Inne przykłady znajdzie Czytelnik poniżej. Warto zauważyć, że jeśli liczba różnych zmiennych w formule wynosi n , to liczba przypadków, które należy zbadać, by sprawdzić, czy formuła jest tautologią, wynosi 2^n .

Kwestia, czy dana formuła jest tautologią rachunku zdań, jest rozstrzygalna. Istnieje bowiem, jak widać, algorytm pozwalający w każdym przypadku, po wykonaniu skończonej liczby kroków, odpowiedzieć na pytanie o tautologiczność dowolnej formuły rachunku zdań.

1.3. Schematy wnioskowań. Wnioskowania niezawodne

Podstawowym zadaniem logiki jest odróżnianie wnioskowań niezawodnych, to jest takich, w których prawdziwość przesłanek przesądza o prawdziwości wniosku, od wnioskowań zawodnych, czyli takich, gdzie prawdziwość przesłanek nie gwarantuje prawdziwości wniosku: przesłanki mogą być prawdziwe, a wniosek fałszywy. W dowodach matematycznych występują wyłącznie wnioskowania niezawodne, i jest to jedna z podstawowych własności odróżniających matematykę od innych nauk⁶.

⁶ W innych dziedzinach nauki, jak też i w życiu codziennym, używa się często wnioskowań zawodnych, jak redukcja, indukcja niepełna czy analogia (por. elementarne podręczniki logiki, np. Z. Ziemiński, *Logika praktyczna*, Wydawnictwo Naukowe PWN, Warszawa 2001). Wnioski w tych rozumowaniach bywają fałszywe przy prawdziwych przesłankach, ale gdy wnioski takie są prawdziwe, w sposób istotny wzbogacają wiedzę, bo wychodzą poza informacje zawarte w przesłankach. Niektóre rodzaje wnioskowań zawodnych są ostatnio intensywnie badane przez logikę w związku z coraz szerszymi

Logika daje narzędzia do kontroli niezawodności wnioskowań; właśnie kontroli niezawodności wnioskowań będzie poświęcony niniejszy paragraf.

DEFINICJA 1.3.1. Schematem wnioskowania *wyrażonym w języku rachunku zdań* jest para uporządkowana $\langle X, \phi \rangle$, gdzie X jest zbiorem formuł rachunku zdań, a ϕ jest formułą.

Jeśli zbiór X jest skończony i składa się z formuł $\phi_1, \phi_2, \dots, \phi_n$, to schemat wnioskowania można zapisać jako $\langle \{\phi_1, \dots, \phi_n\}, \phi \rangle$; przyjęto jednak konwencję

$$\frac{\phi_1, \phi_2, \dots, \phi_n}{\phi},$$

a częściej jeszcze używa się zapisu

$$\begin{array}{c} \phi_1 \\ \phi_2 \\ \dots \\ \phi_n \\ \hline \phi \end{array}.$$

Formuły ϕ_1, \dots, ϕ_n nazywa się schematami przesłanek, a formułę ϕ – schematem wniosku.

DEFINICJA 1.3.2. *Schemat*

$$\frac{\phi_1, \dots, \phi_n}{\phi}$$

jest niezawodny wtedy i tylko wtedy, gdy formuła

$$[(\phi_1) \wedge \dots \wedge (\phi_n)] \rightarrow \phi$$

jest tautologią. Niezawodne schematy wnioskowania nazywa się także regułami logicznymi.

Definicja ta dotyczy wszelkich wnioskowań, nie tylko występujących w matematyce.

Rozważmy przykład, który pochodzi jeszcze ze starożytności:

Jeśli wiesz, że umarłeś, to umarłeś.

Jeśli wiesz, że umarłeś, to nie umarłeś.

Zatem: nie wiesz, że umarłeś.

możliwościami implementacji w komputerach, np. do wyprowadzania konsekwencji z danych. Por. np. P. Cichosz, *Systemy uczące się*, Wydawnictwo Naukowo-Techniczne, Warszawa 2000.

Aby zbadać, czy wnioskowanie to jest niezawodne, wystarczy stwierdzić, czy przebiega ono wedle niezawodnego schematu wnioskowania. Należy więc znaleźć schemat tego wnioskowania. Znalezienie schematu wnioskowania polega z kolei na znalezieniu odpowiednio schematów przesłanek i wniosku (tu przypominamy pojęcie schematu zdania wyrażonego w języku rachunku zdań). W efekcie ustalamy, że schemat rozważanego wnioskowania będzie następujący:

$$\frac{p \rightarrow q \quad (\phi_1) \quad p \rightarrow \neg q \quad (\phi_2)}{\neg p} \quad (\phi)$$

Należy teraz zbadać, czy schemat ten jest schematem niezawodnym, to jest sprawdzić, czy formuła

$$[(\phi_1) \wedge (\phi_2)] \rightarrow (\phi),$$

czyli formuła

$$[(p \rightarrow q) \wedge (p \rightarrow \neg q)] \rightarrow \neg p$$

jest tautologią.

W tym celu stosujemy metodę zero-jedynkową, uzyskując w efekcie jej zastosowania następującą tabelkę:

p	q	$p \rightarrow q$	$\neg q$	$p \rightarrow \neg q$	$(p \rightarrow q) \wedge (p \rightarrow \neg q)$	$\neg p$	$[(p \rightarrow q) \wedge (p \rightarrow \neg q)] \rightarrow \neg p$
1	1	1	0	0	0	0	1
1	0	0	1	1	0	0	1
0	1	1	0	1	1	1	1
0	0	1	1	1	1	1	1

Tak więc badana formuła okazała się tautologią, wobec czego odpowiadający jej schemat jest schematem niezawodnym, przeto badane wnioskowanie jest niezawodne.

DEFINICJA 1.3.3. Ze zdań o schematach $\phi_1, \phi_2, \dots, \phi_n$ wynika logicznie (semantycznie) zdanie o schemacie ϕ wtedy i tylko wtedy, gdy formuła

$$[(\phi_1) \wedge \dots \wedge (\phi_n)] \rightarrow (\phi)$$

jest tautologią. Dedukcją nazywa się wnioskowanie, w którym z przesłanek wynika logicznie wniosek.

Jeśli ϕ wynika logicznie z ϕ_1, \dots, ϕ_n , to mówi się, że ϕ jest logiczną konsekwencją ϕ_1, \dots, ϕ_n .

Czytelnik zechce sprawdzić prawdziwość następującego lematu:

LEMAT 1.3.4. *Jeśli schemat wnioskowania*

$$\frac{\phi_1, \dots, \phi_n}{\phi}$$

jest niezawodny, a formuły ϕ_1, \dots, ϕ_n uzyskują wartość 1, to formuła ϕ też uzyskuje wartość 1.

Konsekwencją tego lematu jest stwierdzenie, że jeśli wnioskowanie przebiega wedle schematu, który jest niezawodny, a przesłanki tego wnioskowania są prawdziwe, to wniosek też będzie prawdziwy, czyli krótko: wnioskowanie, przebiegające wedle schematu niezawodnego, jest wnioskowaniem niezawodnym.

Zdarzyć się jednak może, iż wniosek wnioskowania niezawodnego będzie fałszywy. Ponieważ schematowi tego wnioskowania odpowiada implikacja będąca tautologią, a następnik tej implikacji będzie fałszywy, więc poprzednik będzie też fałszywy. Krótko: fałszywość wniosku przesądza tu o fałszywości przesłanek. Można się o tym przekonać, analizując po prostu tabelkę charakteryzującą implikację.

Zbadamy teraz, czy to nasze rozumowanie, dotyczące fałszywości wniosku wnioskowania niezawodnego samo jest niezawodne. Rozumowanie, które właśnie przeprowadziliśmy, można zapisać następująco:

Jeśli wnioskowanie przebiega wedle schematu niezawodnego,
a przesłanki są prawdziwe,
to wniosek jest prawdziwy.

Zatem: jeśli wnioskowanie przebiega wedle schematu niezawodnego,
a wniosek nie jest prawdziwy,
to przesłanki nie są prawdziwe.

Spytajmy więc, czy zapisane właśnie wnioskowanie samo przebiega wedle schematu niezawodnego.

Schemat tego wnioskowania ma postać

$$\frac{p \wedge q \rightarrow r \quad (\phi_1)}{p \wedge \neg r \rightarrow \neg q \quad (\phi)}$$

Aby stwierdzić, czy schemat ten jest niezawodny, należy sprawdzić, czy tautologią jest implikacja $(\phi_1) \rightarrow (\phi)$, to znaczy implikacja

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

Mamy więc

p	q	r	$p \wedge q$	$p \wedge q \rightarrow r$	$\neg r$	$p \wedge \neg r$	$\neg q$	$p \wedge \neg r \rightarrow \neg q$	$(\phi_1) \rightarrow (\phi)$
1	1	1	1	1	0	0	0	1	1
1	1	0	1	0	1	1	0	0	1
1	0	1	0	1	0	0	1	1	1
1	0	0	0	1	1	1	1	1	1
0	1	1	0	1	0	0	0	1	1
0	1	0	0	1	1	0	0	1	1
0	0	1	0	1	0	0	1	1	1
0	0	0	0	1	1	0	1	1	1

Jest to zatem wnioskowanie niezawodne, dotyczące wnioskowań zgodnych z regułami logicznymi. Inne przykłady Czytelnik znajdzie w zadaniach do tego rozdziału.

1.4. Tautologie rachunku zdań

TWIERDZENIE 1.4.1. *Następujące formuły są tautologiami rachunku zdań:*

$p \rightarrow p$	prawo tożsamości
$p \vee \neg p$	prawo wyłączonego środka, <i>tertium non datur</i> , zwane też prawem wyłączonego trzeciego
$\neg(p \wedge \neg p)$	prawo sprzeczności
$\neg\neg p \leftrightarrow p$	prawo podwójnej negacji ⁷
$(p \rightarrow \neg p) \rightarrow \neg p$	prawo Claviusa ⁸
$(\neg p \rightarrow p) \rightarrow p$	druga wersja prawa Claviusa
$p \wedge \neg p \rightarrow q$	prawo Dunsza Szkota (Dunsa Scotusa) ⁹
$p \rightarrow (\neg p \rightarrow q)$	druga wersja prawa Dunsza Szkota
$((p \rightarrow q) \wedge p) \rightarrow q$	<i>modus ponendo ponens</i> , czyli tryb przez stwierdzenie stwierdzający
$((p \rightarrow q) \wedge \neg q) \rightarrow \neg p$	<i>modus tollendo tollens</i> , czyli tryb przez zaprzeczenie zaprzeczający

⁷ Te cztery prawa były w filozofii znane od dawna; mają one swoją interpretację metafizyczną. W szczególności zasady odpowiadające prawom: wyłączonego środka i sprzeczności są w metafizyce tomistycznej uznawane za naczelne zasady bytu i są znane jako *principium tertii exclusii* i *principium contradictionis*.

⁸ Christofor Clavius (1537–1612), jezuita, logik i matematyk, twórca kalendarza gregoriańskiego; prawo to zwane jest też *dictum mirabilis*.

⁹ Bł. Jan Duns Szkot (1266–1308), franciszkanin, teolog i filozof, z uwagi na subtelność wywodów zwany *doctor subtilis*.

$((p \vee q) \wedge \neg p) \rightarrow q$	<i>modus tollendo ponens</i> , czyli tryb przez zaprzeczenie stwierdzający
$(\neg(p \wedge q) \wedge p) \rightarrow \neg q$	<i>modus ponendo tollens</i> , czyli tryb przez stwierdzenie zaprzeczający
$(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$	prawo transpozycji
$\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$	pierwsze prawo De Morgana ¹⁰
$\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$	drugie prawo De Morgana
$(p \rightarrow q) \leftrightarrow (\neg p \vee q)$	definicja implikacji za pomocą alternatywy i negacji
$(p \rightarrow q) \leftrightarrow \neg(p \wedge \neg q)$	definicja implikacji za pomocą koniunkcji i negacji
$\neg(p \rightarrow q) \leftrightarrow (p \wedge \neg q)$	prawo negowania implikacji
$(p \leftrightarrow q) \leftrightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]$	prawo przekształcania równoważności na implikacje
$\neg(p \leftrightarrow q) \leftrightarrow (p \wedge \neg q) \vee (q \wedge \neg p)$	prawo negowania równoważności
$p \wedge q \rightarrow p$	prawo symplifikacji
$p \wedge q \rightarrow q$	prawo symplifikacji
$p \rightarrow p \vee q$	prawo addycji
$q \rightarrow p \vee q$	prawo addycji
$(p \wedge q) \leftrightarrow (q \wedge p)$	prawo przemienności koniunkcji
$(p \vee q) \leftrightarrow (q \vee p)$	prawo przemienności alternatywy
$(p \wedge (q \wedge r)) \leftrightarrow ((p \wedge q) \wedge r)$	prawo łączności koniunkcji
$(p \vee (q \vee r)) \leftrightarrow ((p \vee q) \vee r)$	prawo łączności alternatywy
$p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$	prawo rozdzielności alternatywy względem koniunkcji
$p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$	prawo rozdzielności koniunkcji względem alternatywy
$(p \rightarrow q) \rightarrow ((q \rightarrow r) \rightarrow (p \rightarrow r))$	prawo sylogizmu hipotetycznego bezkoniunkcyjnego
$(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$	prawo sylogizmu hipotetycznego koniunkcyjnego
$(p \leftrightarrow q) \wedge (q \leftrightarrow r) \rightarrow (p \leftrightarrow r)$	sylogizm hipotetyczny koniunkcyjny dla równoważności
$(p \wedge q \rightarrow r) \rightarrow (p \wedge \neg r \rightarrow \neg q)$	prawo transpozycji złożonej
$((p \wedge q) \rightarrow r) \rightarrow (p \rightarrow (q \rightarrow r))$	prawo eksportacji
$(p \rightarrow (q \rightarrow r)) \rightarrow ((p \wedge q) \rightarrow r)$	prawo importacji
$((p \wedge q) \rightarrow r) \leftrightarrow (p \rightarrow (q \rightarrow r))$	prawo eksportacji–importacji

¹⁰ Augustus De Morgan (1806–1871), matematyk angielski, profesor Uniwersytetu Londyńskiego.

Praw logicznych jest nieskończenie wiele, także z tego powodu, że każda z podanych formuł może być potraktowana jako schemat dla nieskończenie wielu praw. Na przykład $p \rightarrow p$ może reprezentować wszystkie formuły postaci $(\phi) \rightarrow (\phi)$, więc np. $((q \rightarrow p) \rightarrow p) \rightarrow ((q \rightarrow p) \rightarrow p)$, $p \wedge q \rightarrow p \wedge q$ itd. Są też prawa, używane w rozumowaniach matematycznych, nie mające ustalonych nazw, na przykład prawo

$$[(p \rightarrow q) \wedge (q \rightarrow r) \wedge (r \rightarrow p)] \rightarrow [(p \leftrightarrow q) \wedge (p \leftrightarrow r) \wedge (q \leftrightarrow r)]$$

czy prawo

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

Obok opisanej wyżej, tzw. zero-jedynkowej metody rozstrzygnięcia o tautologiczności formuł istnieją inne jeszcze metody. Opis tak zwanej skróconej metody zero-jedynkowej znajdzie Czytelnik na stronie internetowej www.logika.amu.edu.pl/dydaktyka. Tautologiczność formuły można także ustalać, sprowadzając formułę do tzw. postaci normalnej; sposób sprowadzania formuły do takiej postaci znajdzie Czytelnik na tej samej stronie internetowej.

Znaczna większość podanych wyżej praw logicznych to prawa o postaci implikacji, ewentualnie równoważności; służą one do uzasadniania niezawodności wnioskowań. Zgodnie bowiem z definicją niezawodnego schematu wnioskowania, każdemu z tych praw odpowiada schemat wnioskowania niezawodnego. Schemat taki nazywany jest też często regułą wnioskowania niezawodnego lub – gdy z kontekstu wiadomo, że chodzi o wnioskowanie niezawodne – po prostu regułą wnioskowania.

DEFINICJA 1.4.2. Regułą odrywania nazywamy regułę postaci

$$\frac{\phi \rightarrow \psi \quad \phi}{\psi}.$$

Reguła ta odpowiada prawu *modus ponendo ponens* i jest najczęściej spotykaną w logice regułą, używaną także w aksjomatyzacjach logiki¹¹.

Na koniec kilka uwag dotyczących równoważności.

DEFINICJA 1.4.3. Formułę ϕ nazwiemy logicznie równoważną formule ψ wtedy i tylko wtedy, gdy formuła $(\phi) \leftrightarrow (\psi)$ jest tautologią.

¹¹ W angielskojęzycznej literaturze zwana jest po prostu *Modus Ponens* i oznaczana symbolem *MP*.

Tak więc p jest logicznie równoważne $\neg\neg p$, a $\phi \wedge (\psi \vee \chi)$ jest logicznie równoważne $(\phi \wedge \psi) \vee (\phi \wedge \chi)$.

Łatwy w dowodzie jest następujący lemat:

LEMAT 1.4.4. *Jeśli $\phi \leftrightarrow \psi$ jest tautologią i ϕ jest tautologią, to ψ jest także tautologią.*

Można też pokazać, że dowolne dwie tautologie klasycznego rachunku zdań są logicznie równoważne.

1.5. Warunek dostateczny i konieczny

W formułowaniu twierdzeń i dowodów używa się często w matematyce pojęcia warunku dostatecznego (wystarczającego) i koniecznego.

DEFINICJA 1.5.1. *Niech prawdziwe będzie zdanie warunkowe „jeśli p , to q ”. Wówczas to o czym mówi p , jest warunkiem wystarczającym dla tego, o czym mówi q , a to o czym mówi q , jest warunkiem koniecznym dla tego, o czym mówi p . Mówi się wtedy skrótowo, że p jest warunkiem dostatecznym dla q , a q jest warunkiem koniecznym¹² dla p .*

Tak więc, ponieważ prawdziwe jest zdanie warunkowe „jeśli n jest podzielne przez 9, to n jest podzielne przez 3”, więc podzielność przez 9 jest warunkiem wystarczającym dla podzielności przez 3, a podzielność przez 3 jest warunkiem koniecznym dla podzielności przez 9.

Jeśli prawdziwa jest równoważność „ p wtedy i tylko wtedy, gdy q ”, to oczywiście p jest warunkiem dostatecznym i zarazem koniecznym dla q , jak w przykładzie: „ n jest podzielne przez 9 wtedy i tylko wtedy, gdy suma cyfr liczby n jest podzielna przez 9”.

W dowodach matematycznych pojęcie warunku dostatecznego i koniecznego pojawia się najczęściej w dowodach twierdzeń o postaci równoważności. Dowodząc twierdzenia o postaci „ ϕ wtedy i tylko wtedy, gdy ψ ”, pisze się na przykład: „Warunek dostateczny: pokażemy, że ϕ pociąga ψ ”, a potem: „Warunek konieczny: pokażemy teraz, że ψ pociąga ϕ ”. Niekiedy jednak korzysta się z prawa transpozycji i pisze: „Warunek dostateczny: załóżmy, że ψ jest fałszem i pokażmy, że ϕ jest fałszem”, albo: „Warunek konieczny: załóżmy, że ϕ jest fałszem; pokażemy, że wówczas ψ jest fałszem”.

¹² Warunek konieczny zwany jest niekiedy *conditio sine qua non* – „warunek bez którego nie”; znaczy to, że gdyby q nie było prawdą, to i p nie byłoby prawdą.

1.6. Symbolika beznawiasowa

Z różnych powodów warto zaznaczyć, że nawiasy nie są niezbędne w zapisie formuł logiki. Można je wyeliminować, acz dla osoby niewprawnej poglądowość zapisu znacznie zmaleje.

Zacznijmy od tego, że w matematyce znak funkcji umieszcza się czasem między argumentami, pisząc np. $x+y$ czy $v \cdot t$, a czasem przed argumentami, pisząc $f(x, y)$. Zgodnie z tą ostatnią konwencją można by więc napisać $+(x, y) = z$ (albo nawet $+xy = z$) zamiast $x + y = z$, albo $\cdot vt = s$ zamiast $v \cdot t = s$. Okazuje się, że pisanie znaku funkcji przed jej argumentami zachowuje jednoznaczność formuły.

Idea ta leży u podłoża logicznej symboliki beznawiasowej: zamiast spójnik logiczny pisać mi ę dzy argumentami, piszemy go przed argumentami. Używa się w logice za J. Łukasiewiczem następujących symboli:

N	zamiast	\neg ,
C	zamiast	\rightarrow ,
K	zamiast	\wedge ,
A	zamiast	\vee ,
E	zamiast	\leftrightarrow .

Skróty pochodzą odpowiednio od słów: „negacja”, „konsekwencja”¹³, „koniunkcja”, „alternatywa”, „ekwiwalencja”¹⁴. Tak więc zamiast $p \rightarrow q$ piszemy Cpq , zamiast $p \rightarrow (q \rightarrow r)$ piszemy $CpCqr$, a zamiast formuły $(p \rightarrow q) \rightarrow r$ piszemy $CCpqr$. Prawo sylogizmu hipotetycznego bezkoniunkcyjnego to $CCpqCCqrCpr$. Czytelnik zechce też sprawdzić, że prawo rozdzielności koniunkcji względem alternatywy będzie mieć postać

$$EKpAqrAKpqKpr,$$

a prawo eksportacji–importacji postać

$$ECKpqrCpCqr.$$

Polskim śladem w *computer science*, czyli w informatyce, jest tzw. odwrotna notacja polska (*reverse Polish notation*). Jest to notacja beznawiasowa; różnica polega tu na tym, że w odwrotnej notacji polskiej najpierw pisze się argumenty, a potem symbol funkcji.

¹³ Dokładniej od łacińskiego terminu *consequentia*.

¹⁴ Idea logicznej symboliki beznawiasowej pochodzi od polskiego logika Jana Łukasiewicza; w Polsce zwana jest po prostu symboliką Łukasiewicza. Rozpowszechniona w świecie została nazwana „notacją polską” (*Polish notation*).

Zadania

1. Zapisz schematy następujących wypowiedzi, uwzględniając możliwe różne interpretacje, jeśli wypowiedź nie jest jednoznaczna:

- Będziesz informatykiem lub nie będziesz informatykiem.
- Jeśli matematyka posługuje się dedukcją, to jeśli dedukcja nie jest zawodna, to o ile aksjomaty matematyki nie są fałszywe, to twierdzenia matematyki są prawdziwe.
- Będziesz matematykiem lub będziesz informatykiem i założysz własną firmę komputerową.
- Będziesz informatykiem lub będziesz matematykiem i założysz własną firmę komputerową wtedy i tylko wtedy, gdy nie poświęcisz się pracy nauczycielskiej.
- Masz uprawnienia do wykonywania zawodu nauczyciela, jeśli masz przynajmniej licencjat i zdałeś niezbędne egzaminy z przedmiotów pedagogicznych.
- Prawdziwa sztuka powoduje uniesienia ducha, o ile masz duszę artysty lub jesteś w odpowiednim nastroju.

2. Zbuduj tabelki spójników logicznych odpowiadających spójnikom międzyzdaniowym „ani... , ani...”, „tylko wtedy..., gdy...”, „..., choćby nawet...”.

3. Czy uznasz zdanie „ $2 + 2 = 5 \rightarrow$ matematyka jest nauką dedukcyjną” za prawdziwą implikację? Czy uznasz za prawdziwe zdanie „jeśli $2 + 2 = 5$, to matematyka jest nauką dedukcyjną”?

4. Sprawdź, czy poniższe wnioskowania są niezawodne:

Jeśli ktoś kradnie, to podlega karze.

Zatem: jeśli ktoś włamuje się i kradnie, to podlega karze.

Jeśli stok jest zbudowany ze skał osadowych,
a nachylenie stoku jest duże,
to powstają osuwiska ześlizgowe.

Zatem: jeśli nie powstają osuwiska ześlizgowe,
to nachylenie stoku nie jest duże
lub stok nie jest zbudowany ze skał osadowych.

Jeśli piękno polega na wdzięku lub polega na doskonałości,
to nie polega na proporcji części.

Zatem: jeśli piękno polega na proporcji części, to piękno nie polega na wdzięku
i nie polega na doskonałości.

Jeśli ciąg (a_n) jest monotoniczny i jest ograniczony,
to ciąg (a_n) jest zbieżny.

Ciąg (a_n) nie jest zbieżny.

Zatem: jeśli ciąg (a_n) jest ograniczony, to nie jest monotoniczny.

5. Sporządzić tabelki wszystkich możliwych spójników logicznych jednoargumentowych i dwuargumentowych.

6. Zdefiniować koniunkcję za pomocą alternatywy i negacji.

Wskazówka: skorzystać z prawa De Morgana.

7. Opierając się na odpowiednich tautologiach z Twierdzenia 1.4.1, zdefiniować implikację i równoważność za pomocą alternatywy i negacji.

8. Zdefiniować alternatywę, koniunkcję oraz równoważność za pomocą implikacji i negacji.

10. Sprawdzić metodą zero-jedynkową, czy tautologiami są następujące formuły:

- a) $[(p \rightarrow q) \wedge (s \rightarrow \neg q)] \rightarrow (s \rightarrow \neg p)$,
- b) $[(p \rightarrow q) \wedge (r \rightarrow s)] \rightarrow [(p \vee r) \wedge (q \vee s)]$,
- c) $[(p \rightarrow q) \wedge (r \rightarrow s)] \rightarrow [(p \wedge r) \rightarrow (q \wedge s)]$,
- d) $[(p \wedge q) \vee (p \wedge r)] \rightarrow [p \wedge (q \vee (r \wedge s))]$,
- e) $[(p \wedge r) \rightarrow (q \vee s)] \rightarrow [(p \rightarrow q) \wedge (r \rightarrow s)]$.

Rozdział 2

Funkcje logiczne

2.1. Funkcje logiczne – podstawowe definicje

W rozdziale tym przedstawimy ogólne informacje o funkcjach logicznych, czyli funkcjach szczególnym przypadkiem których są funkcje związane ze spójnikami międzydaniowymi rozpatrywanymi w rozdziale 1. Przyjmijmy następującą definicję:

DEFINICJA 2.1.1 Funkcja logiczna *jest to funkcja*

$$f: \{0, 1\}^n \rightarrow \{0, 1\}$$

dla $n \geq 1$, czyli funkcja n -argumentowa ($n \geq 1$) o argumentach i wartościach ze zbioru $\{0, 1\}$.

Elementy 0 i 1 można interpretować na rozmaite sposoby. W szczególności w logice 0 i 1 interpretujemy jako wartości logiczne zdań, a mianowicie 0 jako fałszywość (fałsz), a 1 jako prawdziwość (prawda). W elektronice wartości 0 i 1 oznaczają stany układu: 0 – stan bierny, 1 – stan czynny (technicznie można zrealizować 1 jako wysoki potencjał, a 0 jako niski potencjał, względnie 1 jako sygnał elektryczny, a 0 jako brak sygnału). Mając na myśli interpretację logiczną, nazywa się funkcje logiczne funkcjami prawdziwościami. W elektronice stosuje się nazwę funkcje przełączające.

STWIERDZENIE 2.1.2. *Istnieje 2^{2^n} różnych funkcji logicznych n -argumentowych.*

Dowód. Zauważmy przede wszystkim, że zbiór $\{0, 1\}^n$ składa się ze wszystkich ciągów (a_1, a_2, \dots, a_n) , takich że $a_i = 0$ lub $a_i = 1$ dla każdego $1 \leq i \leq n$. Ciągów takich można utworzyć 2^n . Funkcja logiczna

$f: \{0, 1\}^n \rightarrow \{0, 1\}$ przyporządkowuje każdemu ciągowi (a_1, a_2, \dots, a_n) wartość $f(a_1, a_2, \dots, a_n)$ równą 0 lub 1. Zatem funkcji logicznych n -argumentowych jest tyle, na ile sposobów można określić takie przyporządkowanie, czyli na ile sposobów można ustawić 0 i 1 na 2^n miejscach. Można zaś to uczynić na 2^{2^n} różnych sposobów. Zatem istnieje dokładnie 2^{2^n} różnych n -argumentowych funkcji logicznych. Q.E.D.

Przyjmiemy pewne uporządkowanie funkcji logicznych, które objaśnimy poniżej. Funkcję n -argumentową, która zajmuje i -tą pozycję w tym uporządkowaniu, będziemy oznaczali symbolem f_i^n (przy czym $n \geq 1$ oraz $0 \leq i \leq 2^{2^n} - 1$).

Dla $n = 1$ mamy 2^{2^1} , czyli 4 funkcje logiczne 1-argumentowe. Oto one:

$$f_0^1(1) = 0, f_0^1(0) = 0, \text{ kod: } 00,$$

$$f_1^1(1) = 0, f_1^1(0) = 1, \text{ kod: } 01,$$

$$f_2^1(1) = 1, f_2^1(0) = 0, \text{ kod: } 10,$$

$$f_3^1(1) = 1, f_3^1(0) = 1, \text{ kod: } 11.$$

Dla $n = 2$ otrzymujemy 2^{2^2} , czyli 16 funkcji logicznych 2-argumentowych. Przedstawimy pierwszych dziewięć z nich w następującej tabeli:

$$f_0^2(1, 1) = 0, f_0^2(1, 0) = 0, f_0^2(0, 1) = 0, f_0^2(0, 0) = 0, \\ \text{ - kod: } 0000,$$

$$f_1^2(1, 1) = 0, f_1^2(1, 0) = 0, f_1^2(0, 1) = 0, f_1^2(0, 0) = 1, \\ \text{ - kod: } 0001,$$

$$f_2^2(1, 1) = 0, f_2^2(1, 0) = 0, f_2^2(0, 1) = 1, f_2^2(0, 0) = 0, \\ \text{ - kod: } 0010,$$

$$f_3^2(1, 1) = 0, f_3^2(1, 0) = 0, f_3^2(0, 1) = 1, f_3^2(0, 0) = 1, \\ \text{ - kod: } 0011,$$

$$f_4^2(1, 1) = 0, f_4^2(1, 0) = 1, f_4^2(0, 1) = 0, f_4^2(0, 0) = 0, \\ \text{ - kod: } 0100,$$

$$f_5^2(1, 1) = 0, f_5^2(1, 0) = 1, f_5^2(0, 1) = 0, f_5^2(0, 0) = 1, \\ \text{ - kod: } 0101,$$

$$f_6^2(1, 1) = 0, f_6^2(1, 0) = 1, f_6^2(0, 1) = 1, f_6^2(0, 0) = 0, \\ \text{ - kod: } 0110,$$

$$f_7^2(1, 1) = 0, f_7^2(1, 0) = 1, f_7^2(0, 1) = 1, f_7^2(0, 0) = 1, \\ \text{ - kod: } 0111,$$

$$f_8^2(1, 1) = 1, f_8^2(1, 0) = 0, f_8^2(0, 1) = 0, f_8^2(0, 0) = 0, \\ \text{ - kod: } 1000.$$

Zastosowana tu zasada porządkowania funkcji logicznych jest następująca: Ciągi złożone z symboli 0 i 1 traktujemy jako przedstawienia liczb

naturalnych w systemie dwójkowym, czyli przy bazie 2 (przy tym symbole 0 stojące z lewej strony „nie liczą się”). Zgodnie z tym ciągi argumentów ustawiliśmy w porządku malejącym: dla funkcji 1-argumentowych było to 1 i 0, dla funkcji 2-argumentowych 11 (= 3), 10 (= 2), 01 (= 1) i 00 (= 0). Wypisując ciąg kolejnych wartości funkcji f_i^n , otrzymujemy zapis dwójkowy liczby i . Na przykład dla funkcji f_3^2 otrzymujemy ciąg wartości 0011, czyli liczbę 3, a dla funkcji f_2^2 ciąg wartości 0010, czyli liczbę 2 (o tym informuje nas kod przyporządkowany każdej z funkcji).

Korzystając z tej zasady, łatwo stwierdzić, jak wygląda na przykład funkcja f_{10}^2 . Otóż mamy: $10 = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$. Zatem liczba 10 ma przedstawienie dwójkowe 1010 (czasami pisze się to jako $(1010)_2$, aby podkreślić, że mamy do czynienia z rozwinięciem dwójkowym danej liczby). Otrzymujemy stąd: $f_{10}^2(1, 1) = 1$, $f_{10}^2(1, 0) = 0$, $f_{10}^2(0, 1) = 1$ oraz $f_{10}^2(0, 0) = 0$.

Dla funkcji f_{20}^3 mamy: $20 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0$, czyli $20 = (10100)_2 = (00010100)_2 = (00010100)$. Stąd w szczególności $f_{20}^3(1, 1, 1) = 0$, $f_{20}^3(1, 1, 0) = 0$, $f_{20}^3(1, 0, 1) = 0$, $f_{20}^3(1, 0, 0) = 1$ itd. Dla funkcji f_{200}^3 mamy: $200 = 1 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0$, czyli $200 = (11001000)_2 = (11001000)$. Stąd w szczególności $f_{200}^3(1, 1, 1) = 1$, $f_{200}^3(1, 1, 0) = 1$, $f_{200}^3(1, 0, 1) = 0$, $f_{200}^3(1, 0, 0) = 0$ itd.

W logice szczególne znaczenie ma pięć funkcji odpowiadających spójnikom międzydaniowym, tzn. 1-argumentowa funkcja negacji \neg (czyli funkcja f_1^1) oraz 2-argumentowe funkcje: koniunkcji \wedge (czyli funkcja f_8^2), alternatywy \vee (czyli funkcja f_{14}^2), implikacji \rightarrow (czyli funkcja f_{11}^2) i równoważności \leftrightarrow (czyli funkcja f_9^2). Można je scharakteryzować za pomocą następujących warunków:

$$\neg(1) = 0, \quad \neg(0) = 1$$

oraz

$$\begin{aligned} f_8^2: & \quad 1 \wedge 1 = 1, & 1 \wedge 0 = 0, & 0 \wedge 1 = 0, & 0 \wedge 0 = 0, \\ f_{14}^2: & \quad 1 \vee 1 = 1, & 1 \vee 0 = 1, & 0 \vee 1 = 1, & 0 \vee 0 = 0, \\ f_{11}^2: & \quad 1 \rightarrow 1 = 1, & 1 \rightarrow 0 = 0, & 0 \rightarrow 1 = 1, & 0 \rightarrow 0 = 1, \\ f_9^2: & \quad 1 \leftrightarrow 1 = 1, & 1 \leftrightarrow 0 = 0, & 0 \leftrightarrow 1 = 0, & 0 \leftrightarrow 0 = 1. \end{aligned}$$

Funkcja negacji \neg odpowiada spójnikowi negacji *nie jest tak*, że funkcja koniunkcji \wedge – spójnikowi koniunkcji *i*, funkcja alternatywy \vee – spójnikowi alternatywy *lub*, funkcja implikacji \rightarrow – spójnikowi implikacji *jeżeli ... , to ...*, a funkcja równoważności \leftrightarrow – spójnikowi równoważności *wtedy i tylko wtedy, gdy*.

Dla opisanych funkcji logicznych zachodzą pewne prawa, zwane prawami algebry logiki (odpowiadają one stosownym tautologiom rachunku zdań).

Oto najważniejsze z nich:

- prawa dla 0: $x \wedge 0 = 0$, $x \vee 0 = x$, $x \wedge \neg x = 0$,
- prawa dla 1: $x \vee 1 = 1$, $x \wedge 1 = x$, $x \vee \neg x = 1$,
- prawa pochłaniania: $x \wedge x = x$, $x \vee x = x$,
- prawa przemienności: $x \wedge y = y \wedge x$, $x \vee y = y \vee x$, $x \leftrightarrow y = y \leftrightarrow x$,
- prawa łączności: $(x \wedge y) \wedge z = x \wedge (y \wedge z)$, $(x \vee y) \vee z = x \vee (y \vee z)$,
 $(x \leftrightarrow y) \leftrightarrow z = x \leftrightarrow (y \leftrightarrow z)$,
- prawa rozdzielności: $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$, $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$,
- prawo podwójnej negacji: $\neg\neg x = x$,
- prawa De Morgana: $\neg(x \wedge y) = \neg x \vee \neg y$, $\neg(x \vee y) = \neg x \wedge \neg y$,
- prawo transpozycji: $x \rightarrow y = \neg y \rightarrow \neg x$,
- prawo definiowania \rightarrow : $x \rightarrow y = \neg x \vee y$,
- prawo definiowania \leftrightarrow : $x \leftrightarrow y = (x \rightarrow y) \wedge (y \rightarrow x)$.

Prawa te są prawdziwe dla wszystkich $x, y, z \in \{0, 1\}$.

Dowodzi się tych praw, korzystając z definicji odpowiednich funkcji. I tak dla przykładu, w przypadku pierwszego prawa rozdzielności mamy:

(a) dla $x = 0$ obie strony rozważanego prawa przyjmują wartość 0, a więc są równe,

(b) dla $x = 1$ mamy

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

przy czym korzystamy tutaj z praw dla 1.

2.2. Koniunkcyjna i alternatywna postać normalna

Zajmiemy się teraz zagadnieniem przedstawialności funkcji logicznych w pewnej specjalnej postaci, zwanej postacią normalną.

DEFINICJA 2.2.1. *Mówimy, że funkcja $f(x_1, x_2, \dots, x_n)$ jest przedstawialna za pomocą funkcji f_1, f_2, \dots, f_k wtedy i tylko wtedy, gdy istnieje formuła nazwowa F zbudowana z symboli funkcyjnych f_1, f_2, \dots, f_k (niekoniecznie wszystkich) oraz zmiennych x_1, x_2, \dots, x_n (również niekoniecznie wszystkich), taka że równość $f(x_1, x_2, \dots, x_n) = F$ jest prawdziwa dla wszystkich wartości argumentów x_1, x_2, \dots, x_n .*

STWIERDZENIE 2.2.2 *Funkcja \wedge jest przedstawialna za pomocą funkcji \neg i \vee ; funkcja \vee jest przedstawialna za pomocą \neg oraz \wedge .*

Dowód. Istotnie, wystarczy zauważyć, że na mocy prawa podwójnej negacji oraz praw De Morgana otrzymujemy następujące równości dające potrzebne przedstawienia funkcji \wedge i \vee :

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

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

Q.E.D.

Na mocy praw łączności dla \wedge i \vee w wyrażeniach postaci

$$F_1 \wedge F_2 \wedge \dots \wedge F_n$$

oraz

$$F_1 \vee F_2 \vee \dots \vee F_n$$

nie są konieczne nawiasy wskazujące kolejność wykonywanych działań, gdyż wartości tych wyrażeń nie zależą od tej kolejności. W związku z tym w wyrażeniach tego typu będziemy opuszczali nawiasy.

DEFINICJA 2.2.3. (1) *Każde wyrażenie postaci x lub $\neg x$, gdzie x jest dowolną zmienną, będziemy nazywali literałem.*

(2) *Wyrażenia postaci $L_1 \wedge L_2 \wedge \dots \wedge L_n$, takie że $n \geq 1$, a każde L_i ($1 \leq i \leq n$) jest literałem, nazywamy koniunkcjami elementarnymi. Wyrażenia postaci $L_1 \vee L_2 \vee \dots \vee L_n$, takie że $n \geq 1$, a każde L_i jest literałem ($1 \leq i \leq n$), nazywamy alternatywami elementarnymi.*

(3) *Wyrażenie w koniunkcyjnej postaci normalnej (krótko: kpn) jest to wyrażenie kształtu $A_1 \wedge A_2 \wedge \dots \wedge A_n$, takie że $n \geq 1$ oraz każde A_i dla $1 \leq i \leq n$ jest alternatywą elementarną. Wyrażenie w alternatywnej postaci normalnej (krótko: apn) jest to wyrażenie kształtu $K_1 \vee K_2 \vee \dots \vee K_n$, takie że $n \geq 1$ oraz każde K_i dla $1 \leq i \leq n$ jest koniunkcją elementarną.*

Przykładami koniunkcji elementarnych są więc wyrażenia postaci: x , $\neg y$, $x \wedge \neg y$, $x \wedge y \wedge \neg z$. Przykładami alternatyw elementarnych są: x , $\neg y$, $x \vee \neg y$, $x \vee \neg y \vee z$. Jako przykłady wyrażeń w koniunkcyjnej postaci normalnej mogą służyć wyrażenia: $x \vee \neg y$, $(x \vee \neg y) \wedge (\neg y \vee z)$, a jako przykłady wyrażeń w alternatywnej postaci normalnej wyrażenia: $x \wedge \neg y$, $(x \wedge \neg y) \vee (x \wedge \neg z)$. Widać, że wyrażenie w koniunkcyjnej postaci normalnej to koniunkcja skończenie wielu alternatyw elementarnych, natomiast wyrażenie w alternatywnej postaci normalnej to alternatywa skończenie wielu koniunkcji elementarnych.

Zachodzi następujące podstawowe twierdzenie:

TWIERDZENIE 2.2.4. *Każda funkcja logiczna może być przedstawiona w koniunkcyjnej postaci normalnej i w alternatywnej postaci normalnej.*

Dowód. Rozważmy dowolną funkcję logiczną $f: \{0, 1\}^n \rightarrow \{0, 1\}$. Znajdziemy najpierw jej przedstawienie w alternatywnej postaci normalnej. Wyróżnijmy dwa przypadki:

(I) Dla wszystkich wartości argumentów x_1, x_2, \dots, x_n zachodzi

$$f(x_1, x_2, \dots, x_n) = 0.$$

Wtedy

$$f(x_1, x_2, \dots, x_n) = x_1 \wedge \neg x_1,$$

co daje oczywiście żądane przedstawienie f w apn, gdyż pojedyncza koniunkcja elementarna jest przeciwieństwem wyrażeniem w apn.

(II) Załóżmy teraz, że $f(x_1, x_2, \dots, x_n) = 1$ dla przynajmniej jednego układu argumentów. Niech $(a_1^i, a_2^i, \dots, a_n^i)$, $1 \leq i \leq k$, będą wszystkimi układami argumentów (a_1, a_2, \dots, a_n) , takimi że $f(a_1, a_2, \dots, a_n) = 1$. Dla każdego $1 \leq i \leq k$ tworzymy koniunkcję elementarną $K_i = L_1^i \wedge L_2^i \wedge \dots \wedge L_n^i$, przyjmując, że $L_j^i = x_j$, jeśli $a_j^i = 1$, oraz $L_j^i = \neg x_j$, jeśli $a_j^i = 0$. Oczywiście wyrażenie K_i przyjmuje wartość 1 dla układów argumentów $(a_1^i, a_2^i, \dots, a_n^i)$ dla $1 \leq i \leq k$ oraz wartość 0 dla wszystkich pozostałych układów argumentów. W ten sposób otrzymujemy:

$$f(x_1, x_2, \dots, x_n) = K_1 \vee K_2 \vee \dots \vee K_k.$$

Istotnie, prawa strona przyjmuje wartość 1 dla tych układów argumentów (a_1, a_2, \dots, a_n) , dla których przynajmniej jedna koniunkcja elementarna K_1, K_2, \dots, K_k przyjmuje wartość 1, czyli dokładnie dla układów $(a_1^i, a_2^i, \dots, a_n^i)$, $1 \leq i \leq k$. W konsekwencji lewa i prawa strona powyższego wzoru przyjmują wartość 1 dla tych samych układów argumentów. Dowodzi to prawdziwości rozważanego wzoru.

Aby udowodnić drugą część twierdzenia, postępujemy „dualnie”, tzn. zamieniamy rolę 0 i 1 oraz rolę koniunkcji i alternatywy. Q.E.D.

Rozważmy kilka przykładów:

1. Przedstawmy na początek w apn i kpn funkcję f_9^2 , czyli równoważność. Zgodnie z metodą opisaną w dowodzie powyższego twierdzenia otrzymujemy

$$\text{apn: } f_9^2(x, y) = x \leftrightarrow y = (x \wedge y) \vee (\neg x \wedge \neg y)$$

oraz kpn: $f_9^2(x, y) = x \leftrightarrow y = (\neg x \vee y) \wedge (x \vee \neg y)$.

2. Dla funkcji f_{80}^3 mamy

apn: $f_{80}^3(x, y, z) = (x \wedge y \wedge \neg z) \vee (x \wedge \neg y \wedge \neg z)$

oraz kpn: $f_{80}^3(x, y, z) = (\neg x \vee \neg y \vee \neg z) \wedge (\neg x \vee y \vee \neg z) \wedge (x \vee \neg y \vee \neg z) \wedge (x \vee \neg y \vee z) \wedge (x \vee y \vee \neg z) \wedge (x \vee y \vee z)$.

2.3. Zupełne układy funkcji

DEFINICJA 2.3.1. Układ funkcji logicznych f_1, f_2, \dots, f_k nazywamy zupełnym wtedy i tylko wtedy, gdy każda funkcja logiczna jest przedstawialna za pomocą funkcji tego układu.

Z udowodnionego powyżej twierdzenia głoszącego, że każdą funkcję logiczną można przedstawić zarówno w alternatywnej postaci normalnej, jak i w koniunkcyjnej postaci normalnej, wynika, że układ $\{\neg, \vee, \wedge\}$ jest układem zupełnym. Łatwo zauważyć, że jeśli układ $\{f_1, f_2, \dots, f_k\}$ jest zupełny oraz każda z funkcji f_1, f_2, \dots, f_k może być przedstawiona za pomocą pewnych funkcji g_1, g_2, \dots, g_l , to układ $\{g_1, g_2, \dots, g_l\}$ jest także zupełny. Korzystając z tej własności, otrzymujemy, że następujące układy są także zupełne:

- $\{\neg, \wedge\}$ - wynika to z faktu, że $x \vee y = \neg(\neg x \wedge \neg y)$,
- $\{\neg, \vee\}$ - wynika to z faktu, że $x \wedge y = \neg(\neg x \vee \neg y)$,
- $\{\neg, \rightarrow\}$ - wynika to z faktu, że $x \vee y = \neg x \rightarrow y$.

Ważną rolę w teorii funkcji logicznych odgrywa układ zupełny $\{+, \cdot, 1\}$, gdzie $+$ jest dodawaniem modulo 2, a więc funkcją daną wzorami

$$0 + 0 = 0, \quad 0 + 1 = 1, \quad 1 + 0 = 1, \quad 1 + 1 = 0.$$

Symbol \cdot oznacza zwykle mnożenie, czyli koniunkcję (zatem $x \cdot y = x \wedge y$)¹, a 1 jest funkcją stałą równą 1 (przy czym możemy ją traktować albo jako funkcję 0-argumentową, albo jako funkcję 1-argumentową, tzn. jako funkcję $f(x) = 1$ dla dowolnego x). Zupełność układu $\{+, \cdot, 1\}$ wynika z zupełności układu $\{\neg, \wedge\}$ oraz równości

$$\neg x = x + 1.$$

¹ Znak \cdot czasami opuszczamy i piszemy na przykład xy zamiast $x \cdot y$.

DEFINICJA 2.3.2. (1) *Iloczyn dowolnej liczby różnych zmiennych ze zbioru $\{x_1, x_2, \dots, x_n\}$ nazywamy jednomianami tych zmiennych. Dopuszczamy przy tym iloczyn „pusty” (czyli iloczyn zero zmiennych), który utożsamiamy ze stałą 1.*

(2) *Wielomianem Żegałkina nazywamy wyrażenie będące sumą skończonej liczby różnych jednomianów zmiennych x_1, x_2, \dots, x_n . Przy tym dopuszczamy „pustą” sumę jednomianów, którą utożsamiamy ze stałą 0.*

Zauważmy, że zachodzą następujące wzory:

$$x(y + z) = xy + xz, \quad xy = yx, \quad x + y = y + x, \quad x + x = 0, \quad xx = x.$$

Wzory te wraz z faktem, że układ $\{+, \cdot, 1\}$ jest zupełny, pozwalają łatwo stwierdzić, że każdą funkcję logiczną $f(x_1, x_2, \dots, x_n)$ można przedstawić w postaci wielomianu Żegałkina. Na przykład dla funkcji logicznej $f(x, y) = (x + 1)(x + y + 1)$ mamy

$$(x + 1)(x + y + 1) = xx + xy + x + x + y + 1 = 1 + x + y + xy.$$

TWIERDZENIE 2.3.3. *Każda funkcja logiczna ma dokładnie jedno przedstawienie w postaci wielomianu Żegałkina z dokładnością do kolejności czynników w jednomianach i składników w wielomianie.*

D o w ó d. Należy udowodnić, że dla każdej funkcji logicznej

$$f: \{0, 1\}^n \rightarrow \{0, 1\}$$

istnieje dokładnie jeden zbiór różnych jednomianów $\{M_1, M_2, \dots, M_k\}$, taki że $f(x_1, x_2, \dots, x_n) = M_1 + M_2 + \dots + M_k$. Zauważmy w tym celu, że jednomiany zbudowane ze zmiennych x_1, x_2, \dots, x_n możemy utożsamiać z podzbiórami tego zbioru zmiennych (przy tym przyjmujemy, że zbiór pusty odpowiada stałej 1). Zatem istnieje 2^n takich jednomianów. Z kolei wielomiany Żegałkina można utożsamiać z podzbiórami tego zbioru jednomianów (teraz zbiór pusty odpowiada stałej 0). W konsekwencji istnieje 2^{2^n} różnych wielomianów Żegałkina ze zmiennych x_1, x_2, \dots, x_n . Stwierdzamy zatem, że liczba wielomianów Żegałkina n zmiennych jest równa liczbie wszystkich funkcji logicznych n -argumentowych. W konsekwencji zatem dwa różne wielomiany nie mogą przedstawiać jednej funkcji. Istotnie, gdyby tak było, to istniałaby funkcja logiczna nieprzedstawialna żadnym wielomianem Żegałkina, ale to jest niemożliwe, ponieważ układ $\{+, \cdot, 1\}$ jest zupełny. Ostatecznie więc każdą funkcję logiczną można przedstawić za pomocą dokładnie jednego wielomianu Żegałkina. Q.E.D.

Wyróżnimy jeszcze jedną klasę funkcji logicznych, przyjmując następującą definicję:

DEFINICJA 2.3.4. *Funkcje, które można przedstawić jako sumy skończenie wielu prostych jednomianów, czyli jednomianów bez mnożenia, nazywamy funkcjami liniowymi.*

Przykładami funkcji liniowych są funkcje: $\neg x = x + 1$ oraz $x \leftrightarrow y = x + y + 1$. Natomiast funkcje: $x \wedge y = xy$ oraz $x \vee y = x + y + xy$ nie są funkcjami liniowymi. Łatwo zauważyć, że jeżeli $\{f_1, f_2, \dots, f_k\}$ jest układem funkcji liniowych, to każda funkcja przedstawialna za pomocą funkcji tego układu jest także liniowa. W konsekwencji taki układ nie może być zupełny. A zatem nie są zupełne na przykład układy: $\{+, 1\}$ i $\{\neg, \leftrightarrow\}$.

Na koniec rozważmy jeszcze dwie funkcje logiczne 2-argumentowe, takie że tworzą one, każda z osobna, układy zupełne. Pokażemy też, że są to jedyne takie funkcje 2-argumentowe.

DEFINICJA 2.3.5. (1) Kreską Sheffera nazywamy 2-argumentową funkcję logiczną | daną wzorem $x|y = \neg(x \wedge y) = xy + 1$.

(2) Binegacją nazywamy funkcję logiczną 2-argumentową daną wzorem $x \downarrow y = \neg(x \vee y) = x + y + xy + 1$.

Łatwo sprawdzić, że kreska Sheffera to funkcja f_7^2 , a binegacja to funkcja f_1^2 . Zatem przyjmują one następujące wartości:

$$\begin{array}{cccc} 1|1 = 0, & 1|0 = 1, & 0|1 = 1, & 0|0 = 1, \\ 1 \downarrow 1 = 0, & 1 \downarrow 0 = 0, & 0 \downarrow 1 = 0, & 0 \downarrow 0 = 1. \end{array}$$

Kreska Sheffera odpowiada spójnikowi międzyzdaniewemu „co najwyżej jedno z dwojga ... , ...”, a binegacja – spójnikowi „ani ... , ani ...”.

Układy $\{| \}$ oraz $\{\downarrow\}$ są zupełne. Wynika to z poniższych równości oraz z faktu, że $\{\neg, \wedge\}$ i $\{\neg, \vee\}$ są układami zupełnymi

$$\neg x = \neg(x \wedge x) = x|x,$$

$$x \wedge y = \neg\neg(x \wedge y) = \neg(x|y) = (x|y)|(x|y),$$

$$\neg x = \neg(x \vee x) = x \downarrow x,$$

$$x \vee y = \neg\neg(x \vee y) = \neg(x \downarrow y) = (x \downarrow y) \downarrow (x \downarrow y):$$

Otrzymujemy więc wniosek, że każdą funkcję logiczną można przedstawić za pomocą kreski Sheffera $|$ lub za pomocą binegacji \downarrow i odpowiednich zmiennych.

TWIERDZENIE 2.3.6. *Kreska Sheffera $|$ i binegacja \downarrow są jedynymi 2-argumentowymi funkcjami logicznymi f , takimi że układ $\{f\}$ jest zupełny².*

Dowód. Załóżmy, że $f: \{0,1\}^2 \rightarrow \{0,1\}$ oraz że układ $\{f\}$ jest zupełny. Wykażemy, że $f = |$ lub $f = \downarrow$. Zauważmy, że $f(0,0) = 1$. Istotnie, gdyby tak nie było, to każde wyrażenie F zbudowane tylko ze zmiennej x i symbolu funkcji f przyjmowałoby wartość 0 dla $x = 0$, a więc równość $\neg x = F$ nie byłaby możliwa. Podobnie $f(1,1) = 0$. Rozważmy więc teraz wartości $f(0,1)$ i $f(1,0)$. Możliwe są cztery przypadki:

(A) $f(0,1) = 0$ i $f(1,0) = 0$. Wtedy f jest binegacją, czyli $f = \downarrow$.

(B) $f(0,1) = 0$ i $f(1,0) = 1$. Wtedy $f(x,y) = \neg y = y + 1$. A zatem f jest funkcją liniową, co jest jednak niemożliwe, ponieważ z założenia układ $\{f\}$ jest zupełny.

(C) $f(0,1) = 1$ i $f(1,0) = 0$. Wtedy jednak $f(x,y) = \neg x = x + 1$, czyli f byłaby funkcją liniową, co jest niemożliwe.

(D) $f(0,1) = 1$ i $f(1,0) = 1$. Wtedy f jest kreską Sheffera, czyli $f = |$.
Q.E.D.

Zadania

1. Zapisać w notacji binarnej następujące liczby: 9, 19, 107, $2^6 + 1$.
2. Zapisać w notacji dziesiętnej następujące liczby (zapisane w notacji binarnej): 101010, 10000011, 1100110011, 1000110011.
3. Napisać tabelki dla następujących funkcji: f_{10}^3 , f_{72}^3 , f_{223}^3 , f_{221}^4 .
4. Ile istnieje funkcji logicznych 3-argumentowych i ile istnieje funkcji logicznych 4-argumentowych?
5. Czy następujące wyrażenia są alternatywami elementarnymi, koniunkcjami elementarnymi, wyrażeniami w koniunkcyjnej postaci normalnej, wyrażeniami alternatywnej postaci normalnej:

² Jako pierwszy twierdzenie to udowodnił w 1926 roku polski logik Eustachy Żyliński (1880–1954).

- a) y ,
- b) $\neg x \vee y$,
- c) $x \vee y \vee z$,
- d) $(x \vee y) \vee (y \vee \neg x)$,
- e) $(\neg x \vee z) \vee (\neg x \vee z \vee y)$.

6. Przedstawić w alternatywnej postaci normalnej (apn) i w koniunkcyjnej postaci normalnej (kpn) następujące funkcje logiczne: f_{177}^3 , f_{127}^3 , f_{13}^2 , f_9^2 , f_{65}^3 , f_{163}^3 , f_{42}^3 .

7. Napisać tabelkę i znaleźć numer funkcji logicznej, której postać normalna jest następująca:

- a) $(\neg x \vee \neg y \vee z) \vee (x \vee \neg y \vee \neg z) \vee (x \vee \neg y \vee z) \vee (x \vee y \vee \neg z)$,
- b) $(\neg x \vee \neg y \vee \neg z) \vee (x \vee \neg y \vee z) \vee (\neg x \vee \neg y \vee z)$,
- c) $(x \vee \neg y \vee \neg z) \vee (x \vee \neg y \vee z)$,
- d) $(x \vee y \vee z) \vee (x \vee \neg y \vee z) \vee (\neg x \vee \neg y \vee \neg z)$.

8. Napisać następujące funkcje logiczne w postaci wielomianów Żegajkina:

- a) $f(x, y) = x \vee y$,
- b) $f(x, y) = xy$,
- c) $x \leftrightarrow y$.

9. Prawdziwe jest następujące twierdzenie: *Każdą funkcję logiczną można przedstawić wyłącznie za pomocą koniunkcji i negacji*. Prosta metoda definiowania funkcji za pomocą \wedge i \neg jest następująca:

A. Jeśli $f(x_1, x_2, \dots, x_n) = 1$, to kładziemy $f(x_1, x_2, \dots, x_n) = \neg(x_1 \wedge \neg x_1)$.

B. Niech $f(x_1, x_2, \dots, x_n) = 0$ dla pewnego układu argumentów. Niech zatem $(a_1^i, a_2^i, \dots, a_n^i)$, $1 \leq i \leq k$, będą wszystkimi takimi układami argumentów (a_1, a_2, \dots, a_n) , że $f(a_1, a_2, \dots, a_n) = 0$. Dla każdego $1 \leq i \leq k$ tworzymy formułę $\neg F_i$, gdzie F_i jest koniunkcją literalów tworzoną następująco: jeśli $a_j^i = 1$, to w tworzonej koniunkcji kładziemy x_j , jeśli natomiast $a_j^i = 0$, to w koniunkcji tej kładziemy $\neg x_j$. Funkcję f definiujemy teraz równością $f(x_1, x_2, \dots, x_n) = \neg(F_1) \wedge \dots \wedge \neg(F_k)$.

Przykład. Rozważmy funkcję f_6^2 , definiowaną, jak pamiętamy następująco: $f_6^2(1, 1) = 0$, $f_6^2(1, 0) = 1$, $f_6^2(0, 1) = 1$, $f_6^2(0, 0) = 0$. Zgodnie z podaną tu metodą $f_6^2(x_1, x_2) = \neg(x_1 \wedge x_2) \wedge \neg(\neg x_1 \wedge \neg x_2)$.

a. Dowieść, posługując się jako wzorcem dowodem twierdzenia 2.4, że podana tu metoda definiowania funkcji logicznych jest poprawna. Zauważyć, że jeśli jest poprawna, to np. wszystkie możliwe spójniki logiczne dwuargumentowe są definiowalne za pomocą koniunkcji i negacji w sposób tu wskazany.

b. Używając opisanej tu metody, zdefiniować funkcje z zadania 6.

10. Za pomocą kreski Sheffera zdefiniować koniunkcję, alternatywę i implikację.

11. Zdefiniować koniunkcję, alternatywę i implikację za pomocą binegacji.

Rozdział 3

System aksjomatyczny logiki klasycznej

3.1. Logika klasyczna: syntaktyka

Opiszemy tu system aksjomatyczny rachunku zdań, taki że jego twierdzeniami będą wszystkie i tylko tautologie klasycznego rachunku zdań.

Osobliwością, przynajmniej dla początkującego, jest tu pojęcie dowodu formalnego. Nie przypomina ono pojęcia dowodu, z którym można się spotkać w szkole średniej.

Istnieje wiele aksjomatyzacji klasycznego rachunku zdań. Na ogół dowody formalne poszczególnych tez są długie i żmudne. Aby nie nużyć początkującego Czytelnika długimi dowodami formalnymi, wybraliśmy taki system, w którym dzięki twierdzeniu o dedukcji dowody będą stosunkowo proste i przejrzyste¹. Przypomnijmy definicję formuły rachunku zdań.

DEFINICJA 3.1.1. *Następujące symbole są symbolami języka rachunku zdań:*

p_0, p_1, p_2, \dots	zmienne zdaniowe (ich ilość jest przeliczalna),
$\neg, \rightarrow, \vee, \wedge, \leftrightarrow$	spójniki: negacji, implikacji, alternatywy, koniunkcji i równoważności,
$), ($	nawiasy.

DEFINICJA 3.1.2. *Zbiór \mathfrak{F} poprawnie zbudowanych formuł języka rachunku zdań jest najmniejszym zbiorem spełniającym następujące warunki:*

- (i) $p_i \in \mathfrak{F}$ dla dowolnego $i \in \mathbb{N}$,
- (ii) jeśli $\phi, \psi \in \mathfrak{F}$, to $\neg(\phi) \in \mathfrak{F}$ oraz $(\phi) \rightarrow (\psi), (\phi) \vee (\psi), (\phi) \wedge (\psi), (\phi) \leftrightarrow (\psi) \in \mathfrak{F}$.

¹ Pełny wykład aksjomatycznego systemu rachunku zdań bez stosowania twierdzenia o dedukcji znajdzie Czytelnik np. w podręczniku T. Batoga, *Podstawy logiki*, Wydawnictwo Naukowe UAM, Poznań 2003.

Podobnie jak w definicji formuły poprawnie zbudowanej, poniżej będziemy używać liter ϕ, ψ, χ, ϕ_1 itd. dla oznaczenia dowolnych poprawnie zbudowanych formuł języka rachunku zdań.

Relacją konsekwencji nazwiemy tu pewną relację określoną na iloczynie kartezjańskim $2^{\mathfrak{F}} \times \mathfrak{F}$, czyli relację zachodzącą między zbiorem formuł a formułą. Jeśli taka relacja zachodzi między pewnym zbiorem formuł F a formułą ϕ , to mówi się, że formuła ϕ jest konsekwencją zbioru formuł F . Zbiór formuł F rozbijemy tu na dwa rozłączne podzbiory: niepusty zbiór Ax aksjomatów logicznych (zbiór ten uznamy za ustalony) oraz dodatkowy zbiór Σ formuł; można je nazwać aksjomatami pozalogicznymi. Zbiór Σ to dowolny podzbiór zbioru \mathfrak{F} ; dopuszczamy, by zbiór Σ był zbiorem pustym. Relację konsekwencji można zdefiniować, na przykład podając definicję pojęcia dowodu formalnego, i tak tutaj uczynimy.

DEFINICJA 3.1.3. Dowodem formalnym formuły ϕ w oparciu o zbiory formuł Ax i Σ oraz zbiór reguł \mathcal{R} nazywamy dowolny skończony ciąg formuł $D = \langle \psi_1, \psi_2, \dots, \psi_n \rangle$, taki że

- (i) $\phi = \psi_n$,
- (ii) $\psi_1 \in Ax \cup \Sigma$,
- (iii) dla dowolnego $i \in \{1, \dots, n\}$ albo $\psi_i \in Ax \cup \Sigma$, albo istnieje reguła $R \in \mathcal{R}$, taka że ψ_i powstaje z formuł wcześniejszych w ciągu D przez zastosowanie do nich reguły R .

Formuła ϕ jest syntaktyczną konsekwencją zbioru formuł Σ (przy ustalonym zbiorze aksjomatów logicznych Ax i ustalonym zbiorze reguł wnioskowania \mathcal{R}), gdy istnieje dowód formalny dla ϕ w oparciu o Ax , Σ i \mathcal{R} .

DEFINICJA 3.1.4. Klasyczną konsekwencją zdaniową S nazwiemy tu taką relację konsekwencji na zbiorze formuł \mathfrak{F} , w której zbiór Ax składa się z wszystkich formuł o budowie podpadającej pod jeden ze schematów:

- A1. $\phi \rightarrow (\psi \rightarrow \phi)$,
- A2. $(\phi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\phi \rightarrow \psi) \rightarrow (\phi \rightarrow \chi))$,
- A3. $\phi \wedge \psi \rightarrow \phi$,
- A4. $\phi \wedge \psi \rightarrow \psi$,
- A5. $(\phi \rightarrow \psi) \rightarrow ((\phi \rightarrow \chi) \rightarrow (\phi \rightarrow \psi \wedge \chi))$,
- A6. $\phi \rightarrow \phi \vee \psi$,
- A7. $\psi \rightarrow \phi \vee \psi$,
- A8. $(\phi \rightarrow \psi) \rightarrow ((\chi \rightarrow \psi) \rightarrow (\phi \vee \chi \rightarrow \psi))$,
- A9. $(\neg\phi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \phi)$,
- A10. $(\phi \leftrightarrow \psi) \rightarrow (\phi \rightarrow \psi)$,

- A11. $(\phi \leftrightarrow \psi) \rightarrow (\psi \rightarrow \phi)$,
 A12. $(\phi \rightarrow \psi) \rightarrow ((\psi \rightarrow \phi) \rightarrow (\phi \leftrightarrow \psi))$,

a zbiór reguł inferencyjnych składa się tu wyłącznie z reguły odrywania, zwanej też Modus Ponens, którą oznaczymy symbolem *MP*, to jest reguły

$$\frac{\phi \rightarrow \psi, \phi}{\psi}$$

Aksjomaty te są schematami aksjomatów; każdy z nich reprezentuje nieskończoną klasę formuł, podpadających pod wspólny schemat.

DEFINICJA 3.1.5. *Formuła ϕ jest syntaktyczną S -konsekwencją zbioru Σ wtedy i tylko wtedy, gdy ϕ ma dowód w oparciu o podany wyżej zbiór Ax oraz zbiór Σ i regułę *MP*; piszemy wtedy $\Sigma \vdash_S \phi$. Jeśli $\Sigma \vdash_S \phi$, gdzie Σ jest zbiorem pustym, to ϕ nazwiemy twierdzeniem systemu S i piszemy $\vdash_S \phi$.*

Zauważmy, że $\vdash_S \phi$ znaczy tu po prostu, iż formuła ϕ ma dowód w oparciu o zbiór Ax i *MP*. Logiką (systemem logiki) S będziemy dalej nazywać zarówno relację konsekwencji, oznaczoną wyżej przez S , jak i zbiór takich formuł ϕ , że $\vdash_S \phi$, czyli twierdzeń systemu S .

Podamy teraz przykład dowodu formalnego w oparciu o podany tu zbiór Ax i regułę *MP*. Dowiedzimy mianowicie, że dla dowolnej formuły ϕ , formuła $\phi \rightarrow \phi$ ma dowód formalny w oparciu o Ax i *MP*.

LEMAT 3.1.6. *Dla dowolnej formuły twierdzeniem przedstawionego wyżej systemu S jest formuła*

$$(t0) \quad (\phi \rightarrow \phi).$$

D o w ó d. Poniższy ciąg formuł jest dowodem dla $\phi \rightarrow \phi$:

$$\begin{array}{ll} \psi_1 & (\phi \rightarrow ((\phi \rightarrow \phi) \rightarrow \phi)) \rightarrow ((\phi \rightarrow (\phi \rightarrow \phi)) \rightarrow (\phi \rightarrow \phi)) & (A2) \\ \psi_2 & (\phi \rightarrow ((\phi \rightarrow \phi) \rightarrow \phi)) & (A1) \\ \psi_3 & (\phi \rightarrow (\phi \rightarrow \phi)) \rightarrow (\phi \rightarrow \phi) & (1), (2), MP \\ \psi_4 & (\phi \rightarrow (\phi \rightarrow \phi)) & (A1) \\ \psi_5 & \phi \rightarrow \phi & (3), (4), MP. \end{array}$$

Można sprawdzić, że ciąg $\langle \psi_1, \psi_2, \psi_3, \psi_4, \psi_5 \rangle$ spełnia podaną wyżej definicję dowodu formalnego. Z prawej strony tego formalnego dowodu podany został zwięzły komentarz, skąd biorą się kolejne formuły dowodu.

Pokazaliśmy zatem, że $\vdash_S \phi \rightarrow \phi$, to jest, że dowolna formuła postaci $\phi \rightarrow \phi$ jest twierdzeniem przedstawionego wyżej systemu S ; twierdzenie to oznaczymy przez $(t0)$. (Mówi się czasami krótko, że logika to zbiór konsekwencji zbioru pustego; należy przez to rozumieć, że chodzi tu o pusty

zbiór Σ założeń dodatkowych, pozalogicznych, a nie pusty zbiór aksjomatów logicznych). Ponieważ w tym rozdziale nie będziemy rozważać innych relacji konsekwencji niż opisana tu relacja S , będziemy pisać $\Sigma \vdash \phi$ zamiast $\Sigma \vdash_S \phi$.

Zajmiemy się teraz twierdzeniem o dedukcji. Jednym z zastosowań twierdzenia o dedukcji jest ułatwienie znajdowania formalnych dowodów niektórych twierdzeń logiki.

Twierdzenie 3.1.7. (twierdzenie o dedukcji). *Niech Σ będzie zbiorem formuł, a ϕ i ψ niech będą formułami. Wówczas $\Sigma \cup \{\phi\} \vdash \psi$ wtedy i tylko wtedy, gdy $\Sigma \vdash \phi \rightarrow \psi$.*

Dowód. Niech $D = \langle D_1, \dots, D_n \rangle$ będzie dowodem formuły ψ w oparciu o zbiór $\Sigma \cup \{\phi\}$.

(i) Warunek wystarczający. Przez indukcję po długości dowodu pokażemy, że dla wszystkich i takich, że $1 \leq i \leq n$ prawdą jest, że $\Sigma \vdash \phi \rightarrow D_i$.

(a) Niech $i = 1$. Wówczas na mocy definicji dowodu formalnego $D_1 = \phi$, albo $D_1 \in \Sigma$, albo D_1 jest aksjomatem logicznym (czyli $D_1 \in Ax$).

Przypadek pierwszy: $D_1 = \phi$. Ponieważ udowodniliśmy wyżej, że dowolna formuła postaci $\phi \rightarrow \phi$ ma dowód w oparciu o zbiór Ax i MP , to znaczy $\vdash \phi \rightarrow \phi$, więc skoro $(\phi \rightarrow \phi) = (\phi \rightarrow D_1)$, to $\Sigma \vdash \phi \rightarrow D_1$.

Przypadek drugi: $D_1 \in \Sigma$. Wiadomo, że $(\phi \rightarrow (\psi \rightarrow \phi)) \in Ax$, więc $i(D_1 \rightarrow (\phi \rightarrow D_1)) \in Ax$, zatem stosując *Modus Ponens* stwierdzamy, że $\Sigma \vdash \phi \rightarrow D_1$.

Przypadek trzeci: $D_1 \in Ax$. Podobnie, skoro $(\phi \rightarrow (\psi \rightarrow \phi)) \in Ax$, więc $i(D_1 \rightarrow (\phi \rightarrow D_1)) \in Ax$, a że z założenia $D_1 \in Ax$, więc na mocy *Modus Ponens* $\Sigma \vdash \phi \rightarrow D_1$.

(b) Załóżmy teraz, że $\Sigma \vdash \phi \rightarrow D_k$ dla wszystkich $k < i$. Pokażemy, że $\Sigma \vdash \phi \rightarrow D_i$. Z definicji dowodu formalnego wnosimy, że są tu cztery możliwości: albo $D_i = \phi$, albo $D_i \in \Sigma$, albo $D_i \in Ax$, albo D_i powstaje z formuł wcześniejszych w ciągu D przez zastosowanie do nich reguły MP . W pierwszych trzech przypadkach dowodzimy, że $\Sigma \vdash \phi \rightarrow D_i$ tak samo, jak dla $i = 1$. Zostaje przypadek czwarty: D_i powstaje z formuł D_j, D_m , takich że $D_m = (D_j \rightarrow D_i)$, $m, j < i$. Założenie indukcyjne głosi w tym przypadku, że $\Sigma \vdash \phi \rightarrow (D_j \rightarrow D_i)$ oraz $\Sigma \vdash \phi \rightarrow D_j$. Wiadomo, że $(\phi \rightarrow (D_j \rightarrow D_i)) \rightarrow ((\phi \rightarrow D_j) \rightarrow (\phi \rightarrow D_i)) \in Ax$, stąd oczywiście $\Sigma \vdash (\phi \rightarrow (D_j \rightarrow D_i)) \rightarrow ((\phi \rightarrow D_j) \rightarrow (\phi \rightarrow D_i))$. Korzystamy teraz z założenia indukcyjnego i odrywamy dwa razy, stwierdzając w ten sposób, że $\Sigma \vdash \phi \rightarrow D_i$, co kończy tę część dowodu.

(ii) Warunek konieczny. Niech $\Sigma \vdash \phi \rightarrow \psi$. Zatem $\Sigma \cup \{\phi\} \vdash \phi \rightarrow \psi$. Dowód formalny D formuły $\phi \rightarrow \psi$ uzupełniamy, dodając na jego końcu kolejno formuły ϕ oraz ψ , uzyskując w ten sposób dowód dla formuły ψ .

Ten nowy ciąg D_1 jest dowodem dla ψ w oparciu o zbiór $\Sigma \cup \{\phi\}$, ponieważ ψ można uzyskać z $\phi \rightarrow \psi$ (ostatni element ciągu D) i ϕ (przedostatni element ciągu D_1) przez zastosowanie reguły odrywania. Q.E.D.

Konsekwencją twierdzenia o dedukcji dla logiki klasycznej jest następujące stwierdzenie. Wiadomo, że obok reguły *MP* zbiór twierdzeń systemu S jest zamknięty na stosowanie innych jeszcze reguł; reguły te zwie się regułami wtórnymi. Otóż z twierdzenia o dedukcji wynika, że każdej regule wtórnej, mającej postać

$$\frac{\phi_1, \dots, \phi_n}{\psi},$$

odpowiada twierdzenie logiki klasycznej, mające postać

$$(\phi_1) \wedge \dots \wedge (\phi_n) \rightarrow (\psi).$$

Zachodzi także zależność odwrotna: każdemu twierdzeniu logiki klasycznej postaci $(\phi_1) \wedge \dots \wedge (\phi_n) \rightarrow (\psi)$ odpowiada wtórna reguła wnioskowania, mająca postać

$$\frac{\phi_1, \dots, \phi_n}{\psi}.$$

3.2. Podstawowe twierdzenia logiki klasycznej

LEMAT 3.2.1 *Dla dowolnych formuł ϕ, ψ, χ następujące formuły są twierdzeniami przedstawionego wyżej systemu S :*

- (t1) $(\phi \rightarrow \psi) \rightarrow ((\psi \rightarrow \chi) \rightarrow (\phi \rightarrow \chi)),$
 (t2) $(\phi \rightarrow (\psi \rightarrow \chi)) \rightarrow (\psi \rightarrow (\phi \rightarrow \chi)).$

Dowód. Zacznijmy od (t1). Formuła ta znana jest jako prawo sylogizmu hipotetycznego bezkoniunkcyjnego. Ponieważ dowodzimy twierdzenia o postaci implikacji, skorzystamy tu z twierdzenia o dedukcji. Wystarczy więc założyć poprzednik implikacji i z tego założenia oraz aksjomatów logicznych wyprowadzić za pomocą reguły odrywania następnik implikacji, to jest z $\phi \rightarrow \psi$ wyprowadzić implikację $(\psi \rightarrow \chi) \rightarrow (\phi \rightarrow \chi)$. Druga z formuł też jest implikacją, toteż aby ją udowodnić, wystarczy dodać do założeń formułę $\psi \rightarrow \chi$ i wyprowadzić z niej oraz z formuły $\phi \rightarrow \psi$

formułę $\phi \rightarrow \chi$. Rozumując jeszcze raz w taki sam sposób, stwierdzamy ostatecznie, że aby dowieść formuły (t1), wystarczy założyć formuły $\phi \rightarrow \psi$, $\psi \rightarrow \chi$ oraz ϕ i wyprowadzić z nich formułę χ , korzystając z tych założeń i ewentualnie z aksjomatów logicznych. Krótko: wystarczy udowodnić, iż

$$\phi \rightarrow \psi, \psi \rightarrow \chi, \phi \vdash \chi$$

i zastosować twierdzenie o dedukcji. Dowód ten zapiszemy teraz skrótowo, pisząc w kolejnych wierszach najpierw numer formuły, samą formułę oraz komentarz, skąd się wzięła dana formuła.

(1)	$\phi \rightarrow \psi$	założenie
(2)	$\psi \rightarrow \chi$	założenie
(3)	ϕ	założenie
(4)	ψ	(1), (3), <i>MP</i>
(5)	χ	(2), (4), <i>MP</i> .

Zatem $\phi \rightarrow \psi, \psi \rightarrow \chi, \phi \vdash \chi$. Stosując twierdzenie o dedukcji, uzyskujemy stwierdzenie, że

$$\phi \rightarrow \psi, \psi \rightarrow \chi \vdash \phi \rightarrow \chi,$$

ponowne zastosowanie daje nam

$$\phi \rightarrow \psi \vdash (\psi \rightarrow \chi) \rightarrow (\phi \rightarrow \chi),$$

a trzecie zastosowanie daje nam wreszcie

$$\vdash (\phi \rightarrow \psi) \rightarrow ((\psi \rightarrow \chi) \rightarrow (\phi \rightarrow \chi)),$$

co kończy dowód faktu, że formuła (t1) jest twierdzeniem rozważanego rachunku.

Dowód (t2): Formuła (t2): $(\phi \rightarrow (\rightarrow \psi \rightarrow \chi)) \rightarrow (\psi \rightarrow (\phi \rightarrow \chi))$ jest znana jako prawo komutacji. Rozumując jak poprzednio, dowodzimy, że $(\phi \rightarrow (\psi \rightarrow \chi)), \psi, \phi \vdash \chi$ i korzystamy z twierdzenia o dedukcji. Zastosujmy tu konwencję zapisu dowodu, użytą w dowodzie (t1).

(1)	$\phi \rightarrow (\psi \rightarrow \chi)$	założenie
(2)	ψ	założenie
(3)	ϕ	założenie
(4)	$\psi \rightarrow \chi$	(1), (3), <i>MP</i>
(5)	χ	(2), (4), <i>MP</i> .

Tym sposobem zakończyliśmy dowód lematu. Q.E.D.

Na mocy twierdzenia o dedukcji obu tym twierdzeniom można przyporządkować reguły wtórne: regułę, którą nazwiemy regułą sylogizmu; oznaczymy ją przez *syl*

$$\frac{\phi \rightarrow \psi, \psi \rightarrow \chi}{\phi \rightarrow \chi},$$

a także regułę komutacji (*kom*)

$$\frac{\phi \rightarrow (\psi \rightarrow \chi)}{\psi \rightarrow (\phi \rightarrow \chi)}.$$

Zastosowanie tych reguł pozwoli uprościć niektóre z podawanych niżej dowodów.

Korzystając z (t1) możemy udowodnić prawo Dunsza Szkota.

LEMAT 3.2.2. Dla dowolnych formuł ϕ, ψ twierdzeniem systemu logiki S jest formuła

$$(t3) \quad \neg\phi \rightarrow (\phi \rightarrow \psi).$$

Dowód. Tym razem nie zastosujemy bezpośrednio twierdzenia o dedukcji, skorzystamy jednak z konwencji zapisu dowodu, użytej w poprzednim lemacie.

$$\begin{array}{ll} (1) & (\neg\psi \rightarrow \neg\phi) \rightarrow (\phi \rightarrow \psi), & \text{aksjomat A9} \\ (2) & \neg\phi \rightarrow (\neg\psi \rightarrow \neg\phi), & \text{aksjomat A1} \\ (3) & \neg\phi \rightarrow (\phi \rightarrow \psi). & (1), (2), \text{ syl.} \\ & & \text{Q.E.D.} \end{array}$$

LEMAT 3.2.3. Dla dowolnych formuł ϕ, ψ twierdzeniami systemu logiki S są formuły

$$\begin{array}{ll} (t4.1) & (\psi \rightarrow (\psi \rightarrow \chi)) \rightarrow (\phi \wedge \psi \rightarrow \chi), \\ (t4.2) & (\phi \wedge \psi \rightarrow \chi) \rightarrow (\phi \rightarrow (\psi \rightarrow \chi)), \\ (t4) & (\phi \rightarrow (\psi \rightarrow \chi)) \leftrightarrow (\phi \wedge \psi \rightarrow \chi), \\ (t5) & [(\phi \rightarrow \psi) \wedge \phi] \rightarrow \psi, \\ (t6) & (\phi \rightarrow (\psi \rightarrow (\phi \wedge \psi))). \end{array}$$

Formuła (t4.1) nosi nazwę prawa eksportacji, (t4.2) nosi nazwę prawa importacji; (t4) nazwę prawa importacji-eksportacji a (t5) to prawo tradycyjnie zwane *Modus Ponendo Ponens*.

Dowód. Podamy najpierw dowód (t4.1). Skorzystamy z twierdzenia o dedukcji i udowodnimy, że

$$(\phi \rightarrow (\psi \rightarrow \chi)), \phi \wedge \psi \vdash \chi.$$

(1)	$(\phi \rightarrow (\psi \rightarrow \chi))$	założenie
(2)	$\phi \wedge \psi$	założenie
(3)	$\phi \wedge \psi \rightarrow \phi$	aksjomat A3
(4)	$\phi \wedge \psi \rightarrow \psi$	aksjomat A4
(5)	ϕ	(2), (3), MP
(6)	ψ	(2), (4), MP
(7)	$\psi \rightarrow \chi$	(1), (5), MP
(8)	χ	(6), (7).

Dowód (t4.2): Udowodnimy najpierw, że $\phi, \psi \vdash \phi \wedge \psi$, to jest udowodnimy regułę wtórną, zwaną regułą dołączania koniunkcji (DK); zapisać można ją inaczej

$$\frac{\phi, \psi}{\phi \wedge \psi}$$

Regułę tę zastosujemy w dowodzie (t4.2).

(1)	ϕ	założenie
(2)	ψ	założenie
(3)	$(\phi \rightarrow \phi) \rightarrow ((\phi \rightarrow \psi) \rightarrow (\phi \rightarrow (\phi \wedge \psi)))$	aksjomat A5
(4)	$\phi \rightarrow \phi$	twierdzenie (t0)
(5)	$(\phi \rightarrow \psi) \rightarrow (\phi \rightarrow (\phi \wedge \psi))$	(3), (4), MP
(6)	$\psi \rightarrow (\phi \rightarrow \psi)$	aksjomat A1
(7)	$\phi \rightarrow \psi$	(2), (6), MP
(8)	$\phi \rightarrow (\phi \wedge \psi)$	(5), (6), MP
(9)	$\phi \wedge \psi$	(1), (8), MP.

Udowodnimy teraz, że $\phi \wedge \psi \rightarrow \chi, \phi, \psi \vdash \chi$.

(1)	$\phi \wedge \psi \rightarrow \chi$	założenie
(2)	ϕ	założenie
(3)	ψ	założenie
(4)	$\phi \wedge \psi$	(2), (3), reguła DK
(5)	χ	(1), (4), MP.

Co do dowodu formuły (t4), zauważmy, że, na mocy twierdzenia o dedukcji, aksjomatowi (A12) odpowiada następująca reguła wtórna:

$$\frac{\phi \rightarrow \psi, \psi \rightarrow \phi}{\phi \leftrightarrow \psi}$$

Korzystając z tej reguły, dostajemy natychmiast (t5) z (t4.1) i (t4.2).

Dowód *Modus Ponendo Ponens* (formuła (t5)) dostajemy, stosując prawo eksportacji do implikacji (t0) w wersji

$$(\phi \rightarrow \psi) \rightarrow (\phi \rightarrow \psi).$$

Natomiast (t6) uzyskujemy z reguły *DK* i twierdzenia o dedukcji. Q.E.D.

LEMAT 3.2.4. Dla dowolnej formuły ϕ twierdzeniami systemu S są formuły

$$(t7) \quad \neg\neg\phi \rightarrow \phi,$$

$$(t8) \quad \phi \rightarrow \neg\neg\phi.$$

Dowód (t7):

- | | |
|---|---------------|
| (1) $\neg\neg\phi \rightarrow (\neg\phi \rightarrow \neg\psi)$ | (t3) |
| (2) $(\neg\phi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \phi)$ | aksjomat A9 |
| (3) $\neg\neg\phi \rightarrow (\psi \rightarrow \phi)$ | (1), (2), syl |
| (4) $\psi \rightarrow (\neg\neg\phi \rightarrow \phi)$ | (3), kom. |

Wystarczy teraz zamiast ψ w całym dowodzie wziąć na przykład formułę $\phi \rightarrow \phi$; wówczas można oderwać $\phi \rightarrow \phi$ od (7), aby uzyskać dowodzoną formułę.

Dla ułatwienia zapisu dowodów wprowadzimy dodatkowy skrót. Na przykład (por. wiersz (2) dowodu (t8)), skrót A9, $\phi/\neg\neg\phi$, ψ/ϕ znaczy, że bierzemy aksjomat A9 w wersji różniącej się od podanej w spisie aksjomatów tym, że na miejscu ϕ występuje $\neg\neg\phi$, a na miejscu ψ występuje ϕ . Można to nazwać operacją „pseudopodstawienia”².

Dowód (t8):

- | | |
|---|---------------------------------------|
| (1) $(\neg\neg\neg\phi \rightarrow \neg\phi) \rightarrow (\phi \rightarrow \neg\neg\phi)$ | A9, $\phi/\neg\neg\phi$, ψ/ϕ |
| (2) $\neg\neg\neg\phi \rightarrow \neg\phi$ | (t7), $\phi/\neg\phi$ |
| (3) $\phi \rightarrow \neg\neg\phi$ | (1), (2), MP.
Q.E.D. |

Udowodnimy teraz dwie inne jeszcze niż aksjomat A9 wersje prawa transpozycji.

LEMAT 3.2.5. Dla dowolnych formuł ϕ , ψ twierdzeniami systemu S są formuły

$$(t9) \quad (\phi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \neg\phi),$$

$$(t10) \quad (\phi \rightarrow \psi) \rightarrow (\neg\psi \rightarrow \neg\phi).$$

² Takiego terminu używa na przykład T. Batóg w *Podstawach logiki*, op. cit., s. 124.

Dowód. Udowodnimy najpierw twierdzenie pomocnicze, tzn. formułę

$$(*) \quad (\phi \rightarrow \neg\psi) \rightarrow (\neg\neg\phi \rightarrow \neg\psi).$$

Dowód formuły (*):

(1)	$\phi \rightarrow \neg\psi$	założenie
(2)	$\neg\neg\phi$	założenie
(3)	$\neg\neg\phi \rightarrow \phi$	(t7)
(4)	ϕ	(2), (3), MP
(5)	$\neg\psi$	(1), (4), MP.

Dowód (t9):

(1)	$(\phi \rightarrow \neg\psi) \rightarrow (\neg\neg\phi \rightarrow \neg\psi)$	(*)
(2)	$(\neg\neg\phi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \neg\phi)$	A9, $\phi/\neg\phi$,
(3)	$(\phi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \neg\phi)$	(1), (2), syl.

Dowód (t10):

(1)	$\phi \rightarrow \psi$	założenie
(2)	$\psi \rightarrow \neg\neg\psi$	(t8)
(3)	$\phi \rightarrow \neg\neg\psi$	(1), (2), syl.
(4)	$(\phi \rightarrow \neg\neg\psi) \rightarrow (\neg\psi \rightarrow \neg\phi)$	(t9)
(5)	$\neg\psi \rightarrow \neg\phi$	(3), (4), MP. Q.E.D.

Twierdzeniu (10) przyporządkujemy regułę transpozycji, którą oznaczymy przez (*transp*); jej zastosowanie skróci niektóre z dowodów. Reguła ta ma postać następującą:

$$\frac{\phi \rightarrow \psi}{\neg\psi \rightarrow \neg\phi}.$$

Odnotujmy teraz twierdzenie pomocnicze:

LEMAT 3.2.6. Dla dowolnych formuł ϕ, ψ twierdzeniem systemu S jest formuła

$$(t11) \quad (\phi \rightarrow (\phi \rightarrow \psi)) \rightarrow (\phi \rightarrow \psi).$$

Dowód tego lematu jest prosty, gdy zastosuje się twierdzenie o dedukcji.

Udowodnimy teraz obie wersje prawa Claviusa.

LEMAT 3.2.7. Dla dowolnego ϕ twierdzeniem systemu S są formuły

$$(t12) \quad (\phi \rightarrow \neg\phi) \rightarrow \neg\phi,$$

$$(t13) \quad (\neg\phi \rightarrow \phi) \rightarrow \phi.$$

Dowód (t12):

- (1) $\phi \rightarrow (\neg\phi \rightarrow \psi)$ (t3), kom
- (2) $\phi \rightarrow (\neg\phi \rightarrow \neg(\phi \rightarrow \neg\phi))$ (1), $\psi/\neg(\phi \rightarrow \neg\phi)$
- (3) $\phi \rightarrow (\neg\phi \rightarrow \neg(\phi \rightarrow \neg\phi)) \rightarrow$
 $\rightarrow ((\phi \rightarrow \neg\phi) \rightarrow (\phi \rightarrow \neg(\phi \rightarrow \neg\phi)))$ A2, $\psi/\neg\phi$, $\chi/\neg(\phi \rightarrow \neg\phi)$
- (4) $((\phi \rightarrow \neg\phi) \rightarrow (\phi \rightarrow \neg(\phi \rightarrow \neg\phi)))$ (2), (3), MP
- (5) $(\phi \rightarrow \neg(\phi \rightarrow \neg\phi)) \rightarrow ((\phi \rightarrow \neg\phi) \rightarrow \neg\phi)$ (t9), $\psi/(\phi \rightarrow \neg\phi)$
- (6) $(\phi \rightarrow \neg\phi) \rightarrow ((\phi \rightarrow \neg\phi) \rightarrow \neg\phi)$ (4), (5), syl
- (7) $(\phi \rightarrow \neg\phi) \rightarrow \neg\phi$ (t11), $\phi/(\phi \rightarrow \neg\phi)$, (6), MP.

Dowód (t13):

- (1) $(\neg\phi \rightarrow \neg\neg\phi) \rightarrow \neg\neg\phi$ (t12), $\phi/\neg\phi$
- (2) $(\neg\phi \rightarrow \phi) \rightarrow (\neg\phi \rightarrow \neg\neg\phi)$ (t10)
- (3) $(\neg\phi \rightarrow \phi) \rightarrow \neg\neg\phi$ (1), (2), syl
- (4) $(\neg\phi \rightarrow \phi) \rightarrow \phi$ (3), (t7), MP.
Q.E.D.

Udowodnimy teraz jedno z praw de Morgana.

LEMAT 3.2.8. Dla dowolnych formuł ϕ, ψ twierdzeniami rachunku S są formuły

- (t14.1) $\neg(\phi \wedge \psi) \rightarrow (\neg\phi \vee \neg\psi)$,
- (t14.2) $(\neg\phi \vee \neg\psi) \rightarrow \neg(\phi \wedge \psi)$,
- (t14) $\neg(\phi \wedge \psi) \leftrightarrow (\neg\phi \vee \neg\psi)$.

Dowód (t14.1):

- (1) $\neg\phi \rightarrow \neg\phi \vee \neg\psi$ aksjomat A6
- (2) $(\neg\phi \rightarrow \neg\phi \vee \neg\psi) \rightarrow (\neg(\neg\phi \vee \neg\psi) \rightarrow \neg\neg\phi)$ (t10)
- (3) $\neg(\neg\phi \vee \neg\psi) \rightarrow \neg\neg\phi$ (1), (2), MP
- (4) $\neg(\neg\phi \vee \neg\psi) \rightarrow \phi$ (3), (t7), reguła syl
- (5) $\neg(\neg\phi \vee \neg\psi) \rightarrow \psi$ dowód jak dla (4),
- (6) $(\neg(\neg\phi \vee \neg\psi) \rightarrow \phi) \rightarrow ((\neg(\neg\phi \vee \neg\psi) \rightarrow \psi) \rightarrow$
 $\rightarrow (\neg(\neg\phi \vee \neg\psi) \rightarrow \phi \wedge \psi))$ aksjomat A5
- (7) $\neg(\neg\phi \vee \neg\psi) \rightarrow \phi \wedge \psi$ (6), (4), (5), MP
- (8) $(\neg(\neg\phi \vee \neg\psi) \rightarrow \phi \wedge \psi) \rightarrow$
 $\rightarrow (\neg(\phi \wedge \psi)) \rightarrow \neg\neg(\neg\phi \vee \neg\psi)$ (t10)
- (9) $\neg(\phi \wedge \psi) \rightarrow \neg\neg(\neg\phi \vee \neg\psi)$ (7), (8), MP
- (10) $\neg(\phi \wedge \psi) \rightarrow (\neg\phi \vee \neg\psi)$ (9), (t6), reguła syl.

Dowód (t14.2): Podamy go w skrócie.

- (1) $\phi \wedge \psi \rightarrow \phi$ aksjomat A3
- (2) $\phi \wedge \psi \rightarrow \psi$ aksjomat A4

- (3) $\neg\phi \rightarrow \neg(\phi \wedge \psi)$ (1), reguła *transp*
 (4) $\neg\psi \rightarrow \neg(\phi \wedge \psi)$ (2), reguła *transp*
 (5) $(\neg\phi \vee \neg\psi) \rightarrow \neg(\phi \wedge \psi)$ aksjomat A8, (3), (4), *MP*.

Twierdzenie (t14) dostajemy z (t14.1) i (t14.2), stosując regułę odpowiadającą aksjomatowi A12. Q.E.D.

Udowodnimy teraz prawo sprzeczności, tzn. formułę $\neg(\phi \wedge \neg\phi)$. Zauważmy najpierw, że na mocy prawa komutacji oraz eksportacji łatwo pokazać, że prawu Dunsza Szkota (formule (t3)) można nadać postać

$$(t3.1) \quad (\phi \wedge \neg\phi) \rightarrow \psi$$

dla dowolnych formuł ϕ, ψ .

LEMAT 3.2.9. Dla dowolnej formuły ϕ twierdzeniem systemu S jest formuła

$$(t15) \quad \neg(\phi \wedge \neg\phi).$$

Dowód:

- (1) $(\phi \wedge \neg\phi) \rightarrow \neg(\phi \rightarrow \phi)$ (t3.1)
 (2) $((\phi \wedge \neg\phi) \rightarrow \neg(\phi \rightarrow \phi)) \rightarrow ((\phi \rightarrow \phi) \rightarrow \neg(\phi \wedge \neg\phi))$ (t9)
 (3) $(\phi \rightarrow \phi) \rightarrow \neg(\phi \wedge \neg\phi)$ (1), (2), *MP*
 (4) $\neg(\phi \wedge \neg\phi)$ (t0), (3), *MP*.
 Q.E.D.

Udowodnienie prawa wyłączonego środka wymaga udowodnienia twierdzenia pomocniczego.

LEMAT 3.2.10. Dla dowolnych formuł ϕ, ψ, χ twierdzeniem systemu S jest formuła

$$(t16) \quad (\phi \rightarrow \psi) \rightarrow ((\chi \vee \phi) \rightarrow (\psi \vee \chi)).$$

Dowód: Oprzemy się na twierdzeniu o dedukcji. Mamy

- (1) $\phi \rightarrow \psi$ założenie
 (2) $\chi \vee \phi$ założenie
 (3) $\psi \rightarrow (\psi \vee \chi)$ aksjomat A6
 (4) $\phi \rightarrow (\psi \vee \chi)$ (1), (3), reguła *syl*
 (5) $\chi \rightarrow (\psi \vee \chi)$ aksjomat A7
 (6) $(\chi \rightarrow (\psi \vee \chi)) \rightarrow$
 $\rightarrow ((\phi \rightarrow (\psi \vee \chi)) \rightarrow ((\chi \vee \phi) \rightarrow (\psi \vee \chi)))$ aksjomat A8
 (7) $\psi \vee \chi$ (2), (4), (5), (6), trzy razy *MP*.
 Q.E.D.

Przejdźmy teraz do dowodu prawa wyłącznego środka.

LEMAT 3.2.11. Dla dowolnej formuły ϕ twierdzeniem jest formuła

$$(t17) \quad \phi \vee \neg\phi.$$

Dowód:

- (1) $\neg(\phi \wedge \neg\phi)$ (t15)
- (2) $\neg(\phi \wedge \neg\phi) \rightarrow (\neg\phi \vee \neg\neg\phi)$ (t14.1)
- (3) $\neg\phi \vee \neg\neg\phi$ (1), (2), MP
- (4) $(\neg\neg\phi \rightarrow \phi) \rightarrow ((\neg\phi \vee \neg\neg\phi) \rightarrow (\phi \vee \neg\phi))$ (t16)
- (5) $\phi \vee \neg\phi$ (t7), (2), (4), MP.
Q.E.D.

Udowodnimy teraz twierdzenia łączące implikację z alternatywą i negacją oraz z koniunkcją i negacją.

LEMAT 3.2.12. Dla dowolnych ϕ, ψ twierdzeniami są formuły

- (t18.1) $(\phi \rightarrow \psi) \rightarrow (\neg\phi \vee \psi),$
- (t18.2) $(\neg\phi \vee \psi) \rightarrow (\phi \rightarrow \psi),$
- (t18) $(\phi \rightarrow \psi) \leftrightarrow (\neg\phi \vee \psi),$
- (t19.1) $(\phi \rightarrow \psi) \rightarrow \neg(\phi \wedge \neg\psi),$
- (t19.2) $\neg(\phi \wedge \neg\psi) \rightarrow (\phi \rightarrow \psi),$
- (t19) $(\phi \rightarrow \psi) \leftrightarrow \neg(\phi \wedge \neg\psi).$

Dowód. Zaczniemy od dowodu (t18.2):

- (1) $\neg\phi \rightarrow (\phi \rightarrow \psi)$ (t3)
- (2) $\psi \rightarrow (\phi \rightarrow \psi)$ aksjomat A1
- (3) $(\neg\phi \rightarrow (\phi \rightarrow \psi)) \rightarrow$
 $\rightarrow ((\psi \rightarrow (\phi \rightarrow \psi)) \rightarrow ((\neg\phi \vee \psi) \rightarrow (\phi \rightarrow \psi)))$ aksjomat A8
- (4) $\neg\phi \vee \psi \rightarrow (\phi \rightarrow \psi)$ (1), (2), (3), MP.

Dowód (t18.1):

- (1) $\psi \rightarrow (\neg\phi \vee \psi)$ aksjomat A7
- (2) $(\psi \rightarrow (\neg\phi \vee \psi)) \rightarrow$
 $\rightarrow ((\phi \rightarrow \psi) \rightarrow (\phi \rightarrow (\neg\phi \vee \psi)))$ (t2), reguła kom
- (3) $(\phi \rightarrow \psi) \rightarrow (\phi \rightarrow (\neg\phi \vee \psi))$ (1), (2), MP
- (4) $\phi \rightarrow ((\phi \rightarrow \psi) \rightarrow (\neg\phi \vee \psi))$ (3), reguła kom
- (5) $\neg\phi \rightarrow (\neg\phi \vee \psi)$ aksjomat A6
- (6) $(\neg\phi \rightarrow (\neg\phi \vee \psi)) \rightarrow ((\phi \rightarrow \psi) \rightarrow (\neg\phi \rightarrow (\neg\phi \vee \psi)))$ aksjomat A1
- (7) $(\phi \rightarrow \psi) \rightarrow (\neg\phi \rightarrow (\neg\phi \vee \psi))$ (5), (6), MP

- (8) $\neg\phi \rightarrow ((\phi \rightarrow \psi) \rightarrow (\neg\phi \vee \psi))$ (7), reguła *kom*
 (9) $(\phi \vee \neg\phi) \rightarrow ((\phi \rightarrow \psi) \rightarrow (\neg\phi \vee \psi))$ aksjomat A8, (4), (8), *MP*
 (10) $(\phi \rightarrow \psi) \rightarrow (\neg\phi \vee \psi)$ (t17), (9), *MP*.

Do w ód (t19.1). Wystarczy udowodnić, że twierdzeniem systemu S jest formuła $(\neg\phi \vee \psi) \rightarrow \neg(\phi \wedge \neg\psi)$, to jest wariant prawa de Morgana i zastosować regułę sylogizmu do (t18.1).

Do w ód (t19.2). Wystarczy udowodnić implikację odwrotną do występującej w poprzednim dowodzie, tzn. implikację $\neg(\phi \wedge \neg\psi) \rightarrow (\neg\phi \vee \psi)$ i zastosować regułę sylogizmu do (t18.2).

Twierdzenia: (t18) i (t19) dostajemy z twierdzeń (t18.1), (t18.2) oraz (t19.1) i (t19.2), stosując do nich regułę odpowiadającą aksjomatowi A12.
 Q.E.D.

Czytelnik zechce teraz samodzielnie udowodnić jeszcze kilka następujących twierdzeń.

LEMAT 3.2.13. *Dla dowolnych ϕ, ψ, χ twierdzeniami systemu S są następujące formuły:*

- (t20) $\phi \vee \psi \leftrightarrow \psi \vee \phi,$
 (t21) $\phi \wedge \psi \leftrightarrow \psi \wedge \phi,$
 (t22) $\neg(\phi \vee \psi) \leftrightarrow (\neg\phi \wedge \neg\psi),$
 (t23) $\phi \wedge (\psi \vee \chi) \leftrightarrow (\phi \wedge \psi) \wedge (\phi \wedge \chi),$
 (t24) $(\phi \rightarrow \psi) \leftrightarrow (\phi \leftrightarrow (\phi \wedge \psi)).$

Dla opisywanego systemu S zachodzi twierdzenie o pełności. Odnotujmy tu najprostszą jego wersję. Poprzedzimy ją jednak krótkim wyjaśnieniem.

Czytelnik, który przestudiuje dokładniej informacje o algebrach Boole'a, podane w niniejszym podręczniku, zauważy zapewne, że tabelki dla spójników koniunkcji, alternatywy i negacji można interpretować jako działania przekroju, sumy i dopełnienia w dwuelementowej algebrze Boole'a. Opisane w rozdziale 1 pojęcie wartościowania, to jest przyporządkowywania zmiennym zdaniowym elementów 1 i 0 prowadzące do tabelkowej metody rozstrzygalności, było w istocie wartościowaniem formuł rachunku zdań w dwuelementową algebrę Boole'a. Tautologią, jak pamiętamy, była formuła, która uzyskuje w tej algebrze wartość 1. Najprostszą wersją twierdzenia o pełności jest następująca:

TWIERDZENIE 3.2.14 (twierdzenie o pełności systemu S) *Dla dowolnej formuły ϕ , $\vdash_S \phi$ wtedy i tylko wtedy, gdy przy dowolnym wartościowaniu V zmiennych występujących w formule ϕ w dwuelementową algebrę Boole'a, zachodzi równość $V(\phi) = 1$.*

Zadania

1. Korzystając z twierdzenia o dedukcji, udowodnić, że dla dowolnych ϕ , ψ , χ i θ twierdzeniami systemu S są formuły

- a) $\phi \rightarrow ((\phi \rightarrow \psi) \rightarrow \psi)$,
- b) $(\phi \rightarrow \psi) \rightarrow (\phi \rightarrow (\phi \rightarrow \psi))$,
- c) $(\phi \rightarrow \psi) \rightarrow ((\chi \rightarrow \phi) \rightarrow (\chi \rightarrow \psi))$,
- d) $(\phi \rightarrow \psi) \rightarrow ((\psi \rightarrow \chi) \rightarrow ((\chi \rightarrow \theta) \rightarrow (\phi \rightarrow \theta)))$.

2. Korzystając z twierdzenia o dedukcji i udowodnionych wyżej twierdzeń, wykazać, że dla dowolnych ϕ , ψ , χ twierdzeniami systemu S są następujące formuły:

- a) $(\phi \rightarrow \psi) \wedge (\psi \rightarrow \chi) \rightarrow (\phi \rightarrow \chi)$,
- b) $\phi \rightarrow (\phi \wedge \phi)$,
- c) $(\phi \rightarrow \psi) \wedge (\chi \rightarrow \neg\psi) \rightarrow (\chi \rightarrow \neg\phi)$,
- d) $[(\phi \rightarrow \psi) \wedge \neg\psi] \rightarrow \neg\phi$.

3. Udowodnić, że dla dowolnych ϕ , ψ , χ twierdzeniami systemu S są następujące formuły:

- a) $\phi \vee \psi \leftrightarrow \psi \vee \phi$,
- b) $\phi \wedge \psi \leftrightarrow \psi \wedge \phi$,
- c) $\neg(\phi \vee \psi) \leftrightarrow (\neg\phi \wedge \neg\psi)$,
- d) $\phi \wedge (\psi \vee \chi) \leftrightarrow (\phi \wedge \psi) \vee (\phi \wedge \chi)$,
- e) $(\phi \rightarrow \psi) \leftrightarrow (\phi \leftrightarrow (\phi \wedge \psi))$.

Rozdział 4

Elementy rachunku predykatów

4.1. Wprowadzenie

Przeprowadźmy następujące rozumowanie:

Każdy człowiek jest śmiertelny.
Sokrates jest człowiekiem.

Zatem: Sokrates jest śmiertelny.

Zastosujmy tu metodę badania niezawodności rozumowań, opisaną w rozdziale poprzednim. Schematem pierwszej przesłanki, zapisanym w języku rachunku zdań, będzie p , bo z punktu widzenia rachunku zdań jest to zdanie proste; schematem drugiej przesłanki będzie q , a schematem wniosku będzie r . Tak więc schemat tego rozumowania ma postać

$$\frac{p}{\frac{q}{r}}$$

Łatwo zauważyć, że nie jest to schemat wnioskowania niezawodnego, bo formuła

$$p \wedge q \rightarrow r$$

nie jest tautologią. Nasuwa się jednak nieodparte wrażenie, że wnioskowanie tu jest niezawodne: że jest uzasadnione przez to, iż z przesłanek wynika tu wniosek. Rodzi się więc przypuszczenie, że język rachunku zdań jest za mało precyzyjny, by w jego ramach uzasadnić niezawodność tego wnioskowania. Przypuszczenie to jest słuszne; do pokazania, że wnioskowanie to jest niezawodne, niezbędny jest jednak bardziej wyrafinowany rachunek logiczny – rachunek predykatów, zwany niekiedy rachunkiem kwantyfikatorów.

4.2. Język rachunku predykatów

W języku potocznym, a także w języku matematyki, odróżnia się nazwy indywidualne od nazw generalnych. Nazwy indywidualne to takie, które nadają się na podmiot zdania podmiotowo-orzecznikowego, to jest zdania postaci „ a jest S ”¹, a nazwy generalne to nazwy nadające się na orzecznik w takim zdaniu. Tak więc nazwami indywidualnymi będą nazwy: Witold Kowalski, π , 0, Polskie Towarzystwo Matematyczne, a nazwami generalnymi nazwy: prawnik, liczba niewymierna, liczba naturalna, stowarzyszenie mające osobowość prawną.

Predykatami jednoargumentowymi są wyrażenia, które w połączeniu z jedną nazwą indywidualną tworzą zdania. Przykładem takiego predykatu będzie każda nazwa generalna poprzedzona słowem „jest”, np. „jest prawnikiem” (po dodaniu nazwy indywidualnej mamy np. zdanie: „Witold Kowalski jest prawnikiem”), czy „jest liczbą niewymierną” (podobnie: „ π jest liczbą niewymierną”).

Predykatami dwuargumentowymi są wyrażenia tworzące zdania, gdy uzupełnić je dwiema nazwami indywidualnymi. Przykładami są: „jest starszy od”, „ma więcej mieszkańców niż”, „jest podobny do” czy „jest mniejszy lub równy” (symbolicznie: \leq).

Ogólnie, predykatami n -argumentowymi są wyrażenia tworzące zdania po uzupełnieniu ich n nazwami indywidualnymi. W języku naturalnym można znaleźć predykaty trójargumentowe (np. „... leży między ... a ...”), czteroargumentowe (np. „sojusz między ... a ... przetrwał dłużej niż sojusz między ... a ...”, „iloczyn liczb ..., ... i ... jest mniejszy od liczby ...”), trudno jednak o przykłady predykatów więcej niż czteroargumentowych w języku naturalnym, które nie brzmiałyby sztucznie.

Wróćmy do nazw. Nazwy indywidualne nie muszą być proste, jak nazwa: „Gauss”, π czy e . Mogą być też złożone, jak: „ojciec Gaussa”, $\sin \pi$ czy $\arctg \sin e$. W języku rachunku predykatów nazwy takie nazywa się termami, a wyrażenia tworzące bardziej skomplikowane nazwy z nazw prostszych zwie się tradycyjnie symbolami funkcyjnymi, choć powstające z ich pomocą nazwy złożone nie muszą wyznaczać zależności funkcyjnych. Tak więc mamy symbole funkcyjne jednoargumentowe („ojciec ...”, „starszy brat ...”, „wielbiciel ...”, symbole wszystkich funkcji jednoargumentowych, jak \sin , \sinh itd.), symbole funkcyjne dwuargumen-

¹ Przypominamy, że w zdaniu postaci „ a jest S ” wyrażenie reprezentowane przez literę a jest podmiotem, a reprezentowane przez S – orzecznikiem.

towe („ojciec ... lub matka ...”, $+$, \cdot , \cup , \cap) i ogólnie symbole funkcyjne n -argumentowe.

Obok formuł, które reprezentują dowolne predykaty i termy, język rachunku predykatów zawiera kwantyfikatory. Są to symbole zastępujące wyrażenia „dla każdego ...” (tzw. duży kwantyfikator, zapisywany jako \forall) i „istnieje ...” lub „dla pewnego ...” (tzw. mały kwantyfikator, zapisywany jako \exists). Kwantyfikator duży zwany jest też ogólnym albo generalnym, a mały – szczegółowym albo egzystencjalnym².

Predykaty będziemy zapisywać za pomocą symboli P_k^n , gdzie górny indeks n wskazuje liczbę argumentów danego predykatu, a dolny wskaźnik k mówi o tym, że jest to predykat n -argumentowy k -ty z kolei. Podobnie, za pomocą symboli postaci F_i^m zapisywać będziemy symbole funkcyjne.

DEFINICJA 4.2.1. *Następujące symbole są znakami języka rachunku predykatów:*

a_1, a_2, a_3, \dots	stałe indywiduowe
x_1, x_2, x_3, \dots	zmiennie indywiduowe
$P_1^1, P_2^1, P_3^1, \dots$	predykaty jednoargumentowe
$P_1^2, P_2^2, P_3^2, \dots$	predykaty dwuargumentowe
$P_1^3, P_2^3, P_3^3, \dots$	predykaty trójargumentowe
.....	
$P_1^n, P_2^n, P_3^n, \dots$	predykaty n -argumentowe
.....	
$F_1^1, F_2^1, F_3^1, \dots$	symbole funkcyjne jednoargumentowe
$F_1^2, F_2^2, F_3^2, \dots$	symbole funkcyjne dwuargumentowe
$F_1^3, F_2^3, F_3^3, \dots$	symbole funkcyjne trójargumentowe
.....	
$F_1^n, F_2^n, F_3^n, \dots$	symbole funkcyjne n -argumentowe
.....	
$\neg, \wedge, \vee, \rightarrow, \leftrightarrow$	spójniki logiczne
\forall, \exists	kwantyfikatory
$()$,	znaki pomocnicze: nawiasy i przecinek.

DEFINICJA 4.2.2. (i) *Każda zmienna indywiduowa i stała indywiduowa jest termem.*

(ii) *Jeśli $\alpha_1, \dots, \alpha_n$ są termami, to $F_k^n(\alpha_1, \dots, \alpha_n)$ jest termem (dla dowolnych n i k).*

² W literaturze używane są inne jeszcze zapisy kwantyfikatorów. Duży kwantyfikator zapisywany bywa następująco: $\bigwedge, \Pi, (x)$, a mały za pomocą symboli $\bigvee, \Sigma, (Ex)$.

(iii) Nie ma innych termów poza zmiennymi indywidualowymi, statycznymi indywidualowymi i takimi, które powstają na mocy reguły (ii).

DEFINICJA 4.2.3. Formułą zdaniową atomową jest każde wyrażenie postaci $P_k^n(\alpha_1, \dots, \alpha_n)$, gdzie $\alpha_1, \dots, \alpha_n$ są dowolnymi termami.

DEFINICJA 4.2.4. (i) Każda formuła zdaniowa atomowa jest formułą zdaniową rachunku predykatów.

(ii) Jeśli ϕ, ψ są formułami zdaniowymi języka rachunku predykatów, to $\neg(\phi)$, $(\phi) \wedge (\psi)$, $(\phi) \vee (\psi)$, $(\phi) \leftrightarrow (\psi)$, $(\phi) \rightarrow (\psi)$, $\forall x_i(\phi)$ i $\exists x_j(\phi)$ są formułami zdaniowymi języka rachunku predykatów.

(iii) Nie ma innych formuł zdaniowych języka rachunku predykatów poza formułami atomowymi i takimi formułami, które powstają dzięki zastosowaniu reguły (ii).

DEFINICJA 4.2.5. Jeśli formuła ma postać $\forall x_i(\phi)$ lub $\exists x_i(\phi)$, to mówimy, że odpowiedni kwantyfikator wiąże zmienną x_i .

Podobnie jak w przypadku rachunku zdań, pomija się indeksy, pisząc x zamiast x_1 , y zamiast x_2 , z zamiast x_3 itd.

Przykładem formuły zdaniowej atomowej będzie np. $\sin x \leq 1$ czy też $x \cap y \subseteq x \cup y$.

Dalej, predykaty dwuargumentowe w matematyce często pisze się między termami, a nie przed termami, jak to widać z podanych właśnie przykładów. Innymi przykładami takich formuł zdaniowych będą: $\forall x(y \leq z \rightarrow x + y \leq x + z)$ czy $\exists x(x \leq |y|)$.

DEFINICJA 4.2.6. Wyrażenie ϕ w formule $\exists x(\phi)$ i w $\forall y(\phi)$ nazywamy zasięgiem odpowiedniego kwantyfikatora.

Czytelnik zechce wskazać zasięg kwantyfikatorów w formule

$$\forall x(P_1^1(x) \rightarrow \exists y(P_1^2(x, y) \vee \exists z(P_3^1(z))))$$

i w formule

$$\forall x(0 \leq x \rightarrow \exists y(0 \leq x + y)).$$

Czasem, kiedy wiadomo, jaki jest zasięg kwantyfikatora, nawiasów się nie używa; zamiast więc $\exists x(\forall y(x \leq |y|))$ pisze się po prostu $\exists x \forall y(x \leq |y|)$.

Definicję zmiennej związanej poprzedzimy następującą uwagą. Zgodnie z definicją formuły zdaniowej, poprawnie zbudowana będzie np. formuła $\forall x(y = y)$; poprzedzać kwantyfikatorem wiążącym zmienną x_i można

bowiem formuły nie zawierające zmiennej x_i . Zmienną, która występuje bezpośrednio po symbolu kwantyfikatora, uznamy za zmienną związaną, choćby nawet nie występowała w zasięgu tego kwantyfikatora.

DEFINICJA 4.2.7. *Zmienna x_i występująca w danym miejscu w formule zdaniowej jest w tym miejscu związana wtedy i tylko wtedy, gdy występuje w zasięgu kwantyfikatora wiążącego x_i lub jest zmienną wiązaną przez jakiś kwantyfikator. Zmienna występująca w danej formule jest związana w tej formule, gdy jest związana w każdym miejscu, w którym występuje w tej formule.*

Jeśli zmienna występująca w danej formule nie jest związana w danej formule, nazywamy ją zmienną wolną.

DEFINICJA 4.2.8. *Zdaniem języka rachunku predykatów nazywamy formułę zdaniową nie zawierającą żadnych zmiennych wolnych.*

Czytelnik zechce zauważyć, że w formule

$$P_1^1(x) \vee \exists x \forall z P_1^2(x, y)$$

zmienna x jest wolna na jednym miejscu, a na drugim związana, zmienna z jest związana w tej formule, natomiast zmienna y jest wolna w całej tej formule.

DEFINICJA 4.2.9. *Tautologią rachunku predykatów albo prawem rachunku predykatów jest formuła zdaniowa rachunku predykatów, prawdziwa przy dowolnym rozumieniu występujących w niej predykatów, symboli funkcyjnych, stałych indywidualnych i zmiennych.*

Przykładami tautologii będą w szczególności wszystkie formuły, powstałe z tautologii rachunku zdań poprzez konsekwentne podstawienie formuł zdaniowych rachunku predykatów za zmienne zdaniowe, np. z tautologii $p \rightarrow p$ uzyskujemy tautologie

$$P_1^1(y) \rightarrow P_1^1(y),$$

$$\forall x (P_1^2(x, y) \wedge P_3^1(y)) \rightarrow \forall x (P_1^2(x, y) \wedge P_3^1(y))$$

itd. Istnieją także specyficzne tautologie rachunku predykatów, na przykład formuła

$$\neg \forall x \phi(x) \leftrightarrow \exists x \neg \phi(x).$$

Listę przykładów tautologii podamy niżej.

Niezbędne są tu następujące uwagi:

1. Niekiedy predykat „=” (znak równości) jest uznawany za spójnik logiczny. Wyróżnia się go wtedy wśród pozostałych spójników języka rachunku predykatów jako predykat specyficzny i charakteryzuje specjalnymi aksjomatami. Taką wersję rachunku predykatów nazywa się *rachunkiem predykatów z identycznością*.

2. W scharakteryzowanym wyżej języku rachunku predykatów kwantyfikatory wiążą zmienne indywidualne; taki rachunek nazywa się *rachunkiem predykatów I rzędu*. Można jednak rozważać wersję rachunku predykatów, w której dopuszcza się obok kwantyfikacji zmiennych indywidualnych także kwantyfikowanie predykatów jednoargumentowych (np. reprezentujących nazwy zbiorów) czy więcej argumentowych (np. reprezentujących nazwy relacji). Rachunek taki nazywa się *rachunkiem predykatów II rzędu*.

3. Inaczej niż rachunek zdań ze swoją metodą zero-jedynkową, rachunek predykatów jest *nierozstrzygalny*. Nie istnieje (jeśli matematyka jest niesprzeczna) żadna prosta, mechaniczna, efektywna metoda pozwalająca w skończonej liczbie z góry przewidzianych kroków orzekać o dowolnej formule języka rachunku predykatów, czy formuła ta jest, czy nie jest tautologią rachunku predykatów. Alonzo Church³ udowodnił, że metody takiej nie ma.

4. Można jednak (i to uczyniono) zaksjomatyzować rachunek predykatów i udowodnić, że z podanego zbioru aksjomatów da się wyprowadzić wszystkie i tylko tautologie rachunku predykatów. Można więc wyprowadzić jedne prawa rachunku predykatów z innych i w ten sposób dochodzić do nowych praw rachunku predykatów. Ujęcia aksjomatyczne są przedstawiane we wszystkich bardziej zaawansowanych podręcznikach logiki matematycznej⁴, skrótowe ujęcie zawiera też paragraf 7 tego rozdziału.

4.3. Formułowanie wypowiedzi w języku rachunku predykatów

Zajmiemy się teraz schematami zdań, zapisywanymi w języku rachunku predykatów. Z uwagi na to, iż, jak zobaczymy, w rachunku predykatów można bardzo dokładnie oddać strukturę wewnętrzną zdania, będziemy

³ Alonzo Church (1903–1995), logik amerykański, udowodnił w 1936 roku twierdzenie o nierozstrzygalności rachunku predykatów I rzędu.

⁴ Np. T. Batóg, *Podstawy logiki*, op. cit.

mówić nie o zapisie schematów zdań, lecz po prostu o zapisie zdań języka matematyki czy języka potocznego w języku rachunku predykatów.

Zacznijmy od zdania

„Euklides jest matematykiem”.

Nazwa „matematyk” to nazwa generalna, więc, jak pamiętamy, zwrot „- jest matematykiem” będzie predykatem jednoargumentowym. Niech więc symbol $P_1^1(-)$ będzie skrótem dla predykatu „- jest matematykiem”, a stała indywidualowa a_1 skraca nazwę indywidualną „Euklides”. Wobec tego rozważane zdanie można zapisać jako

$$P_1^1(a_1).$$

Wprowadzając stosowne skróty, można podobnie zapisać zdania proste, takie jak „ π jest liczbą niewymierną” czy „ e jest podstawą logarytmów naturalnych”; π i e są stałymi nazwowymi.

Niech następnym zdaniem będzie

„Każdy człowiek jest matematykiem”.

Niech symbol $P_2^1(\dots)$ będzie skrótem dla predykatu „... jest człowiekiem” i jak wyżej, $P_1^1(-)$ będzie skrótem dla predykatu „- jest matematykiem”. Zdanie to można zapisać w postaci

$$\forall x (P_2^1(x) \rightarrow P_1^1(x)).$$

Rozpatrzmy następne zdanie

„Niektórzy ludzie są matematykami”.

Korzystając z wprowadzonych właśnie skrótów, zdanie to można zapisać jako

$$\exists x (P_2^1(x) \wedge P_1^1(x)),$$

a zdanie

„Niektórzy ludzie nie są matematykami”

można wtedy zapisać jako

$$\exists x (P_2^1(x) \wedge \neg P_1^1(x)).$$

W zdaniach języka potocznego, a także w formułach zdaniowych języka matematyki, kwantyfikatory występują nie tylko na początku wypowiedzi,

ale także wewnątrz niej, jak w przykładach: „Istnieje matematyk, znający wszystkie działy matematyki”, „Ka ż d y człowiek ma jaki ś ta-
lent”, „Dla ka ż d e j liczby naturalnej istnieje liczba od niej większa”.
Na marginesie zauważmy, że wiele wypowiedzi języka potocznego jest wie-
loznacznych z uwagi na brak kwantyfikatorów⁵.

Zapiszmy w języku rachunku predykatów podane wyżej przykłady.

Korzystając z wprowadzonych wyżej skrótów oraz wprowadzając skrót $P_1^2(*, **)$ dla dwuargumentowego predykatu „* zna **” oraz skrót $P_3^1(-)$ dla predykatu „- jest działem matematyki”, zdanie „Istnieje matematyk, znający wszystkie działy matematyki” zapisujemy następująco:

$$\exists x (P_1^1(x) \wedge \forall y (P_3^1(y) \rightarrow P_1^2(y, x))).$$

Dla zapisu zdania „Ka ż d y człowiek ma jakiś talent” przyjmiemy wprowadzony wyżej skrót dla zwrotu „- jest człowiekiem” oraz wprowadzimy dwa nowe skróty: $P_2^2(\sim, \approx)$ dla dwuargumentowego predykatu „ \sim ma \approx ” oraz $P_4^1(|)$ dla predykatu „| jest talentem”; zdanie to ma wówczas postać

$$\forall x (P_2^1(x) \rightarrow \exists y (P_4^1 \wedge P_4^2(x, y))).$$

Czasem, dla większej przejrzystości zapisu, warto używać innego zapisu, nie nawiązującego wprost do podanych wyżej symboli predykatywnych. Tak więc predykat „- jest człowiekiem” można zapisywać jako „C(-)”, „ \sim ma \approx ” jako $M(\sim, \approx)$, a „| jest talentem” jako $T(|)$. Analizowane zdanie miałyby teraz bardziej czytelny, równoważny zapis

$$\forall x (C(x) \rightarrow \exists y (T(y) \wedge M(x, y))).$$

Wreszcie ostatni przykład zapiszemy, używając standardowej notacji matematycznej; wprowadzimy tylko skrót $N(\dots)$ dla predykatu „ \dots jest liczbą naturalną”. Zdanie: „Dla ka ż d e j liczby naturalnej istnieje liczba od niej większa” ma postać

$$\forall x (N(x) \rightarrow \exists y (N(y) \wedge x \leq y)).$$

Inne przykłady, których zapisanie w języku rachunku predykatów dla nabrania wprawy zalecamy, znajdzie Czytelnik na liście zadań do tego rozdziału.

⁵ Np. w wypowiedzi: „Polscy matematycy rozwijają nowe kierunki matematyki” nie wiadomo, czy chodzi o wszystkich polskich matematyków, czy o niektórych i czy o wszystkie nowe kierunki, czy o niektóre. Są tu więc następujące możliwości: „Ka ż d y polski matematyk rozwija ka ż d y nowy kierunek”, „Ka ż d y polski matematyk rozwija ja-
kiś nowy kierunek”, „Niektórzy polscy matematycy rozwijają wszystkie nowe kierunki”
i „Niektórzy polscy matematycy rozwijają jakieś nowe kierunki”.

4.4. Przykłady tautologii rachunku predykatów

Przyjmijmy tu następującą umowę: litery ϕ, ψ, χ, ϕ_1 będą teraz reprezentować dowolne formuły zdaniowe języka rachunku predykatów. Pisząc $\phi(x), \psi(x, y)$ itp., zaznaczamy, że formuły ϕ, ψ itd. zawierają zmienne wolne x czy x, y . Dalej, przez $\phi(x/\alpha)$ oznaczmy formułę ϕ , w której na miejsce zmiennej wolnej x podstawiono – wszędzie tam, gdzie x jest wolna – formułę nazwową (tj. zmienną lub stałą indywidualową) α ; jeśli α jest stałą a , to zamiast $\phi(x/a)$ piszemy niżej $\phi(a)$.

TWIERDZENIE 4.4.1. *Następujące formuły są tautologiami rachunku predykatów I rzędu:*

$\forall x\phi(x) \leftrightarrow \forall y\phi(x/y)$	o ile y nie występuje w $\phi(x)$ jako zmienna wolna
$\exists x\phi(x) \leftrightarrow \exists y\phi(x/y)$	o ile y nie występuje w $\phi(x)$ jako zmienna wolna
$\forall x\phi(x) \rightarrow \phi(x)$	prawo zwane <i>dictum de omni</i>
$\forall x\phi(x) \rightarrow \phi(a)$	prawo także zwane <i>dictum de omni</i>
$\phi(x) \rightarrow \exists x\phi(x)$	prawo zwane <i>dictum de sigulo</i>
$\phi(a) \rightarrow \exists x\phi(x)$	inna postać <i>dictum de singulo</i>
$\forall x\phi(x) \rightarrow \exists x\phi(x)$ ⁶ .	

Drugą ważną grupą są prawa De Morgana:

$$\neg\forall x\phi(x) \leftrightarrow \exists x\neg\phi(x)$$

$$\neg\exists x\phi(x) \leftrightarrow \forall x\neg\phi(x).$$

Trzecią grupę stanowią prawa rozdzielności:

$\forall x(\phi(x) \wedge \psi(x)) \leftrightarrow \forall x\phi(x) \wedge \forall x\psi(x)$	prawo rozdzielności dużego kwantyfikatora względem koniunkcji
$\exists x(\phi(x) \vee \psi(x)) \leftrightarrow \exists x\phi(x) \vee \exists x\psi(x)$	prawo rozdzielności małego kwantyfikatora względem alternatywy
$\forall x\phi(x) \vee \forall x\psi(x) \rightarrow \forall x(\phi(x) \vee \psi(x))$	prawo rozdzielności dużego kwantyfikatora względem alternatywy
$\exists x(\phi(x) \wedge \psi(x)) \rightarrow \exists x\phi(x) \wedge \exists x\psi(x)$	prawo rozdzielności małego kwantyfikatora względem koniunkcji

⁶ Podane tu tautologie, w których mamy do czynienia z podstawianiem, można uogólnić w taki sposób, aby za zmienną podstawiać term, niekoniecznie będący zmienną czy stałą; niezbędne są jednak wtedy pewne ograniczenia dotyczące podstawiania. Takie ujęcia są prezentowane w podręcznikach logiki matematycznej. Por. np. T. Batóg, *Podstawy logiki*, op.cit.

$\forall x (\phi(x) \rightarrow \psi(x)) \rightarrow (\forall x \phi(x) \rightarrow \forall x \psi(x))$	prawo rozdzielności dużego kwantyfikatora względem implikacji
$\forall x (\phi(x) \rightarrow \psi(x)) \rightarrow (\exists x \phi(x) \rightarrow \exists x \psi(x))$	prawo rozdzielności małego kwantyfikatora względem implikacji
$\forall x (\phi(x) \rightarrow \psi(x)) \wedge \phi(x/a) \rightarrow \psi(x/a).$	

Ostatnia grupa to prawa przestawiania kwantyfikatorów:

$\forall x \forall y \phi(x, y) \leftrightarrow \forall y \forall x \phi(x, y)$	prawo przestawiania dużych kwantyfikatorów
$\exists x \exists y \phi(x, y) \leftrightarrow \exists y \exists x \phi(x, y)$	prawo przestawiania małych kwantyfikatorów
$\exists x \forall y \phi(x, y) \rightarrow \forall y \exists x \phi(x, y)$	prawo przestawiania dużego i małego kwantyfikatora.

Zwracamy uwagę na to, że jeśli w powyższym spisie tautologii formuła będąca tautologią ma postać implikacji, to implikacja w drugą stronę nie jest tautologią.

4.5. Kwantyfikatory o ograniczonym zakresie

W przedstawionych wyżej przykładach tautologii zmienna wiązana przez kwantyfikator przebiegać może nazwy dowolnych obiektów. Czasem jednak warto przyjąć, że bierze się pod uwagę tylko obiekty z ustalonego wcześniej zbioru. Zrobić to można na dwa sposoby. Po pierwsze, zawiadomić czytelnika w komentarzu do rozważań, że dalej rozważa się tylko obiekty z ustalonego zbioru. Po drugie, za kwantyfikatorem⁷ zamiast samej zmiennej umieścić warunek, który ma spełnić zmienna. Sposoby te nie są rozłączne: w matematyce na ogół używa się ich jednocześnie. Tak więc np. ogranicza się rozważania do liczb jakiegoś rodzaju (naturalnych, rzeczywistych czy zespolonych), a pod kwantyfikatorem umieszcza się jakiś warunek, jaki mają spełniać te liczby.

Formalnie wprowadza się następujące skróty:

zamiast

$$\forall x (\phi(x) \rightarrow \psi(x))$$

pisze się

$$\forall (\phi(x)) (\psi(x)),$$

⁷ Gdy używa się symbolu \wedge czy \vee , to pod kwantyfikatorem.

a zamiast

$$\exists x (\phi(x) \wedge \psi(x))$$

pisze się

$$\exists (\phi(x)) (\psi(x)).$$

Założmy teraz, że przedmiotem naszego zainteresowania są liczby rzeczywiste, a symbole n, n_0 reprezentują nazwy liczb naturalnych. Formułę „ciąg $\{a_n\}$ jest zbieżny do granicy g ” można teraz zapisać (opuszczając nawiasy dotyczące zasięgu kwantyfikatorów) za pomocą kwantyfikatorów o ograniczonym zakresie następująco:

$$\forall(\varepsilon > 0) \exists n_0 \forall(n > n_0) (|a_n - g| < \varepsilon),$$

a formułę „ s jest punktem skupienia ciągu $\{a_n\}$ ” następująco:

$$\forall(\varepsilon > 0) \forall n_0 \exists(n > n_0) (|a_n - s| < \varepsilon).$$

Czytelnik zechce zapisać powyższe definicje, eliminując kwantyfikatory o ograniczonym zakresie.

Warto zauważyć, że dla kwantyfikatorów o ograniczonym zakresie obowiązują zwykle prawa De Morgana, to jest

$$\neg \forall (\phi(x)) (\psi(x)) \leftrightarrow \exists (\phi(x)) (\neg \psi(x))$$

oraz

$$\neg \exists (\phi(x)) (\psi(x)) \leftrightarrow \forall (\phi(x)) (\neg \psi(x)).$$

Można obrazowo powiedzieć, że „obracają się” tylko kwantyfikatory, a warunki nakładane na zmienną pozostają niezaniegowane.

Pokażemy teraz, że zachodzi pierwsza z równoważności. Mamy

$$\begin{aligned} \neg \forall (\phi(x)) (\psi(x)) &\leftrightarrow \neg (\forall x (\phi(x) \rightarrow \psi(x))) \\ &\leftrightarrow \exists x \neg (\phi(x) \rightarrow \psi(x)) \\ &\leftrightarrow \exists x (\phi(x) \wedge \neg \psi(x)) \\ &\leftrightarrow \exists (\phi(x)) (\neg \psi(x)). \end{aligned}$$

Korzystamy tu kolejno z definicji kwantyfikatora o ograniczonym zakresie, prawa De Morgana, prawa negowania implikacji (por. spis tautologii w poprzednim rozdziale), i ponownie z definicji kwantyfikatora o ograniczonym zakresie.

Czytelnik zechce udowodnić analogicznie drugie z praw De Morgana.

Prawa te są bardzo użyteczne, gdy z jakichś powodów trzeba zanegować stwierdzenie zapisane za pomocą kwantyfikatorów o ograniczonym zakresie,

zwłaszcza dowodząc nie wprost. Na przykład stwierdzenie, że ciąg $\{a_n\}$ spełnia warunek Cauchy'ego (czyli ciąg $\{a_n\}$ jest ciągiem Cauchy'ego) ma postać

$$\forall(\varepsilon > 0) \exists n_0 \forall(n > n_0) \forall(m > n_0) (|a_n - a_m| < \varepsilon),$$

a negację tego stwierdzenia łatwo uzyskujemy za pomocą podanych wyżej wariantów prawa De Morgana

$$\exists(\varepsilon > 0) \forall n_0 \exists(n > n_0) \exists(m > n_0) \neg(|a_n - a_m| < \varepsilon),$$

czyli

$$\exists(\varepsilon > 0) \forall n_0 \exists(n > n_0) \forall(m > n_0) (|a_n - a_m| \geq \varepsilon).$$

Podobnie, znana definicja Cauchy'ego granicy funkcji rzeczywistej w punkcie x_0 wygląda następująco:

$$\forall(\varepsilon > 0) \exists(\delta > 0) \forall(x \neq x_0) (|x - x_0| < \delta \rightarrow |f(x) - g| < \varepsilon).$$

Negując ją, po zastosowaniu powyższych wariantów praw De Morgana, mamy

$$\begin{aligned} &\neg \forall(\varepsilon > 0) \exists(\delta > 0) \forall(x \neq x_0) (|x - x_0| < \delta \rightarrow |f(x) - g| < \varepsilon) \leftrightarrow \\ &\leftrightarrow \exists(\varepsilon > 0) \forall(\delta > 0) \exists(x \neq x_0) \neg(|x - x_0| < \delta \rightarrow |f(x) - g| < \varepsilon) \leftrightarrow \\ &\leftrightarrow \exists(\varepsilon > 0) \forall(\delta > 0) \exists(x \neq x_0) (|x - x_0| < \delta \wedge |f(x) - g| \geq \varepsilon). \end{aligned}$$

Niekiedy, zwłaszcza, gdy używa się dla kwantyfikatorów znaków \wedge i \vee , nie bierze się w nawiasy warunków, które ma spełnić zmienna. Przy używanej przez nas notacji opuszczamy takie nawiasy, jeśli nie zachodzi obawa nieporozumienia.

4.6. Kwantyfikatory ilościowe

Jeśli język rachunku predykatów wyróżnia dwuargumentowy predykat identityczności = w zwykłym jego znaczeniu, to język taki pozwala na wyrażenie ilości. Można w nim mianowicie wyrazić następujące zwroty:

Istnieje co najmniej jeden obiekt o własności W :

$$\exists x W(x).$$

Co najwyżej jeden obiekt x , ma własność W :

$$\forall x \forall y (W(x) \wedge W(y) \rightarrow x = y)$$

(gdyby były takie dwa, to musiałyby być tym samym obiektem)⁸.

Istnieje dokładnie jeden x o własności W to tyle, co: istnieje przynajmniej jeden x o własności W i co najwyżej jeden x ma własność W , to znaczy

$$\exists x W(x) \wedge \forall x \forall y (W(x) \wedge W(y) \rightarrow x = y)$$

lub też krócej

$$\exists x (W(x) \wedge \forall y (W(y) \rightarrow x = y)).$$

Istnieją przynajmniej dwa różne obiekty o własności W

$$\exists x \exists y (W(x) \wedge W(y) \wedge x \neq y).$$

Co najwyżej dwa obiekty mają własność W

$$\forall x \forall y \forall z (W(x) \wedge W(y) \wedge W(z) \rightarrow x = y \vee x = z \vee y = z).$$

Wobec tego istnieją dokładnie dwa różne obiekty o własności W to tyle, co: istnieją przynajmniej dwa różne obiekty o własności W i co najwyżej dwa takie obiekty mają własność W , czyli

$$\begin{aligned} &\exists x \exists y (W(x) \wedge W(y) \wedge x \neq y) \wedge \\ &\wedge \forall x \forall y \forall z (W(x) \wedge W(y) \wedge W(z) \rightarrow x = y \vee x = z \vee y = z) \end{aligned}$$

lub nieco krócej

$$\exists x \exists y (W(x) \wedge W(y) \wedge x \neq y \wedge \forall z (W(z) \rightarrow x = z \vee y = z)).$$

Czytelnik zechce teraz zapisać zwrot: istnieją dokładnie trzy obiekty o własności W , pamiętając, że znaczy to tyle co: istnieją przynajmniej trzy różne obiekty o własności W , a gdyby były cztery, to któryś z tej czwórki byłby identyczny z którymś z pozostałych. Podobnie dla dowolnego n .

⁸ Wnikliwy Czytelnik zauważy, że na gruncie prawa transpozycji złożonej, formuła ta jest równoważna stwierdzeniu

$$\forall x \forall y (W(x) \wedge x \neq y \rightarrow \neg W(y)),$$

głoszącemu, że gdy x ma własność W , a y jest innym obiektem, to y już nie może mieć własności W .

4.7. System aksjomatyczny rachunku predykatów

Istnieje wiele aksjomatyzacji rachunku zdań, ale aksjomatyzacji rachunku predykatów przedstawiono w literaturze zaledwie kilka. Poniżej zaprezentujemy stosunkowo najprostsze ujęcie aksjomatyczne. Wyczerpujący wykład aksjomatycznego rachunku predykatów przedstawiany jest w ramach wykładu logiki matematycznej.

Definicję języka rachunku predykatów i niezbędnych pojęć, jak zasięgu kwantyfikatora, zmiennej wolnej i związanej podano wyżej. Zdefiniujemy tu pewne pojęcie konsekwencji przez podanie definicji dowodu formalnego. Zgodnie z uwagami podanymi przy okazji opisu aksjomatycznego rachunku zdań, pojęcie dowodu można sprecyzować, podając listę aksjomatów logicznych, aksjomatów pozalogicznych oraz reguł wnioskowania. Aksjomaty pozalogiczne można podawać dowolne (np. aksjomaty teorii grup, arytmetyki Peana, teorii mnogości itp.); logikę interesują tylko aksjomaty logiczne.

DEFINICJA 4.7.1 *Aksjomatami logicznymi są wszystkie i tylko te formuły, które powstają z tautologii rachunku zdań przez dokonanie konsekwentnych podstawień formuł zdaniowych rachunku predykatów za zmienne zdaniowe, występujące w danej tautologii.*

Ponieważ dla przedstawionego wyżej systemu S rachunku zdań zachodzi twierdzenie o pełności, można w definicji tej zamienić słowo „tautologia” przez „twierdzenie systemu S ”.

Niech $\phi(x)$ będzie formułą zawierającą zmienną wolną x . Przez $\phi(x/\alpha)$ oznaczamy (por. paragraf 4.) formułę powstającą z $\phi(x)$ przez wpisanie na miejsce zmiennej wolnej x formuły α , gdzie α jest albo zmienną indywidualową, albo stałą indywidualową⁹.

DEFINICJA 4.7.2 *Klasyczną konsekwencją logiczną S nazwiemy tu relację konsekwencji, wyznaczoną przez podany w poprzedniej definicji zbiór aksjomatów logicznych oraz przez zbiór następujących pięciu reguł:*

REGUŁA PODSTAWIANIA

$$\frac{\phi(x)}{\phi(x/\alpha)},$$

gdzie α jest stałą indywidualową lub zmienną indywidualową.

⁹ Przedstawiana tu wersja aksjomatyczna rachunku predykatów nie uwzględnia takich termów, które nie są stałymi indywidualowymi czy zmiennymi indywidualowymi. Wykład aksjomatycznego rachunku zdań, uwzględniający podstawianie dowolnych termów za zmienne indywidualowe – por. T. Batóg, *Podstawy logiki*, op. cit.

REGUŁA ODRYWANIA

$$\frac{\phi \rightarrow \psi, \phi}{\psi}.$$

REGUŁA OPUSZCZANIA DUŻEGO KWANTYFIKATORA

$$\frac{\phi \rightarrow \forall x \psi}{\phi \rightarrow \psi}.$$

REGUŁA DOŁĄCZANIA DUŻEGO KWANTYFIKATORA

$$\frac{\phi \rightarrow \psi}{\phi \rightarrow \forall x \psi},$$

o ile x nie jest wolne w ϕ .

REGUŁA OPUSZCZANIA MAŁEGO KWANTYFIKATORA

$$\frac{(\exists x \phi) \rightarrow \psi}{\phi \rightarrow \psi}.$$

REGUŁA DOŁĄCZANIA MAŁEGO KWANTYFIKATORA

$$\frac{\phi \rightarrow \psi}{(\exists x \phi) \rightarrow \psi},$$

o ile x nie jest wolne w ψ .

Czasem wśród reguł pojawia się

REGUŁA GENERALIZACJI

$$\frac{\phi}{\forall x \phi},$$

ale gdy pojęcie dowodu jest definiowane za pomocą scharakteryzowanych wyżej aksjomatów logicznych oraz pozostałych reguł z naszej listy, to reguła ta jest regułą wtórną.

Reguły te wraz z aksjomatami logicznymi wyznaczają pojęcie dowodu formalnego; dowód definiowany przez podane wyżej aksjomaty logiczne i reguły nazwiemy S -dowodem¹⁰.

Niech Σ będzie pewnym podzbiorem zbioru wszystkich formuł języka rachunku predykatów.

DEFINICJA 4.7.3. *Formuła ϕ jest syntaktyczną S -konsekwencją zbioru Σ ($\Sigma \vdash_S \phi$) wtedy i tylko wtedy, gdy ϕ ma S -dowód oparty o zbiór Σ formuł. Jeśli Σ jest zbiorem pustym, to ϕ nazwiemy twierdzeniem systemu S i piszemy $\vdash_S \phi$.*

¹⁰ Ogólna definicja dowodu znajduje się w rozdziale 2.

A oto trzy najprostsze przykłady dowodów formalnych:

LEMAT 4.7.4. Dla dowolnej formuły ϕ twierdzeniem systemu S są formuły:

- (t1) $\phi \rightarrow \exists x \phi$,
 (t2) $\forall x \forall y \phi \rightarrow \forall y \forall x \phi$,
 (t3) $\exists x \forall y \phi \rightarrow \forall y \exists x \phi$.

Dowód:

Dowód t1:

- (1) $\exists x \phi \rightarrow \exists x \phi$ aksjomat; podstawienie w $p \rightarrow p$
 (2) $\phi \rightarrow \exists x \phi$ (1), reguła opuszczania \exists .

Dowód t2, czyli prawa przestawiania dużych kwantyfikatorów:

- (1) $\forall x \forall y \phi \rightarrow \forall x \forall y \phi$ aksjomat; podstawienie w $p \rightarrow p$
 (2) $\forall x \forall y \phi \rightarrow \phi$ (1), dwa razy reguła opuszczania \forall
 (3) $\forall x \forall y \phi \rightarrow \forall y \forall x \phi$. (2), dwa razy reguła dołączania \forall .

Dowód t3, czyli prawa przestawiania dużego i małego kwantyfikatora:

- (1) $\forall y \phi \rightarrow \forall y \phi$ podstawienie w $p \rightarrow p$
 (2) $\forall y \phi \rightarrow \phi$ (1), reguła opuszczania \forall
 (3) $(\forall y \phi \rightarrow \phi) \rightarrow$
 $\rightarrow ((\phi \rightarrow \exists x \phi) \rightarrow (\forall x \phi \rightarrow \exists x \phi))$ syllogizm hipotetyczny
 (4) $\forall y \phi \rightarrow \exists x \phi$ (2), t1, (3), reguła MP
 (5) $\exists x \forall y \phi \rightarrow \exists x \phi$ (4), reguła dołączania \exists
 (6) $\exists x \forall y \phi \rightarrow \forall y \exists x \phi$ (5), reguła dołączania \forall .

Trzeci wiersz tego dowodu powstaje przez podstawienie w prawie syllogizmu hipotetycznego bezkoniunkcyjnego, tj. w formule

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

Q.E.D.

Precyzyjne zdefiniowanie pojęcia tautologii rachunku predykatów jest znacznie bardziej skomplikowane niż w przypadku rachunku zdań. Wymaga ono formalnego sprecyzowania pojęcia prawdy¹¹; podawać go tu nie będziemy. Poprzestańmy na intuicyjnej definicji, podanej w rozdziale 2.

¹¹ Jako pierwszy formalną definicję prawdy dla formuł języka rachunku predykatów podał Alfred Tarski w 1933 roku.

Przypomnijmy więc, że tautologią rachunku predykatów nazywamy taką formułę rachunku predykatów, która jest prawdziwa przy dowolnym rozumieniu występujących w niej stałych nazwowych, zmiennych nazwowych, symboli funkcyjnych i predykatów.

Możemy teraz sformułować pewną wersję twierdzenia o pełności. Gwarantuje ono, że przedstawiony tu system rachunku predykatów obejmuje wszystkie tautologie i tylko tautologie.

TWIERDZENIE 4.7.5 (o pełności rachunku predykatów) *Niech ϕ będzie formułą języka rachunku predykatów. Wówczas $\vdash_S \phi$ wtedy i tylko wtedy, gdy ϕ jest tautologią rachunku predykatów.*

Dowód tego twierdzenia wykracza jednak zdecydowanie poza ramy tego podręcznika.

Zadania

1. Zapisać w języku rachunku predykatów następujące zdania:
 - a. Archimedes jest matematykiem.
 - b. Każdy matematyk jest człowiekiem.
 - c. Niektórzy matematycy są ludźmi.
 - d. Żaden matematyk nie jest człowiekiem.
 - e. Niektórzy matematycy nie są ludźmi.
 - f. Tylko ludzie są matematykami.
2. Jaką wartość logiczną ma zdanie „Każde kwadratowe koło jest okrągłe?”
Wskazówka: Zapisać w języku rachunku predykatów:
3. Podaj schematy następujących zdań:
 - a. Każdy A jest B .
 - b. Niektóre A są B .
 - c. Żaden A nie jest B .
 - d. Niektóre A nie są B .

W logice tradycyjnej zdania takie są zwane zdaniami z kwadratu logicznego. Badając wnioski, w których występowały takie zdania, przyjmowano jednak, że nazwy A i B są niepuste, tj. że istnieją obiekty będące A i obiekty będące B . W szczególności rozważając zdania postaci (a), z uwagi na własności implikacji, odróżniano przypadek, w którym nazwa A jest niepusta (używano wówczas słowa „każdy”) od przypadku, gdy dopuszcza się pustość nazwy A (używano wówczas słowa „wszelki”).

Podaj schematy zdań a – d, uwzględniając niepustość nazw A i B .

Jaką wartość logiczną ma zdanie „Wszelkie kwadratowe koło jest okrągłe?”

4. Zapisz w języku rachunku predykatów schemat wnioskowania:

Każdy człowiek jest śmiertelny.
 Sokrates jest człowiekiem.

 Zatem: Sokrates jest śmiertelny.

Czy schematowi tego wnioskowania odpowiada tautologia rachunku predykatów?

5. Zapisz w języku rachunku predykatów następujące zdania:

- a. Każda miłość jest pierwsza, najgorętsza, najszczerza (znana piosenka).
- b. Niejednego, którego podziwiają wszyscy ludzie, nie podziwia żaden domownik (M. de Montaigne).
- c. Każda potwora znajdzie swego amatora (prysłowie ludowe).
- d. Każdy ma swoją żabę, co przed nim ucieka, i swojego zająca, którego się boi (A. Mickiewicz).
- e. Nikt tu nigdy niczego nie czyni niepotrzebnie (miesięcznik „Delta”). Co pozytywnego głosi to zdanie?

6. Zapisz w języku rachunku predykatów następujące wypowiedzi:

- a. Poznaniacy są porządni i oszczędni.
- b. Ludzie nie lubią płacić podatków.
- c. Teologowie rozprawiają o sprawach Bożych i niebieskich.

Uwzględni różne możliwości rozumienia tych wypowiedzi, związane z kwantyfikacją.

7. Zakładając, że zmienne indywidualne $n, n_1, n_2, n_3 \dots$ przebiegają nazwy liczb naturalnych i korzystając z predykatów $=$ i \leq oraz symbolu 0 dla zera, a także stałych funkcyjnych $+$ i \cdot zapisać następujące zdania i formuły zdaniowe:

- a) n jest liczbą pierwszą,
- b) n jest dzielnikiem liczby m ,
- c) n jest liczbą parzystą,
- d) istnieje najmniejsza liczba,
- e) nie istnieje największa liczba,
- f) między liczbą a jej podwojeniem istnieje co najmniej jedna liczba pierwsza,
- g) każda liczba parzysta jest sumą dwóch liczb pierwszych,
- h) n jest pierwiastkiem równania kwadratowego o współczynnikach a, b, c .

8. Niech $S(n)$ skraca formułę nazwową „następnik liczby naturalnej n ”. Wykorzystując założenia poprzedniego zadania, zapisać następujące zdania:

- a. Zero nie jest następnikiem żadnej liczby.
- b. Każda liczba różna od zera jest następnikiem pewnej liczby.
- c. Jeśli liczba jest następnikiem jakiejś liczby, to jest ona różna od zera.
- d. Jeśli dwie liczby są różne, to ich następniki też są różne.
- e. Każda liczba jest różna od swego następnika.
- f. Jeśli liczba jest różna od swego następnika, to następnik tej liczby jest różny od następnika następnika tej liczby.

9. Korzystając z założeń z zadania 7 i kwantyfikatorów ilościowych, zapisz następujące zdania:

- a. Istnieje dokładnie jedna liczba najmniejsza.
- b. Istnieje dokładnie jedna najmniejsza parzysta liczba pierwsza.
- c. Każda liczba ma dokładnie jeden następnik.
- d. Każda liczba pierwsza ma dokładnie dwa różne dzielniki.
- e. Jeżeli równanie kwadratowe o współczynnikach a , b , c ma rozwiązanie, to istnieje dokładnie jedno rozwiązanie lub dokładnie dwa różne rozwiązania tego równania.

10. Korzystając z tych samych zmiennych indywiduowych dla wszystkich obiektów geometrycznych, predykatu „... leży na $-$ ” zapisywanego symbolem $L(\dots, -)$, predykatów: „... jest punktem” ($Pt(\dots)$), „ $-$ jest linią prostą” ($Ln(-)$) i „... jest płaszczyzną” ($Pl(\dots)$), oraz predykatów języka geometrii: „... jest równoległa do” (\parallel) i „... jest prostopadła do ...” (\perp), ewentualnie wprowadzając dodatkowe predykaty, zapisać następujące zdania:

- a. Nie istnieją dwie różne proste równoległe.
- b. Jeśli dwie proste są prostopadłe, to nie są równoległe.
- c. Jeśli dwie proste są prostopadłe, to mają dokładnie jeden punkt wspólny.
- d. Przez dwa różne punkty przechodzi dokładnie jedna prosta.
- e. Dowolna prosta albo leży na danej płaszczyźnie, albo nie ma z nią punktów wspólnych, albo ma dokładnie jeden punkt wspólny.
- f. Dla dowolnych trzech różnych punktów istnieje dokładnie jedna płaszczyzna, na której leżą te trzy punkty.
- g. Dwa dowolne koła albo się nie przecinają, albo mają dokładnie jeden punkt wspólny, albo mają dokładnie dwa punkty wspólne.
- h. Jeśli dwie różne proste leżą na tej samej płaszczyźnie, to albo są równoległe, albo mają dokładnie dwa punkty wspólne.
- i. Przez punkt nie leżący na danej prostej przechodzi dokładnie jedna prosta równoległa do danej prostej.

11. Napisać negacje zdań z poprzedniego zadania.

12. Korzystając z podręczników analizy matematycznej i definicji kwantyfikatorów o ograniczonym zakresie, zapisać i zanegować warunki definiujące pojęcia:

- a) ciągu ograniczonego,
- b) ciągu zbieżnego,
- c) zbieżności punktowej ciągu funkcyjnego,
- d) zbieżności jednostajnej ciągu funkcyjnego.

Rozdział 5

Podstawy teorii zbiorów

5.1. Uwagi wstępne

Pojęcie zbioru należy do najbardziej podstawowych pojęć matematyki. Wynika to z tego, że wszystkie niemal pojęcia matematyki definiuje się w terminach zbiorów. Pojęcie zbioru zastąpiło w końcu XIX wieku używane dotąd nieprecyzyjne pojęcie wielkości.

Zauważmy na początek, że słowo „zbiór” ma w języku potocznym dwa wyraźnie różne znaczenia, które określać będziemy jako znaczenie kolektywne i znaczenie dystrybutywne. W znaczeniu kolektywnym zbiór pewnych przedmiotów to całość złożona z tych przedmiotów. To właśnie znaczenie słowa „zbiór” mamy na myśli, mówiąc, że biblioteka jest zbiorem książek czy że łańcuch jest zbiorem ogniów. W tym znaczeniu zbiór konkretnych przedmiotów jest innym konkretnym przedmiotem. Zwrot „ x jest elementem zbioru A ” znaczy tu tyle, co „ x jest częścią zbioru A ”. Teorię zbiorów w sensie kolektywnym stworzył polski logik Stanisław Leśniewski (1886–1939) i nazywa się ona mereologią.

Drugie znaczenie słowa „zbiór” to znaczenie zwane dystrybutywnym. Przy tym znaczeniu zdanie „Wenus jest elementem zbioru planet Układu Słonecznego” znaczy tyle, co „Wenus jest planetą Układu Słonecznego”, a zdanie „3 jest elementem zbioru liczb naturalnych” – tyle samo, co „3 jest liczbą naturalną”. Zbiór w sensie dystrybutywnym nie musi być zatem konkretnym, zmysłowo poznawalnym przedmiotem, nawet jeśli jego elementy są takimi przedmiotami.

Zbiory w sensie dystrybutywnym bada teoria mnogości. Takie właśnie pojęcie zbioru jest przydatne w matematyce. Teoria mnogości została stworzona w latach 1874–1897 przez matematyka niemieckiego Georga Cantora (1845–1918). Oczywiście Cantor opierał się na pewnych rozważaniach

wcześniejszych, ale dopiero w jego pracach teoria zbiorów przybrała postać wystarczająco dojrzałą i całościową¹.

Cantor rozumiał w swej teorii pojęcie zbioru w sposób intuicyjny. Poprzestawanie na takim tylko rozumieniu doprowadziło w końcu XIX wieku do pojawienia się na gruncie teorii mnogości antynomii, tzn. rozumowań pozornie poprawnych, prowadzących jednak do pary sprzecznych ze sobą wniosków. Aby uniknąć antynomii, matematycy zaksjomatyzowali teorię mnogości (i w ten sposób sprecyzowali pojęcie zbioru)².

Aksjomatyczne ujęcie teorii mnogości jest niezbędne, gdy chcemy zajmować się samym pojęciem zbioru, jego istotą i własnościami. Jeśli jednak interesuje nas teoria mnogości tylko jako narzędzie pozwalające precyzyjnie ujmować rozmaite kwestie w matematyce i prowadzić poprawne i ściśle rozumowania dotyczące różnych dziedzin matematyki, to wystarczy teoria mnogości w duchu Cantora, tzn. opierająca się na intuicyjnym tylko pojęciu zbioru. Teorię taką, w odróżnieniu od aksjomatycznej teorii mnogości, nazywa się *naiwną teorią mnogości* (przymiotnik „naiwna” nie ma tu znaczenia pejoratywnego!). I taką właśnie teorię mnogości będziemy rozwijali w tej książce.

Przed właściwymi rozważaniami podamy jeszcze kilka uwag o notacji. Język teorii mnogości jest ubogi. Składa się z dwóch predykatów: równości $=$ i przynależności elementu do zbioru \in oraz zmiennych³. Możliwe jest zapisywanie formuł teorii mnogości przy użyciu tylko jednego rodzaju zmiennych (pisze się wtedy na przykład $x \in y$) – czyni się tak, badając samą teorię mnogości. W zastosowaniach jednak wygodniej jest używać co najmniej dwóch rodzajów zmiennych: zmienne $x, y, z \dots$ (z indeksami lub bez indeksów) reprezentują elementy, a zmienne A, B, C, \dots, X, Y, Z (znów z indeksami lub bez nich) reprezentują zbiory⁴. Formułami atomowymi języka teorii mnogości będą formuły typu: $x_i \in A_j$, $A_i = A_j$ czy $x_i = x_k$.

Obok zmiennych oraz predykatów specyficznych, symbolami języka teorii zbiorów są wszystkie symbole logiczne (czyli spójniki i kwantyfikatory);

¹ Na temat rozwoju teorii mnogości i problemów filozoficznych związanych z tą teorią zob. np. R. Murawski, *Filozofia matematyki. Zarys dziejów*, Wydawnictwo Naukowe PWN, Warszawa 2001 (wyd. II) oraz *Współczesna filozofia matematyki*, Wydawnictwo Naukowe PWN, Warszawa 2002.

² Opis antynomii oraz aksjomatykę teorii mnogości Zermela–Fraenkla znaleźć można na przykład w rozdziale 10 książki R. Murawskiego i K. Świrydowicza, *Wstęp do teorii mnogości*, Wydawnictwo Naukowe UAM, Poznań 2005.

³ Symbol \in pochodzi od pierwszej litery greckiego słowa $\epsilon\sigma\tau\iota$, które znaczy „być”. Został on wprowadzony przez Giuseppe Peana (1858–1932).

⁴ Czasami używać będziemy jeszcze trzeciego rodzaju zmiennych \mathcal{A}, \mathcal{B} itd. reprezentujących rodziny zbiorów.

za ich pomocą można tworzyć (w sposób wskazany w poprzednim rozdziale) z formuł elementarnych formuły bardziej skomplikowane. Napis $x \in A$ czytamy jako: x należy do (jest elementem) zbioru A . Jeżeli obiekt x nie jest elementem zbioru A , to zamiast $\neg(x \in A)$ piszemy krótko $x \notin A$. Podobnie piszemy $A \neq B$ zamiast $\neg(A = B)$. Mówiąc o kilku elementach x_1, \dots, x_n zbioru A , będziemy pisali krótko $x_1, \dots, x_n \in A$.

Często, zwłaszcza w przykładach, pojawiać się będą zbiory liczb, które będziemy oznaczali następująco: zbiór liczb naturalnych jako \mathbb{N} , zbiór liczb całkowitych – \mathbb{Z} , zbiór liczb wymiernych – \mathbb{Q} , zbiór liczb rzeczywistych – \mathbb{R} i w końcu zbiór liczb zespolonych – \mathbb{C} .

O predykanie równości = zakłada się w szczególności, że reprezentuje on relację zwrotną, symetryczną i przechodnią (por. paragraf 6.2), tzn. spełnia dla dowolnych obiektów x, y, z odpowiednio warunki: $x = x$, $x = y \leftrightarrow y = x$ oraz $x = y \wedge y = z \rightarrow x = z$; podobnie dla dowolnych zmiennych reprezentujących zbiory A, B, C .

5.2. Zasada ekstensjonalności

Zbiór uznajemy za określony, gdy znamy wszystkie jego elementy. Równość dwóch zbiorów określa podstawowa w teorii mnogości zasada ekstensjonalności, będąca jednym z aksjomatów teorii mnogości.

ZASADA EKSTENSJONALNOŚCI. Dwa zbiory są równe wtedy i tylko wtedy, gdy mają dokładnie te same elementy.

Symbolicznie możemy zapisać ją jako

$$A = B \leftrightarrow \forall x (x \in A \leftrightarrow x \in B).$$

Z zasady tej wynika bezpośrednio, że

$$A \neq B \leftrightarrow \exists x [(x \notin A \wedge x \in B) \vee (x \in A \wedge x \notin B)],$$

tzn. zbiory A i B są różne (nie są identyczne) wtedy i tylko wtedy, gdy istnieje obiekt x , taki że jest on elementem zbioru A , ale nie należy do zbioru B lub na odwrót.

Zbiór, którego jedynymi elementami są x_1, \dots, x_n , oznaczamy symbolem $\{x_1, \dots, x_n\}$. W konsekwencji symbol $\{x\}$ oznacza zbiór złożony z dokładnie jednego elementu x . Należy ten zbiór odróżniać od samego elementu x . Zbiór postaci $\{x\}$ zwany bywa z angielska *singletonem*.

Z zasady ekstensjonalności wynika, że na przykład zbiór $\{2, 5\}$ oraz zbiór $\{5, 2\}$ są równe, podobnie jak $\{2, 5\} = \{2, 2, 5\} = \{2, 2, 5, 5\}$ itd. Ogólnie $\{a\} \neq \{a, b\}$ wtedy i tylko wtedy, gdy $a \neq b$. Gdy $a = b$, to $\{a\} = \{a, b\} = \{a, a\}$. Mamy też $\{x\} \neq \{\{x\}\}$.

W praktyce matematycznej definiujemy często zbiory nie poprzez wymienienie ich elementów (co na przykład w przypadku zbiorów nieskończonych jest niemożliwe), a poprzez wskazanie przysługującej im własności. Definicja ma wtedy postać

$$x \in A \leftrightarrow x \in U \wedge \varphi(x)$$

lub w innej formie

$$A = \{x : x \in U \wedge \varphi(x)\},$$

gdzie U jest wcześniej danym zbiorem, a $\varphi(x)$ jest funkcją zdaniową. To drugie wyrażenie czytamy: „ A jest zbiorem wszystkich x , które należą do U i mają własność φ ”. Pisze się też czasem krócej

$$A = \{x \in U : \varphi(x)\},$$

a dwukropek zastępuje się też niekiedy kreską, pisząc

$$A = \{x \in U | \varphi(x)\}.$$

Czasami, gdy zbiór U jest znany, piszemy krótko

$$x \in A \leftrightarrow \varphi(x)$$

albo

$$A = \{x : \varphi(x)\}.$$

Zauważmy, iż $\{x : \varphi(x)\} = \{y : \varphi(y)\}$, tzn. że nie jest istotne, jakiej użyje się zmiennej. Z definicji wynika, że zachodzi następująca prosta zależność:

$$y \in \{x : \varphi(x)\} \leftrightarrow \varphi(y).$$

Przykładem definicji omawianego typu może być definicja zbioru liczb parzystych jako zbioru $\{x \in \mathbb{Z} : 2|x\}$ lub $\{x \in \mathbb{Z} : \exists y (y \in \mathbb{Z} \wedge x = y + y)\}$, czy definicja zbioru liczb pierwszych mająca postać

$$\{x \in \mathbb{N} : \forall z (z|x \longrightarrow z = 1 \vee z = x)\},$$

czyli

$$\{x \in \mathbb{N} : \forall z (\exists y (x = y \cdot z) \longrightarrow z = 1 \vee z = x)\},$$

tzn.

$$\{x \in \mathbb{N} : \forall y \forall z (x = y \cdot z \longrightarrow z = 1 \vee z = x)\}.$$

5.3. Relacja inkluzji. Zbiór pusty i zbiór potęgowy

Pomiędzy zbiorami może zachodzić nie tylko relacja równości, ale także relacja inkluzji (zawierania się). Oznaczamy ją symbolem \subseteq i definiujemy następująco:

$$A \subseteq B \leftrightarrow \forall x(x \in A \rightarrow x \in B).$$

Na przykład $\mathbb{N} \subseteq \mathbb{Z}$ oraz $\{x \in \mathbb{N} : 6|x\} \subseteq \{x \in \mathbb{N} : 2|x \wedge 3|x\}$.

LEMAT 5.3.1. *Relacja inkluzji ma następujące własności:*

- (1) *zwrotność, tzn. $A \subseteq A$,*
- (2) *antysymetria, tzn. $A \subseteq B \wedge B \subseteq A \rightarrow A = B$,*
- (3) *przechodność, tzn. $A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C$.*

D o w ó d. Zwrotność relacji inkluzji jest konsekwencją tautologii o postaci $p \rightarrow p$.

Antysymetria wynika z prawa: $[(p \rightarrow q) \wedge (q \rightarrow p)] \leftrightarrow (p \leftrightarrow q)$ oraz zasady ekstensjonalności.

Przechodność jest konsekwencją prawa sylogizmu hipotetycznego, tzn. $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$. Istotnie, załóżmy, że $A \subseteq B \wedge B \subseteq C$.
Zatem

$$\forall x(x \in A \rightarrow x \in B)$$

oraz

$$\forall x(x \in B \rightarrow x \in C).$$

Niech x_0 będzie dowolnym danym elementem zbioru A . Na mocy założeń mamy

$$x_0 \in A \rightarrow x_0 \in B$$

oraz

$$x_0 \in B \rightarrow x_0 \in C.$$

Podstawiając w prawie sylogizmu hipotetycznego, otrzymujemy

$$(x_0 \in A \rightarrow x_0 \in B) \wedge (x_0 \in B \rightarrow x_0 \in C) \rightarrow (x_0 \in A \rightarrow x_0 \in C).$$

Z założenia wynika, że $(x_0 \in A \rightarrow x_0 \in B) \wedge (x_0 \in B \rightarrow x_0 \in C)$. Stąd za pomocą reguły odrywania otrzymujemy $x_0 \in C$. Ponieważ jednak element x_0 był dowolny, zatem

$$\forall x(x \in A \rightarrow x \in C),$$

czyli $A \subseteq C$. Q.E.D.

Zauważmy, że podane własności inkluzji są analogiczne do własności relacji \leq wśród liczb rzeczywistych. Analogia nie jest jednak pełna, gdyż każde dwie liczby rzeczywiste są porównywalne w sensie relacji \leq (tzn. dla dowolnych liczb rzeczywistych a i b zachodzi $a \leq b \vee b \leq a$), podczas gdy nie każde dwa zbiory są porównywalne w sensie relacji \subseteq . Istotnie, na przykład zbiory $\{2, 3\}$ i $\{3, 5\}$ są nieporównywalne, ponieważ ani $\{2, 3\} \subseteq \{3, 5\}$, ani też $\{3, 5\} \subseteq \{2, 3\}$.

Oprócz opisanej relacji inkluzji \subseteq wprowadzamy jeszcze tzw. inkluzję właściwą \subsetneq , którą definiujemy następująco:

$$A \subsetneq B \leftrightarrow A \subseteq B \wedge A \neq B.$$

Czasami zamiast $A \subsetneq B$ pisze się $A \subset B$. Przykładami relacji inkluzji właściwej mogą być: $\mathbb{N} \subsetneq \mathbb{Z}$, $\{x \in \mathbb{N} : 6|x\} \subsetneq \{x \in \mathbb{N} : 2|x\}$.

LEMAT 5.3.2. *Relacja inkluzji właściwej ma następujące własności:*

- (1') *przeciwność, tzn. $\neg(A \subsetneq A)$,*
- (2') *przeciwsymetria, tzn. $A \subsetneq B \rightarrow \neg(B \subsetneq A)$,*
- (3') *przechodność, tzn. $A \subsetneq B \wedge B \subsetneq C \rightarrow A \subsetneq C$.*

Dowód tych własności pozostawiamy Czytelnikowi.

W teorii mnogości (i w matematyce) wygodne okazuje się pojęcie zbioru nie zawierającego żadnego elementu. Zbiór taki nazywamy *zbiorem pustym*. Definiujemy go następująco:

DEFINICJA 5.3.3. *Zbiorem pustym nazywamy zbiór*

$$\{x : x = x \wedge x \neq x\}.$$

Oznaczamy go symbolem \emptyset .

Zauważmy, że ponieważ wśród własności równości założonych na początku naszych rozważań (por. paragraf 5.1) była własność $x = x$ dla każdego x , więc moglibyśmy właściwie przyjąć $\emptyset = \{x : x \neq x\}$. Zauważmy też, że skoro tautologią jest prawo Dunsza Szkota, czyli formuła $p \wedge \neg p \rightarrow q$, więc prawdą też będzie formuła $x = x \wedge x \neq x \rightarrow x \in A$, a że $x \in \emptyset \leftrightarrow x = x \wedge x \neq x$, więc zgodnie z tym implikacja: $x \in \emptyset \rightarrow x \in A$ jest prawdziwa dla każdego zbioru A i dowolnego elementu x . Stąd $\forall x (x \in \emptyset \rightarrow x \in A)$, czyli $\emptyset \subseteq A$. Otrzymaliśmy zatem, że zbiór pusty jest podzbiorem każdego zbioru.

Czasami definiuje się zbiór pusty trochę inaczej, przyjmując, że

$$\emptyset = \{x \in A : x \neq x\},$$

gdzie A jest pewnym danym zbiorem. Zauważmy, że definicja ta nie zależy od wyboru zbioru A . Istotnie, dla dowolnych zbiorów A i B oraz dla każdego x mamy: $x \in A \wedge x \neq x \leftrightarrow x \in B \wedge x \neq x$. Ze względu na przyjęte ogólne założenie $x = x$ jest to równoważność dwu zdań fałszywych, a więc równoważność prawdziwa. Podobnie dla dowolnego zbioru A i dla każdego x mamy: $x \in A \wedge x \neq x \leftrightarrow x \neq x$. Stąd, w oparciu o zasadę ekstensjonalności, dochodzimy do wniosku, że wszystkie tego typu definicje zbioru pustego są sobie równoważne i definiują ten sam obiekt, tzn. zbiór pusty \emptyset . Dodajmy jeszcze, że zamiast $x = x \wedge x \neq x$ można by tu użyć dowolnej pary własności sprzecznych, tj. pary $\varphi(x) \wedge \neg\varphi(x)$.

DEFINICJA 5.3.4. *Rodzinę wszystkich podzbiorów danego zbioru A nazywać będziemy zbiorem potęgowym zbioru A i oznaczać symbolem $\mathcal{P}(A)$ lub 2^A .*

Mamy zatem

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

Na mocy definicji otrzymujemy w szczególności: $\emptyset \in \mathcal{P}(A)$, $A \in \mathcal{P}(A)$, czyli $\{\emptyset, A\} \subseteq \mathcal{P}(A)$ dla dowolnego zbioru A .

Dla przykładu rozważmy zbiór $A = \{1, 2, 3\}$. Mamy teraz

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

Widać, że zbiór A miał 3 elementy, a zbiór $\mathcal{P}(A)$ ma 8 elementów, czyli 2^3 elementów. Jest to zależność ogólna.

LEMAT 5.3.5. *Jeśli zbiór A jest skończony i ma n elementów, to zbiór potęgowy $\mathcal{P}(A)$ ma 2^n elementów.*

D o w ó d. Lemat ten wynika z zasad kombinatoryki. Istotnie, podzbiór zbioru A można określić, przyporządkowując jego elementom odpowiednio liczby 1 bądź 0 w zależności od tego, czy zaliczymy dany element do definiowanego podzbioru, czy nie. Stąd podzbiorów zbioru A jest tyle, na ile sposobów możemy dokonać opisanego przyporządkowania, czyli tyle, ile jest kombinacji n -elementowych z powtórzeniami zbioru 2-elementowego, a tych, jak uczy kombinatoryka, jest właśnie 2^n . Q.E.D.

Opisana zależność pomiędzy liczbą elementów zbioru A i liczbą elementów jego zbioru potęgowego wyjaśnia też genezę symbolu 2^A , stosowanego czasami na oznaczenie zbioru potęgowego.

5.4. Działania na zbiorach

Określimy teraz działania na zbiorach. Niech więc dane będą zbiory A i B . Przyjmujemy następujące definicje.

DEFINICJA 5.4.1. (1) Suma zbiorów A i B jest to zbiór $A \cup B$ spełniający warunek

$$x \in A \cup B \iff x \in A \vee x \in B,$$

czyli

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

(2) Przekrój (iloczyn, część wspólna) zbiorów A i B jest to zbiór $A \cap B$ spełniający warunek

$$x \in A \cap B \iff x \in A \wedge x \in B,$$

czyli

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

(3) Różnica zbiorów A i B jest to zbiór $A \setminus B$ spełniający warunek

$$x \in A \setminus B \iff x \in A \wedge x \notin B,$$

czyli

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

(4) Różnica symetryczna zbiorów A i B jest to zbiór $A \div B$ spełniający warunek⁵

$$x \in A \div B \iff (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B),$$

czyli

$$A \div B = \{x : (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)\}.$$

Łatwo zauważyć, że $A \div B = (A \setminus B) \cup (B \setminus A)$.

DEFINICJA 5.4.2. Zbiory A i B nazywamy rozłącznymi wtedy i tylko wtedy, gdy $A \cap B = \emptyset$.

LEMAT 5.4.3. Jeśli zbiory A i B są podzbioremi ustalonego zbioru U , to $A \cup B$, $A \cap B$, $A \setminus B$ oraz $A \div B$ są także zawarte w U , czyli zbiór $\mathcal{P}(U)$ jest zamknięty ze względu na działania sumy \cup , przekroju \cap , różnicy \setminus i różnicy symetrycznej \div .

⁵ W literaturze oznacza się różnicę symetryczną także symbolem $A \dot{\cup} B$.

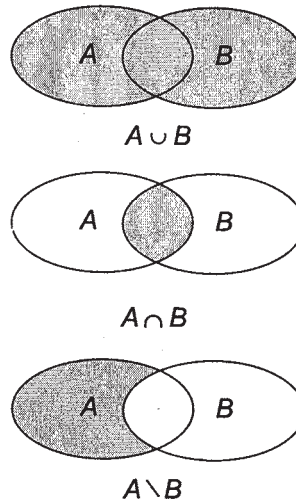
Jeśli ograniczamy się do rozważania podzbiorów ustalonego zbioru U (zwanego wtedy przestrzenią albo uniwersum albo zbiorem uniwersalnym), to możemy wprowadzić jeszcze jedno działanie, a mianowicie dopełnienie.

DEFINICJA 5.4.4. Dopełnieniem zbioru A w zbiorze (względem zbioru) (uniwersum) U nazywamy zbiór A' spełniający równość

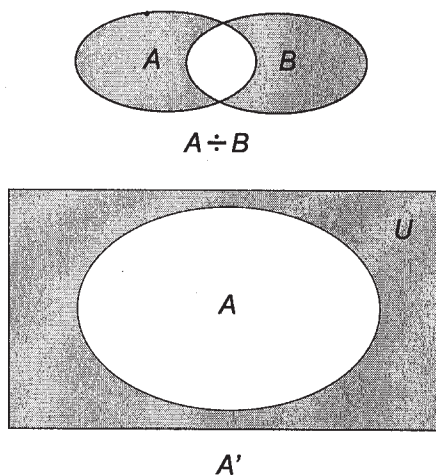
$$A' = U \setminus A = \{x \in U : x \notin A\}.$$

Zauważmy, że – w odróżnieniu od wprowadzonych wyżej działań sumy, przekroju, różnicy i różnicy symetrycznej – działanie dopełnienia nie ma charakteru absolutnego, tzn. jest działaniem względnym, czyli wartość działania na danym argumencie A zależy od uniwersum U , względem którego bierzemy dopełnienie. Dla przykładu założmy, że przestrzeń U jest zbiorem liczb rzeczywistych \mathbb{R} . Wtedy dopełnienie \mathbb{Z}' zbioru \mathbb{Z} liczb całkowitych jest równe zbiorowi złożonemu z liczb niewymiernych i z wymiernych liczb niecałkowitych. Z drugiej strony, jeśli jako uniwersum przyjąć zbiór \mathbb{Z} , to dopełnienie \mathbb{Z}' będzie równe \emptyset .

Graficzną ilustracją działań na zbiorach są tzw. diagramy Venna⁶. Pozwalają one zilustrować wprowadzone działania następująco:



⁶ John Venn (1834–1923), logik angielski, jeden z pionierów logiki matematycznej. Wprowadził on diagramy do logiki (w pracy z roku 1880 i następnie w książce z 1881) jako narzędzie do rozwiązywania problemów logicznych. Diagramy Venna są modyfikacją metody diagramów zaproponowanej przez L. Eulera.



Wprowadzone powyżej działania na zbiorach mają oczywiście rozmaite własności. Ich badaniem zajmuje się tzw. algebra zbiorów. Udowodnimy teraz kilka takich własności (pokazując przy okazji typowe metody ich dowodzenia).

Zacznijmy od pokazania, że dla dowolnych zbiorów A, B, C zachodzi następująca własność:

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

Istotnie, niech x będzie dowolny. Załóżmy, że $x \in A \setminus (B \cup C)$. Z definicji działań na zbiorach mamy: $x \in A \wedge x \notin (B \cup C)$, co równoważne jest temu, że $x \in A \wedge \neg(x \in B \cup C)$, czyli $x \in A$ oraz $\neg(x \in B \vee x \in C)$. Na mocy praw De Morgana dla rachunku zdań jest to równoważne temu, że: $x \in A$ oraz $x \notin B \wedge x \notin C$, czyli $x \in A \wedge x \notin B \wedge x \notin C$, a zatem (na mocy praw idempotentności oraz łączności koniunkcji) równoważne wyrażeniu: $(x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C)$, czyli (na mocy definicji działań) wyrażeniu: $x \in (A \setminus B) \cap (A \setminus C)$. Ponieważ element x był dowolny, zatem powyższe równoważności zachodzą dla każdego x . Stąd, na mocy zasady ekstensjonalności, otrzymujemy dowodzoną własność.

Zwykle zapisujemy powyższe rozumowanie jako ciąg równoważności pewnych formuł, tzn. w postaci następującej (pamiętając, że rozważamy dowolny ustalony element x):

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

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

W podobny sposób dowodzi się też, że dla dowolnych zbiorów A, B, C

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

Udowodnione powyżej własności nazywa się prawami De Morgana dla zbiorów.

TWIERDZENIE 5.4.5. *Jeżeli U jest danym uniwersum i zbiory A oraz B są zawarte w U , to $B \setminus A = B \cap A'$.*

Dowód. Należy pokazać, że dla dowolnego elementu x

$$x \in B \setminus A \leftrightarrow x \in B \cap A'.$$

W tym celu, na mocy tautologii rachunku zdań

$$[(p \rightarrow q) \wedge (q \rightarrow p)] \leftrightarrow (p \leftrightarrow q),$$

wystarczy pokazać, że dla dowolnego elementu x

$$x \in B \setminus A \longrightarrow x \in B \cap A' \quad \text{oraz} \quad x \in B \cap A' \longrightarrow x \in B \setminus A.$$

Niech więc x będzie dowolnym elementem. Załóżmy, że $x \in B \setminus A$. Zatem, na mocy definicji, $x \in B$ i $x \notin A$. Stąd $x \in U, x \in B$ i $x \notin A$. Zatem $x \in B \wedge x \in A'$, czyli $x \in B \cap A'$. W ten sposób udowodniliśmy pierwszą z implikacji. Aby udowodnić drugą z nich, załóżmy, że $x \in B \cap A'$. Wtedy na mocy definicji $x \in B$ i $x \in A'$, czyli $x \in B$ i $x \notin A$, zatem $x \in B \setminus A$.

Z dowolności elementu x mamy ostatecznie

$$\forall x (x \in B \setminus A \leftrightarrow x \in B \cap A'),$$

co na mocy zasady ekstensjonalności daje równość $B \setminus A = B \cap A'$. Q.E.D.

Podstawowym twierdzeniem algebry zbiorów jest twierdzenie następujące:

TWIERDZENIE 5.4.6. *Dla dowolnych podzbiorów ustalonego uniwersum U zachodzą następujące równości:*

- | | |
|--|---|
| (1) $A \cup B = B \cup A,$ | (1') $A \cap B = B \cap A,$ |
| (2) $A \cup (B \cap C) = (A \cup B) \cap C,$ | (2') $A \cap (B \cup C) = (A \cap B) \cup C,$ |
| (3) $A \cup (B \cap C) =$
$= (A \cup B) \cap (A \cup C),$ | (3') $A \cap (B \cup C) =$
$= (A \cap B) \cup (A \cap C),$ |
| (4) $A \cup \emptyset = A,$ | (4') $A \cap U = A,$ |
| (5) $A \cup U = U,$ | (5') $A \cap \emptyset = \emptyset.$ |

Dowód. (1) Na mocy zasady ekstensjonalności wystarczy pokazać, że dla dowolnego elementu x zachodzi równoważność

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

czyli

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

Jest to jednak oczywiste na mocy prawa przemienności alternatywy

$$p \vee q \leftrightarrow q \vee p.$$

Podobnie – opierając się tym razem na prawie przemienności koniunkcji – otrzymujemy własność (1').

Własności (2) i (2') dowodzimy podobnie, korzystając teraz odpowiednio z praw łączności dla alternatywy i koniunkcji.

W dowodzie własności (3) wykorzystujemy prawo rozdzielności alternatywy względem koniunkcji. Istotnie, na mocy tego prawa oraz definicji działań mamy

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

Analogicznie – korzystając tym razem z prawa rozdzielności koniunkcji względem alternatywy – dowodzimy prawa (3').

Aby dowieść własności (4), wystarczy zauważyć, że tautologią jest formuła $p \vee 0 \leftrightarrow p$, gdzie 0 oznacza dowolne zdanie fałszywe, na przykład zdanie $x \in \emptyset$ (czyli innymi słowy alternatywa zdania p i zdania fałszywego ma tę samą wartość logiczną co zdanie p). Dla dowodu prawa (5') korzystamy z tautologii $p \wedge 0 \leftrightarrow 0$.

Pozostaje zatem udowodnić prawa (4') oraz (5). Zaczniemy od własności (4'). Niech więc x będzie dowolnym elementem i przypuśćmy, że $x \in A$. Ponieważ założyliśmy, że $A \subseteq U$, więc stąd także $x \in U$. Zatem $x \in A \wedge x \in U$, czyli $x \in A \cap U$. Na odwrót, jeśli $x \in A \cap U$, to z definicji przekroju $x \in A \wedge x \in U$. Na mocy prawa symplifikacji $p \wedge q \rightarrow p$ i reguły odrywania otrzymujemy stąd $x \in A$. Obie te implikacje dają nam równość (4').

Dla dowodu równości (5) założmy najpierw, że $x \in U$. Na mocy tautologii $q \rightarrow p \vee q$ oraz reguły odrywania otrzymujemy $x \in A \vee x \in U$. Zatem mamy implikację $x \in U \rightarrow x \in A \vee x \in U$. Na odwrót, niech $x \in A \cup U$. Wtedy $x \in A$ lub $x \in U$. W pierwszym przypadku, tzn. gdy $x \in A$, na mocy generalnego założenia, iż $A \subseteq U$, mamy $x \in U$. W drugim przypadku, gdy założymy, iż $x \in U$, otrzymamy oczywiście, na mocy prawa tożsamości, że $x \in U$. W każdym więc przypadku mamy $x \in U$. Stąd implikacja $x \in A \cup U \rightarrow x \in U$, co dowodzi ostatecznie prawa (5). Q.E.D.

Własności (1) i (1') nazywają się odpowiednio prawem przemienności sumy i przekroju, własności (2) i (2') nazywają się odpowiednio prawem łączności sumy i przekroju, prawo (3) nazywa się prawem rozdzielności sumy względem przekroju, a prawo (3') – prawem rozdzielności przekroju względem sumy.

Zauważmy, że na mocy praw przemienności możemy pisać po prostu $A_1 \cup A_2 \cup A_3 \cup \dots \cup A_n$ oraz $A_1 \cap A_2 \cap A_3 \cap \dots \cap A_n$, nie troszcząc się o rozmieszczenie nawiasów, które jest tutaj obojętne i może być jakiegokolwiek. Dla ustalenia uwagi wyrażenia te rozumiemy będziemy jako

$$(\dots((A_1 \cup A_2) \cup A_3) \cup \dots) \cup A_n \quad \text{oraz} \quad (\dots((A_1 \cap A_2) \cap A_3) \cap \dots) \cap A_n.$$

Zachodzą tu także uogólnione prawa przemienności sumy i przekroju, tzn. prawa

$$A_1 \cup A_2 \cup \dots \cup A_n = A_{i_1} \cup A_{i_2} \cup \dots \cup A_{i_n}$$

oraz

$$A_1 \cap A_2 \cap \dots \cap A_n = A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_n},$$

gdzie i_1, i_2, \dots, i_n to dowolna permutacja liczb $1, 2, \dots, n$, czyli ciąg liczb $1, 2, \dots, n$ ustawionych w dowolnej kolejności bez powtórzeń.

TWIERDZENIE 5.4.7 (prawa De Morgana). *Dla dowolnych zbiorów A i B zawartych w uniwersum U zachodzą równości*

$$(A \cup B)' = A' \cap B' \quad \text{oraz} \quad (A \cap B)' = A' \cup B'.$$

Dowód. Pokażemy, że $(A \cup B)' = A' \cap B'$. Dowód drugiej zależności, tzn. $(A \cup B)' = A' \cap B'$, jest podobny (pozostawiamy go Czytelnikowi). Dla dowolnego $x \in U$ mamy

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

Q.E.D.

TWIERDZENIE 5.4.8. Dodawanie i mnożenie zbiorów są działaniami idempotentnymi, tzn. dla dowolnego zbioru A zachodzi: $A \cup A = A$ oraz $A \cap A = A$. Spełnione są też następujące prawa pochłaniania:

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

Dowód. Idempotentność dodawania i mnożenia zbiorów wynikają bezpośrednio z praw idempotentności dla alternatywy i koniunkcji, tzn. z tautologii: $p \vee p \leftrightarrow p$ oraz $p \wedge p \leftrightarrow p$. Prawa pochłaniania łatwo otrzymać z definicji odpowiednich działań i z tautologii: $p \vee (p \wedge q) \leftrightarrow p$ oraz $p \wedge (p \vee q) \leftrightarrow p$.

Q.E.D.

LEMAT 5.4.9. Przekrój dwóch zbiorów jest zawarty w każdym z czynników. Suma dwóch zbiorów zawiera każdy ze składników, tzn.

$$A \cap B \subseteq A \quad \text{i} \quad A \cap B \subseteq B$$

oraz

$$A \subseteq A \cup B \quad \text{i} \quad B \subseteq A \cup B.$$

Dowód. Pierwsza część twierdzenia wynika z praw symlifikacji

$$p \wedge q \longrightarrow p \quad \text{oraz} \quad p \wedge q \longrightarrow q,$$

druga natomiast z praw addycji

$$p \longrightarrow p \vee q \quad \text{i} \quad q \longrightarrow p \vee q.$$

Q.E.D.

Zauważmy na koniec naszych rozważań, że zależności podane w twierdzeniu 5.4.6 ustawione zostały w pary. Wskazują one na dualność operacji sumy \cup i przekroju \cap oraz uniwersum U i zbioru pustego \emptyset . Łatwo zauważyć, że jeśli jakieś twierdzenie algebry zbiorów, dające się zapisać za pomocą działań \cup, \cap oraz dopełnienia $'$ i równości $=$, jest wnioskiem z własności (1)–(5) oraz (1')–(5') twierdzenia 5.4.6, to wtedy również twierdzenie dualne do niego, czyli twierdzenie otrzymane przez zastąpienie \cup przez \cap i na odwrót oraz U przez \emptyset i na odwrót, także daje się wyprowadzić z warunków (1)–(5) oraz (1')–(5') twierdzenia 5.4.6. Otrzymujemy w ten sposób następujące twierdzenie zwane zasadą dualności dla algebry zbiorów:

TWIERDZENIE 5.4.10 (zasada dualności). *Twierdzenie dualne do twierdzenia algebry zbiorów jest także twierdzeniem algebry zbiorów.*

5.5. Algebry Boole'a

Algebra zbiorów rozważana w poprzednim rozdziale jest szczególnym przykładem typu struktury często występującego w rozmaitych dziedzinach matematyki, a zwanego algebrą Boole'a⁷. Definicja tego pojęcia jest następująca:

DEFINICJA 5.5.1. Algebrą Boole'a nazywamy strukturę \mathbf{A} postaci

$$\langle A, \cup, \cap, -, 0, 1 \rangle,$$

gdzie A jest zbiorem, $0, 1 \in A$ oraz $-$ jest działaniem jednoargumentowym, a \cup i \cap są działaniami dwuargumentowymi w zbiorze A , spełniającymi dla wszystkich $x, y, z \in A$ następujące równości:

(B1) (prawa przemienności)

$$x \cup y = y \cup x, \quad x \cap y = y \cap x,$$

(B2) (prawa łączności)

$$(x \cup y) \cup z = x \cup (y \cup z), \quad (x \cap y) \cap z = x \cap (y \cap z),$$

(B3) (prawa rozdzielności)

$$x \cup (y \cap z) = (x \cup y) \cap (x \cup z), \quad x \cap (y \cup z) = (x \cap y) \cup (x \cap z),$$

⁷ Od nazwiska matematyka angielskiego George'a Boole'a (1815–1864), jednego z twórców i pionierów nowoczesnej logiki matematycznej.

(B4) (*prawa dla 0 i 1*)

$$x \cup 0 = x, \quad x \cap 1 = x,$$

(B5) (*prawa dopełnienia*)

$$x \cup -x = 1, \quad x \cap -x = 0.$$

Działania \cup, \cap i $-$ nazywane są odpowiednio dodawaniem, mnożeniem i dopełnieniem (booleowskim). Równości (B1)–(B5) nazywamy aksjomatami algebry Boole'a.

Przykładem algebry Boole'a może być struktura

$$\mathbf{2} = \langle \{0, 1\}, \vee, \wedge, \neg, 0, 1 \rangle,$$

gdzie zbiór $\{0, 1\}$ to zbiór wartości logicznych, a \vee, \wedge, \neg to działania odpowiadające spójnikom logicznym alternatywy, koniunkcji i negacji. Algebrę tę nazywa się algebrą dwójkową.

Inny przykład to algebra wszystkich podzbiorów danego zbioru U określona następująco: Niech U będzie dowolnym danym zbiorem niepustym. Rozważmy strukturę $\langle \mathcal{P}(U), \cup, \cap, ', \emptyset, U \rangle$, gdzie $\mathcal{P}(U)$ jest rodziną wszystkich podzbiorów zbioru U , a $\cup, \cap, '$ są działaniami sumy, przekroju i dopełnienia (do uniwersum U) podzbiorów zbioru U . Łatwo spostrzec, że w strukturze takiej spełnione są wszystkie aksjomaty algebry Boole'a (por. twierdzenie 5.4.6 z poprzedniego paragrafu).

Zauważmy, że w definicji algebry Boole'a nie korzysta się z symbolu \in ; intuicyjnie jednak zmienne x, y itd. rozumie się jako zmienne przebiegające nazwy zbiorów. Można powiedzieć, że aksjomaty algebry Boole'a charakteryzują działania \cup, \cap i $'$, nie używając pojęcia należenia \in .

Pokażemy teraz, że w każdej algebrze Boole'a $\mathbf{A} = \langle A, \cup, \cap, -, 0, 1 \rangle$ prawdziwe są następujące równości:

$$(B6) \quad x \cup x = x, \quad x \cap x = x,$$

$$(B7) \quad x \cup 1 = 1, \quad x \cap 0 = 0$$

dla każdego $x \in A$. Istotnie mamy

$$x = x \cup 0 = x \cup (x \cap -x) = (x \cup x) \cap (x \cup -x) = (x \cup x) \cap 1 = x \cup x.$$

Korzystamy tu po kolei z praw (B4), (B5), (B3), (B5) i (B4). W ten sposób otrzymaliśmy pierwszą z równości (B6). Dowód drugiej jest następujący:

$$x = x \cap 1 = x \cap (x \cup -x) = (x \cap x) \cup (x \cap -x) = (x \cap x) \cup 0 = x \cap x.$$

Jak widać, przebiega on podobnie jak dowód pierwszej równości, z tym że zastąpiliśmy wszędzie 0 przez 1, 1 przez 0, \cup przez \cap i \cap przez \cup . O dowodach takich mówimy, że są dualne.

Udowodnijmy teraz pierwszą z równości (B7). Mamy

$$x \cup 1 = x \cup (x \cup -x) = (x \cup x) \cup -x = x \cup -x = 1.$$

Korzystamy tutaj z praw (B5), (B2), (B6) i jeszcze raz (B5). Dowód drugiej z równości (B7) jest dualny.

Przykłady te pokazują pewną ogólniejszą własność. Otóż niech φ będzie zdaniem sformułowanym w języku algebry Boole'a, tzn. zdaniem zawierającym zmienne, stałe 0 i 1, symbole działań $\cup, \cap, '$ oraz symbol równości i spójniki logiczne. Niech φ^d oznacza zdanie otrzymane ze zdania φ przez konsekwentne zastąpienie 0 przez 1, 1 przez 0, symbolu \cup przez \cap , a symbolu \cap przez \cup . Tak otrzymane zdanie φ^d nazywamy dualizacją zdania φ .

Niech $\mathbf{A} = \langle A, \cup, \cap, -, 0, 1 \rangle$ będzie algebrą Boole'a. Strukturę \mathbf{A}^d postaci $\langle A, \cap, \cup, -, 1, 0 \rangle$ nazywamy algebrą dualną do algebry \mathbf{A} . Łatwo zauważyć, że jeśli zdanie φ jest prawdziwe w algebrze \mathbf{A} , to zdanie dualne φ^d jest prawdziwe w algebrze dualnej \mathbf{A}^d . W konsekwencji struktura \mathbf{A}^d jest też algebrą Boole'a. Istotnie, jeżeli φ jest jednym z aksjomatów algebry Boole'a, to zdanie φ^d jest też aksjomatem algebry Boole'a, a więc φ^d jest prawdziwe w \mathbf{A} . Stąd zdanie φ^{dd} , czyli zdanie φ , jest prawdziwe w \mathbf{A}^d .

Zachodzi teraz następujące twierdzenie, które jest bardzo użytecznym narzędziem w dowodzeniu rozmaitych zależności dla algebr Boole'a:

TWIERDZENIE 5.5.2 (zasada dualności). *Jeżeli zdanie φ w języku algebr Boole'a jest prawdziwe w każdej algebrze Boole'a, to zdanie φ^d jest też prawdziwe w każdej algebrze Boole'a.*

Dowód. Załóżmy, że zdanie φ jest prawdziwe w każdej algebrze Boole'a. Niech \mathbf{A} będzie dowolną daną algebrą Boole'a. Zatem struktura \mathbf{A}^d jest także algebrą Boole'a. Na mocy założenia, zdanie φ jest prawdziwe w \mathbf{A}^d , a stąd φ^d jest prawdziwe w algebrze \mathbf{A}^{dd} , czyli w algebrze \mathbf{A} . Q.E.D.

Z zasady dualności i twierdzenia o pełni logiki pierwszego rzędu, które jest podstawowym twierdzeniem logiki matematycznej, wynika, że dualizacja φ^d każdego zdania φ sformułowanego w języku algebr Boole'a i będącego konsekwencją (tzn. dającego się wydedukować z) aksjomatów algebry Boole'a jest także konsekwencją tych aksjomatów. W związku z tym wystarczy zawsze udowodnić tylko jedno z pary zdań dualnych. Dodajmy jeszcze, że stosowanie tej zasady wymaga jednak pewnej ostrożności. Otóż

można ją stosować tylko w odniesieniu do zdań o opisanej powyżej budowie, tzn. zawierających tylko określone symbole. Zauważmy też, że zasada dualności, sformułowana na końcu poprzedniego paragrafu (w odniesieniu do algebry podzbiorów danego zbioru U), jest szczególnym przypadkiem udowodnionej ogólnej zasady dualności.

Na koniec udowodnimy jeszcze kilka praw dotyczących działania dopełnienia w algebrach Boole'a. Zaczniemy od następującego prawa:

$$(B8) \quad x \cup y = 1 \wedge x \cap y = 0 \longrightarrow -x = y.$$

Ponieważ $y = -x$ spełnia obie równości po lewej stronie powyższej implikacji, więc sens prawa (B8) można wysłowić, mówiąc, że $-x$ jest jedynym elementem y , takim że $x \cup y = 1$ i $x \cap y = 0$.

Dla dowodu prawa (B8) założymy, że $x \cup y = 1 \wedge x \cap y = 0$. Mamy wtedy

$$\begin{aligned} -x &= -x \cap 1 = -x \cap (x \cup y) = \\ &= (-x \cap x) \cup (-x \cap y) = 0 \cup (-x \cap y) = -x \cap y, \\ y &= y \cap 1 = y \cap (x \cup -x) = \\ &= (y \cap x) \cup (y \cap -x) = 0 \cup (y \cap -x) = y \cap -x. \end{aligned}$$

Stąd, na mocy praw przemienności (B1), otrzymujemy: $-x = y$.

Udowodnijmy jeszcze następujące prawa:

$$(B9) \quad -0 = 1, \quad -1 = 0,$$

$$(B10) \quad -(-x) = x,$$

$$(B11) \quad -(x \cup y) = -x \cap -y, \quad -(x \cap y) = -x \cup -y.$$

Prawa (B11) nazywamy prawami De Morgana dla algebry Boole'a (podane w poprzednim rozdziale prawa De Morgana dla zbiorów są szczególnym przypadkiem tych praw).

Dla dowodu (B9) wystarczy zauważyć, że równości $0 \cup 1 = 1$ i $0 \cap 1 = 0$ są prawdziwe na mocy (B7) i (B4). Zatem, opierając się na implikacji (B8), otrzymujemy bezpośrednio (B9). Podobnie (B10) wynika z (B5). Aby dowieść (B11), zauważmy, że

$$(x \cup y) \cup (-x \cap -y) = (x \cup y \cup -x) \cap (x \cup y \cup -y) = 1 \cap 1 = 1$$

oraz

$$(x \cup y) \cap (-x \cap -y) = (x \cap -x \cap -y) \cup (y \cap -x \cap -y) = 0 \cup 0 = 0.$$

Korzystając z tych równości oraz z prawa (B8), otrzymujemy pierwsze z praw (B11). Dowód drugiego z praw (B11) jest dualny.

Związek między algebraami Boole'a i algebraami wszystkich podzbiorów jakiegoś zbioru podaje następujące twierdzenie Stone'a:

TWIERDZENIE 5.5.3 (twierdzenie Stone'a). *Każda algebra Boole'a A jest izomorficzna z podalgebrą algebry wszystkich podzbiorów pewnego zbioru U .*

Zadania

1. Wymienić elementy następujących zbiorów:

- a) \emptyset ,
- b) $\{\emptyset\}$,
- c) $\{\{\emptyset\}, \emptyset\}$,
- d) $\{\{a\}, a, b\}$,
- e) $\{\{a\}, a, \emptyset\}$,
- f) $\{x \in \mathbb{N} : n \leq 10\}$,
- g) $\{x \in \mathbb{R} : 2x^2 - 3x + 1 \neq 0\}$,
- h) $\{x \in \mathbb{R} : x^2 + 1 = 0\}$,
- i) $\{x \in \mathbb{C} : x^2 + 1 = 0\}$.

2. Pokazać, że:

- a) $\{a, a, b, b\} = \{b, a\}$,
- b) $\emptyset \neq \{\emptyset\}$,
- c) $\emptyset \subseteq \emptyset$,
- d) $\emptyset \subsetneq \{\emptyset\}$,
- e) $\{\emptyset\} \neq \{\{\emptyset\}, \emptyset\}$.

3. Jakie związki pomiędzy obiektami a, b, c, d muszą zachodzić, aby spełnione były następujące równości:

- a) $\{a, b, c\} = \{a, b, d\}$,
- b) $\{\{a\}, \{b, c\}\} = \{\{d\}, \{c, d\}\}$,
- c) $\{\{a, b\}, c\} = \{\{a\}, \{d\}\}$,
- d) $\{\{a\}, \{b\}\} = \{\{\emptyset\}\}$.

Uwaga: rozważyć też przypadek, gdy któryś z obiektów a, b, c, d to \emptyset .

4. Zakładając, że różne małe litery oznaczają różne obiekty, wyznaczyć zbiory $A \cup B$, $A \cap B$, $A \setminus B$ i $B \setminus A$, gdy

- a) $A = \{a, b, c\}$, $B = \{a, c, d\}$,
- b) $A = \{a, b, c\}$, $B = \{c\}$,
- c) $A = \{\emptyset\}$, $B = \{\emptyset, \{\emptyset\}\}$,
- d) $A = \{n \in \mathbb{N} : 2|n\}$, $B = \{n \in \mathbb{N} : 2|(n+1)\}$,
- e) $A = \{n \in \mathbb{Z} : 2|n\}$, $B = \{n \in \mathbb{N} : 2|n\}$.

5. Znaleźć sumę, przekrój oraz różnice $A \setminus B$ i $B \setminus A$ następujących zbiorów:

- a) $A = \{x \in \mathbb{R} : x \geq 1\}$, $B = \{x \in \mathbb{N} : x > 2\}$,
 b) $A = \{x \in \mathbb{Z} : x \geq -2\}$, $B = \{x \in \mathbb{N} : x < 10\}$,
 c) $A = \{x \in \mathbb{R} : x > \sqrt{2}\}$, $B = \{x \in \mathbb{R} : x < \sqrt{2}\}$.

6. Zbadać, czy pomiędzy zbiorami A i B zachodzi w którąś ze stron relacja inkluzji:

- a) $A = \emptyset$, $B = \{a, b\}$,
 b) $A = \{a\}$, $B = \{\{a\}, \{\{a\}\}\}$,
 c) $A = \{x \in \mathbb{R} : x^2 - 1 = 0\}$, $B = \{x \in \mathbb{R} : x^2 - 2x + 1 = 0\}$,
 d) $A = \{x \in \mathbb{N} : x^3 > 3\}$, $B = \{x \in \mathbb{N} : x^3 > 9\}$,
 e) $A = \{x \in \mathbb{R} : |x| > 1\}$, $B = \{x \in \mathbb{N} : x > 1\}$,
 f) $A =$ zbiór trapezów, $B =$ zbiór równoległoboków.

7. Udowodnić, że dla dowolnych zbiorów A, B, C, D prawdziwe są następujące równości:

- a) $(A \cap B) \cup (A \cap B') = A$,
 b) $A \cap (B \setminus A) = \emptyset$,
 c) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$,
 d) $A \setminus (B \cup C) = (A \setminus B) \setminus C$,
 e) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$,
 f) $(A \setminus B) \cap C' = A \cap (B \cup C)'$,
 g) $(A \setminus B) \cup C = [(A \cup C) \setminus B] \cup (B \cap C)$,
 h) $(A \setminus B) \cap (C \setminus D) = (A \cap C) \setminus (B \cup D)$.

8. Dowieść, że dla dowolnych zbiorów A, B, C, D prawdziwe są następujące równości:

- a) $A \div B = (A \cup B) \setminus (A \cap B)$,
 b) $A \div B = B \div A$,
 c) $A \div A = \emptyset$,
 d) $(A \div B) \div C = A \div (B \div C)$,
 e) $A \cup (B \div C) = (A \cup B) \div (A \cup C)$,
 f) $A \cap (B \div C) = (A \cap B) \div (A \cap C)$.

9. Sprawdzić, czy zachodzą następujące związki (jeśli nie zachodzą, znaleźć kontrprzykład):

- a) $(A' \cap B)' \cap A = A$,
 b) $(A \cap B) \cup (C \cap D) = (A \cup C) \cap (A \cup D) \cap (B \cup C) \cap (B \cup D)$,
 c) $A \cap (B \setminus C) = (A \setminus C) \setminus (B \setminus C)$,
 d) $(A \setminus B) \setminus C = (A \setminus B) \cup (A \cap C)$,
 e) $A \div (A \div B) = B$,
 f) $A \cup B = (A \div B) \cup (A \cap B)$,
 g) $A \div B = \emptyset \leftrightarrow (A = B)$,
 h) $B \subseteq A \rightarrow (A \setminus B) \cup B = A$,
 i) $B \subseteq A \rightarrow A \cap (B \cup C) = B \cup (A \cap C)$.

10. Korzystając z równości podanych w twierdzeniu 5.4.6 udowodnić następujące równości:

- a) $(A \cap C) \cup (B \cap C \cap A) = A \cap C$,
 b) $A \cup (B \setminus C) = (A \cup B) \cap (A \setminus C)$,
 c) $((A \cap B) \cup C) \cap B = (B \cap C) \cup (A \cap B)$,
 d) $(A \cap B) \cup (A \cap C) \cup (B \cap C) = (A \cup B) \cap (A \cup C) \cap (B \cup C)$.

11. Dowieść następujących implikacji i równoważności:

- a) $A \subseteq B \rightarrow A \cap C \subseteq B \cap C$,
 b) $A \subseteq B \rightarrow A \cup C \subseteq B \cup C$,
 c) $A \subseteq B \rightarrow C \setminus B \subseteq C \setminus A$,
 d) $A \subseteq B \wedge C \subseteq D \rightarrow A \cap C \subseteq B \cap D$,
 e) $A \subseteq B \wedge C \subseteq D \rightarrow A \cup C \subseteq B \cup D$,
 f) $A \subseteq B \cap C \leftrightarrow A \subseteq B \wedge A \subseteq C$,
 g) $A \cap B \subseteq C \leftrightarrow A \subseteq (B' \cup C)$.

12. Znaleźć wszystkie podzbiory następujących zbiorów:

- a) $\{a, b, c, d\}$,
 b) $\{\{a\}, a, \emptyset\}$,
 c) $\{\{\{a\}\}, \{a\}, a\}$,
 d) $\{\{a, b, c\}, \{a, b\}, \{a\}, a\}$.

13. Ile istnieje dwuelementowych podzbiorów zbioru 10-elementowego? Ile istnieje trzelementowych podzbiorów takiego zbioru? Ile istnieje k -elementowych podzbiorów zbioru n -elementowego ($k \leq n$)? (*Wskazówka*: skorzystaj z podręcznika omawiającego podstawy kombinatoryki).

Rozdział 6

Relacje

6.1. Wprowadzenie. Definicja relacji

W języku potocznym słowem relacja określa się związek pomiędzy jakimiś rozważanymi obiektami. Mówimy więc na przykład, że dwie proste l_1 i l_2 są równoległe, że liczba naturalna y jest podzielna przez liczbę naturalną x (lub że x dzieli y) czy że Adam Kowalski jest starszym bratem Zosi Kowalskiej lub że Poznań leży między Berlinem a Warszawą. Oczywiście takie potoczne określenie relacji jako związku między obiektami nie wystarcza w matematyce. Stąd potrzeba uściślenia tego pojęcia i oparcia go na jakimś solidniejszym fundamencie. Tym fundamentem będzie dla nas pojęcie zbioru.

Aby zdefiniować precyzyjnie pojęcie relacji potrzebne będzie pojęcie pary. Wyróżniamy pary nieuporządkowane i pary uporządkowane. Otóż przez parę nieuporządkowaną (krótko: parę) elementów x i y rozumiemy zbiór złożony dokładnie z x i y , tzn. zbiór $\{x, y\}$. Oczywiście, na mocy zasady ekstensjonalności: $\{x, y\} = \{y, x\}$ oraz $\{x, x\} = \{x\}$. Przez pojęcie pary uporządkowanej rozumiemy obiekt, oznaczany jako $\langle x, y \rangle$, złożony z dwóch elementów, ale taki że istotne jest, który element jest pierwszy, a który drugi. Postulujemy zatem, by pojęcie pary uporządkowanej spełniało warunek: $\langle x, y \rangle = \langle u, v \rangle$ wtedy i tylko wtedy, gdy $x = u$ i $y = v$. Obiekt o takich własnościach można określić na różne sposoby. W tym wykładzie przyjmujemy następującą definicję:

DEFINICJA 6.1.1. Parą uporządkowaną $\langle x, y \rangle$ nazywać będziemy zbiór $\{\{x\}, \{x, y\}\}$. Element x nazywamy pierwszą współrzędną, a element y drugą współrzędną pary $\langle x, y \rangle$ ¹.

¹ Definicja ta pochodzi od polskiego matematyka Kazimierza Kuratowskiego

Okazuje się, że podana tu definicja Kuratowskiego spełnia warunki nakładane na pojęcie pary uporządkowanej.

TWIERDZENIE 6.1.2. *Para uporządkowana $\langle x, y \rangle$ jest wyznaczona jednoznacznie przez elementy x i y . Ponadto $\langle x, y \rangle = \langle u, v \rangle$ wtedy i tylko wtedy, gdy $x = u$ oraz $y = v$.*

D o w ó d. Jednoznaczność wynika z definicji pary uporządkowanej oraz z zasady ekstensjonalności. Dla dowodu drugiej części twierdzenia założymy najpierw, że $x = u$ i $y = v$. Wtedy oczywiście $\{x\} = \{u\}$ oraz $\{x, y\} = \{u, v\}$, a w konsekwencji także $\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}$, czyli $\langle x, y \rangle = \langle u, v \rangle$. Na odwrót, założymy, że $\langle x, y \rangle = \langle u, v \rangle$. Rozróżnimy dwa przypadki: (I) $u = v$ oraz (II) $u \neq v$. W przypadku I mamy: $\langle u, v \rangle = \{\{u\}, \{u, v\}\} = \{\{u\}, \{u, u\}\} = \{\{u\}\}$. Zatem $\langle x, y \rangle = \{\{x\}, \{x, y\}\} = \{\{u\}\}$. Stąd $\{x\} = \{x, y\} = \{u\}$. A więc $x = y = u = v$. W przypadku II zgodnie z założeniem $u \neq v$. Zatem zbiór $\{u, v\}$ ma dwa elementy, a więc $\{x\} \neq \{u, v\}$. Stąd $\{u, v\} = \{x, y\}$ oraz $\{u\} = \{x\}$. Czyli $u = x$ i skoro $\{x, v\} = \{x, y\}$, zatem $v = y$. Q.E.D.

Mając pojęcie pary uporządkowanej, możemy (przez indukcję względem n) zdefiniować ogólne pojęcie n -ki ($n \geq 2$) uporządkowanej. Krok indukcyjny wygląda następująco:

$$\langle x_1, x_2, \dots, x_{n+1} \rangle = \langle \langle x_1, x_2, \dots, x_n \rangle, x_{n+1} \rangle.$$

DEFINICJA 6.1.3. *Niech dane będą dwa zbiory X i Y . Produktem (iloczynem) kartezjańskim zbiorów X i Y nazywamy zbiór*

$$X \times Y = \{\langle x, y \rangle : x \in X \wedge y \in Y\}.$$

Podobnie definiujemy produkt kartezjański $X_1 \times \dots \times X_n$ n zbiorów X_1, \dots, X_n .

Potocznie relację rozumie się – jak to wskazywaliśmy powyżej – jako związek elementów, ale nic nie stoi na przeszkodzie, aby na użytek matematyki relację utożsamić ze zbiorem par, trójek itd. elementów połączonych tym związkiem.

Pojęcie n -ki uporządkowanej pozwala na zdefiniowanie w sposób precyzyjny ogólnego pojęcia relacji.

(1896–1980), a podana została w pracy *Sur la notion de l'ordre dans la théorie des ensembles*, *Fundamenta Mathematicae* 2, 1921, 161–171.

DEFINICJA 6.1.4. Niech $n \geq 2$. Relacją n -członową nazywamy dowolny zbiór, którego elementami są n -ki uporządkowane. Mówimy, że relacja n -członowa R jest relacją w zbiorze X wtedy i tylko wtedy, gdy R jest zbiorem n -ek uporządkowanych elementów X , tzn. $R \subseteq \underbrace{X \times \dots \times X}_n$.

Gdy $n = 2$, to mówimy o relacjach binarnych, gdy $n = 3$ – o relacjach ternarnych. Jeśli dopuścić pojęcie 1-ki uporządkowanej (którą utożsamić można po prostu z elementem), to mówić można też o relacjach 1-członowych (zwanych relacjami unarnymi). Pojęcie to pokrywa się jednak z pojęciem zbioru.

6.2. Relacje binarne i ich własności. Działania na relacjach binarnych

Od tej pory ograniczymy się do rozważania tylko relacji binarnych. Zamiast $\langle x, y \rangle \in R$ pisać będziemy po prostu xRy .

DEFINICJA 6.2.1. Niech R będzie relacją binarną, to znaczy podzbiorem zbioru $X \times Y$. Dziedziną lewostronną relacji R nazywamy zbiór²

$$D_R = \{x : \exists y (xRy)\},$$

a dziedziną prawostronną nazywamy zbiór

$$D_R^* = \{y : \exists x (xRy)\}.$$

Sumę $D_R \cup D_R^*$ nazywamy polem relacji R .

Jeśli relacja R jest n -członowa ($n \geq 3$), to mówimy o i -tej dziedzinie relacji R ($1 \leq i \leq n$) i określamy ją analogicznie.

Jeżeli $R \subseteq X \times X$, to relację R nazywamy relacją w zbiorze X . Łatwo zauważyć, że podana na początku jako przykład relacja równoległości prostych może być rozumiana jako relacja binarna w zbiorze X wszystkich prostych na danej płaszczyźnie. Wtedy $D_R = D_R^* = X$. W przypadku relacji podzielności mamy do czynienia z relacją binarną w zbiorze \mathbb{N} liczb naturalnych. Dziedziną lewostronną jest zbiór \mathbb{N} , a prawostronną zbiór $\mathbb{N} \setminus \{0\}$ (zbiór \mathbb{N} pozbawiony liczby 0). W trzecim przykładzie,

² W literaturze spotkać można też termin dziedziną na określenie tego, co nazwa-
liśmy tutaj dziedziną lewostronną i termin przeciwdziedziną na określenie dziedziny
prawostronnej. Używa się też czasami innych symboli. I tak dziedzinę lewostronną relacji
 R oznacza się także jako $D(R)$, a dziedzinę prawostronną jako $D^*(R)$ czy jako $\check{D}(R)$.

tn. w przypadku relacji R bycia bratem, mamy relację w zbiorze wszystkich ludzi. Dziedzina lewostronna D_R jest teraz równa zbiorowi wszystkich mężczyzn mających rodzeństwo, a dziedzina prawostronna D_R^* – zbiorowi wszystkich ludzi mających brata.

Dla relacji binarnych określimy teraz szereg własności, które pozwolą wyróżnić w dalszym ciągu różne typy relacji ważne ze względu na rolę, jaką pełnią one w matematyce.

DEFINICJA 6.2.2. Niech R będzie relacją w zbiorze X , to znaczy zachodzi $R \subseteq X \times X$. Mówimy, że relacja R jest³:

- (1) zwrotna wtedy i tylko wtedy, gdy $\forall x \in X (xRx)$,
- (2) przeciwwrotna wtedy i tylko wtedy, gdy $\forall x \in X \neg(xRx)$, czyli innymi słowy $\neg\exists x \in X (xRx)$,
- (3) niezwrotna wtedy i tylko wtedy, gdy $\neg\forall x \in X (xRx)$, czyli innymi słowy $\exists x \in X \neg(xRx)$,
- (4) symetryczna wtedy i tylko wtedy, gdy

$$\forall x \in X \forall y \in X (xRy \longrightarrow yRx),$$

- (5) przeciwsymetryczna (asymetryczna) wtedy i tylko wtedy, gdy

$$\forall x \in X \forall y \in X (xRy \longrightarrow \neg yRx),$$

- (6) antysymetryczna (słabo antysymetryczna, na wpół przeciwsymetryczna) wtedy i tylko wtedy, gdy

$$\forall x \in X \forall y \in X (xRy \wedge yRx \longrightarrow x = y),$$

- (7) przechodnia wtedy i tylko wtedy, gdy

$$\forall x \in X \forall y \in X \forall z \in X (xRy \wedge yRz \longrightarrow xRz),$$

- (8) spójna wtedy i tylko wtedy, gdy

$$\forall x \in X \forall y \in X (xRy \vee yRx \vee x = y),$$

- (9) diagonalna wtedy i tylko wtedy, gdy

$$\forall x \in X [xRx \wedge \forall y \in X (y \neq x \rightarrow \neg xRy \wedge \neg yRx)],$$

- (10) totalna wtedy i tylko wtedy, gdy $\forall x \in X \forall y \in X (xRy)$.

³ Ponieważ terminologia w zakresie własności relacji nie jest jednoznacznie ustalona, podajemy tu, obok nazw, które będą używane dalej, także nazwy, które można spotkać w innych podręcznikach.

Przykładem relacji zwrotnej jest relacja identyczności $=$ w dowolnym danym zbiorze X czy relacja podzielności $|$ w zbiorze $\mathbb{N} \setminus \{0\}$.

Przeciwwrotna jest relacja mniejszości $<$ w zbiorze \mathbb{R} liczb rzeczywistych i relacja ojcostwa w zbiorze wszystkich ludzi. Relacja mniejszości $<$ jest też przykładem relacji niezwrótnej.

Przykładem relacji symetrycznej może być relacja równoległości \parallel w zbiorze prostych na danej płaszczyźnie.

Jako przykład relacji przeciwsymetrycznej można podać relację bycia większym $>$ w zbiorze liczb rzeczywistych \mathbb{R} oraz relację bycia dwukrotnością w zbiorze $\mathbb{N} \setminus \{0\}$, czyli relację $xRy \leftrightarrow x = 2y$.

Antysymetryczne są dla przykładu relacja \leq w zbiorze \mathbb{R} oraz relacja inkluzji \subseteq w dowolnej danej rodzinie zbiorów.

Przykładem relacji przechodniej może być relacja podzielności $|$ w zbiorze \mathbb{N} i relacja inkluzji \subseteq w dowolnej danej rodzinie zbiorów.

Jako przykład relacji spójnej można podać relację \leq w zbiorze \mathbb{R} .

Wreszcie przykładem relacji diagonalnej jest relacja równości $=$ w dowolnym danym zbiorze, a przykładem relacji totalnej – relacja określona jako $x = y \vee x \neq y$.

Na relacjach można wykonywać pewne działania. Ponieważ relacje są specjalnymi zbiorami (tzn. zbiorami par czy ogólnie n -ek uporządkowanych), więc w szczególności określone są dla nich w zwykły sposób takie działania, jak suma, przekrój, różnica, różnica symetryczna czy wreszcie dopełnienie. I tak na przykład sumę $R \cup S$ relacji R i S w zbiorze X określamy następująco:

$$\langle x, y \rangle \in R \cup S \leftrightarrow \langle x, y \rangle \in R \vee \langle x, y \rangle \in S.$$

Innymi słowy $x(R \cup S)y \leftrightarrow xRy \vee xSy$. Podobnie dla przekroju $R \cap S$ mamy

$$\langle x, y \rangle \in R \cap S \leftrightarrow \langle x, y \rangle \in R \wedge \langle x, y \rangle \in S.$$

Zatem $x(R \cap S)y \leftrightarrow xRy \wedge xSy$. Analogicznie definiujemy różnicę, różnicę symetryczną oraz dopełnienie relacji.

Istnieją jednak dwa działania specyficzne dla relacji (tzn. nie mające swych odpowiedników dla zwykłych zbiorów). Są to działania konwersu (relacji odwrotnej) i iloczynu względnego (złożenia relacji).

DEFINICJA 6.2.3. Niech R i S będą relacjami w zbiorze X . Konwersem relacji R nazywamy relację \check{R} określoną wzorem $x\check{R}y \leftrightarrow yRx$.

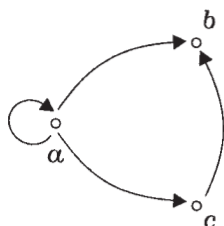
Iloczynem względnym (złożeniem) relacji R i S nazywamy relację $R \circ S$ określoną następująco:

$$x(R \circ S)y \leftrightarrow \exists z \in X [xRz \wedge zSy].$$

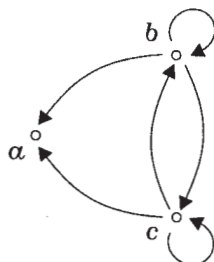
Łatwo zauważyć, że na przykład sumą relacji bycia ojcem i relacji bycia matką w zbiorze wszystkich ludzi jest relacja bycia rodzicem, natomiast przekrojem relacji \leq i relacji \geq w zbiorze \mathbb{R} liczb rzeczywistych jest relacja identyeczności $=$. Konwersem relacji podzielności jest relacja bycia dzielnikiem, a iloczynem względnym relacji bycia żoną i relacji bycia synem jest relacja bycia synową.

Relacje na zbiorach skończonych można reprezentować za pomocą diagramów i za pomocą macierzy.

Niech więc dana będzie relacja $R = \{\langle a, b \rangle, \langle a, c \rangle, \langle a, a \rangle, \langle c, b \rangle\}$. Wyróżnijmy na płaszczyźnie punkty odpowiadające elementom a, b i c , a następnie połączmy strzałkami te punkty, pomiędzy którymi zachodzi relacja R . Otrzymujemy następujący rysunek, który nazywać będziemy diagramem relacji R



Podobnie diagramem relacji $R = \{\langle b, a \rangle, \langle b, b \rangle, \langle b, c \rangle, \langle c, b \rangle, \langle c, c \rangle, \langle c, a \rangle\}$ będzie rysunek



Relacje na skończonym zbiorze można też reprezentować za pomocą macierzy. To, że relacja zachodzi pomiędzy elementami x i y zaznaczamy, pisząc 1 na skrzyżowaniu wiersza odpowiadającego x i kolumny odpowiadającej y , a symbol 0, jeśli relacja między nimi nie zachodzi. Zgodnie z tym

macierz pierwszej z rozważanych powyżej relacji wyglądać będzie następująco:

$$\begin{array}{c|ccc} & a & b & c \\ \hline a & 1 & 1 & 1 \\ b & 0 & 0 & 0 \\ c & 0 & 1 & 0 \end{array}$$

Macierz odpowiadającą drugiej relacji będzie taka

$$\begin{array}{c|ccc} & a & b & c \\ \hline a & 0 & 0 & 0 \\ b & 1 & 1 & 1 \\ c & 1 & 1 & 1 \end{array}$$

Niektóre własności relacji można łatwo zinterpretować, posługując się diagramem lub macierzą danej relacji. Tak na przykład relacja R jest symetryczna, jeśli – dla dowolnych elementów x i y – albo strzałce biegnącej z x do y towarzyszy strzałka z y do x , albo też nie są one połączone żadną strzałką. Zwrotność ilustruje „pętelka” na każdym punkcie. Łatwo też podać interpretację przeciwsymetrii i przeciwzwrotności, a także diagonalności i totalności (pozostawiamy to Czytelnikowi jako łatwe ćwiczenie).

Przy przedstawieniu macierzowym relacji, zwrotność wyraża się tym, że na głównej przekątnej występują same jedynki, a symetria jako symetria macierzy względem głównej przekątnej. Relacja jest diagonalna, gdy jej macierza jest diagonalna, tzn. gdy na głównej przekątnej występują same jedynki, a poza przekątną same zera (stąd też pochodzi nazwa tej własności relacji).

6.3. Relacje równoważności

DEFINICJA 6.3.1. Niech R będzie relacją binarną w zbiorze X , czyli $R \subseteq X \times X$. Mówimy, że R jest relacją równoważności wtedy i tylko wtedy, gdy R jest

- (1) zwrotna, tzn. $\forall x \in X (xRx)$,
- (2) symetryczna, tzn. $\forall x \in X \forall y \in X (xRy \rightarrow yRx)$,
- (3) przechodnia, tzn. $\forall x \in X \forall y \in X \forall z \in X (xRy \wedge yRz \rightarrow xRz)$.

Oto kilka przykładów relacji równoważności:

- (1) relacja identyczności = w dowolnym zbiorze X ,
- (2) relacja podobieństwa w zbiorze wszystkich figur geometrycznych na danej płaszczyźnie,

(3) relacja \equiv_n przystawania modulo n w zbiorze liczb całkowitych \mathbb{Z} dla dowolnego danego $n \in \mathbb{N}$, tzn. relacja

$$x \equiv_n y \leftrightarrow \exists z (x - y = n \cdot z) \leftrightarrow n|(x - y),$$

(4) relacja zamieszkiwania w tym samym budynku wśród mieszkańców Poznania.

Zamiast „relacja równoważności” mówi się czasami „relacja równoważnościowa” lub „relacja równościowa”. Jeśli R jest relacją równoważności, to zamiast R pisze się czasami \sim lub \approx .

DEFINICJA 6.3.2. Niech R będzie relacją równoważności w zbiorze X i niech $x \in X$. Klasą abstrakcji (klasą równoważności) elementu x względem relacji R nazywamy zbiór $[x]_R = \{y \in X : xRy\}$.

Jeśli wiadomo, o jaką relację chodzi, to czasami będziemy opuszczali wskaźnik R i pisali po prostu $[x]$.

Następujące twierdzenie podaje podstawowe własności klas abstrakcji:

TWIERDZENIE 6.3.3. Niech R będzie relacją równoważności w niepustym zbiorze X . Wtedy dla dowolnych elementów $x, y, z \in X$

- (1) $x \in [x]_R$,
- (2) $[x]_R = [y]_R$ wtedy i tylko wtedy, gdy xRy ,
- (3) jeśli $[x]_R \neq [y]_R$, to $[x]_R \cap [y]_R = \emptyset$.

D o w ó d. Własność (1) wynika bezpośrednio z założonej zwrotności relacji R .

Dla dowodu własności (2) założymy, że $[x]_R = [y]_R$. Zatem, na mocy własności (1), $x \in [y]_R$, czyli yRx , a stąd oczywiście xRy . W ten sposób pokazaliśmy implikację w prawo. Dla dowodu implikacji odwrotnej założymy, że xRy i niech z będzie dowolnym elementem X . Jeśli $z \in [x]_R$, to xRz , czyli także zRx . Ale z założenia xRy . Z własności przechodniości relacji R mamy zatem zRy , czyli $z \in [y]_R$. Pokazaliśmy więc, że $[x]_R \subseteq [y]_R$. Podobnie dowodzi się inkluzji odwrotnej. Ostatecznie więc jeśli xRy , to $[x]_R = [y]_R$.

Aby dowieść własności (3), założymy, że $[x]_R \neq [y]_R$. Przypuśćmy (dla dowodu nie wprost), że $[x]_R \cap [y]_R \neq \emptyset$. Niech $z \in [x]_R \cap [y]_R$. Stąd $z \in [x]_R$ i $z \in [y]_R$, czyli xRz i yRz , a zatem xRz i zRy , a więc xRy . Stąd, na mocy własności (2), mamy $[x]_R = [y]_R$, co jednak jest sprzeczne z założeniem. Ostatecznie więc jeśli $[x]_R \neq [y]_R$, to $[x]_R \cap [y]_R = \emptyset$. Q.E.D.

Dla relacji równoważności zachodzi następujące ważne twierdzenie mające liczne zastosowania w matematyce, w szczególności do definiowania nowych pojęć. Jest ono konsekwencją poprzedniego twierdzenia.

TWIERDZENIE 6.3.4 (zasada abstrakcji). *Każda relacja równoważności R w niepustym zbiorze X ustala podział zbioru X na rozłączne i niepuste podzbiory (mianowicie na klasy abstrakcji) w taki sposób, że dwa elementy x, y zbioru X należą do tego samego podzbioru wtedy i tylko wtedy, gdy xRy .*

Zbiór wszystkich klas abstrakcji relacji R w zbiorze X oznacza się przez X/R .

Prostym przykładem zastosowania zasady abstrakcji do definiowania nowych pojęć może być definicja kierunku na danej płaszczyźnie. Otóż niech X będzie zbiorem wszystkich prostych na danej płaszczyźnie Q i niech R będzie relacją równoległości w zbiorze X , tzn. dla dowolnych dwóch prostych l_1 i l_2 płaszczyzny Q zachodzi $l_1 R l_2$ wtedy i tylko wtedy, gdy $l_1 \parallel l_2$. Kierunek na płaszczyźnie Q możemy teraz określić jako klasę abstrakcji relacji R w X . Bardziej skomplikowanych (technicznie) przykładów zastosowania zasady abstrakcji dostarczają konstrukcje zbioru \mathbb{Z} liczb całkowitych na bazie zbioru \mathbb{N} liczb naturalnych i konstrukcja zbioru \mathbb{Q} liczb wymiernych na bazie zbioru \mathbb{Z} liczb całkowitych, czy wreszcie konstrukcja zbioru \mathbb{R} liczb rzeczywistych na bazie zbioru \mathbb{Q} liczb wymiernych⁴.

Istnieje także własność niejako odwrotna do zasady abstrakcji, tzn. każdy podział $\{X_i : i \in I\}$ danego zbioru X , czyli taka rodzina parami rozłącznych zbiorów $X_i \subseteq X$, że ich suma równa się X , wyznacza relację równoważności R w X , taką że jej klasy abstrakcji pokrywają się ze zbiorami X_i stanowiącymi podział zbioru X . Istotnie, wystarczy przyjąć, że

$$xRy \leftrightarrow \exists i \in I (x \in X_i \wedge y \in X_i)$$

dla dowolnych $x, y \in X$.

Łatwo zauważyć, że jeśli relacja R jest relacją równoważności, to jej ograniczenie do którejś z klas abstrakcji (tzn. podzbiór tej relacji, będący klasą abstrakcji) będzie relacją totalną. Oczywiście relacja totalna jest zawsze relacją równoważności.

⁴ Znaleźć je można na przykład w książce R. Murawskiego i K. Świrydowicza, *Wstęp do teorii mnogości*, Wydawnictwo Naukowe UAM, Poznań 2005, paragraf 4.4. Por. też zadania 21, 22 i 23 poniżej.

Diagram relacji równoważności w zbiorze skończonym (jeśli rozpatrywana relacja nie jest totalna) składa się z izolowanych podzbiorów, z których każdy jest podrelacją totalną relacji wyjściowej.

Zadania

1. Kiedy para $\langle a, b \rangle$ jest zbiorem jednopunktowym?

2. Znaleźć iloczyn kartezjański $A \times B$ następujących zbiorów A i B :

- a) $A = \{a, b\}$, $B = \{c, d, e\}$,
- b) $A = \{b, c\}$, $B = \{a, c\}$,
- c) $A = \{a\}$, $B = \{a, b, c, d\}$.

Czy tu $A \times B = B \times A$?

3. Kiedy $A \times B = B \times A$?

4. Zakładając, że punkty na płaszczyźnie (tj. punkty produktu $\mathbb{R} \times \mathbb{R}$) to pary $\langle a, b \rangle$ liczb o odciętej a i rzędnej b , znaleźć produkt $A \times B$ i $B \times A$ następujących zbiorów i zilustrować graficznie te produkty:

- a) $A = \{x \in \mathbb{R} : 0 < x \leq 1\}$, $B = \{x \in \mathbb{R} : 0 \leq x < 1\}$,
- b) $A = \{x \in \mathbb{R} : 0 < x \leq 1\}$, $B = \{x \in \mathbb{R} : -2 \leq x < -1\}$,
- c) $A = \{x \in \mathbb{R} : x \leq 1\}$, $B = \{x \in \mathbb{R} : x \leq 1\}$,
- d) $A = \{x \in \mathbb{R} : |x| \leq 1\}$, $B = \{x \in \mathbb{R} : |x| \leq 2\}$.

5. Sprawdzić, czy prawdziwe są równości i inkluzje:

- a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$,
- b) $A \times (B \cap C) = (A \times B) \cap (A \times C)$,
- c) $(A \setminus B) \times C = (A \setminus B) \times (A \setminus C)$,
- d) $A \times (B \setminus C) = (A \times C) \setminus (A \times C)$,
- e) $A \times (B \times C) = (A \times B) \times C$,
- f) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.

6. Korzystając z równości a i b z poprzedniego zadania oraz z równości dla zbiorów, udowodnić następujące równości:

- a) $(A \times C) \cup ((B \cap A) \times C) = A \times C$,
- b) $(A \times B)' \cap C = (A' \times C) \cup (B' \times C)$,
- c) $(C \times A) \cup (C \times A') = (C \times B) \cup (C \times B')$,
- d) $(A \times C) \cap ((B \cup A) \times C) = (A \times C) \cup ((B \cap A) \times C)$.

7. Podaj przykłady relacji binarnych, w których:

- a) dziedzina jest rozłączna z przeciwdziedzina,
- b) dziedzina jest podzbiorem właściwym przeciwdziedziny,
- c) dziedzina jest identyczna z przeciwdziedzina,
- d) dziedzina jest równa przeciwdziedzini, pomniejszonej o jeden element.

8. Pokazać, że każda relacja asymetryczna jest przeciwzrotna. (*Wskazówka*: skorzystać z prawa Claviusa).

9. Scharakteryzuj własności następujących relacji, określonych w kwadracie zbioru $\{a, b, c, d\}$:

- $\{\langle a, a \rangle, \langle b, b \rangle, \langle c, c \rangle, \langle d, d \rangle\}$,
- $\{\langle a, b \rangle, \langle b, a \rangle, \langle c, c \rangle\}$,
- $\{\langle a, b \rangle, \langle b, c \rangle, \langle c, a \rangle, \}$,
- $\{\langle a, b \rangle, \langle b, a \rangle, \langle c, d \rangle, \langle d, c \rangle\}$.

Narysuj diagramy i macierze tych relacji.

10. Czy relacja diagonalna jest symetryczna? Czy jest przechodnia? Czy jest antysymetryczna?

11. Scharakteryzuj własności następujących relacji:

- $R \subseteq \mathbb{Z} \times \mathbb{Z}; xRy \leftrightarrow 2|x + y$,
- $R \subseteq \mathbb{N} \times \mathbb{N} \setminus \{0\}; xRy \rightarrow x|y$,
- $R \subseteq \mathbb{R} \times \mathbb{R}; xRy \leftrightarrow (x^2 = y^2)$,
- $R \subseteq \mathbb{R} \times \mathbb{R}; xRy \leftrightarrow |x| + |y| = 3$,
- $R \subseteq \mathbb{R} \times \mathbb{R}; xRy \leftrightarrow |x| + |y| \neq 3$.

12. Jakie własności mają następujące relacje na liczbach rzeczywistych:

- $xRy \leftrightarrow |x| = |y|$,
- $xRy \leftrightarrow x \cdot y = 0$,
- $xRy \leftrightarrow x + y = 2$,
- $xRy \leftrightarrow x \cdot y > 0$,
- $xRy \leftrightarrow x + y|2$.

Jeśli któraś z relacji jest równoważnością, wyznaczyć klasy abstrakcji.

13. Niech \mathcal{F} będzie zbiorem wszystkich formuł języka rachunku zdań, a \mathfrak{T} zbiorem tautologii klasycznego rachunku zdań. Jakie własności mają następujące relacje w produkcie $\mathcal{F} \times \mathcal{F}$:

- $\phi R_1 \psi \leftrightarrow (\phi \rightarrow \psi) \in \mathfrak{T}$,
- $\phi R_2 \psi \leftrightarrow (\phi \leftrightarrow \psi) \in \mathfrak{T}$,
- $\phi R_3 \psi \leftrightarrow (\phi \vee \neg \psi) \in \mathfrak{T}$.

14. Znaleźć na zbiorze trzyelementowym wszystkie relacje

- zwrotne,
- przeciwzrotne,
- symetryczne,
- zwrotne i symetryczne,
- antysymetryczne⁵.

15. Jakie własności posiada relacja pusta?

⁵ Zauważyć, że antysymetrię można wyrazić implikacją $xRy \wedge x \neq y \rightarrow \neg yRx$.

16. Znaleźć złożenia $R \circ S$, $S \circ R$, $R \circ R$, $R \circ S \circ T$ następujących relacji, określonych w kwadracie zbioru $\{a, b, c, d\}$:

$$R = \{\langle a, b \rangle, \langle b, a \rangle, \langle c, d \rangle, \langle d, a \rangle\},$$

$$S = \{\langle a, c \rangle, \langle c, d \rangle, \langle d, d \rangle\},$$

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

Narysować diagramy i macierze odpowiednich relacji.

17. Znaleźć wszystkie relacje równoważności na zbiorze czteroelementowym.

18. Zdefiniować relację równoważności odpowiadającą następującym podziałom zbioru A :

a) $A = \{a, b, c, d, e\}$; podział: $B = \{a, b, c\}$, $C = \{d, e\}$,

b) $A = \mathbb{Z}$; podział: $B = \mathbb{N} \setminus \{0\}$, $C = \{0\}$, $D = \{x \in \mathbb{Z} : -x \in B\}$,

c) $A = \mathbb{C}$ (zbiór liczb zespolonych, rozumiany jako zbiór punktów płaszczyzny); podział dany jest przez okręgi o środku w punkcie $\langle 0, 0 \rangle$.

19. Sprawdzić, że relacja $R \subseteq \mathbb{R} \times \mathbb{R}$, zdefiniowana równoważnością

$$xRy \iff (x - y) \in \mathbb{Q},$$

jest relacją równoważności i znaleźć $[\sqrt{2}]_R$ i $[1]_R$.

20. Sprawdzić, że relacja $R \subseteq \mathbb{R} \times \mathbb{R}$, zdefiniowana równoważnością

$$xRy \iff \exists z \in \mathbb{Z} (x - y) = z,$$

jest relacją równoważności i znaleźć $[\sqrt{3}]_R$ i $[0]_R$.

21. Niech będzie dany zbiór \mathbb{N} liczb naturalnych z działaniami $+$, \cdot oraz $-$, przy czym to ostatnie działanie jest określone tylko wtedy, gdy odjemna nie jest mniejsza od odjemnika, tzn. $x - y$ jest określone wtedy i tylko wtedy, gdy $x \geq y$. Rozważmy zbiór $\mathbb{N} \times \mathbb{N}$ i określmy w nim relację \sim następująco:

$$\langle m_1, n_1 \rangle \sim \langle m_2, n_2 \rangle \quad \text{wtedy i tylko wtedy, gdy} \quad m_1 + n_2 = m_2 + n_1.$$

Udowodnić, że relacja \sim jest relacją równoważności. (Klasy abstrakcji tej relacji \sim są w istocie liczbami całkowitymi).

22. Niech \mathbb{Z}^* będzie zbiorem liczb całkowitych różnych od zera, tzn.

$$\mathbb{Z}^* = \{x \in \mathbb{Z} : x \neq 0\}.$$

Rozważmy zbiór $\mathbb{Z} \times \mathbb{Z}^*$, czyli zbiór par uporządkowanych $\langle m, n \rangle$, takich że $m, n \in \mathbb{Z}$ oraz $n \neq 0$. W zbiorze tym określamy następującą relację:

$$\langle m_1, n_1 \rangle \sim \langle m_2, n_2 \rangle \quad \text{wtedy i tylko wtedy, gdy} \quad m_1 \cdot n_2 = m_2 \cdot n_1.$$

Udowodnić, że relacja \sim jest relacją równoważności. (Klasy abstrakcji tej relacji \sim można traktować jako liczby wymierne).

23. Rozważmy zbiór X złożony ze wszystkich ciągów liczb wymiernych $(a_n)_{n \in \mathbb{N}}$ spełniających warunek Cauchy'ego, tzn. warunek

$$\forall \varepsilon \in \mathbb{Q}, \varepsilon > 0 \exists n_0 \in \mathbb{N} \forall n \in \mathbb{N} \forall k \in \mathbb{N} (n > n_0 \rightarrow |a_n - a_{n+k}| < \varepsilon).$$

(Zauważmy, że warunek Cauchy'ego jest warunkiem koniecznym i dostatecznym zbieżności). W zbiorze X wprowadzamy relację \approx określoną następująco:

$$(a_n) \approx (b_n) \quad \text{wtedy i tylko wtedy, gdy} \\ \forall \varepsilon \in \mathbb{Q}, \varepsilon > 0 \exists N \forall n > N (|a_n - b_n| < \varepsilon).$$

Zatem dwa ciągi (a_n) i (b_n) liczb wymiernych są w relacji \approx , jeśli są zbieżne do tej samej granicy. Udowodnić, że relacja \approx jest relacją równoważności. (Klasy abstrakcji relacji \approx to liczby rzeczywiste).

Rozdział 7

Funkcje

7.1. Definicja funkcji. Rodzaje funkcji

Pojęcie funkcji jest jednym z najważniejszych pojęć w matematyce. Potocznie rozumie się funkcję jako przyporządkowanie (jednym obiektom innych obiektów). Pojęcie funkcji kształtowało się powoli i stopniowo¹. W końcu uzyskano precyzyjne pojęcie funkcji zdefiniowane na gruncie teorii mnogości. Pozwala ono na rozważanie już nie tylko konkretnych danych funkcji, ale na badanie zbiorów funkcji czy – na jeszcze wyższym stopniu abstrakcji – na traktowanie funkcji jako pojedynczych punktów przestrzeni funkcyjnych.

Funkcje definiować będziemy jako specjalnego typu relacje (utożsamiając przy tym funkcję z jej wykresem, czyli grafem). Przyjmujemy zatem następującą definicję:

DEFINICJA 7.1.1. *Relację $R \subseteq X \times Y$ nazywamy funkcją wtedy i tylko wtedy, gdy spełnione są następujące dwa warunki:*

$$\forall x \in D_R \exists y \in Y (xRy),$$

$$\forall x \in X \forall y \in Y \forall z \in Y (xRy \wedge xRz \rightarrow y = z).$$

Definicja mówi więc, że funkcja jest to relacja, czyli zbiór par uporządkowanych elementów zbiorów X i Y , takich że dla każdego elementu x zbioru X istnieje dokładnie jeden element y zbioru Y , taki że para $\langle x, y \rangle$ należy do relacji R . Wprowadziwszy symbol $\exists!$ jako znaczący tyle, co „istnieje

¹ Uwagi na temat rozwoju pojęcia funkcji znaleźć można na przykład w książce R. Murawskiego i K. Świrydowicza, *Wstęp do teorii mnogości*, Wydawnictwo Naukowe UAM, Poznań 2005, paragraf 5.1.

dokładnie jedno”², możemy więc powiedzieć, że relację $R \subseteq X \times Y$ nazywamy funkcją wtedy i tylko wtedy, gdy

$$\forall x \in D_R \exists! y \in Y (xRy).$$

Jeśli relacja R jest funkcją, to – zgodnie z tradycją – zamiast R piszemy f, g, \dots . To jedyne x , takie że xRy oznaczamy wtedy zwykle symbolem $f(x)$ i nazywamy wartością funkcji f na argumentie x . Lewostronną dziedzinę funkcji f (traktowanej jako relacja binarna), czyli zbiór D_f nazywamy zbiorem argumentów (i oznaczamy zwykle jako $\text{dom}(f)$ – od angielskiego *domain*), a dziedzinę prawostronną, czyli zbiór D_f^* nazywamy zbiorem wartości funkcji lub przeciwdziedziną (i oznaczamy jako $\text{rng}(f)$ – od angielskiego *range*). Jeśli $f \subseteq X \times Y$ jest funkcją oraz $D_f = X$, to piszemy $f : X \rightarrow Y$ i mówimy, że f przekształca (odwzorowuje) zbiór X w zbiór Y .

Z definicji 7.1.1 i z zasady ekstensjonalności wynika bezpośrednio, że dwie funkcje są równe wtedy i tylko wtedy, gdy mają równe dziedziny i przyjmują te same wartości dla każdego argumentu. Zbiór wszystkich funkcji ze zbioru X w zbiór Y oznaczać będziemy symbolem Y^X . Zatem Y^X jest podzbiorem zbioru $\mathcal{P}(X \times Y)$.

Jeśli dane są dwie funkcje f i g , takie że $f \subseteq g$, to funkcję g nazywamy przedłużeniem funkcji f , a funkcję f obcięciem funkcji g . Szczególnym przypadkiem tej operacji jest następująca operacja:

DEFINICJA 7.1.2. *Niech $f : X \rightarrow Y$ i niech $A \subseteq X$. Obcięciem funkcji f do zbioru A nazywamy funkcję $f_A = f \cap (A \times Y)$.*

Zamiast symbolu f_A czasem używa się także symbolu $f \upharpoonright A$.

Wyróżnimy teraz kilka rodzajów funkcji.

DEFINICJA 7.1.3. *Funkcję $f : X \rightarrow Y$ nazywamy różnowartościową (jednojednoznaczną, iniekcją, monomorfizmem) wtedy i tylko wtedy, gdy*

$$\forall x_1 \in X \forall x_2 \in X [x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2)],$$

czyli innymi słowy (na mocy prawa transpozycji)

$$\forall x_1 \in X \forall x_2 \in X [f(x_1) = f(x_2) \rightarrow x_1 = x_2].$$

Piszemy wtedy $f : X \rightarrow Y$ lub $f : X \xrightarrow{1-1} Y$.

² Jest to kwantyfikator ilościowy – por. definicje takich kwantyfikatorów w rozdziale 4.

Przykładami funkcji różnowartościowych są wszystkie ściśle rosnące (malejące) funkcje rzeczywiste zmiennej rzeczywistej. Przykładem funkcji, która nie jest różnowartościowa, może być funkcja $\sin x$ dla $0 \leq x \leq \pi$ czy funkcja $f(\rho, \varphi) = \langle \rho, \cos \varphi, \rho \sin \varphi \rangle$ dla $0 \leq \rho \leq 1$ i $0 \leq \varphi \leq 2\pi$, czyli funkcja odwzorowująca punkty prostokąta $[0, 1] \times [0, 2\pi]$ na punkty koła o środku w początku układu współrzędnych i promieniu 1. Istotnie w tym drugim przypadku środek koła, czyli punkt $(0, 0)$, odpowiada $\rho = 0$ i dowolnemu $\varphi \in [0, 2\pi]$.

DEFINICJA 7.1.4. Funkcję $f : X \rightarrow Y$ nazywamy funkcją na zbiór Y (suriekcją, epimorfizmem) wtedy i tylko wtedy, gdy

$$\forall y \in Y \exists x \in X [y = f(x)].$$

Piszemy wtedy $f : X \rightarrow Y$ lub $f : X \xrightarrow{na} Y$.

DEFINICJA 7.1.5. Funkcję $f : X \rightarrow Y$ nazywamy bijekcją wtedy i tylko wtedy, gdy f jest iniekcją i suriekcją (czyli jest różnowartościowa i „na”). Piszemy wtedy $f : X \xrightarrow[na]{1-1} Y$.

7.2. Operacje na funkcjach

Na funkcjach możemy wykonywać rozmaite operacje, w szczególności ważna jest operacja funkcji odwrotnej oraz operacja superpozycji (składania). Jeśli funkcja $f : X \xrightarrow[na]{1-1} Y$ jest bijekcją, to możemy wtedy określić funkcję odwrotną $f^{-1} : Y \rightarrow X$ w następujący sposób:

$$x = f^{-1}(y) \leftrightarrow y = f(x).$$

Zauważmy, że założenie, iż wyjściowa funkcja f jest iniekcją, jest potrzebne po to, by relacja f^{-1} była w ogóle funkcją, zaś założenie, iż funkcja f jest suriekcją pociąga, że dziedziną funkcji odwrotnej jest cały zbiór Y . Operacja prowadząca od funkcji f do funkcji odwrotnej f^{-1} jest analogiczna do operacji konwersu, określonej dla dowolnych relacji. Łatwo zauważyć, że na przykład funkcją odwrotną do funkcji $f(x) = ax + b$ ($a \neq 0$) jest funkcja $f^{-1}(y) = \frac{1}{a} \cdot y - \frac{b}{a}$, a funkcją odwrotną do funkcji $f(x) = x^3$ jest funkcja $f^{-1}(y) = \sqrt[3]{y}$.

Operacja superpozycji (składania) jest analogiczna do operacji iloczynu względnego, określonej dla dowolnych relacji. Niech więc dane będą dwie funkcje, tzn. funkcja $f : X \rightarrow Y$ i funkcja $g : Y \rightarrow Z$. Superpozycją

funkcji f i g nazywamy funkcję $f \circ g : X \rightarrow Z$ określoną następującym wzorem³:

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

czyli inaczej

$$f \circ g = \{\langle x, z \rangle \in X \times Z : \exists y \in Y [\langle x, y \rangle \in f \wedge \langle y, z \rangle \in g]\}.$$

Operacja superpozycji jest łączna, ale na ogół nie jest przemienne. Istotnie, aby wykazać łączność operacji \circ rozważmy trzy funkcje

$$f : X \rightarrow Y, \quad g : Y \rightarrow Z \quad \text{oraz} \quad h : Z \rightarrow U.$$

Pokażemy, że $f \circ (g \circ h) = (f \circ g) \circ h$. Niech więc dana będzie dowolna para uporządkowana $\langle x, u \rangle \in f \circ (g \circ h)$. Wtedy istnieje element $y \in Y$, taki że $\langle x, y \rangle \in f \wedge \langle y, u \rangle \in g \circ h$. Zatem dla pewnego elementu $z \in Z$ mamy $\langle y, z \rangle \in g \wedge \langle z, u \rangle \in h$. Stąd $\langle x, z \rangle \in f \circ g$ oraz $\langle z, u \rangle \in h$, czyli $\langle x, u \rangle \in (f \circ g) \circ h$. W ten sposób pokazaliśmy, że $f \circ (g \circ h) \subseteq (f \circ g) \circ h$. Podobnie pokazuje się, że także $(f \circ g) \circ h \subseteq f \circ (g \circ h)$, co na mocy zasady ekstensjonalności dowodzi ostatecznie równości $f \circ (g \circ h) = (f \circ g) \circ h$.

Aby pokazać, że operacja superpozycji nie zawsze jest przemienne, wystarczy podać stosowny kontrprzykład. Rozważmy więc funkcje f i g odwzorowujące zbiór liczb rzeczywistych \mathbb{R} w zbiór \mathbb{R} , dane wzorami

$$f(x) = 1 + x \quad \text{oraz} \quad g(x) = 1 - x.$$

Wtedy

$$(f \circ g)(x) = g(f(x)) = 1 - (1 + x) = -x$$

oraz

$$(g \circ f)(x) = f(g(x)) = 1 + (1 - x) = 2 - x.$$

Zatem istotnie $(f \circ g) \neq (g \circ f)$.

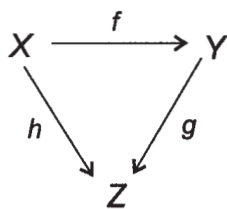
Zauważmy jeszcze, że jeśli funkcja $f : X \rightarrow Y$ jest bijekcją, tzn. $f : X \xrightarrow[\text{na}]{1-1} Y$, to $(f \circ f^{-1})(x) = x$ oraz $(f^{-1} \circ f)(y) = y$ dla dowolnych $x \in X$ i $y \in Y$.

W zbiorze wszystkich funkcji $f : X \xrightarrow[\text{na}]{1-1} X$ szczególne znaczenie ma funkcja $I : X \rightarrow X$, taka że $I(x) = x$ dla dowolnego x . Nazywamy ją funkcją identycznościową. Łatwo można pokazać, że zbiór wszystkich funkcji

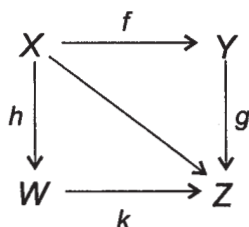
³ W literaturze można znaleźć też oznaczenie $g \circ f$ zamiast przyjętej tu przez nas notacji $f \circ g$. Ta ostatnia dopasowana jest do relacji i ma podkreślać fakt, że złożenie (superpozycja) funkcji jest szczególnym przypadkiem operacji składania relacji.

$f: X \xrightarrow[\text{na}]{1-1} X$ tworzy grupę ze względu na operację składania funkcji i brania funkcji odwrotnej. Funkcja identycznościowa I jest tu elementem neutralnym, tzn. dla dowolnej funkcji $f: X \xrightarrow[\text{na}]{1-1} X$ mamy $f \circ f^{-1} = f^{-1} \circ f = I$.

Operację składania funkcji ilustruje się często graficznie za pomocą diagramów postaci



Diagram



nazywamy przemiennym wtedy i tylko wtedy, gdy $h \circ k = f \circ g$.

TWIERDZENIE 7.2.1. Niech $f: X \rightarrow Y$ oraz $g: Y \rightarrow Z$. Wtedy

- (1) jeśli f i g są iniekcjami, to $f \circ g$ jest także iniekcją,
- (2) jeśli f i g są suriekcjami, to $f \circ g$ jest także suriekcją,
- (3) jeśli f i g są bijekcjami, to $f \circ g$ jest także bijekcją.

D o w ó d. Wystarczy oczywiście udowodnić tylko (1) i (2). Niech więc, dla dowodu (1), f i g będą iniekcjami i rozważmy dwa dowolne elementy $x_1, x_2 \in X$, takie że $x_1 \neq x_2$. Wtedy $f(x_1) \neq f(x_2)$. Zatem mamy $g(f(x_1)) \neq g(f(x_2))$. Stąd $(f \circ g)(x_1) \neq (f \circ g)(x_2)$. A więc $f \circ g$ jest iniekcją.

Dla dowodu (2) założymy, że f i g są suriekcjami i niech z będzie dowolnym elementem zbioru Z . Wtedy istnieje $y \in Y$, taki że $z = g(y)$. Z drugiej strony istnieje też $x \in X$, taki że $y = f(x)$. Ostatecznie więc istnieje $x \in X$, taki że $z = (f \circ g)(x)$. Czyli funkcja $f \circ g$ jest suriekcją. Q.E.D.

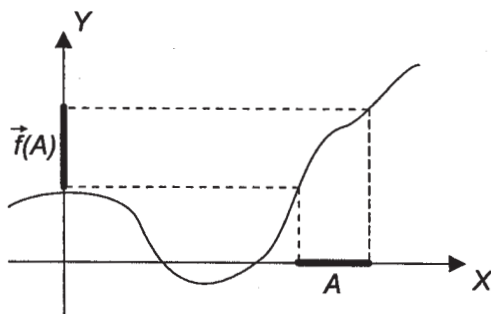
7.3. Obrazy i przeciwobrazy oraz ich własności

Wprowadzimy teraz ważne pojęcia obrazu i przeciwobrazu zbioru przez funkcję.

DEFINICJA 7.3.1. Niech $f : X \rightarrow Y$ i niech $A \subseteq X$. Obrazem zbioru A przez funkcję f nazywamy zbiór

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

Zatem obraz zbioru A przez funkcję f jest to zbiór złożony dokładnie z wartości funkcji f dla wszystkich argumentów ze zbioru A . W przypadku funkcji $\mathbb{R} \rightarrow \mathbb{R}$ możemy go zilustrować za pomocą następującego rysunku:



Dodajmy, że w literaturze spotkać można też inne oznaczenia, na przykład $f^*(A)$ czy po prostu $f(A)$. Ten ostatni symbol może być mylący, gdyż może oznaczać też wartość funkcji f na argumentcie A .

Z definicji obrazu wynika bezpośrednio, że $\vec{f}(A) \subseteq \vec{f}(X) \subseteq Y$. Jeżeli $\vec{f}(X) = Y$, to funkcja f jest suriekcją. Łatwo też zauważyć, że $\vec{f}(\emptyset) = \emptyset$, $\vec{f}(A) \neq \emptyset$ dla każdego $A \neq \emptyset$ (i oczywiście $f \neq \emptyset$) oraz $\vec{f}(A) \subseteq \vec{f}(B)$ dla dowolnych $A \subseteq B \subseteq X$.

Dla przykładu obrazem zbioru \mathbb{R} liczb rzeczywistych (czyli obrazem prostej $(-\infty, \infty)$) przez funkcję \sin jest przedział domknięty $[-1, 1]$. Ten sam przedział jest też obrazem przedziału $[0, 2\pi]$ przez tę samą funkcję. Zatem

$$\vec{\sin}((-\infty, \infty)) = [-1, 1] = \vec{\sin}([0, 2\pi]).$$

Dla funkcji $f(x) = x^2$ mamy $\vec{f}([-1, 0]) = \vec{f}([0, 1]) = [0, 1]$.

Związek operacji obrazu i działań na zbiorach podaje następujące twierdzenie⁴:

TWIERDZENIE 7.3.2. *Niech $f : X \rightarrow Y$ i niech $A_1, A_2 \subseteq X$. Wtedy*

- (1) $\vec{f}(A_1 \cup A_2) = \vec{f}(A_1) \cup \vec{f}(A_2)$,
- (2) $\vec{f}(A_1 \cap A_2) \subseteq \vec{f}(A_1) \cap \vec{f}(A_2)$,
- (3) $\vec{f}(A_1 \setminus A_2) \supseteq \vec{f}(A_1) \setminus \vec{f}(A_2)$.

Zauważmy, że w punktach (2) i (3) mamy tylko inkluzję! Nie można „jej wzmocnić” do równości zachodzącej dla dowolnej funkcji f . Istotnie, rozważmy funkcję $f : \mathbb{R} \rightarrow \mathbb{R}$ daną wzorem $f(x) = x^2$ i niech $A_1 = [-1, 0]$ oraz $A_2 = [0, 1]$. Wtedy $A_1 \cap A_2 = \{0\}$ i $\vec{f}(A_1 \cap A_2) = \{0\}$. Z drugiej strony $\vec{f}(A_1) = \vec{f}(A_2) = [0, 1]$ oraz $\vec{f}(A_1) \cap \vec{f}(A_2) = [0, 1]$. Zatem $\vec{f}(A_1 \cap A_2) \subsetneq \vec{f}(A_1) \cap \vec{f}(A_2)$. Mamy też $A_1 \setminus A_2 = [-1, 0)$, $\vec{f}(A_1 \setminus A_2) = (0, 1]$, $\vec{f}(A_1) \setminus \vec{f}(A_2) = \emptyset$. Zatem znów mamy $\vec{f}(A_1 \setminus A_2) \supsetneq \vec{f}(A_1) \setminus \vec{f}(A_2)$.

Okazuje się jednak, że dla pewnych funkcji (tzn. przy pewnych dodatkowych założeniach na funkcję f) można otrzymać we wzorach (2) i (3) równość. Mówi o tym następujące twierdzenie:

TWIERDZENIE 7.3.3. *Niech $f : X \rightarrow Y$. Następujące warunki są równoważne:*

- (1) *funkcja f jest różnowartościowa,*
- (2) *dla dowolnych zbiorów $A_1, A_2 \subseteq X$, $\vec{f}(A_1 \cap A_2) = \vec{f}(A_1) \cap \vec{f}(A_2)$,*
- (3) *dla dowolnych zbiorów $A_1, A_2 \subseteq X$, $\vec{f}(A_1 \setminus A_2) = \vec{f}(A_1) \setminus \vec{f}(A_2)$.*

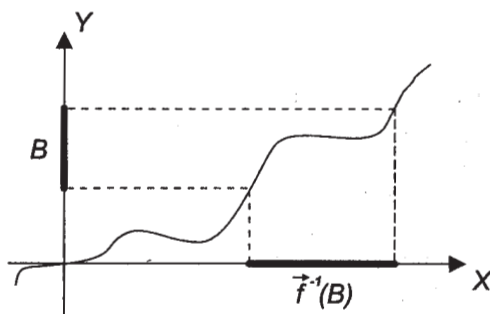
Wprowadzimy teraz pojęcie „odwrotne” do pojęcia obrazu, tzn. pojęcie przeciwobrazu.

DEFINICJA 7.3.4. *Niech $f : X \rightarrow Y$ i niech $B \subseteq Y$. Przeciwobrazem zbioru B przez funkcję f nazywamy zbiór*

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

Zatem przeciwobraz zbioru B przez funkcję $f : X \rightarrow Y$ jest to zbiór złożony z tych argumentów x zbioru X , dla których wartość funkcji f jest elementem („wpada do”) zbioru B . W przypadku funkcji $\mathbb{R} \rightarrow \mathbb{R}$ można je zilustrować następująco:

⁴ Dowód tego twierdzenia, jak i twierdzeń 7.3.3 oraz 7.3.5 znaleźć można na przykład w książce R. Murawskiego i K. Świrydowicza, *Wstęp do teorii mnogości*, Wydawnictwo Naukowe UAM, Poznań 2005, paragraf 5.4.



Podobnie jak to było w przypadku obrazu zbioru przez funkcję, także w przypadku przeciwobrazu możemy w literaturze spotkać też inne oznaczenia, na przykład: $f^{-1} * (B)$ czy po prostu $f^{-1}(B)$. Pierwszy z tych symboli może być mylący, ponieważ może też oznaczać obraz zbioru B przez funkcję odwrotną f^{-1} , drugi z symboli może natomiast oznaczać też wartość funkcji f^{-1} na argumentcie B . Dlatego wybraliśmy właśnie symbole „strzałkowe”.

Łatwo zauważyć, że przeciwobrazem przedziału $[-1, 1]$ przez funkcję sinus jest cała prosta rzeczywista $(-\infty, \infty)$, czyli zbiór \mathbb{R} , tzn. $\overrightarrow{\sin^{-1}}([-1, 1]) = (-\infty, \infty)$. Mamy też $\overrightarrow{\sin^{-1}}((1, \infty)) = \emptyset$.

Zachodzi interesujący związek między przeciwobrazem zbioru przez funkcję i obrazem tego zbioru przez funkcję odwrotną do funkcji danej. Istotnie, niech $f : X \rightarrow Y$ będzie funkcją różnowartościową i „na”. Wtedy istnieje funkcja odwrotna do funkcji f , czyli $f^{-1} : Y \rightarrow X$. Dla dowolnego zbioru $B \subseteq Y$ mamy teraz

$$\overrightarrow{f^{-1}}(B) = \{f^{-1}(y) : y \in B\} = \{x : f(x) \in B\} = \overrightarrow{f}^{-1}(B).$$

Zatem dla funkcji różnowartościowej: przeciwobraz zbioru jest równy jego obrazowi przez funkcję odwrotną.

Związek między działaniami na zbiorach a operacją przeciwobrazu podaje następujące twierdzenie:

TWIERDZENIE 7.3.5. Niech $f : X \rightarrow Y$ oraz $B_1, B_2 \subseteq Y$. Wtedy

- (1) $\overrightarrow{f}^{-1}(B_1 \cup B_2) = \overrightarrow{f}^{-1}(B_1) \cup \overrightarrow{f}^{-1}(B_2)$,
- (2) $\overrightarrow{f}^{-1}(B_1 \cap B_2) = \overrightarrow{f}^{-1}(B_1) \cap \overrightarrow{f}^{-1}(B_2)$,
- (3) $\overrightarrow{f}^{-1}(B_1 \setminus B_2) = \overrightarrow{f}^{-1}(B_1) \setminus \overrightarrow{f}^{-1}(B_2)$.

Zadania

1. Czy następujące relacje są funkcjami:

- $R \subseteq \mathbb{R} \times \mathbb{R}, xRy \leftrightarrow x^2 = y,$
- $R \subseteq \mathbb{R} \times \mathbb{R}, xRy \leftrightarrow x = y^2,$
- $R \subseteq \mathbb{R}^+ \times \mathbb{R}^+, xRy \leftrightarrow x = y^2,$
- $R \subseteq \mathbb{R}^+ \times \mathbb{R}^+, xRy \leftrightarrow y = \ln x,$
- $R \subseteq \mathbb{R}^+ \times \mathbb{R}^+, xRy \leftrightarrow |x - y| = 1,$
- $R \subseteq \mathbb{R}^+ \times \mathbb{R}^+, xRy \leftrightarrow |y| - |x| = 1,$
- $R \subseteq \mathbb{C} \times \mathbb{C}, z_1Rz_2 \leftrightarrow \operatorname{Re} z_1 = 2 \operatorname{Im} z_2,$ gdzie $\operatorname{Re} z$ i $\operatorname{Im} z$ oznaczają odpowiednio część rzeczywistą i urojoną liczby $z,$
- $R \subseteq \mathbb{C} \times \mathbb{C}, xRy \leftrightarrow y = \sqrt{x}.$

2. Czy poniższe funkcje $f: \mathbb{R} \rightarrow \mathbb{R}$ są 1-1? Czy są „na”? Jeśli funkcja f jest „na”, to podać dla jakiego zbioru $X \subseteq \mathbb{R}$ ta funkcja f jest „na”.

- $f(x) = e^x,$
- $f(x) = x^5 + 1,$
- $f(x) = x^3 - x,$
- $f(x) = [x],$ gdzie $[x]$ oznacza część całkowitą liczby $x,$
- $f(x) = x - [x],$
- $f(x) = x + [x].$

3. Niech $U \neq \emptyset$. Dla dowolnego zbioru $X \subseteq U$ definiujemy tzw. funkcję charakterystyczną $\chi_X^U: X \rightarrow \{1, 0\}$ za pomocą następujących warunków: $\chi_X^U(x) = 1,$ jeśli $x \in X,$ $\chi_X^U(x) = 0,$ jeśli $x \in U \setminus X$. Udowodnić, że⁵

- $\chi_U^U(x) = 1,$
- $\chi_\emptyset^U(x) = 0,$
- $\chi_{A \setminus B}(x) = \chi_A(x) - \chi_B(x),$
- $\chi_{A^c}(x) = 1 - \chi_A(x),$
- $\chi_{A \cap B}(x) = \chi_A(x) \cdot \chi_B(x),$
- $\chi_{A \cup B}(x) = \chi_A(x) \oplus \chi_B(x),$ gdzie $0 \oplus 0 = 0, 0 \oplus 1 = 1 \oplus 0 = 1 \oplus 1 = 1.$

4. Znaleźć podobne zależności dla sumy, przekroju i różnicy zbiorów, przyjmując następującą definicję funkcji charakterystycznej zbioru $X: \chi_X^U(x) = 1,$ jeśli $x \in U \setminus X,$ $\chi_X^U(x) = 0,$ jeśli $x \in X$.

5. Niech X_n będzie zbiorem macierzy $n \times n$ o wyrazach rzeczywistych ($n > 0$) i niech $f_1: X_n \rightarrow \mathbb{R}$ będzie funkcją zdefiniowaną następująco: $f_1(T) = \operatorname{Tr}(T),$ gdzie $\operatorname{Tr}(T)$ oznacza ślad macierzy $T,$ to jest iloczyn wszystkich elementów występujących na głównej przekątnej. Czy f_1 jest 1-1? Czy jest „na”? Znaleźć przeciwobraz zera i jedynki.

6. W podobny sposób zanalizuj przekształcenie przyporządkowujące macierzy jej wyznacznik.

7. Niech I_X oznacza odwzorowanie identycznościowe zbioru $X,$ tzn. spełniające warunek $I_X(x) = x$. Pokazać, że zbiór wszystkich funkcji różnowartościowych,

⁵ Od punktu c opuszczamy górny indeks U .

przekształcających zbiór X na zbiór X jest grupą ze względu na składanie funkcji; elementem neutralnym będzie tu funkcja I_X , a elementem odwrotnym do funkcji f będzie funkcja f^{-1} . Czy założenia, że rozpatrywane funkcje są 1-1 i „na”, są istotne? Czy w podobny sposób można skonstruować grupę, biorąc różne zbiory X i Y oraz zbiór przekształceń jednego zbioru na drugi?

8. Niech $f : X \rightarrow Y$ będzie bijekcją. Pokazać, że

- f^{-1} jest też bijekcją,
- $f^{-1} \circ f = I_X$,
- $f \circ f^{-1} = I_Y$.

9. Niech $R \subseteq X \times Y$. Powiemy, że relacja R łączy jednoznacznie elementy zbiorów X i Y , gdy dla dowolnego $x \in X$ istnieje dokładnie jeden taki $y \in Y$, że xRy i odwrotnie: dla dowolnego $y \in Y$ istnieje dokładnie jeden taki $x \in X$, że xRy .

- Pokazać, że R jest relacją łączącą wzajemnie jednoznacznie elementy zbiorów X i Y wtedy i tylko wtedy, gdy $R \circ R^{-1} = I_X$ i $R \circ R^{-1} = I_Y$.
- Czy prawdą jest, że: R łączy dokładnie jeden element zbioru A z dokładnie jednym elementem zbioru B wtedy i tylko wtedy, gdy $R \circ R^{-1} = I_A$ i $R^{-1} \circ R = I_B$?
- Jeśli nie, to jakie założenia są potrzebne, aby uzyskać kolejno równości $R \circ R^{-1} = I_A$, $R^{-1} \circ R = I_B$?

10. Niech $f : X \rightarrow X$. Czy z tego, że $h \circ f = h$ dla dowolnej funkcji $h : X \rightarrow X$ wynika, że $f = I_X$? Czy z tego, że $f \circ h = h$ dla dowolnej funkcji $h : X \rightarrow X$ wynika, że $f = I_X$?

11. Pokazać, że jeśli f i g są funkcjami 1-1 i „na”, to $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

12. Wyznaczyć wszystkie funkcje kwadratowe, takie że obrazem odcinka $[0, 2]$ jest odcinek $[0, 2]$.

13. Wyznaczyć wszystkie funkcje kwadratowe, takie że przeciwobraz odcinka $[0, 2]$ jest zbiorem pustym.

14. Niech $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ będzie funkcją zadaną równością $f(\langle x, y \rangle) = \min(x, y)$, gdzie $\min(x, y)$ oznacza mniejszą z liczb x, y . Znaleźć $\vec{f}^{-1}(\{-1\})$.

15. Niech $f : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ będzie funkcją zadaną równością $f(\langle x, y \rangle) = |x - y|$. Znaleźć $\vec{f}^{-1}(\{1\})$.

16. Niech $f : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ będzie funkcją zadaną równością $f(\langle x, y \rangle) = |x| - |y|$. Znaleźć $\vec{f}^{-1}(\{1\})$.

17. Niech $f : X \rightarrow Y$ będzie funkcją i niech $A \subseteq X$, $C \subseteq Y$. Udowodnić następujące zależności:

- Jeśli $A \subseteq B \subseteq X$, to $\vec{f}(A) \subseteq \vec{f}(B)$.
- $A \subseteq \vec{f}^{-1}(\vec{f}(A))$, o ile f^{-1} istnieje.
- $[\vec{f}(A)]' \subseteq \vec{f}(A')$.

18. Niech $f : X \rightarrow Y$ będzie funkcją 1 - 1 i „na”, niech $A \subseteq X$, $B \subseteq Y$. Udowodnić następujące zależności:

- a) $[\overrightarrow{f^{-1}}(B)]' = \overrightarrow{f^{-1}}(B')$,
- b) $\overrightarrow{f}(A) \cap B = \overrightarrow{f}(A \cap \overrightarrow{f}^{-1}(B))$,
- c) $\overrightarrow{f}(A) \subseteq B \leftrightarrow A \subseteq \overrightarrow{f}^{-1}(B)$.

Rozdział 8

Relacje porządkujące

8.1. Rodzaje relacji porządkujących

Relacja porządkująca ma być relacją ustalającą kolejność elementów, czy ogólniej – hierarchię elementów danego zbioru. Podstawowe przykłady to relacje \leq w zbiorze \mathbb{N} czy \mathbb{Z} , które liniowo porządkują te zbiory. Z różnych jednak powodów warto rozpatrywać relacje o słabszych własnościach. Zaczniemy więc od relacji o własnościach stosunkowo najslabszych, a kolejne pojęcia uzyskamy, wzmacniając własności relacji.

DEFINICJA 8.1.1. *Relację binarną R na zbiorze X nazywamy relacją częściowo porządkującą zbiór X (albo krócej: częściowym porządkiem na X), jeśli jest zwrotna, antysymetryczna i przechodnia, to znaczy dla dowolnych $x, y, z \in X$ spełnia warunki:*

- (1) xRx ,
- (2) $xRy \wedge yRx \rightarrow x = y$,
- (3) $xRy \wedge yRz \rightarrow xRz$.

Przykładami relacji częściowego porządku są: relacja \leq dla liczb całkowitych, wymiernych czy rzeczywistych, czy relacja bycia podzbiorem (por. lemat 5.3.1 o własnościach relacji inkluzji, rozdział 5).

DEFINICJA 8.1.2. *Zbiór X z relacją częściowego porządku R nazywamy zbiorem częściowo uporządkowanym i oznaczamy go przez $\langle X, R \rangle$.*

Relacjami częściowo porządkującymi (zwanymi też krótko częściowymi porządkami) zajmiemy się dokładniej w następnym paragrafie.

W zbiorze częściowo uporządkowanym $\langle X, R \rangle$ mogą istnieć elementy, które nie są R -porównywalne, tj. takie że ani xRy , ani yRx . Przykładem jest relacja diagonalna R na X : łatwo zauważyć, że jest ona częściowym

porządkiem, ale oczywiście jest, że żaden element $x \in X$ nie jest R -porównywalny z żadnym innym. Porównywalność elementów zbioru i ustalanie ich kolejności jest zapewnione przez inny rodzaj porządku – mianowicie porządek liniowy. Definicję liniowego porządku uzyskujemy, dodając do definicji częściowego porządku warunek spójności, czyli porównywalności.

DEFINICJA 8.1.3. *Para $\langle X, R \rangle$ jest zbiorem liniowo uporządkowanym wtedy i tylko wtedy, gdy R jest relacją częściowego porządku, a ponadto jest spójna, tj. dla dowolnych $x, y \in X$ spełnia warunek*

$$(4) \quad x \neq y \rightarrow xRy \vee yRx.$$

Czytelnik sprawdzi, że warunek (iv) można równoważnie wyrazić formułami

$$x = y \vee xRy \vee yRx$$

oraz

$$(x \neq y \wedge \neg xRy) \rightarrow yRx.$$

Przykładami relacji liniowo porządkujących są relacje \leq dla \mathbb{N} , \mathbb{Q} i \mathbb{R} . Każdy łańcuch (por. niżej) w zbiorze częściowo uporządkowanym stanowi przykład zbioru liniowo uporządkowanego.

Przez analogię do liczb, porządek częściowy i porządek liniowy oznacza się zwykle symbolem \leq .

Zarówno z częściowym porządkiem, jak i z porządkiem liniowym można związać relację $<$, definiowaną następująco:

$$x < y \text{ wtedy i tylko wtedy, gdy } x \leq y \wedge x \neq y.$$

Tak zdefiniowana relacja $<$ stanowi przykład ostrego (silnego) porządku; jest to uogólnienie ostrej nierówności dla liczb i dla inkluzji właściwej (por. lemat 5.3.2 z rozdziału 5 o własnościach relacji inkluzji właściwej).

DEFINICJA 8.1.4. *Relacja binarna $<$ w zbiorze X jest silnym porządkiem albo ostrym porządkiem wtedy i tylko wtedy, gdy jest przeciwzwrotna, asymetryczna (przeciwsymetryczna) i przechodnia, to jest dla dowolnych $x, y, z \in X$ spełnia warunki:*

$$(1') \quad \neg(x < x),$$

$$(2') \quad x < y \rightarrow \neg y < x,$$

$$(3') \quad x < y \wedge y < z \rightarrow x < z.$$

Jeśli ponadto relacja $<$ jest spójna, to nazwiemy ją relacją silnego (albo ostrego) porządku liniowego¹.

Można zauważyć, że określona właśnie relacja $<$, generowana przez relację częściowego porządku, jest silnym porządkiem, a gdy $<$ jest generowana przez relację \leq liniowego porządku, to jest silnym liniowym porządkiem.

Oryginalny przykład ostrego porządku liniowego stanowi tzw. hierarchia dziobania w stadzie kur: istnieje w stadzie taka kura, która dziobie wszystkie kury, następnie taka, która jest dziobana tylko przez tę pierwszą, a dziobie wszystkie pozostałe; jest trzecia kura, dziobana przez dwie pierwsze, a dziobiąca wszystkie pozostałe itd; ostatnia w hierarchii kura jest dziobana przez wszystkie kury ze stada, a nie dziobie żadnej kury².

Wreszcie najsilniejszym pojęciem jest dobry porządek. Relacjom dobrze porządkującym poświęcimy paragraf 8.3.

Terminologia dotycząca porządków nie jest w polskiej literaturze do końca ustalona. Nadużywając terminu „porządek”, można powiedzieć, że jak dotychczas nie ma porządku w definicji porządku.

Dla przykładu: niektórzy autorzy częściowe porządki nazywają po prostu porządkami (np. H. Rasiowa, A. Wojciechowska), a niektórzy zbiorem uporządkowanym nazywają zbiór z relacją porządku ostrego czy ścisłego³. Dodać należy, że z uwagi na zastosowania istnieje potrzeba jeszcze subtelniejszego niż w dotychczasowych badaniach rozróżniania różnych słabych porządków, co dodatkowo komplikuje terminologię. Wprowadza się w szczególności pojęcia słabsze od pojęcia częściowego porządku – relację *quasi-porządku* (jest to relacja zwrotna i przechodnia), *porządku częściowego w ścisłym sensie* (jest to relacja antysymetryczna i przechodnia) oraz relację *tolerancji* (jest to relacja zwrotna i symetryczna). Wszystko to jest ostrzeżeniem dla Czytelnika, aby za każdym razem, gdy ma do czynienia z publikacją o relacjach porządkujących, zaczął od przestudiowania terminologii wprowadzanej przez danego autora.

Autorzy niniejszego podręcznika mają wrażenie, że posługują się terminologią najbardziej rozpowszechnioną.

¹ Wystarczy założyć, że ostry porządek to relacja przeciwzwrotna i przechodnia; asymetria wynika z tych dwóch własności.

² Wynika to z badań Schielderupa-Ebbego; por. S. Mika, *Spoleczne podstawy zachowania*, w: T. Tomaszewski (red.), *Psychologia*, Państwowe Wydawnictwo Naukowe, Warszawa 1976, 134.

³ Np. M. Semeniuk-Polkowska w tłumaczeniu książki J.A. Szrejdera, *Równość, podobieństwo, porządek*, Wydawnictwo Naukowo-Techniczne, Warszawa 1975.

8.2. Zbiory częściowo uporządkowane

Jak pamiętamy, relacją częściowego porządku nazywamy relację zwrotną, antysymetryczną i przechodnią.

Przypomnijmy, że przykładami relacji częściowego porządku są: relacja \leq dla liczb całkowitych, wymiernych oraz rzeczywistych czy relacja bycia podzbiorem, i że zbiór $\langle X, \leq \rangle$, gdzie \leq jest częściowym porządkiem, nazywamy zbiorem częściowo uporządkowanym.

Tak więc zbiorami częściowo uporządkowanymi są zbiory $\langle \mathbb{R}, \leq \rangle$, $\langle \mathbb{Q}, \leq \rangle$ czy $\langle \mathcal{P}(A), \subseteq \rangle$, gdzie \mathbb{R} jest zbiorem liczb rzeczywistych, \mathbb{Q} – zbiorem liczb wymiernych, a $\mathcal{P}(A)$ – zbiorem wszystkich podzbiórów danego zbioru A . Relacją częściowego porządku jest relacja podzielności w zbiorze liczb naturalnych czy całkowitych, gdy ze zbiorów tych usunie się liczbę 0; zbiorem częściowo uporządkowanym będzie więc zbiór $\langle \mathbb{N} \setminus \{0\}, | \rangle$.

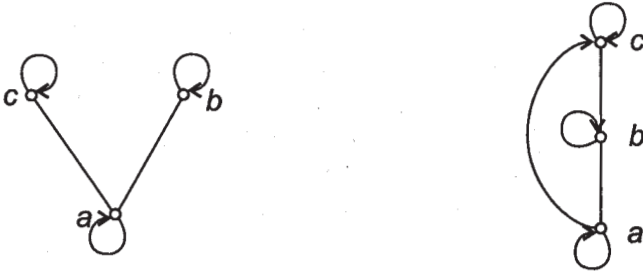
Przykładami skończonych zbiorów częściowo uporządkowanych są zbiory następujące:

$$\langle \{a, b, c\}, \{ \langle a, b \rangle, \langle a, c \rangle, \langle a, a \rangle, \langle c, c \rangle, \langle b, b \rangle \} \rangle$$

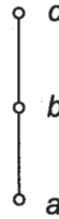
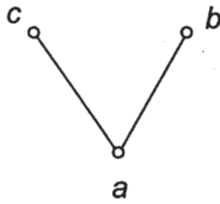
oraz

$$\langle \{a, b, c\}, \{ \langle a, b \rangle, \langle b, c \rangle, \langle a, c \rangle, \langle a, a \rangle, \langle b, b \rangle, \langle c, c \rangle \} \rangle.$$

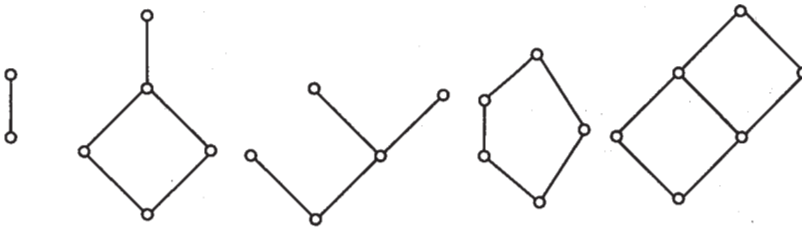
Diagramy tych zbiorów są następujące:



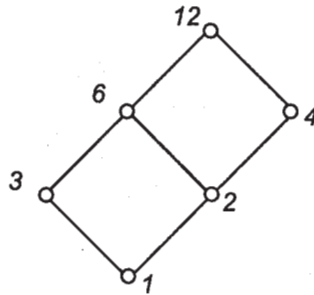
Ponieważ dalej będziemy się też posługiwać diagramami, przyjmiemy następującą konwencję ich rysowania. Skoro z założenia rozważana relacja jest zwrotna, nie rysujemy „pętelki” na każdym punkcie; ponieważ jest przechodnia, w przypadku gdy $x \leq y$ i $y \leq z$ nie łączymy punktów reprezentujących x i z . Ostatnią umową będzie, że punkty narysowane niżej są „mniej ważne” niż punkty narysowane wyżej, a jeśli punkt x leżący niżej jest połączony z y , który leży wyżej, to będzie to oznaczać, że $x \leq y$. W konsekwencji oba te diagramy przyjmą bardziej przejrzystą postać



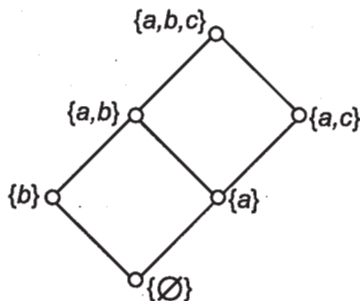
Inne przykłady skończonych relacji częściowego porządku to relacje o następujących diagramach:



Rozważmy relację podzielności określoną na zbiorze $\{1, 2, 3, 4, 6, 12\}$. Porządek w tym zbiorze ilustruje diagram



Zbiór $X = \{\emptyset, \{a\}, \{b\}, \{a, b\}, \{a, c\}, \{a, b, c\}\}$ z relacją \subseteq jest także zbiorem częściowo uporządkowanym; jego diagram jest następujący:



Widać, że zbiory te są „takie same”: choć ich elementy są różne i relacja jest inaczej określona, to jednak diagramy tych porządków są takie same. Te dwa zbiory częściowo uporządkowane stanowią przykład zbiorów izomorficznych.

DEFINICJA 8.2.1. *Zbiory częściowo uporządkowane $\langle X, \leq_1 \rangle$ i $\langle Y, \leq_2 \rangle$ są izomorficzne wtedy i tylko wtedy, gdy istnieje funkcja $f : X \rightarrow Y$ wzajemnie jednoznaczna i „na”, spełniająca warunek*

$$\forall x_1 \forall x_2 (x_1 \leq_1 x_2 \leftrightarrow f(x_1) \leq_2 f(x_2)).$$

W matematyce na ogół utożsamia się obiekty izomorficzne, będziemy zatem utożsamiać izomorficzne zbiory częściowo uporządkowane.

TWIERDZENIE 8.2.2 (twierdzenie o reprezentacji relacji częściowo porządkujących). *Każdy niepusty zbiór częściowo uporządkowany $\langle X, \leq \rangle$ jest izomorficzny z pewną rodziną podzbiorów zbioru X , uporządkowaną relacją inkluzji.*

Dowód. Niech $a \in X$ i niech $(x_0] = \{x \in X : x \leq x_0\}$ (zbiór $(a]$ wyobrażamy sobie jako „stożek” o czubku a), i niech $\mathcal{A} = \{(a] : a \in X\}$. Łatwo sprawdzić, że zbiór $\langle \mathcal{A}, \subseteq \rangle$ jest zbiorem częściowo uporządkowanym.

Niech teraz $f : X \rightarrow \mathcal{A}$ będzie funkcją zadaną zależnością $f(x) = (x]$. Pokażemy, że funkcja f jest izomorfizmem zbiorów $\langle X, \leq \rangle$ i $\langle \mathcal{A}, \subseteq \rangle$.

Po pierwsze, f jest „na”, ponieważ każdy element zbioru \mathcal{A} jest wyznaczony przez jakiś element zbioru X .

Po drugie, f jest różnowartościowa. Załóżmy bowiem, że $(x] = (y]$. Skoro $x \in (x]$, więc $x \in (y]$, a stąd $x \leq y$. Podobnie, skoro $y \in (y]$, więc $y \leq x$. Z antysymetrii relacji \leq wynika teraz, że $x = y$.

Pokażemy wreszcie, że $x \leq y \leftrightarrow f(x) \subseteq f(y)$, tzn. $x \leq y \leftrightarrow (x] \subseteq (y]$.

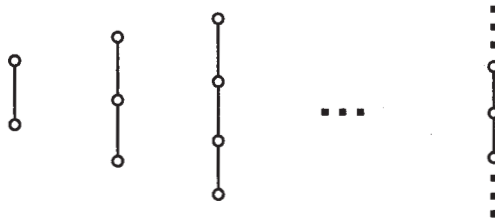
Niech więc $x \leq y$ i niech $x_0 \in (x]$; pokażemy, że $x_0 \in (y]$. Skoro $x_0 \in (x]$, więc $x_0 \leq x$. Z przechodności relacji \leq wynika teraz, że $x_0 \leq y$, a stąd $x_0 \in (y]$, zatem $(x] \subseteq (y]$.

Niech teraz $(x] \subseteq (y]$. Wobec tego dla dowolnego x_0 , jeśli $x_0 \in (x]$, to $x_0 \in (y]$. Zatem dla dowolnego x_0 , jeśli $x_0 \leq x$, to $x_0 \leq y$. W konsekwencji, biorąc $x_0 = x$, uzyskujemy implikację: jeśli $x \leq x$, to $x \leq y$. Ale skoro relacja \leq jest zwrotna, więc $x \leq x$, zatem $x \leq y$, co kończy dowód. Q.E.D.

DEFINICJA 8.2.3. *Niech $\langle X, \leq \rangle$ będzie zbiorem częściowo uporządkowanym. Zbiór $Y \subseteq X$ nazywamy łańcuchem, jeśli relacja \leq jest spójna w Y , tj. dla dowolnych $x, y \in Y$ spełnia warunek*

$$x \neq y \rightarrow (x \leq y \vee y \leq x).$$

Łańcuchami są w szczególności porządki o diagramach



Inny przykład łańcucha to następująca rodzina A podzbiorów zbioru X :

$$A = \{\emptyset, \{x_1\}, \{x_1, x_2\}, \{x_1, x_2, x_3\}, \{x_1, x_2, x_3, x_4\}, \dots\}$$

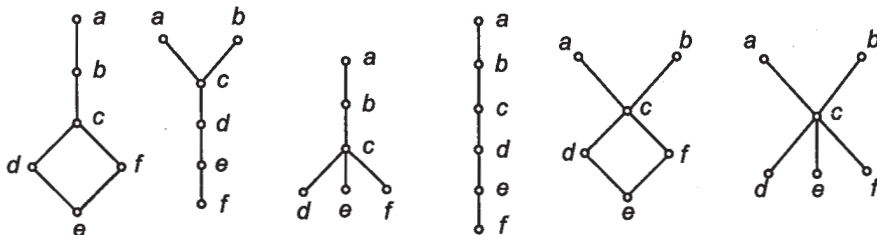
z relacją \subseteq , gdzie x_1, x_2, x_3, \dots to różne elementy zbioru X .

DEFINICJA 8.2.4. Niech $\langle A, \leq \rangle$ będzie zbiorem częściowo uporządkowanym i niech $B \subseteq A$. Element $x_0 \in A$ jest ograniczeniem górnym zbioru B wtedy i tylko wtedy, gdy x_0 spełnia warunek

$$\forall y (y \in B \rightarrow y \leq x_0).$$

Nie wymaga się tu, aby $x_0 \in B$, acz się tego nie wyklucza. Ograniczeń górnych danego zbioru może być więcej niż jedno.

Rozważmy dla przykładu następujące zbiory częściowo uporządkowane:



W powyższych przykładach każdy z elementów zbioru $\{a, b, c\}$ jest ograniczeniem górnym zbioru $\{c, d, e, f\}$.

Podobnie definiuje się ograniczenie dolne.

DEFINICJA 8.2.5. Niech $\langle A, \leq \rangle$ będzie zbiorem częściowo uporządkowanym i niech $B \subseteq A$. Element $x_0 \in A$ jest ograniczeniem dolnym zbioru B wtedy i tylko wtedy, gdy x_0 spełnia warunek

$$\forall y (y \in B \rightarrow x_0 \leq y).$$

DEFINICJA 8.2.6. Niech $\langle A, \leq \rangle$ będzie zbiorem częściowo uporządkowanym. Element $x_0 \in A$ nazywamy elementem największym wtedy i tylko wtedy, gdy $\forall x (x \in A \rightarrow x \leq x_0)$, tzn. gdy wszystkie elementy zbioru A są mniejsze lub równe x_0 . Podobnie definiujemy element najmniejszy, jako taki, od którego wszystkie różne od niego elementy są większe, tzn. element x_0 spełniający warunek $\forall x (x \in A \rightarrow x_0 \leq x)$.

Nie każdy zbiór częściowo uporządkowany ma element najmniejszy i największy. Na przykład zbiór liczb naturalnych ze zwykłym porządkiem \leq ma element najmniejszy, ale nie ma największego. Czytelnik zechce przejrzeć narysowane wyżej diagramy zbiorów częściowo uporządkowanych i sprawdzić, w których istnieją elementy największe i najmniejsze.

Pojęcie elementu najmniejszego i największego pozwala z kolei zdefiniować pojęcie supremum i infimum, czyli kresu górnego i dolnego.

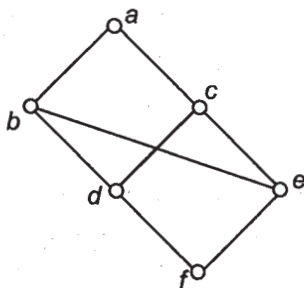
DEFINICJA 8.2.7. Niech $\langle A, \leq \rangle$ będzie zbiorem częściowo uporządkowanym i niech $B \subseteq A$. Supremum albo kresem górnym zbioru B nazywamy element najmniejszy w zbiorze wszystkich ograniczeń górnych zbioru B , jeśli istnieje element najmniejszy w tym zbiorze ograniczeń. Podobnie, infimum albo kres dolny definiujemy jako element największy w zbiorze wszystkich ograniczeń dolnych, o ile istnieje element największy w zbiorze ograniczeń dolnych.

Supremum zbioru B oznacza się symbolem $\sup_{\leq}(B)$, lub, gdy relacja \leq jest ustalona, symbolem $\sup(B)$, a infimum oznacza się symbolem $\inf_{\leq}(B)$ lub $\inf(B)$.

Krótko: supremum (kres górny) zbioru B to najmniejsze ograniczenie górne zbioru B , jeśli istnieje, a infimum (kres dolny) to największe ograniczenie dolne, jeśli istnieje.

Na przykład w zbiorze wszystkich figur płaskich okrąg jest kresem górnym zbioru wszystkich wielokątów opisanych na okręgu (gdy relacją jest inkluzja).

W powyższych przykładach supremum zbioru $\{c, d, e, f\}$ stanowił element c . Natomiast w poniższym przykładzie istnieje ograniczenie górne dla zbioru $\{d, e, f\}$, ale nie istnieje najmniejsze ograniczenie górne, czyli supremum tego zbioru. Ograniczeniami górnymi zbioru $\{d, e, f\}$ są bowiem elementy a, b i c , ale – co łatwo zauważyć – nie istnieje element najmniejszy w rozpatrywanym zbiorze ograniczeń górnych, tj. w zbiorze $\{a, b, c\}$, ponieważ żaden z elementów a, b i c nie ogranicza z dołu wszystkich elementów zbioru $\{d, e, f\}$. Zatem nie istnieje $\sup\{d, e, f\}$.



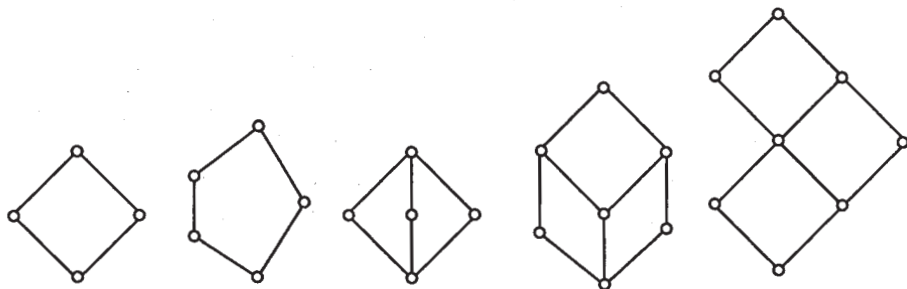
Podobne przykłady można pokazać także dla ograniczenia dolnego i infimum.

Zauważmy, że kres (zarówno górny, jak i dolny) jeśli istnieje, to jest tylko jeden.

DEFINICJA 8.2.8. *Kratą nazywa się zbiór częściowo uporządkowany $\langle A, \leq \rangle$, taki że dla dowolnych dwóch elementów $a, b \in A$ istnieje najmniejsze ograniczenie górne względem relacji \leq i największe ograniczenie dolne względem tej relacji.*

Krótko: kratą jest taki zbiór częściowo uporządkowany, w którym dla dowolnych dwóch elementów istnieje supremum i infimum.

Najprostszymi przykładami krat są zbiory częściowo uporządkowane o następujących diagramach:



Łatwo się przekonać, że każda krata skończona ma element największy i element najmniejszy.

Kratami są też wszystkie łańcuchy. Teoria krat jest bujnie rozwijającą się teorią matematyczną, posiadającą liczne zastosowania.

Od elementu największego należy odróżnić element maksymalny i odpowiednio od elementu najmniejszego – element minimalny.

DEFINICJA 8.2.9. *Niech $\langle A, \leq \rangle$ będzie zbiorem częściowo uporządkowanym. Element x_0 jest elementem maksymalnym wtedy i tylko wtedy, gdy*

spełnia warunek $\neg \exists y (y \in A \wedge x_0 \leq y \wedge y \neq x_0)$, tzn. nie istnieje element większy od x_0 . Podobnie definiuje się element minimalny, jako taki, od którego nie istnieją mniejsze, tzn. taki element x_0 , który spełnia warunek $\neg \exists y (y \in A \wedge y \leq x_0 \wedge y \neq x_0)$.

Można zauważyć, że każdy element największy jest maksymalny. Nie jest natomiast prawdziwe stwierdzenie, że każdy element maksymalny jest największy. Wskazuje na to następujący przykład:



Nie istnieje tu element większy od x_0 , więc x_0 jest elementem maksymalnym, ale w zbiorze z porządkiem zaprezentowanym na diagramie nie istnieje element największy, to jest ograniczający z góry wszystkie elementy tego zbioru. Podobnie y_0 jest też elementem maksymalnym. Pokazany tu przykład wskazuje, że elementów maksymalnych (i analogicznie minimalnych) w danym zbiorze może być więcej niż jeden.

Rozważmy jeszcze inne przykłady.

1. W zbiorze (\mathbb{N}, \leq) istnieje element najmniejszy (jest on też elementem minimalnym), ale nie ma ani elementu maksymalnego, ani największego.

2. Każdy niepusty skończony zbiór częściowo uporządkowany ma co najmniej jeden element minimalny i co najmniej jeden element maksymalny.

3. Jeśli zbiór nie jest skończony, to nie muszą w nim istnieć elementy maksymalne i minimalne. Wskazuje na to następujący przykład:

W zbiorze wszystkich funkcji $f : \mathbb{R} \rightarrow \mathbb{R}$ wprowadzamy porządek \leq następującą równoważnością:

$$f \leq g \leftrightarrow \forall x (f(x) \leq g(x)).$$

Relacja \leq między funkcjami jest częściowym porządkiem, bo, co łatwo sprawdzić, jest zwrotna, antysymetryczna i przechodnia. Zauważmy teraz, że dla każdej funkcji f istnieje funkcja od niej „większa”, to jest taka funkcja g , że $f \leq g$; wystarczy jako g wziąć funkcję $g(x) = f(x) + 1$. Wynika z tego, że w zbiorze wszystkich funkcji rzeczywistych nie istnieje element maksymalny, więc nie istnieje też element największy. Podobne rozważania prowadzą do wniosku, że nie istnieje tu także element najmniejszy i minimalny.

Pojęcia elementu maksymalnego (nie największego!) oraz ograniczenia górnego występują w lemacie, mającym w dowodach matematycznych bardzo ważne zastosowania.

LEMAT 8.2.10 (lemat Kuratowskiego–Zorna): *Niech $\langle A, \leq \rangle$ będzie zbiorem częściowo uporządkowanym. Jeśli każdy łańcuch $L \subseteq A$ elementów zbioru A ma ograniczenie górne, to w zbiorze A istnieje element maksymalny.*

Lemat Kuratowskiego–Zorna jest równoważny aksjomatowi wyboru (por. paragraf następny).

8.3. Zbiory dobrze uporządkowane

Wyróżnimy jeszcze jeden rodzaj relacji porządkujących odgrywających bardzo ważną rolę w matematyce, a mianowicie tzw. dobre porządki.

DEFINICJA 8.3.1. *Relację $R \subseteq X \times X$ nazywamy dobrym porządkiem wtedy i tylko wtedy, gdy relacja R jest częściowym porządkiem, takim że*

$$\forall A \subseteq X, A \neq \emptyset \exists a \in A \forall x \in A (aRx).$$

Zgodnie z tą definicją relacja $R \subseteq X \times X$ jest dobrym porządkiem wtedy i tylko wtedy, gdy R jest relacją zwrotną, antysymetryczną i przechodnią oraz taką, że każdy niepusty podzbiór A zbioru X ma element najmniejszy (pierwszy) w sensie (względem) relacji R .

Łatwo pokazać, że każdy dobry porządek jest relacją spójną, czyli że każdy dobry porządek jest także porządkiem liniowym. Istotnie, niech $R \subseteq X \times X$ będzie dobrym porządkiem i rozważmy dowolne dwa różne elementy $x, y \in X$. Wtedy zbiór $\{x, y\}$ jest niepustym podzbiorem X , czyli $\emptyset \neq \{x, y\} \subseteq X$. Zgodnie z definicją dobrego porządku istnieje w tym zbiorze element najmniejszy. Jeśli tym elementem najmniejszym jest x , to wtedy xRy , a jeśli jest nim y , to wtedy yRx . Ostatecznie więc $xRy \vee yRx$, czyli relacja R jest spójna.

Ponieważ dobry porządek jest porządkiem (liniowym), więc zgodnie z przyjętą w poprzednim rozdziale konwencją, zamiast xRy będziemy pisać $x \leq y$. Jeśli \leq jest dobrym porządkiem w zbiorze X , to parę uporządkowaną $\langle X, \leq \rangle$ nazywać będziemy zbiorem dobrze uporządkowanym.

Przykładem dobrego porządku może być relacja \leq w zbiorze liczb naturalnych \mathbb{N} . Zauważmy, że zwykła relacja \leq nie jest dobrym porządkiem w zbiorze liczb całkowitych \mathbb{Z} ani w zbiorze liczb rzeczywistych \mathbb{R} .

Dla zbiorów dobrze uporządkowanych zachodzi bardzo ważna i często wykorzystywana własność zwana *zasadą indukcji*.

TWIERDZENIE 8.3.2 (zasada indukcji). *Niech $\langle X, \leq \rangle$ będzie zbiorem dobrze uporządkowanym i niech $\varphi(v)$ będzie funkcją zdaniową o jednej zmiennej wolnej v przebiegającej zbiór X . Załóżmy, że*

(1) *najmniejszy element zbioru X ma własność φ ,*

(2) *dla dowolnego elementu $x \in X$, jeżeli wszystkie elementy poprzedzające x mają własność φ , to również element x ma własność φ .*

Wtedy każdy element zbioru X ma własność φ .

Dowód. Załóżmy, że \leq jest dobrym porządkiem w zbiorze X i że funkcja zdaniowa φ ma własności (1) i (2). Przypuśćmy dla dowodu nie wprost, że nie jest prawdą, iż wszystkie elementy zbioru X mają własność φ , tzn. że $\exists(x \in X) \neg\varphi(x)$. Zatem $Z = \{x \in X : \neg\varphi(x)\}$ jest niepusty. Ponieważ $\langle X, \leq \rangle$ jest dobrym porządkiem, więc w zbiorze Z istnieje element najmniejszy. Oznaczmy go przez z_0 . Ponieważ $z_0 \in Z$, zatem $\neg\varphi(z_0)$. Z własności (1) wynika, że z_0 nie jest najmniejszym elementem zbioru X . Z drugiej strony, ponieważ z_0 jest najmniejszym elementem zbioru Z , więc

$$\forall y(y < z_0 \rightarrow \varphi(y)).$$

Na mocy własności (2) mamy zatem $\varphi(z_0)$, co przeczy stwierdzonej wyżej własności $\neg\varphi(z_0)$. Ostatecznie więc przypuszczenie, że istnieją elementy zbioru X , które nie mają własności φ , doprowadziło do sprzeczności, zatem $\forall x \in X \varphi(x)$. Q.E.D.

WNIOSEK 8.3.3. *Jeżeli φ jest funkcją zdaniową o dziedzinie \mathbb{N} , taką że*

(1') $\varphi(0)$,

(2') $\forall n \in \mathbb{N} (\varphi(n) \rightarrow \varphi(n+1))$,

to $\forall n \in \mathbb{N} \varphi(n)$.

Dowód. Zauważmy, że ponieważ 0 jest najmniejszym elementem zbioru \mathbb{N} w sensie naturalnego porządku \leq między liczbami naturalnymi, to też warunek (1') pokrywa się z warunkiem (1) poprzedniego twierdzenia. Z drugiej strony, ponieważ n poprzedza $n+1$, więc warunek (2') wniosku jest silniejszy niż warunek (2) twierdzenia (jest to bowiem implikacja o słabszym poprzedniku). Zatem na mocy zasady indukcji otrzymujemy tezę $\forall n \in \mathbb{N} \varphi(n)$. Q.E.D.

Podany powyżej wniosek to znana zasada indukcji matematycznej. Stawowi ona jeden z (najważniejszych) aksjomatów arytmetyki liczb naturalnych, czyli teorii aksjomatycznej charakteryzującej liczby naturalne i działania na nich. Teorię tę nazywa się zwykle arytmetyką Peana⁴.

Arytmetyka Peana jest to teoria oparta na rachunku predykatów pierwszego rzędu. Jej pozalogiczne pojęcia pierwotne to: stała nazwowa 0 (zero), symbol funkcyjny 1-argumentowy S (następnik) oraz dwa symbole funkcyjne 2-argumentowe: $+$ (dodawanie) i \cdot (mnożenie). Aksjomaty pozalogiczne są następujące:

- (1) $S(x) = S(y) \rightarrow x = y$,
- (2) $\neg[S(x) = 0]$,
- (3) $x + 0 = x$,
- (4) $x + S(y) = S(x + y)$,
- (5) $x \cdot 0 = 0$,
- (6) $x \cdot S(y) = x \cdot y + x$,
- (7) $\varphi(0) \wedge \forall x[\varphi(x) \rightarrow \varphi(S(x))] \rightarrow \forall x\varphi(x)$,

gdzie φ jest dowolną formułą języka arytmetyki Peana. Zauważmy, że ostatni aksjomat jest schematem nieskończenie wielu aksjomatów – dla każdej formuły φ otrzymujemy jeden aksjomat (schemat ten nazywa się schematem indukcji).

Zasada indukcji jest często wykorzystywana w dowodach matematycznych. Jeśli mianowicie należy udowodnić, że pewna własność zachodzi dla wszystkich liczb naturalnych, to zgodnie z zasadą indukcji wystarczy pokazać, że zachodzi ona dla liczby 0 (czy ogólniej: dla pierwszej liczby naturalnej, dla której rozważana własność ma zachodzić), a następnie rozważyć dowolną, ale ustaloną liczbę k i założywszy, że badana własność zachodzi dla k , pokazać, że zachodzi też dla liczby następnej, tzn. dla $k + 1$. Zilustrujmy to przykładem. Udowodnijmy mianowicie, że suma n pierwszych liczb parzystych jest równa $n(n + 1)$, tzn. dla każdej liczby naturalnej n zachodzi równość

$$2 + 4 + 6 + \dots + 2n = n(n + 1).$$

Dla $n = 1$ mamy jedną tylko liczbę parzystą, a mianowicie 2. Stąd lewa strona naszego wzoru równa się 2. Prawa zaś jest równa $1 \cdot (1 + 1)$, czyli także 2. Teraz krok indukcyjny: niech k będzie dowolną liczbą naturalną

⁴ Od nazwiska matematyka włoskiego Giuseppe Peana (1858–1932), który jako pierwszy zaksjomatyzował arytmetykę liczb naturalnych.

i załóżmy, że dla niej zachodzi nasza równość, tzn. że suma pierwszych k liczb parzystych jest równa $k(k+1)$, czyli

$$2 + 4 + 6 + \dots + 2k = k(k+1).$$

To jest założenie indukcyjne. Teza indukcyjna głosi, że suma pierwszych $k+1$ liczb parzystych jest równa $(k+1)(k+2)$. Istotnie mamy

$$2 + 4 + 6 + \dots + 2k + 2(k+1) = k(k+1) + 2(k+1) = (k+1)(k+2).$$

Wykazaliśmy zatem tezę indukcyjną, korzystając z założenia indukcyjnego. Na mocy zasady indukcji możemy zatem stwierdzić, że dla każdej liczby naturalnej n suma pierwszych n liczb parzystych jest równa $n(n+1)$.

Rozważmy jeszcze jeden przykład: udowodnijmy mianowicie, że suma pierwszych n liczb nieparzystych jest równa n^2 , czyli że dla każdej liczby naturalnej n

$$1 + 3 + 5 + \dots + (2n-1) = n^2.$$

Istotnie, dla $n=1$ mamy po lewej stronie liczbę 1, a po prawej 1^2 , czyli też 1. Teraz niech k będzie dowolną ustaloną liczbą naturalną i załóżmy (jest to założenie indukcyjne), że zachodzi dla niej dowodzona równość, tzn.

$$1 + 3 + 5 + \dots + (2k-1) = k^2.$$

Pokażemy, że (i to jest teza indukcyjna), że zachodzi ona także dla następnej liczby naturalnej, czyli dla $k+1$, tzn.

$$1 + 3 + 5 + \dots + (2k-1) + (2k+1) = (k+1)^2.$$

Mamy

$$1 + 3 + 5 + \dots + (2k-1) + (2k+1) = k^2 + (2k+1) = k^2 + 2k + 1 = (k+1)^2.$$

* * *

Na początku rozważań tego paragrafu podaliśmy tylko jeden przykład zbioru dobrze uporządkowanego. Trudno jest podać inne naturalne przykłady zbiorów uporządkowanych. Z faktem tym kontrastuje następujące twierdzenie:

TWIERDZENIE 8.3.4 (o dobrym uporządkowaniu; Zermelo 1904). *Dla każdego zbioru X istnieje relacja \leq dobrze porządkująca zbiór X .*

Z twierdzenia tego wynika w szczególności, że zbiór liczb rzeczywistych \mathbb{R} można dobrze uporządkować, tzn. że istnieje relacja dobrze porządkująca \mathbb{R} . Można pokazać, że relacja taka jest bardzo skomplikowana, tzn. stopień jej złożoności, mierzony złożonością formuły definiującej taką relację dobrego porządku na \mathbb{R} , jest bardzo wysoki (przy tym złożoność formuły mierzymy liczbą i rodzajem kwantyfikatorów niezbędnych w takiej definicji). Nie możemy tu oczywiście podawać bardzo trudnego dowodu tych faktów. Zauważmy tylko, że wyjaśniają one, dlaczego nie ma naturalnych przykładów dobrych porządków zbioru liczb rzeczywistych czy innych zbiorów liczb znanych z praktyki matematycznej.

Twierdzenie o dobrym uporządkowaniu wyprowadza się (w aksjomatycznej teorii mnogości) z aksjomatu wyboru, co więcej, aksjomat ten jest równoważny twierdzeniu o dobrym uporządkowaniu.

AKSJOMAT WYBORU. *Dla każdej rodziny zbiorów niepustych i parami rozłącznych istnieje zbiór mający z każdym ze zbiorów tej rodziny po dokładnie jednym elemencie wspólnym (zbiór ten nazywa się selektorem).*

Czasami aksjomatowi wyboru nadaje się też inną postać.

AKSJOMAT WYBORU (druga postać). *Dla dowolnej rodziny \mathcal{A} zbiorów niepustych istnieje funkcja wyboru, tzn. funkcja przyporządkowująca każdemu zbiorowi z rodziny \mathcal{A} pewien jego element.*

Można pokazać, że oba sformułowania aksjomatu wyboru są sobie równoważne.

W matematyce używa się także innych zasad, które są równoważne aksjomatowi wyboru. Chodzi tu w szczególności o lemat Kuratowskiego–Zorna i o lemat Teichmüllera–Tukeya.

LEMAT KURATOWSKIEGO–ZORNA. *Jeśli dla każdego liniowo uporządkowanego podzbioru X_0 zbioru częściowo uporządkowanego X istnieje ograniczenie górne, to w zbiorze X istnieje element maksymalny.*

Zanim sformułujemy lemat Teichmüllera–Tukeya, musimy wprowadzić pewne nowe pojęcie. Otóż będziemy mówili, że dana własność Φ , mogąca przysługiwać podzbiom pewnego zbioru X , jest własnością skończonego charakteru wtedy i tylko wtedy, gdy zbiór pusty \emptyset ma własność Φ oraz, dla każdego $X_0 \subseteq X$, zbiór X_0 ma własność Φ wtedy i tylko wtedy, gdy ma ją każdy skończony podzbiór zbioru X_0 .

LEMAT TEICHMÜLLERA–TUKEYA. *Niech Φ będzie pewną własnością charakteru skończonego mogącą przysługiwać podzbiom pewnego zbioru X .*

Dowolny podzbiór zbioru X mający własność Φ jest zawarty w maksymalnym zbiorze $X_0 \subseteq X$ mającym własność Φ , tj. w takim zbiorze X_0 mającym własność Φ , że dla każdego $X_1 \subseteq X$ mającego własność Φ i takiego, że $X_0 \subseteq X_1$, mamy $X_0 = X_1$.

Wszystkie opisane wyżej zasady są sobie równoważne, tzn. zachodzi następujące twierdzenie:

Twierdzenie 8.3.5. *Wszystkie poniższe zasady są sobie równoważne:*

- aksjomat wyboru,
- twierdzenie Zermela o dobrym uporządkowaniu,
- lemat Kuratowskiego-Zorna,
- lemat Teichmüllera-Tukeya.

Aksjomat wyboru i opisane wyżej zasady mu równoważne odgrywają bardzo ważną rolę w matematyce i są wykorzystywane w dowodach wielu ważnych twierdzeń analizy, algebry, topologii, teorii miary, analizy funkcjonalnej itd.

Zadania

1. Pokazać, że każda relacja przeciwzwrotna i przechodnia jest przeciwsymetryczna.
2. Niech R będzie relacją quasi-porządkującą w zbiorze X , tj. zwrotną i przechodnią. Niech S_R będzie relacją zdefiniowaną następująco: xS_Ry wtedy i tylko wtedy, gdy $xRy \wedge yRx$.
 - a. Pokazać, że S_R jest relacją równoważności.
 - b. Oznaczmy przez $[x]$ klasę abstrakcji relacji S_R . Pokazać, że relacja \leq na klasach abstrakcji, zdefiniowana równoważnością: $[x] \leq [y]$ wtedy i tylko wtedy, gdy xRy , jest relacją częściowo porządkującą w zbiorze klas abstrakcji.
3. Niech \leq będzie częściowym porządkiem w zbiorze X . Pokazać, że relacja ostrego porządku generowana przez \leq , to jest relacja definiowana równoważnością: $x < y$ wtedy i tylko wtedy, gdy $x \leq y \wedge x \neq y$, jest przeciwzwrotna i przechodnia.
4. Sprawdzić, że dla dowolnego zbioru X , para $(\mathcal{P}(X), \subseteq)$ jest zbiorem częściowo uporządkowanym.
5. Narysować diagram zbioru uporządkowanego $(\mathcal{P}(\{a, b, c, d\}), \subseteq)$.
6. Sprawdzić, że dla dowolnego zbioru X , para $(\mathbb{N} \setminus \{0\}, |)$, gdzie $|$ jest relacją podzielności, jest zbiorem częściowo uporządkowanym.

7. Narysować diagram zbioru częściowo uporządkowanego

$$\langle \{x \in \mathbb{N} : 1 \leq x \leq 10\}, | \rangle.$$

8. Narysować diagramy zbiorów częściowo uporządkowanych

$$\langle \{2, 3, 5, 6, 10, 15\}, | \rangle \text{ oraz } \langle \{\{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}\}, \subseteq \rangle$$

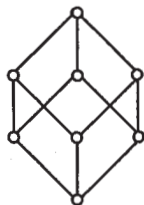
i zauważyć, że są to zbiory izomorficzne; zdefiniować funkcję będącą izomorfizmem tych zbiorów.

9. Narysować diagramy następujących zbiorów częściowo uporządkowanych, których uniwersum stanowi zbiór $\{a, b, c, d\}$, a relację stanowią następujące pary:

- $\{\langle a, a \rangle, \langle b, b \rangle, \langle c, c \rangle, \langle d, d \rangle, \langle a, d \rangle, \langle b, d \rangle, \langle c, d \rangle\}$,
- $\{\langle a, a \rangle, \langle b, b \rangle, \langle c, c \rangle, \langle d, d \rangle, \langle a, c \rangle, \langle b, c \rangle, \langle c, d \rangle, \langle a, d \rangle, \langle b, d \rangle\}$,
- $\{\langle a, a \rangle, \langle b, b \rangle, \langle c, c \rangle, \langle d, d \rangle, \langle a, b \rangle, \langle a, c \rangle, \langle d, c \rangle\}$.

10. Narysować diagramy wszystkich (z dokładnością do izomorfizmu) zbiorów częściowo uporządkowanych jedno-, dwu- i trzejelementowych.

11. zilustrować twierdzenie o reprezentacji zbiorów częściowo uporządkowanych, biorąc zbiór uporządkowany przez relację \leq następującym diagramie:



12. Udowodnić, że element największy jest zarazem maksymalny.

13. Pokazać, że w zbiorze $\mathbb{N} \setminus \{0, 1\}$ z relacją podzielności istnieje nieskończenie wiele elementów minimalnych. (*Wskazówka*: rozważyć liczby pierwsze).

14. Wiadomo⁵, że relacja \approx na zbiorze \mathcal{F} wszystkich formuł języka rachunku zdań, zdefiniowana następująco:

$$\phi \approx \psi \text{ wtedy i tylko wtedy, gdy } (\phi \leftrightarrow \psi) \in \mathfrak{T},$$

jest relacją równoważności na zbiorze formuł rachunku zdań \mathcal{F} (symbolem \mathfrak{T} oznaczamy tu zbiór tautologii rachunku zdań). Oznaczmy przez \mathcal{F}/\approx zbiór wszystkich klas abstrakcji względem \approx . Na zbiorze \mathcal{F}/\approx zdefiniujemy teraz relację \leq następująco:

$$[\phi]_{\approx} \leq [\psi]_{\approx} \text{ wtedy i tylko wtedy, gdy } (\phi \rightarrow \psi) \in \mathfrak{T}.$$

- Udowodnić, że relacja \leq jest relacją częściowego porządku.
- Znaleźć elementy największy i najmniejszy w zbiorze $\langle \mathcal{F}/\approx, \leq \rangle$.
(*Wskazówka*: rozważyć odpowiednio zbiory tautologii i negacji tautologii).

⁵ Por. zadanie 13, rozdział 6.

15. Dlaczego zbiory $\langle \mathbb{Z}, \leq \rangle$ i $\langle \mathbb{R}, \leq \rangle$ nie są dobrze uporządkowane?
16. Czy zbiór wszystkich ułamków postaci $\frac{1}{n}$ ($n \in \mathbb{N}$) z relacją \leq jest dobrze uporządkowany?
17. Pokazać, że porządek liniowy w zbiorze skończonym jest dobrym porządkiem w tym zbiorze.
18. Udowodnić, że każdy zbiór skończony można dobrze uporządkować.
19. Na ile sposobów można dobrze uporządkować zbiór skończony n -elementowy?
20. Niech $\langle X, \leq \rangle$ będzie zbiorem częściowo uporządkowanym. Element y nazywamy (bezpośrednim) następnikiem elementu x wtedy i tylko wtedy, gdy xRy , ale nie istnieje taki z , różny od x i y , że xRz i zRy , formalnie

$$xRy \wedge \forall z(xRz \wedge zRy \rightarrow z = x \vee z = y).$$

- a. Pokazać, że jeśli $\langle X, \leq \rangle$ jest zbiorem dobrze uporządkowanym, to każdy jego element z wyjątkiem elementu ostatniego (jeśli element taki istnieje w X) ma bezpośredni następnik.
- b. Sprawdzić, że funkcja $S : \mathbb{N} \rightarrow \mathbb{N}$, zadana równością: $S(n) = n + 1$, definiuje bezpośredni następnik elementu n w zbiorze $\langle \mathbb{N}, \leq \rangle$, gdzie \leq jest zwykłą relacją „mniejsze lub równe”.
21. Uporządkujemy zbiór \mathbb{Z} liczb całkowitych w następujący ciąg: $0, -1, 1, -2, 2, \dots, -n, n, -(n+1), n+1, \dots$
- a. Zdefiniować dokładnie relację \preceq , porządkującą w podany sposób zbiór \mathbb{Z} , tak aby \preceq była częściowym porządkiem.
- b. Pokazać, że $\langle \mathbb{Z}, \preceq \rangle$ jest zbiorem dobrze uporządkowanym.
- c. Zdefiniować funkcję bezpośredniego następnika w zbiorze $\langle \mathbb{Z}, \preceq \rangle$.
- d. Pokazać, że zbiory $\langle \mathbb{N}, \leq \rangle$ i $\langle \mathbb{Z}, \preceq \rangle$ są izomorficzne.
22. Czy relacja odwrotna do dobrego porządku zawsze jest dobrym porządkiem?
23. Czy w każdym zbiorze dobrze uporządkowanym dowolny element, oprócz pierwszego, ma bezpośredni poprzednik (bezpośredni poprzednik definiujemy analogicznie do bezpośredniego następnika)?

Rozdział 9

Teoria mocy

9.1. Wprowadzenie

Teoria mocy zajmująca się kwestią liczości zbiorów i porównywaniem ich liczości jest jednym z głównych działów teorii mnogości. Stanowiła ona też jeden z zasadniczych tematów rozważań Georga Cantora, twórcy teorii mnogości. To on właśnie wprowadził pojęcie mocy zbioru i pojęcie liczby kardynalnej (będące uogólnieniem pojęcia liczości czy liczby elementów w zbiorze) oraz udowodnił podstawowe własności liczb kardynalnych. Szczególne znaczenie miały jego rozważania dotyczące zbiorów nieskończonych oraz badania dotyczące mocy konkretnych zbiorów znanych z praktyki badawczej matematyków, zwłaszcza zbiorów liczb (naturalnych, wymiernych, rzeczywistych).

Zanim wprowadzimy podstawowe pojęcia teorii mocy, zacznijmy od pewnej intuicji. Wyobraźmy sobie mianowicie dziecko, które otrzymało dwa pudełka cukierków i zastanawia się, czy w obu pudełkach jest ich tyle samo. Aby rostrzygnąć tę kwestię, może ono albo (1) policzyć cukierki w obu pudełkach i uzyskane tak liczby porównać (o ile oczywiście jest już na tyle rozwinięte, że potrafi wykonywać takie operacje), albo też (2) wyjmować jednocześnie po jednym cukierku z każdego z pudełek (czyli łączyć elementy obu pudełek w pary) i tak otrzymane pary odkładać na bok, po czym, jeśli cukierki wyczerpią się jednocześnie w obu pudełkach, będzie mogło stwierdzić, że zawierały one po tyle samo cukierków, a jeśli nie, to że w jednym z pudełek było ich więcej. Zauważmy, że sposób drugi jest prostszy i nie wymaga żadnych właściwie uprzednich umiejętności (w szczególności rachowania). Jest on też bardziej uniwersalny, ponieważ (w odróżnieniu od pierwszego sposobu) może być zastosowany nie tylko do zbiorów skończonych, ale i do zbiorów nieskończonych (tu oczywiście nie

będziemy już mówić o cukierkach, chcąc uniknąć pytania o to, czy może być aktualnie nieskończenie wiele cukierków!).

Zapytajmy, co właściwie robi dziecko, wyjmując jednocześnie po jednym cukierku z każdego z pudełek i odkładając taką parę na bok? Otóż, mówiąc językiem matematyki, dziecko określa funkcję różnowartościową ze zbioru złożonego z cukierków znajdujących się w jednym z pudełek do zbioru złożonego z cukierków w drugim pudełku. Gdy cukierki wyczerpią się jednocześnie (czyli gdy określana przez nie funkcja okaże się funkcją „na”, tzn. suriekcją), to dziecko stwierdza, że w obu pudełkach było ich tyle samo, czyli że liczba cukierków w obu pudełkach była taka sama¹. Ta właśnie intuicja leży u podstaw fundamentalnego w teorii mocy pojęcia równoliczności. Przyjmujemy mianowicie następującą definicję:

DEFINICJA 9.1.1. *Mówimy, że dwa zbiory X i Y są równoliczne (lub tej samej mocy) wtedy i tylko wtedy, gdy istnieje funkcja odwzorowująca wzajemnie jednoznacznie zbiór X na zbiór Y .*

Jeśli zbiory X i Y są równoliczne, to piszemy wtedy $X \sim Y$. Zatem mamy

$$X \sim Y \leftrightarrow \exists f [f : X \xrightarrow[\text{na}]{1-1} Y].$$

LEMAT 9.1.2. *Relacja równoliczności jest relacją równoważności.*

D o w ó d. Należy wykazać, że relacja równoliczności \sim jest zwrotna, symetryczna i przechodnia. Rozważmy zatem dowolny zbiór X . Łatwo widzieć, że funkcja tożsamościowa $I : X \rightarrow X$, taka że $I(x) = x$, jest bijekcją zbioru X na siebie. Zatem $X \sim X$ i w konsekwencji relacja równoliczności jest zwrotna. Aby udowodnić jej symetryczność, rozważmy dwa dowolne zbiory X i Y oraz załóżmy, że $X \sim Y$. To oznacza, że istnieje funkcja różnowartościowa f odwzorowująca X na Y . Zgodnie z własnościami bijekcji (por. paragraf 7.3) funkcja odwrotna do funkcji f , tzn. funkcja f^{-1} , jest bijekcją między zbiorem Y i zbiorem X . Zatem $Y \sim X$. Dla dowodu własności przechodniości rozważmy wreszcie trzy dowolne zbiory X, Y, Z i załóżmy, że $X \sim Y$ oraz $Y \sim Z$. To oznacza, że dla pewnych bijekcji f i g mamy $f : X \xrightarrow[\text{na}]{1-1} Y$ oraz $g : Y \xrightarrow[\text{na}]{1-1} Z$. Stąd superpozycja tych funkcji, czyli funkcja

¹ Metoda ta nie dostarcza informacji na temat tego, ile cukierków jest w pudełku. Jest więc podobna do sposobów, jakie stosowali ludzie pierwotni przy „liczeniu” elementów jakiegoś zbioru, co robiono zwykle przez porównywanie elementów tego zbioru z pewnym ustalonym wzorcem. O pierwotnych sposobach ustalania liczebności można przeczytać w interesującej książce Georgesa Ifraha, *Dzieje liczby, czyli historia pewnego wynalazku*, Ossolineum, Wrocław 1991.

$f \circ g : X \rightarrow Z$ jest bijekcją zbioru X i zbioru Z (por. twierdzenie 7.3.1).
Zatem zbiory X i Z są równoliczne, czyli $X \sim Z$. Q.E.D.

9.2. Liczby kardynalne. Twierdzenie Cantora–Bernsteina

Skoro relacja równoliczności jest relacją równoważności, więc możemy mówić o jej klasach abstrakcji. Przyjmujemy zatem następującą definicję:

DEFINICJA 9.2.1. *Klasy abstrakcji relacji równoliczności \sim nazywamy mocami zbiorów albo liczbami kardynalnymi. Moc zbioru A oznaczamy przez \overline{A} lub przez $\text{card}(A)$.*

Symbol \overline{A} został wprowadzony przez Cantora. Podwójna kreska nad literą A ma wyrażać podwójny proces abstrakcji: abstrahujemy mianowicie zarówno od jakości elementów zbioru A , jak i od ich porządku. Symbol $\text{card}(A)$ pochodzi zaś od angielskiego słowa *cardinality* – liczba kardynalna, moc.

Najprostszy przykładami liczb kardynalnych są liczby naturalne. Możemy więc powiedzieć na przykład, że liczba 2 jest to klasa abstrakcji zbiorów dwuelementowych, a więc w szczególności klasa abstrakcji (względem relacji równoliczności) zbioru $\{\text{prawda}, \text{fałsz}\}$. Ogólnie liczbami naturalnymi będziemy nazywali moce (liczby kardynalne) zbiorów skończonych, przy czym to ostatnie pojęcie definiujemy, opierając się na pojęciu zbioru nieskończonego. Otóż przyjmujemy następującą definicję:

DEFINICJA 9.2.2. *Zbiór X nazywamy nieskończonym wtedy i tylko wtedy, gdy jest on równoliczny z pewnym swoim podzbiorem właściwym, tzn. gdy istnieje zbiór $Y \subsetneq X$, taki że $X \sim Y$. Mówimy zaś, że zbiór X jest skończony wtedy i tylko wtedy, gdy nie jest on nieskończony.*

Podana definicja zbioru nieskończonego pochodzi od Richarda Dedekinda.

Własność, o której mówi definicja zbiorów nieskończonych, podana przez Dedekinda, spotykamy często w matematyce. Wskazują na to następujące przykłady zbiorów nieskończonych:

1. Zbiór liczb naturalnych jest równoliczny ze zbiorem liczb parzystych. Funkcją ustalającą równoliczność jest tu funkcja $f(x) = 2x$.

2. Podobnie równoliczne są dwa dowolne przedziały (a, b) i (c, d) liczb rzeczywistych czy dowolny dany przedział (a, b) i cały zbiór liczb rzeczywistych \mathbb{R} , czyli prosta $(-\infty, \infty)$. Aby pokazać tę ostatnią własność, wystarczy zauważyć, że funkcja $\operatorname{tg} x$ ustala równoliczność przedziału $(-\frac{\pi}{2}, \frac{\pi}{2})$ i prostej $(-\infty, \infty)$ oraz skorzystać z faktu, że dowolne dwa przedziały otwarte są równoliczne, a relacja równoliczności jest przechodnia.

3. Można też pokazać², że dla dowolnych liczb rzeczywistych a, b oraz c, d , takich że $a < b$ i $c < d$, mamy $(a, b) \sim [c, d]$.

4. Zbiory równoliczne nie muszą mieć tego samego wymiaru: można na przykład udowodnić, że przedział $(0, 1)$ jest równoliczny z kwadratem $(0, 1] \times (0, 1]$ bez punktu $(1, 1)$.

Podstawowym twierdzeniem pozwalającym ustalać równoliczność konkretnych zbiorów jest następujące twierdzenie Cantora–Bernsteina:

TWIERDZENIE 9.2.3 (Cantor–Bernstein). *Jeśli zbiór A jest równej mocy z pewnym podzbiorem zbioru B , a zbiór B jest równej mocy z pewnym podzbiorem zbioru A , to zbiory A i B są równoliczne.*

WNIOSEK 9.2.4. *Jeżeli $C \subseteq B \subseteq A$ oraz $A \sim C$, to również $B \sim A$ i $B \sim C$.*

Twierdzenie Cantora–Bernsteina, a zwłaszcza wniosek z niego są często stosowanymi narzędziami pozwalającymi ustalić równoliczność dwu danych zbiorów. Dla przykładu pokażemy – używając wniosku z twierdzenia Cantora–Bernsteina – że kwadrat bez brzegu K jest równoliczny z kołem S z brzegiem. W tym celu rozważmy dwa dowolne kwadraty K_1 i K_2 bez brzegu, takie że $K_1 \subseteq S \subseteq K_2$ (zarówno kwadraty, jak i koło traktujemy jako zbiory punktów na danej płaszczyźnie). Łatwo pokazać – wykorzystując na przykład rzut środkowy – że $K_1 \sim K_2$ oraz $K_1 \sim K$. Na mocy wniosku dostajemy stąd $K_1 \sim S$, co z kolei, na mocy przechodności i symetrii relacji równoliczności, daje $K \sim S$.

Przykład ten, podobnie jak i poprzednie mogą sugerować, że wszystkie właściwie zbiory nieskończone są sobie równoliczne i że w konsekwencji istnieje tylko jedna nieskończoność. Jest to jednak wniosek błędny. Otóż w dalszym ciągu pokażemy (por. paragraf 9.4), że istnieje wiele zbiorów nieskończonych nierównolicznych z sobą, a zatem istnieje wielka różnorodność nieskończoności.

² Dowód znaleźć można na przykład w książce R. Murawskiego i K. Świrydowicza, *Wstęp do teorii mnogości*, Wydawnictwo Naukowe UAM, Poznań 2005. Tam także znaleźć można dowody innych twierdzeń podanych w tym rozdziale bez dowodu.

9.3. Zbiory przeliczalne

Zbiory, których elementy można przeliczyć (przynajmniej teoretycznie), nazywać będziemy przeliczalnymi. Ścisła definicja jest następująca:

DEFINICJA 9.3.1. *Zbiór X nazywamy przeliczalnym wtedy i tylko wtedy, gdy X jest skończony lub równoliczny ze zbiorem liczb naturalnych \mathbb{N} .*

Szczególnie interesujące są oczywiście nieskończone zbiory przeliczalne. Moc zbioru \mathbb{N} liczb naturalnych (a zatem i moc każdego nieskończonego zbioru przeliczalnego) oznaczamy (za Cantorem) symbolem³ \aleph_0 .

Oto kilka przykładów nieskończonych zbiorów przeliczalnych: zbiór liczb nieparzystych, zbiór \mathbb{Z} liczb całkowitych, zbiór odwrotności liczb naturalnych dodatnich, czyli zbiór $\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\}$, zbiór liczb pierwszych.

Łatwo zauważyć, że zbiór nieskończony jest przeliczalny wtedy i tylko wtedy, gdy jego elementy można ustawić w ciąg nieskończony

$$a_0, a_1, a_2, \dots$$

Istotnie, jeśli zbiór nieskończony X jest przeliczalny, to na mocy definicji istnieje bijekcja $f: \mathbb{N} \xrightarrow{1-1} X$. Funkcja ta wyznacza oczywiście ciąg nieskończony: $a_0 = f(0), a_1 = f(1), a_2 = f(2), \dots$. Zatem elementy zbioru X można ustawić w ciąg nieskończony. Na odwrót, ustawienie elementów zbioru X w ciąg nieskończony, to nic innego jak określenie bijekcji $f: \mathbb{N} \xrightarrow{1-1} X$.

TWIERDZENIE 9.3.2. *Zbiór \mathbb{Q} liczb wymiernych jest przeliczalny, dokładniej*

$$\overline{\mathbb{Q}} = \aleph_0.$$

D o w ó d. Rozważmy na początek zbiór \mathbb{Q}^+ wszystkich liczb wymiernych dodatnich, czyli zbiór $\mathbb{Q}^+ = \{r \in \mathbb{Q} : r > 0\}$. Ustawmy elementy tego zbioru w tablicę według następującej zasady: w pierwszym wierszu umieszczamy w porządku malejącym liczby wymierne (czyli ułamki) o liczniku 1, w drugim – kolejne liczby wymierne o liczniku 2, w trzecim – liczby wymierne o liczniku 3 itd. W ten sposób otrzymujemy następującą tablicę:

³ Jest to pierwsza litera alfabetu hebrajskiego „alef” z indeksem zero.

$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{5}$...
$\frac{2}{1}$	$\frac{2}{2}$	$\frac{2}{3}$	$\frac{2}{4}$	$\frac{2}{5}$...
$\frac{3}{1}$	$\frac{3}{2}$	$\frac{3}{3}$	$\frac{3}{4}$	$\frac{3}{5}$...
$\frac{4}{1}$	$\frac{4}{2}$	$\frac{4}{3}$	$\frac{4}{4}$	$\frac{4}{5}$...
$\frac{5}{1}$	$\frac{5}{2}$	$\frac{5}{3}$	$\frac{5}{4}$	$\frac{5}{5}$...
...

W tablicy tej występuje każda liczba ze zbioru \mathbb{Q}^+ , co więcej, każda występuje wielokrotnie. Ustawiamy teraz elementy tej tablicy w ciąg według następującej zasady: najpierw wstawiamy te ułamki, w których suma licznika i mianownika wynosi 2, potem te ułamki, w których suma licznika i mianownika wynosi 3, dalej ułamki o sumie licznika i mianownika 4 itd. (poszczególne grupy zaznaczamy klamrami, pisząc pod nimi sumę licznika i mianownika). Otrzymujemy w ten sposób ciąg

$$\underbrace{\frac{1}{1}}_2, \underbrace{\frac{2}{1}, \frac{1}{2}}_3, \underbrace{\frac{3}{1}, \frac{2}{2}, \frac{1}{3}}_4, \underbrace{\frac{4}{1}, \frac{3}{2}, \frac{2}{3}, \frac{1}{4}}_5, \underbrace{\frac{5}{1}, \frac{4}{2}, \frac{3}{3}, \frac{2}{4}, \frac{1}{5}}_6, \dots$$

Wykreślmy z tego ciągu wyrazy powtarzające się, tzn. jeśli jakiś wyraz pojawia się po raz drugi, trzeci itd., to wykreślamy to drugie, trzecie itd. jego wystąpienie. W ten sposób otrzymamy ciąg nieskończony zawierający wszystkie liczby wymierne dodatnie, co więcej, każdą dokładnie jeden raz. Mamy więc w szczególności ciąg

$$\frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \frac{1}{3}, \frac{4}{1}, \frac{3}{2}, \frac{2}{3}, \frac{1}{4}, \frac{5}{1}, \frac{1}{5}, \dots$$

Aby otrzymać teraz ciąg składający się z wszystkich liczb wymiernych, wystarczy wziąć ciąg następujący:

$$0, \frac{1}{1}, -\frac{1}{1}, \frac{2}{1}, -\frac{2}{1}, \frac{1}{2}, -\frac{1}{2}, \frac{3}{1}, -\frac{3}{1}, \frac{1}{3}, -\frac{1}{3}, \frac{4}{1}, -\frac{4}{1}, \dots$$

W ten sposób pokazaliśmy, że wszystkie elementy zbioru \mathbb{Q} liczb wymiernych można ustawić w ciąg nieskończony, a zatem zbiór \mathbb{Q} jest nieskończony przeliczalny, czyli jest mocy \aleph_0 . Q.E.D.

Stosując metodę wykorzystaną w dowodzie powyższego twierdzenia, można udowodnić następujące twierdzenie o mocy sumy przeliczalnej liczby zbiorów przeliczalnych:

TWIERDZENIE 9.3.3. *Suma przeliczanej liczby zbiorów przeliczalnych jest zbiorem przeliczalnym.*

Za pomocą tego twierdzenia można uzyskać interesujące informacje na temat ważnych (na przykład z punktu widzenia algebry) zbiorów.

WNIOSEK 9.3.4. *Dla dowolnego $n \in \mathbb{N}$, zbiór W_n wielomianów n -tego stopnia o współczynnikach całkowitych jest przeliczalny.*

WNIOSEK 9.3.5. *Zbiór W wszystkich wielomianów o współczynnikach całkowitych jest przeliczalny.*

9.4. Zbiory nieprzeliczalne

W poprzednim paragrafie rozważaliśmy zbiory przeliczalne, czyli równoliczne ze zbiorem \mathbb{N} liczb naturalnych (lub też skończone). Pokazaliśmy w szczególności, że zbiór \mathbb{Q} liczb wymiernych jest przeliczalny. Naturalne jest więc teraz pytanie o moc zbioru \mathbb{R} liczb rzeczywistych.

Zauważmy przede wszystkim, że $\mathbb{R} \sim (0, 1)$. Zatem wystarczy zapytać o moc przedziału $(0, 1)$. Odpowiedź przynosi następujące twierdzenie:

TWIERDZENIE 9.4.1. *Przedział $(0, 1)$ nie jest przeliczalny.*

D o w ó d. Przypuśćmy, dla dowodu nie wprost, że przedział $(0, 1)$ jest przeliczalny. Znaczy to, że wszystkie elementy tego przedziału można ustawić w ciąg $x_1, x_2, x_3, x_4, \dots$. Zauważmy, że każda liczba x z przedziału $(0, 1)$ ma dokładnie jedno nieskończone rozwinięcie dziesiętne. Zatem elementy $x_1, x_2, x_3, x_4, \dots$ przedziału $(0, 1)$ możemy przedstawić w następującej tabelicy:

$$\begin{aligned} x_1 &= 0, a_{11} a_{12} a_{13} a_{14} \dots \\ x_2 &= 0, a_{21} a_{22} a_{23} a_{24} \dots \\ x_3 &= 0, a_{31} a_{32} a_{33} a_{34} \dots \\ x_4 &= 0, a_{41} a_{42} a_{43} a_{44} \dots \\ &\dots, \end{aligned}$$

gdzie $a_{ij} \in \{0, 1, \dots, 9\}$. Ponieważ chcemy mieć rozwinięcia nieskończone, więc w przypadku rozwinięcia skończonego zastępujemy ostatnią cyfrę znaczącą (czyli różną od zera) przez cyfrę o jeden mniejszą, a następującą po niej zera przez 9. W ten sposób liczba x_i ma postać $0, a_{i1} a_{i2} a_{i3} a_{i4} \dots$, gdzie nie wszystkie a_{ij} ($j = 1, 2, 3, \dots$) są od pewnego miejsca równe 0.

Rozważmy teraz nową liczbę $x = 0, b_1 b_2 b_3 b_4 \dots$, taką że $b_1 \neq a_{11}$, $b_2 \neq a_{22}$, $b_3 \neq a_{33}$, $b_4 \neq a_{44}, \dots$ oraz $b_i \neq 0$ i $b_i \neq 9$. Oczywiście liczba $x \in (0, 1)$ oraz $x \neq x_1$ (ponieważ $b_1 \neq a_{11}$), $x \neq x_2$ (ponieważ $b_2 \neq a_{22}$), $x \neq x_3$ (ponieważ $b_3 \neq a_{33}$) itd. W ten sposób otrzymaliśmy sprzeczność z założeniem, że przedział $(0, 1)$ jest przeliczalny, czyli że w ciągu $x_1, x_2, x_3, x_4, \dots$ są wszystkie jego elementy. Ostatecznie więc przedział $(0, 1)$ nie jest przeliczalny. Q.E.D.

W ten sposób pokazaliśmy, że w szczególności zbiór \mathbb{R} liczb rzeczywistych, ani żaden zbiór z nim równoliczny, nie jest przeliczalny, czyli jest nieprzeliczalny.

DEFINICJA 9.4.2. Zbiór X równoliczny ze zbiorem liczb rzeczywistych, czyli taki że $X \sim \mathbb{R}$, nazywamy zbiorem mocy kontinuum. Moc kontinuum oznaczamy gotycką literą \mathfrak{c} . Zatem $\overline{\mathbb{R}} = \mathfrak{c}$.

Przykładami zbiorów mocy kontinuum są w szczególności: prosta (którą można utożsamić ze zbiorem \mathbb{R} liczb rzeczywistych), półprosta (utożsamiana z przedziałem $(0, \infty)$), dowolny przedział otwarty lub domknięty, kwadrat z brzegiem lub bez brzegu, płaszczyzna (którą można utożsamić z iloczynem kartezjańskim $\mathbb{R} \times \mathbb{R}$) czy przestrzeń 3-wymiarowa (czyli $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$).

Można teraz postawić naturalne pytanie: czy istnieje zbiór $X \subseteq \mathbb{R}$, taki że $\aleph_0 < \overline{X} < \mathfrak{c}$, tzn. czy istnieją nieprzeliczalne zbiory liczb rzeczywistych o mocy mniejszej niż moc całego zbioru \mathbb{R} ? Odpowiedź na to pytanie może brzmieć oczywiście: TAK lub NIE. Odpowiedź negatywną, czyli stwierdzenie

każdy zbiór X liczb rzeczywistych jest albo przeliczalny, albo mocy kontinuum,

tzn. zdanie

$$\forall X \subseteq \mathbb{R} [\overline{X} = \aleph_0 \vee \overline{X} = \mathfrak{c}],$$

nazywamy hipotezą kontinuum i oznaczamy symbolem CH (od angielskiego *continuum hypothesis*).

Nad hipotezą kontinuum zastanawiał się już Cantor. Nie potrafił jej rozstrzygnąć. W pewnym momencie zaczął nawet z tego powodu wątpić w wartość naukową stworzonej przez siebie teorii mnogości.

Problem kontinuum został rozwiązany dopiero w połowie XX wieku, przy czym rozwiązanie było zaskakujące: nie dawało ani odpowiedzi pozytywnej, ani negatywnej. Pokazano mianowicie, że hipoteza kontinuum

jest zdaniem nierozstrzygalnym na gruncie aksjomatycznej teorii mnogości (czyli teorii, która precyzyjnie formułuje własności zbiorów, a przez to *implicite* definiuje pojęcie zbioru).

Innym pytaniem, które można postawić w kontekście badania zbiorów nieprzeliczalnych, jest pytanie o to, czy istnieją zbiory o mocy większej niż zbiory mocy kontinuum? Ogólnie możemy pytać, czy dla dowolnej danej liczby kardynalnej m istnieje liczba kardynalna n , taka że $m < n$? Przy tym relację mniejszości $<$ rozumiemy tu w sensie następującej definicji:

DEFINICJA 9.4.3. *Jeżeli m i n są liczbami kardynalnymi, to $m < n$ wtedy i tylko wtedy, gdy istnieją zbiory A i B , takie że $\overline{\overline{A}} = m$, $\overline{\overline{B}} = n$ oraz $A \not\subseteq B$ i $\neg(A \sim B)$.*

Odpowiedź na postawione pytanie daje następujące twierdzenie, pochodzące od Cantora:

TWIERDZENIE 9.4.4 (Cantor). *Dla dowolnego zbioru X zachodzi*

$$\overline{\overline{X}} < \overline{\overline{\mathcal{P}(X)}},$$

ozn. moc zbioru potęgowego jest większa od mocy danego zbioru.

Twierdzenie Cantora o zbiorze potęgowym pozwala na stwierdzenie istnienia całej nieskończonej hierarchii nieskończonych liczb kardynalnych. Istotnie, oznaczmy przez 2^m moc zbioru $\mathcal{P}(X)$ dla X takiego, że $\overline{\overline{X}} = m$ (notacja ta jest uogólnieniem faktu, że w przypadku zbiorów skończonych, jeśli moc zbioru X jest równa n , to moc zbioru potęgowego $\mathcal{P}(X)$ jest równa 2^n). Twierdzenie Cantora głosi więc, że

$$\forall m (m < 2^m).$$

W ten sposób, wychodząc od mocy zbioru liczb naturalnych, czyli od \aleph_0 , otrzymujemy całą nieskończoną hierarchię nieskończonych liczb kardynalnych

$$\aleph_0, 2^{\aleph_0}, 2^{2^{\aleph_0}}, \dots$$

Korzystając z pewnych własności liczb kardynalnych, można pokazać, że:

(i) Zbiór wszystkich ciągów nieskończonych o wyrazach rzeczywistych ma moc c .

(ii) Zbiór wszystkich funkcji ciągłych zmiennej rzeczywistej o wartościach rzeczywistych ma moc c .

(iii) Zbiór wszystkich funkcji zmiennej rzeczywistej o wartościach rzeczywistych ma moc 2^c .

* * *

Aby ułatwić Czytelnikowi zapamiętanie rozważań zawartych w poprzednich paragrafach tego rozdziału, przytoczymy następujący wierszyk⁴:

Opowieść z 1001 mocy

Moc jest to klasa równoważności
 Zbioru w relacji równoliczności.
 Dla zbiorów, co są w tej samej klasie
 Zawsze bijekcję utworzyć da się.
 Funkcja ta, która ma być bijekcją,
 Musi iniekcją być i suriekcją.
 Że jest iniekcją, to w innych słowach
 Znaczą, że jest różnowartościowa.
 Nazwa „suriekcja” oznacza zdanie,
 Że jest to „na” zbiór odwzorowanie.
 Zbiory bywają zwykle dzielone
 Na te skończone i nieskończone.
 Zwłaszcza te drugie nas zadziwiają,
 Bo całkiem inne własności mają.
 Mówimy, że zbiór jest przeliczalny
 Gdy ma moc zbioru liczb naturalnych.
 Te zbiory liczb są z nim równoliczne:
 Wymierne oraz algebraiczne.
 Tę moc przebadał Cantor dopiero
 I ją oznaczył przez \aleph_0 .
 Są jeszcze inne nieskończoności,
 Które niezwykle mają własności.
 No, bo na przykład, kto by powiedział,
 Że równej mocy jest każdy przedział?
 Lub czy to fakt jest dość oczywisty,
 Że tyleż jest też liczb rzeczywistych?

⁴ Wierszyk ten przytaczamy za miesięcznikiem „Delta” 9/92. Nie jest to poezja zbyt wysokich lotów, ale może pomóc w zapamiętaniu ważniejszych kwestii związanych z teorią mocy.

Punktów na prostej? A i do tego
Podzbiorów zbioru przeliczalnego?
Moc tę kontinuum nazywamy
Oraz literą „ c ” oznaczamy.
Gdy większe chcemy uzyskać moce,
Musimy liczbę 2 podnieść do c .
Tyle podzbiorów, co każdy przyzna
ma zbiór \mathbb{R}^2 – czyli płaszczyzna.
Gdy 2 do mocy tej podniesiemy –
Kolejną, większą moc dostaniemy.
Czynność tę można kontynuować
I dalsze moce tak konstruować.
Tak otrzymamy ciąg nieskończony
Z coraz to większych mocy tworzony.
Więc można podać do wiadomości:
Jest nieskończoność nieskończoności!

Zadania

1. Udowodnić, że jeśli zbiory A i B są skończone, to $A \sim B$ dokładnie wtedy, gdy A i B mają tę samą liczbę elementów.
2. Udowodnić, że jeśli $A_1 \sim B_1$ i $A_2 \sim B_2$, to $A_1 \times A_2 \sim B_1 \times B_2$.
3. Udowodnić, że jeśli zbiory A_1 i A_2 są rozłączne oraz zbiory B_1 i B_2 są rozłączne, oraz $A_1 \sim B_1$ i $A_2 \sim B_2$, to $A_1 \cup A_2 \sim B_1 \cup B_2$.
4. Udowodnić, że dowolny zbiór rozłącznych przedziałów prostej jest przeliczalny. Wynioskować stąd, że zbiór ekstremów funkcji ciągłej o wartościach rzeczywistych jest przeliczalny.
5. Udowodnić, że dowolny zbiór przedziałów prostej, mających końce wymierne, jest przeliczalny.
6. Udowodnić, że zbiór wszystkich skończonych podzbiorów zbioru liczb naturalnych jest nieskończony, lecz przeliczalny.
7. Pokazać, że jeśli A i B są zbiorami przeliczalnymi, to $A \cap B$, $A \cup B$, $A \setminus B$ i $A \times B$ są też przeliczalne.
8. Zdefiniować funkcje, wyznaczające równoliczność następujących zbiorów:
 - a) zbiór liczb parzystych i liczb nieparzystych,
 - b) zbiór liczb całkowitych dodatnich i zbiór liczb całkowitych,

- c) zbiór punktów półprostej otwartej i zbiór punktów prostej,
 - d) zbiór punktów okręgu o promieniu 1 i okręgu o promieniu 2 (funkcję uogólnić na dowolne dwa okręgi),
 - e) zbiór punktów sfery n -wymiarowej o promieniu 1 oraz sfery n -wymiarowej o promieniu 2 (funkcję uogólnić na dowolne dwie sfery n -wymiarowe),
 - f) zbiór punktów koła domkniętego o promieniu 1 i koła domkniętego o promieniu 2,
 - g) zbiór punktów domkniętej kuli n -wymiarowej o promieniu 1 i domkniętej kuli n -wymiarowej o promieniu 2.
9. Korzystając z tego, że odcinek i kwadrat są równoliczne, pokazać, że jeśli zbiór A jest mocy kontinuum, to zbiór $A \times A$ także ma moc kontinuum.
10. Pokazać, że zbiór punktów płaszczyzny ma moc kontinuum.
11. Pokazać, że jeśli rozłączne zbiory A, B mają moc kontinuum, to zbiór $A \cup B$ też ma moc kontinuum.
12. Pokazać, że suma przeliczalnej liczby rozłącznych zbiorów mocy kontinuum ma również moc kontinuum.
13. Korzystając z twierdzenia Cantora–Bernsteina i przechodniości relacji równoliczności, udowodnić równoliczność następujących zbiorów:
- a) odcinek domknięty i kwadrat z brzegami,
 - b) odcinek domknięty i kwadrat bez brzegów,
 - c) koło z brzegiem i odcinek z końcami,
 - d) koło bez brzegu i trójkąt,
 - e) prosta i prostokąt,
 - f) dwa dowolne wieloboki,
 - g) trójkąt i odcinek z końcami,
 - h) trójkąt i prosta.
14. Korzystając z twierdzenia Cantora–Bernsteina i przechodniości równoliczności oraz zadania 13, udowodnić równoliczność następujących zbiorów:
- a) kula domknięta trójwymiarowa i odcinek bez końców,
 - b) kula otwarta trójwymiarowa i sześcian domknięty,
 - c) kwadrat domknięty i sześcian bez brzegów (tj. bez ścian i krawędzi),
 - d) jednostkowa kula n -wymiarowa i dowolna kostka n -wymiarowa,
 - e) jednostkowa kula n -wymiarowa i dowolna kostka m -wymiarowa.

Dodatek

Uwagi historyczne

Logika jest jedną z najstarszych dyscyplin naukowych. Wyodrębnił ją z filozofii jeszcze Arystoteles (384–322 p.n.e.); może on być uznany za pierwszego logika. Rozważając mianowicie paradoksalne, a czasem zwyczajnie błędne argumentacje sofistów, wpadł na pomysł zebrania i skatalogowania niezawodnych schematów wnioskowania i w ten sposób dał początek pierwszemu systemowi logiki.

Nazwa „logika” nie jest nazwą jednoznaczną. Czasami logiką nazywa się tylko logikę formalną, a czasem do szeroko rozumianej logiki zalicza się ogólną teorię znaku, zwaną semiotyką, a także ogólną metodologię nauk, która zajmuje się maksymalnie skutecznymi sposobami poznawania świata (metodami badawczymi) i wytworami czynności poznawczych – teoriami naukowymi, w tym także teoriami matematycznymi.

Poniżej podamy uwagi dotyczące historii logiki, ograniczając się do historii logiki formalnej i metodologii nauk matematycznych.

Arystoteles skoncentrował się na badaniu związków pomiędzy zdaniem postaci: „każde S jest P ”, „żadne S nie jest P ”, „niektóre S są P ” i „niektóre S nie są P ”; efektem tych badań było sformułowanie szeregu praw logicznych, dotyczących związków pomiędzy takimi zdaniem. W ten sposób opisany został pierwszy system logiki, zwany logiką nazw; istotne jest to, że już Arystoteles używał zmiennych dla nazw. Dziś system ten można uznać za fragment rachunku predykatów.

Następcy Arystotelesa system ten rozwinęli i dopracowali; logika nazw, nazywana dialektyką weszła potem w skład siedmiu sztuk wyzwolonych (*artes liberales*), nauczanych na średniowiecznych uniwersytetach. Była ona uznawana za naukę podstawową, więc wchodziła obok gramatyki i retoryki w skład uniwersyteckiego kursu elementarnego – *trivium*. W kształcie opracowanym przez średniowiecznych logików, zwłaszcza Piotra Hiszpana

(1226–1277, lekarza i logika, późniejszego papieża Jana XXI), logika nazw była długo wykładana jako część filozofii i to w niezmiennym od średniowiecza kształcie. Taką logikę wykładano humanistom aż do połowy XX wieku¹.

Początki rachunku zdań także sięgają starożytności. Usystematyzowanie wcześniejszych fragmentarycznych odkryć i szereg nowych wyników w zakresie rachunku zdań zawdzięczamy szkole stoików. Pierwszym filozofem-stoikiem, zajmującym się logiką, był Chryzyp (ok. 280–205 p.n.e.); w szczególności jako pierwszy sformułował i zaakceptował zasadę dwuwartościowości. Stoicy jako pierwsi użyli terminu „logika”; logika była dla nich nauką o *logosie*, tak jak go wówczas rozumiano, to jest o rozumie i mowie.

Stoicy jako pierwsi też podjęli próbę budowy logiki zdań jako systemu. Zdawali sobie sprawę z odmienności logiki zdań i logiki nazw; logika zdań miała poprzedzać logikę nazw. Znali negację, implikację i alternatywę. To co odkryli, to szereg reguł wnioskowań niezawodnych w ramach rachunku zdań.

W średniowieczu badania nad rachunkiem zdań kontynuował William Ockham (ok. 1300–1349), największy logik średniowiecza, posługujący się wszystkimi podstawowymi spójnikami logicznymi i znający 26 praw logiki klasycznej. Logika jednak jako dyscyplina naukowa została zdominowana na dwadzieścia z górą wieków przez arystotelesowską logikę nazw.

Idea „mechanizacji wnioskowań”, prowadząca do idei systemu sformalizowanego i metody rozstrzygania o poprawności wnioskowań pojawiła się w XIII wieku. Sformułował ją kataloński poeta, uczonej i nawracający muzułmanów misjonarz katolicki Ramon Lull (Rajmundus Lullus, 1232–1316). Skonstruował on przyrząd mechaniczny, zwany „młynkiem Lullusa” – pierwszą „maszynę logiczną”. Za jej pomocą można było znaleźć niektóre prawa logiczne. Ideę sztucznego języka, złożonego z arbitralnych symboli, całkowicie oderwanego od mowy potocznej i służącego wszystkim naukom, a także ideę mechanizacji wnioskowań znajdujemy też u niemieckiego filozofa, matematyka oraz reprezentanta wielu innych nauk i sztuk Gottfrieda Wilhelma Leibniza (1646–1716).

Współczesna logika formalna zaczyna się od angielskiego logika i matematyka George’a Boole’a (1815–1864), który tworzy niezależną od arystotelesowskiej logikę nazw, zawierającą „dodawanie logiczne”, „mnożenie

¹ Do dziś zresztą podręczniki logiki dla humanistów zawierają wykład tradycyjnego rachunku nazw, choćby dla umożliwienia śledzenia rozważań tych uczonych i filozofów, którzy w swoim czasie używali takiej logiki w swych dziełach; z podręczników polskich por. w tym zakresie np. Z. Ziemiński, *Logika praktyczna*, Wydawnictwo Naukowe PWN, Warszawa 2001.

logiczne” i „odejmowanie logiczne”, pojmowane na wzór działań arytmetycznych. Podaje równości i nierówności dla takich nazw, analogiczne do równości i nierówności algebraicznych. Kierunek, zapoczątkowany przez Boole’a, zwany jest algebrą logiki; potraktowane ściśle algebraicznie rozważania Boole’a dały początek tzw. teorii algebr Boole’a; teoria ta ma dziś wiele zastosowań.

Badania nad podstawami matematyki, podjęte w XIX wieku, owocują z jednej strony powstaniem teorii mnogości (o czym niżej), a z drugiej – badaniami nad teorią rozumowań matematycznych. Efektem tych badań był pierwszy (implikacyjno-negacyjny) system aksjomatyczny rachunku zdań, aksjomatyzujący cały rachunek zdań, podany w roku 1879 przez niemieckiego logika Gottloba Fregego (1848–1925), zwanego filozofem filozofów. System ten przedstawiony był za pomocą bardzo skomplikowanej symboliki², toteż nie wpłynął wówczas na logikę w takim stopniu, w jakim na to zasługiwał.

Drugim systemem aksjomatycznym, obejmującym cały rachunek zdań, tym razem przedstawionym w czytelny sposób, był system angielskiego filozofa, logika, matematyka (i ekscentryka) Bertranda Russella (1872–1970), zaprezentowany w trzytomowym dziele *Principia Mathematica* (1910–1913); współautorem dzieła był filozof i matematyk Alfred North Whitehead. Opierając się na dorobku G. Fregego i włoskiego logika Giuseppe Peana, Russell dał pełny system logiki matematycznej, w tym pełen rachunek zdań, a także przedstawił pewną wersję rachunku predykatów.

Wiek XX zaczyna się w matematyce Międzynarodowym Kongresem Matematyków w Paryżu (w sierpniu 1900 roku). Na kongresie tym największy ówczesny matematyk David Hilbert (1862–1943) wygłosił wykład, w którym próbował nakreślić problematykę, którą jego zdaniem będzie żyć XX-wieczna matematyka. Sformułował w szczególności 23 problemy otwarte, zwane od tej pory problemami Hilberta, których rozwiązanie miało być wyzwaniem dla matematyki. Hilbert doceniał wartość rozważań nad podstawami matematyki, doskonale znał ówczesną logikę, a część swej energii twórczej poświęcił m.in. logice oraz filozofii matematyki. Nie powinno więc dziwić, że wśród 23 problemów matematycznych jako drugi na liście był problem niesprzeczności matematyki, a jako pierwszy problem hipotezy continuum (por. rozdział 9).

Badania nad problemem dowodu niesprzeczności matematyki i nad ugruntowaniem jej w ten sposób dały początek tzw. teorii dowodu oraz

² Por. R. Murawski, *Rozwój symboliki logicznej*, Wydawnictwo Naukowe UAM, Poznań 1988.

metamatematyce, które wpłynęły bardzo silnie na rozwój logiki oraz metodologii i podstaw matematyki.

Rewolucyjne znaczenie miały wyniki austriackiego matematyka i logika Kurta Gödla (1906–1978). Gödel udowodnił mianowicie dwa twierdzenia zwane dziś twierdzeniami Gödla o niezupełności. Pierwsze z nich mówi, że każda niesprzeczna teoria zawierająca arytmetykę liczb naturalnych jest istotnie niezupełna, tzn. w każdej takiej teorii istnieją zdania prawdziwe, lecz niedowodliwe, czyli nie dające się wywieść z przyjętego układu aksjomatów. Co więcej, cechy tej nie można usunąć poprzez dołączenie nowych aksjomatów, gdyż wtedy pojawią się nowe zdania o opisanej własności. Twierdzenie to wskazuje na pewną ograniczoność poznawczą metody aksjomatycznej. Jego konsekwencją jest m.in. to, że nie można zaksjomatyzować wszystkich prawd o liczbach naturalnych oraz to, że arytmetyka liczb naturalnych (i wiele innych teorii) jest nierozstrzygalna, tzn. nie istnieje mechaniczna metoda (algorytm) pozwalająca oddzielić twierdzenia arytmetyki od innych zdań. Drugie twierdzenie Gödla mówi, że w żadnej niesprzecznej teorii T zawierającej arytmetykę liczb naturalnych nie można udowodnić jej własnej niesprzeczności — zawsze trzeba użyć w takim dowodzie środków silniejszych niż te, które są dopuszczalne w teorii T . Zatem w konsekwencji nie istnieją w matematyce absolutne dowody niesprzeczności³.

Przedstawiając historię logiki, nie można nie wspomnieć o dorobku logików polskich. Historia logiki polskiej zaczyna się w XX wieku od razu liczącymi się w skali światowej wynikami Jana Łukasiewicza (1878–1956). Obok Łukasiewicza działali w okresie międzywojennym także: Alfred Tarski (od 1939 roku osiadły w USA, autor m.in. definicji prawdy w językach nauk dedukcyjnych oraz wielu innych wyników z logiki i matematyki), Stanisław Leśniewski (autor oryginalnego podejścia do podstaw matematyki), a także zmarli w czasie II wojny światowej Adolf Lindenbaum, Mordechaj Wajsberg, Mojżesz Presburger i Leon Chwistek⁴.

Oryginalnym wkładem logików polskich drugiej połowy XX wieku jest realizacja sformułowanego przez A. Tarskiego programu algebraizacji logiki, to jest zastosowania algebry do badań nad logiką, zwłaszcza nad mającymi coraz to szersze zastosowania logikami nieklasycznymi. Program ten był

³ Dokładne informacje na temat wyników Gödla i ich konsekwencji znaleźć można na przykład w książce R. Murawskiego, *Funkcje rekurencyjne i elementy metamatematyki. Problemy zupełności, rozstrzygalności, twierdzenia Gödla*, Wydawnictwo Naukowe UAM, Poznań 2000 (wyd. III).

⁴ Bliższe informacje o logikach polskich okresu międzywojennego można znaleźć w monografii J. Woleńskiego, *Filozoficzna Szkoła Lwowsko-Warszawska*, Państwowe Wydawnictwo Naukowe, Warszawa 1985.

realizowany m.in. przez Helenę Rasiową, Romana Sikorskiego, Stanisława Jaśkowskiego i jest do dziś kontynuowany przez ich uczniów.

Matematycy polscy wnieśli też bardzo znaczący wkład w rozwój teorii mnogości⁵. Pionierską rolę odegrał tu Wacław Sierpiński, którego *Zarys teorii mnogości*, wydany w roku 1912, był jednym z pierwszych podręczników z tej dziedziny na świecie. Powstała po I wojnie światowej Polska Szkoła Matematyczna skoncentrowała się wokół zagadnień związanych z teorią mnogości i jej zastosowaniami. Uzyskano w tym zakresie wiele znaczących wyników (wspomnijmy tu tylko prace Wacława Sierpińskiego, Kazimierza Kuratowskiego i Andrzeja Mostowskiego). Założone w Warszawie w roku 1920 czasopismo *Fundamenta Mathematicae* poświęcone było teorii mnogości i podstawom matematyki⁶. Wkrótce stało się ono centralnym w skali światowej organem skupiającym prace z teorii mnogości i działów z nią związanych.

⁵ Więcej na ten temat – por. R. Murawski i K. Świrydowicz, *Wstęp do teorii mnogości*, op. cit., rozdział 10 oraz paragrafy 3.1 i 7.4. Por. także R. Murawski, *Filozofia matematyki. Zarys dziejów*, Wydawnictwo Naukowe PWN, Warszawa 2001 (wyd. II) (rozdziały 11 i 14 oraz Dodatek I) oraz *Współczesna filozofia matematyki*, Wydawnictwo Naukowe PWN, Warszawa 2002.

⁶ Było to pierwsze w świecie czasopismo matematyczne poświęcone jednemu tylko działowi matematyki.

Literatura

Istnieje bogata literatura z zakresu logiki matematycznej i teorii mnogości. Podajemy tutaj jedynie mały jej wybór w języku polskim, uwzględniając przede wszystkim pozycje, które mogą być przydatne dla studentów pragnących rozszerzyć i pogłębić swą wiedzę po przestudiowaniu tego podręcznika.

- BATÓG T., *Podstawy logiki*, Wydawnictwo Naukowe UAM, Poznań 2003 (wydanie IV).
- BEN-ARI M., *Logika matematyczna w informatyce*, Wydawnictwa Naukowo-Techniczne, Warszawa 2005.
- BORKOWSKI L., *Wprowadzenie do logiki i teorii mnogości*, Towarzystwo Naukowe KUL, Lublin 1991.
- GUZICKI W., ZAKRZEWSKI P., *Wykłady ze wstępu do matematyki. Wprowadzenie do teorii mnogości*, Wydawnictwo Naukowe PWN, Warszawa 2005.
- GUZICKI W., ZAKRZEWSKI P., *Wstęp do matematyki. Zbiór zadań*, Wydawnictwo Naukowe PWN, Warszawa 2005.
- HUZAR Z., *Elementy logiki dla informatyków*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2002.
- KURATOWSKI K., *Wstęp do teorii mnogości i topologii*, Państwowe Wydawnictwo Naukowe, Warszawa 1980 (wydanie VIII).
- KURATOWSKI K., MOSTOWSKI A., *Teoria mnogości*, Nakładem Polskiego Towarzystwa Matematycznego z subwencji Ministerstwa Szkolnictwa Wyższego, Warszawa–Wrocław 1952 (wydanie I); Państwowe Wydawnictwo Naukowe, Warszawa 1966 (wydanie II); Państwowe Wydawnictwo Naukowe, Warszawa 1978 (wydanie III) [poszczególne wydania bardzo różnią się między sobą].
- ŁAWROW I.A., MAKSIMOWA Ł. L., *Zadania z teorii mnogości, logiki matematycznej i teorii algorytmów*, Wydawnictwo Naukowe PWN, Warszawa 2004.
- MAREK W., ONYSZKIEWICZ J., *Elementy logiki i teorii mnogości w zadaniach*, Wydawnictwo Naukowe PWN, Warszawa 2003 (wydanie XI).
- MURAWSKI R., ŚWIRYDOWICZ K., *Wstęp do teorii mnogości*, Wydawnictwo Naukowe UAM, Poznań 2005.
- MUSIELAK J., *Wstęp do matematyki*, Państwowe Wydawnictwo Naukowe, Warszawa 1970.

- RASIOVA H., *Wstęp do matematyki współczesnej*, Wydawnictwo Naukowe PWN, Warszawa 2003 (wydanie XIII).
- SIERPIŃSKI W., *Zarys teorii mnogości*, Kasa im. Mianowskiego, Warszawa 1928.
- SIERPIŃSKI W., *Wstęp do teorii mnogości i topologii*, Państwowe Zakłady Wydawnictw Szkolnych, Warszawa 1965 (wydanie II).
- SŁUPECKI J., BORKOWSKI L., *Elementy logiki i teorii mnogości*, Państwowe Wydawnictwo Naukowe, Warszawa 1984 (wydanie IV).
- SŁUPECKI J., HAŁKOWSKA K., PIRÓG-RZEPECKA K., *Logika i teoria mnogości*, Wydawnictwo Naukowe PWN, Warszawa 1994 (wydanie II).
- SŁUPECKI J., HAŁKOWSKA K., PIRÓG-RZEPECKA K., *Logika matematyczna*, Wydawnictwo Naukowe PWN, Warszawa 1999 (wydanie II).
- STANOSZ B., *Wprowadzenie do logiki formalnej*, Wydawnictwo Naukowe PWN, Warszawa 2001 (wydanie XIII).
- STANOSZ B., *Ćwiczenia z logiki*, Wydawnictwo Naukowe PWN, Warszawa 2002.
- TRZĘSICKI K., *Logika i teoria mnogości. Ujęcie systematyczno-historyczne*, Akademicka Oficyna Wydawnicza EXIT, Warszawa 2003.
- WOJCIECHOWSKA A., *Elementy logiki i teorii mnogości*, Państwowe Wydawnictwo Naukowe, Warszawa 1979.

Skorowidz symboli

$=$	równość, identyczność 73, 74
\neg	spójnik negacji 10, 11, 13, 38
\rightarrow	spójnik implikacji 10, 11, 13, 38
\leftrightarrow	spójnik równoważności 10, 11, 13, 38
\equiv	spójnik równoważności 10, 11, 13, 38
\vee	spójnik alternatywy 10, 11, 13, 38
\wedge	spójnik koniunkcji 10, 11, 13, 38
$\&$	spójnik koniunkcji 11
N	spójnik negacji 11, 24
C	spójnik implikacji 11, 24
K	spójnik koniunkcji 11, 24
A	spójnik alternatywy 11, 24
E	spójnik równoważności 11, 24
p_1, p_2, p_3, \dots	zmienne zdaniowe 13, 38
f_i^n	i -ta funkcja logiczna n -argumentowa 28
\neg	funkcja negacji 29
\rightarrow	funkcja implikacji 29
\leftrightarrow	funkcja równoważności 29
\equiv	funkcja równoważności 29
\vee	funkcja alternatywy 29
\wedge	funkcja koniunkcji 29
$ $	kreska Sheffera 35
\downarrow	binegacja 35
\vdash_S	S -konsekwencja syntaktyczna 40
\forall	kwantyfikator duży (uniwersalny, ogólny) 55
\exists	kwantyfikator mały (egzystencjalny, szczegółowy) 55
\bigwedge	kwantyfikator duży (uniwersalny, ogólny) 55
\bigvee	kwantyfikator mały (egzystencjalny, szczegółowy) 55
\prod	kwantyfikator duży (uniwersalny, ogólny) 55
(x)	kwantyfikator duży (uniwersalny, ogólny) 55
\sum	kwantyfikator mały (egzystencjalny, szczegółowy) 55

$(\exists x)$	kwantyfikator mały (egzystencjalny, szczegółowy) 55
P_k^n	k -ty predykat n -członowy (n -argumentowy) 55
F_i^m	i -ty symbol funkcyjny m -argumentowy 55
\in	relacja należenia 73
\mathbb{N}	zbiór liczb naturalnych 74
\mathbb{Z}	zbiór liczb całkowitych 74
\mathbb{Q}	zbiór liczb wymiernych 74
\mathbb{R}	zbiór liczb rzeczywistych 74
\mathbb{C}	zbiór liczb zespolonych 74
\subseteq	relacja inkluzji 76
\subsetneq	relacja inkluzji właściwej 77
\subset	relacja inkluzji właściwej 77
\emptyset	zbiór pusty 77
$\mathcal{P}(A)$	zbiór potęgowy 78
2^A	zbiór potęgowy 78
$A \cup B$	suma zbiorów 79
$A \cap B$	przekrój (iloczyn, część wspólna) zbiorów 79
$A \setminus B$	różnica zbiorów 79
$A - B$	różnica symetryczna zbiorów 79
$A \div B$	różnica symetryczna zbiorów 79
A'	dopełnienie zbioru 80
$\langle x, y \rangle$	para uporządkowana elementów x i y 93
$\langle x_1, \dots, x_n \rangle$	n -ka uporządkowana 94
$X \times Y$	produkt (iloczyn) kartezjański X i Y 94
$D(R)$	dziedzina lewostronna relacji R 95
$D^*(R)$	dziedzina prawostronna relacji R 95
$R \cup S$	suma relacji R i S 97
$R \cap S$	przekrój (iloczyn, część wspólna) relacji R i S 97
$R \setminus S$	różnica relacji R i S 97
$R - S$	różnica symetryczna relacji R i S 97
$R \div S$	różnica symetryczna relacji R i S 97
R'	dopełnienie relacji R 97
\check{R}	konwers relacji R 97
$R \circ S$	iloczyn względny (złożenie) relacji R i S 97
\sim	relacja równoważności 100
\approx	relacja równoważności 100
$[x]_R$	klasa abstrakcji elementu x względem relacji R 100
$[x]$	klasa abstrakcji elementu x 100
X/R	zbiór wszystkich klas abstrakcji relacji R w zbiorze X 101
$f : X \rightarrow Y$	funkcja ze zbioru X w zbiór Y 107
$\text{dom}(f)$	zbiór argumentów (dziedzina) funkcji f 107
$\text{rng}(f)$	zbiór wartości (przeciwdziedzina) funkcji f 107
Y^X	zbiór wszystkich funkcji z X w Y 107
f_A	obcięcie funkcji f do zbioru A 107

$f \upharpoonright A$	obcięcie funkcji f do zbioru A 107
$f : X \mapsto Y$	funkcja różnowartościowa (iniekcja) ze zbioru X w zbiór Y 107
$f : X \xrightarrow{1-1} Y$	funkcja różnowartościowa (iniekcja) ze zbioru X w zbiór Y 107
$f : X \twoheadrightarrow Y$	funkcja „na” (suriekcja) ze zbioru X w zbiór Y 108
$f : X \xrightarrow{na} Y$	funkcja „na” (suriekcja) ze zbioru X w zbiór Y 108
$f : X \xrightarrow{1-1} Y$	bijekcja ze zbioru X w zbiór Y 108
f^{-1}	funkcja odwrotna do funkcji f 108
$f \circ g$	złożenie (superpozycja) funkcji f i g 109
$\vec{f}(A)$	obraz zbioru A przez funkcję f 111
$f * (A)$	obraz zbioru A przez funkcję f 111
$f(A)$	obraz zbioru A przez funkcję f 111
$\vec{f}^{-1}(B)$	przeciwwobraz zbioru B przez funkcję f 112
$f^{-1}(B)$	przeciwwobraz zbioru B przez funkcję f 113
$f^{-1} * (B)$	przeciwwobraz zbioru B przez funkcję f 113
$\inf_{\leq}(A)$	infimum zbioru A względem relacji \leq 124
$\sup_{\leq}(A)$	supremum zbioru A względem relacji \leq 124
S	funkcja następnika 129
$card(A)$	moc (liczba kardynalna) zbioru A 137
\overline{A}	moc (liczba kardynalna) zbioru A 137
\aleph_0	moc zbioru przeliczalnego 140
c	moc kontinuum 142
CH	hipoteza kontinuum 142
2^m	moc zbioru potęgowego zbioru o mocy m 143
$m \leq n$	relacja mniejszości lub równości wśród liczb kardynalnych 143

Skorowidz terminów

- aksjomat ekstensjonalności 74
 - wyboru 131, 132
- aksjomaty algebry Boole'a 86, 87
 - arytmetyki Peana 129
- algebra Boole'a 86
 - dualna 88
 - dwójkowa 87
 - zbiorów 81
- alternatywa 10
 - elementarna 31
- alternatywna postać normalna 31
- argument funkcji 86

- bijekcja 87
- binegacja 35

- część wspólna zbiorów 50

- dedukcja 18
- definicja implikacji za pomocą alternatywy i negacji 21, 30
 - implikacji za pomocą koniunkcji i negacji 21
 - indukcyjna 14
- diagram przemienny 110
 - relacji 98
- dictum de omni 61
- dictum de singulo 61
- dobry porządek 127
- dopełnienie relacji 97
 - zbioru 80
- dowód formalny 39
- dualizacja 88

- dziedzina funkcji 107
 - relacji 95
 - *i*-ta 95
 - lewostronna 95
 - prawostronna (przeciwdziedzina) 95

- element 73
 - maksymalny 125
 - minimalny 126
 - najmniejszy 124
 - największy 124
 - zbioru 73
- epimorfizm 108

- formuła języka rachunku zdań 14, 38
- formuła zdaniowa języka rachunku predykatów 56
 - atomowa 56
- funkcja 106
 - identycznościowa 109
 - jednojednoznaczna 107
 - logiczna 27
 - liniowa 35
 - „na” 108
 - odwrotna 108
 - prawdziwościowa 27
 - przełączająca 27
 - różnowartościowa 107
 - zdaniowa 10

- hipoteza kontinuum 142

- iloczyn kartezjański 94

- zbiorów 79
- względny relacji 98
- implikacja 10
- indukcja 128
- infimum 124
- iniekcja 107
- inkluzja 76
- właściwa 77

- jednomian 34

- klasa abstrakcji 100
- równoważności 100
- klasyczna konsekwencja zdaniowa 39
- koniunkcja 10
- elementarna 31
- koniunkcyjna postać normalna 31
- konwers relacji 97
- krata 125
- kres dolny 124
- górny 124
- kreska Sheffera 35
- kwantyfikikator 55
- duży 55
- egzystencjalny 55
- ilościowy 64, 65
- mały 55
- ogólny 55
- o ograniczonym zakresie 62, 63
- szczegółowy 55
- uniwersalny 55

- lemat Kuratowskiego–Zorna 127, 131,
- liczba kardynalna 137

- łańcuch 122, 123

- macierz relacji 99
- metoda badania tautologiczności 15
- moc zbioru 1137
- modus ponendo ponens 20, 44
- ponendo tollens 21
- tollendo ponens 21
- tollendo tollens 20
- monomorfizm 107

- następnik implikacji 11
- nazwa generalna 54
- indywidualna 54
- negacja 10
- n -ka uporządkowana 94

- obcięcie funkcji 107
- obraz zbioru przez funkcję 111
- ograniczenie dolne 123
- górne 123

- para nieuporządkowana 93
- uporządkowana 93, 94
- pole relacji 95
- poprzednik implikacji 11
- porządek 117
- prawa addycji 21
- Claviusa 20, 47
- definiowania \rightarrow dla funkcji logicznych 30
- definiowania \leftrightarrow dla funkcji logicznych 30
- De Morgana dla zbiorów 82, 84
- – dla funkcji logicznych 30
- – dla kwantyfikatorów 61
- – – o ograniczonym zakresie 63
- – dla rachunku zdań 21, 48
- dla jedynki 30
- dla zera 30
- Dunsza Szkota (Dunsa Scotusa) 20, 44
- eksportacji 21, 44
- importacji 21, 44
- łączności alternatywy 21
- – koniunkcji 21
- komutacji 43
- pochłaniania 30, 85
- przemienności alternatywy 21, 30
- – koniunkcji 21
- rozdzielnosci alternatywy względem koniunkcji 21, 30
- – koniunkcji względem alternatywy 21, 30
- łączności przekroju 84, 86
- – sumy 84, 86

- podwójnej negacji 20
- przemienności przekroju 84, 86
- - sumy 84, 86
- przestawiania dużego i małego kwantyfikatora 62, 68
- przestawiania dużych kwantyfikatorów 62, 68
- przestawiania małych kwantyfikatorów 62
- rozdzielności dużego kwantyfikatora względem koniunkcji 61
- - - względem alternatywy 61
- - - względem implikacji 62
- - małego kwantyfikatora względem alternatywy 61
- - - względem koniunkcji 61
- - - względem implikacji 62
- - przekroju względem sumy 84, 86
- - sumy względem przekroju 84, 86
- sprzeczności 20, 49
- sylogizmu hipotetycznego 21
- - bezkoniunkcyjnego 42
- - dla równoważności 21
- symplifikacji 21
- tożsamości 20
- transpozycji 21, 30
- - złożonej 21
- wyłączonego środka 20, 50
- predykat 54, 55
- produkt kartezjański 94
- przeciwwobraz zbioru przez funkcję 112
- przedłużenie funkcji 107
- przekrój relacji 97
- zbiorów 79
- przestrzeń 80
- pseudopodstawienie 46

- rachunek predykatów 53
- - I rzędu 58
- - II rzędu 58
- - z identycznością 58
- rachunek zdań 9
- reguła dołączania dużego kwantyfikatora 67
- - małego kwantyfikatora 67
- - koniunkcji 45
- generalizacji 67
- komutacji 44
- logiczna wnioskowania 22
- Modus Ponens 40
- odrywania 22
- opuszczania dużego kwantyfikatora 67
- podstawiania dla rachunku predykatów 66
- sylogizmu 44
- transpozycji 47
- wtórna 42
- relacja 93, 95
- antysymetryczna 96
- asymetryczna 96
- binarna 95
- częściowo porządkująca 117
- diagonalna 96
- dobrego porządku 127
- konsekwencji 39
- liniowo porządkująca 118
- niezwrotna 96
- n -członowa 95
- odwrotna 97
- ostrego porządku 118
- przechodnia 96
- przeciwsymetryczna 96
- przeciwwrotna 96
- równoliczności 136
- równoważności 99
- silnego porządku 118
- spójna 96
- symetryczna 96
- ternarna 95
- totalna 96
- unarna 95
- zwrotna 96
- równoliczność zbiorów 136
- równoważność 10
- różnica relacji 97
- symetryczna relacji 97
- symetryczna zbiorów 79
- zbiorów 79

- schemat indukcji 129
 – wnioskowania 17
 – niezawodny 13
 – zdania 13
 singleton 74
 składanie funkcji 108
 spójnik zdaniowy 10
 – – ekstensjonalny 12
 – – intensjonalny 12
 suma relacji 97
 – zbiorów 79
 superpozycja funkcji 108
 supremum 124
 suriekcja 108
 syntaktyczna konsekwencja 39
 – S -konsekwencja 40
 symbol funkcyjny 54, 55
 symbolika beznawiasowa 24
 system teorii Zermela–Fraenkla ZF 73

 tautologia rachunku predykatów 57
 – – zdań 15
 term 54, 55
 twierdzenie Cantora–Bernsteina 138
 – Cantora o mocy zbioru potęgowego 143
 – o dedukcji 41
 – o pełności systemu S 51
 – o pełności rachunku predykatów 69
 – o reprezentacji relacji częściowo porządkujących 122
 – Stone’a o reprezentacji algebr Boole’a 90
 – systemu S 40
 – Zermela o dobrym uporządkowaniu 130

 uniwersum 80

 wartość funkcji 107
 – logiczna 9
 warunek dostateczny 23
 – konieczny 23
 – konieczny i dostateczny 23
 wielomian Żegalkina 34
 własność charakteru skończonego 131
 wnioskowanie niezawodne 16, 19
 – zawodne 16
 wynikanie 16
 – logiczne 18

 zasada abstrakcji 101
 – dualności 86, 88
 – ekstensjonalności 74
 – indukcji 128
 zasięg kwantyfikatora 56
 zbiory rozłączne 79
 zbiór 72, 73
 – częściowo uporządkowany 117
 – dobrze uporządkowany 127
 – liniowo uporządkowany 118
 – mocy kontinuum 142
 – nieprzeliczalny 141
 – nieskończony 137
 – potęgowy 78
 – przeliczalny 139
 – pusty 77
 – skończony 137
 – uniwersalny 51
 – w sensie dystrybutywnym 72
 – – – kolektywnym 72
 zbiory izomorficzne częściowo uporządkowane 122
 zdania sprzeczne 13
 zdanie 9
 – języka rachunku predykatów 57
 – proste 10
 – w sensie logicznym 9
 – złożone 10
 zmienna wolna 57
 – zdaniowa 14
 – związana 57
 zupełny układ funkcji logicznych 33

Skorowidz nazwisk

- Arystoteles (384–322 p.n.e.) 147
- Batóg Tadeusz (1934–) 38, 46, 58,
61, 66, 152
- Ben-Ari M. 152
- Bernstein Felix (1878–1956) 138
- Boole George (1815–1864) 86, 148
- Borkowski Ludwik (1914–1993) 152,
153
- Cantor Georg (1845–1918) 72, 135,
138, 142, 143, 144
- Cauchy Augustin-Louis (1789–1857)
64
- Chryzyp (ok. 280–205 p.n.e.) 148
- Church Alonzo (1903–1995) 58
- Chwistek Leon (1884–1944) 158
- Clavius Christofor (Schüssel)
(1537–1612) 20
- Dedekind Richard (1831–1916) 137
- De Morgan Augustus (1806–1971) 21
- Duns Szkot (Scotus) Jan (1266–1308)
20
- Euler Leonhard (1707–1783) 80
- Frege Gottlob (1848–1925) 149
- Gödel Kurt (1906–1978) 150
- Guzicki Wojciech 152
- Halkowska Katarzyna 153
- Hilbert David (1862–1943) 11, 149
- Huzar Z. 152
- Ifrah Georges (1947–) 136
- Jaśkowski Stanisław (1906–1965) 151
- Kuratowski Kazimierz (1896–1980) 93,
127, 131, 132, 151, 152
- Leibniz Gottfried Wilhelm (1646–1716)
84, 148
- Leśniewski Stanisław (1886–1939) 72,
150
- Lindenbaum Adolf (1904–1941(?)) 150
- Lullus Rajmundus (1232–1316) 148
- Ławrow I. A. 152
- Lukasiewicz Jan (1878–1956) 9, 11,
24, 150
- Maksimowa Ł. L 152
- Malinowski Grzegorz 9
- Marek Wiktor 152
- Mostowski Andrzej (1913–1975) 151,
152
- Murawski Roman (1949–) 12, 73, 101,
106, 112, 138, 149, 152
- Musielak Julian (1928–) 152
- Ockham William (ok. 1300–1349) 148
- Onyszkiewicz Janusz 152
- Peano Giuseppe (1858–1932) 11, 73,
129, 149

- Peirce Charles Sanders (1839–1914) 11
Piotr Hiszpan (1226–1277) 147
Piróg-Rzepecka Katarzyna 153
Post Emil L. (1897–1954) 9
Presburger Mojżesz (? –1943(?)) 150
- Rasiowa Helena (1914–1994) 119, 151, 153
Russell Bertrand (1872–1970) 11, 149
- Schröder Ernst (1841–1902) 11
Sierpiński Wacław (1882–1969) 151, 153
Sikorski Roman (1920–1983) 151
Słupecki Jerzy (1904–1987) 153
Stanosz B. 153
Stone Marshall Harvey (1903–1989) 90
Świrydowicz Kazimierz (1951–) 9, 73, 101, 106, 112, 138, 152
- Tarski Alfred (1901–1983) 68, 150
Teichmüller Oswald (1913–1943) 131, 132
Trzęsicki Kazimierz 153
Tukey John W. (1915–2000) 131, 132
- Venn John (1834–1923) 80
- Wajsberg Mordechaj (1902–?) 150
Whitehead Alfred North (1961–1947) 149
Wojciechowska Agnieszka 119, 153
Woleński Jan (1940–) 150
- Zakrzewski P. 152
Zermelo Ernst (1871–1953) 73, 130
Ziembiński Zygmunt (1920–1996) 16, 148
Zorn Max August (1906–) 127, 131, 132
Żyliński Eustachy (1880–1954) 36

Książka zawiera wykład podstawowych zagadnień logiki matematycznej i teorii mnogości przeznaczony dla zaocznych studentów informatyki. Część pierwsza poświęcona jest rachunkowi zdań i rachunkowi predykatów oraz funkcjom logicznym i aksjomatycznemu ujęciu logiki klasycznej. Część druga to wykład elementów tzw. naiwnej (tzn. nieaksjomatycznej) teorii mnogości (algebra zbiorów, relacje, funkcje, teoria mocy). Do książki dołączono dodatek zawierający uwagi historyczne o rozwoju logiki i teorii mnogości.

* * *

Roman Murawski – profesor zwyczajny na Wydziale Matematyki i Informatyki Uniwersytetu im. Adama Mickiewicza w Poznaniu, kierownik Zakładu Logiki Matematycznej; zajmuje się logiką matematyczną i podstawami matematyki oraz filozofią i historią matematyki i logiki.

Kazimierz Świrydowicz - profesor Uniwersytetu im. Adama Mickiewicza w Poznaniu, pracuje w Zakładzie Logiki Matematycznej na Wydziale Matematyki i Informatyki; zajmuje się logikami nieklasycznymi, algebrą uniwersalną i prawniczymi zastosowaniami logiki.

ISBN 978-83-232-3055-7

