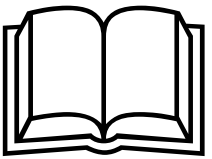
Олександр Лялецький

ОКРЕМІ РОЗДІЛИ ДИСКРЕТНОЇ МАТЕМАТИКИ

Матеріали лекцій з дисципліни "Дискретна математика"



Київ 2018

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра комп'ютерних наук

Олександр Лялецький

ОКРЕМІ РОЗДІЛИ ДИСКРЕТНОЇ МАТЕМАТИКИ

Матеріали лекцій з дисципліни "Дискретна математика"

Київ 2018

УДК 51

Укладач: **О.В. Лялецький** – кандидат фіз.- мат. наук, ст. наук. співроб., доц. кафедри комп'ютерних наук факультету інформаційних технологій Національного університету біоресурсів і природокористування України

Рецензенти: **М.М. Глазунов** – доктор фіз.-мат. наук, ст. наук. співроб., проф. кафедри електроніки Національного авіаційного університету України

В.Г. Скобелєв – доктор фіз.-мат. наук, проф., провідний наук. співроб. отдела теорії цифрових автоматів Института кібернетики ім. В.М. Глушкова НАНУ

О.М. Нещадим – кандидат фіз.-мат. наук, доц., доц. кафедри комп'ютерних наук Національного університету біоресурсів і природокористування України

О.В. Лялецький
Окремі розділи дискретної математики (Матеріали лекцій з дисципліни "Дискретна математика') / Лялецький Олександр Вадимович. – К.: Арталекс-Принт, 2018. – 134 арк.

У стислій формі даються спеціальні розділи дискретної математики, що відносяться до теорії чисел, теорії множин, основних понять теорії відповідностей, функцій і відношень та вступу в теорію булевих функцій, без знання яких стає вельми проблематичною можливість розуміння, вивчення та використання теоретичних і прикладних основ інформатики і математики, що вивчаються на бакалаврському і магістерському рівнях у вищих навчальних закладах природничо-наукового профилю за спеціальностями з інформаційних технологій.

Рекомендовано до друку Вченою радою факультету інформаційних технологій Національного університету біоресурсів і природокористування України (протокол № 4 від 22.10.2018)

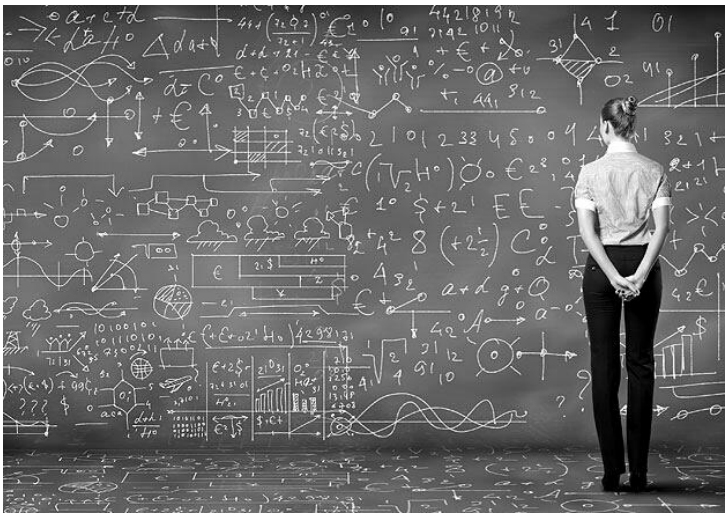
Передмова

У наш час існує багато різних підручників, посібників, книг і навіть монографій, присвячених дискретній математиці або окремим її розділам. Але, незважаючи на це, перед викладачами математичних дисциплін вищих навчальних закладів часто постає наступна проблема.

Виявляється, що значна кількість студентів перших курсів, які навчаються на на деяких природничонаукових факультетах, а також на таких факультетах, як економічний, соціологічний та інших, де математика потрібна для отримання знань з ряду предметів, не завжди достатньою мірою володіє матеріалом з курсу шкільної математики. Зокрема, це стосується знань про числа. Через це у студентів виникають ускладнення зі сприйняттям та засвоєнням нового матеріалу, що викладається в курсі математики в рамках навчальних програм університетів та інститутів, оскільки математичні дисципліни вимагають досить упорядкованих знань розділу про числа, до того ж у взаємозв'язку з іншими розділами математики. Тому доводиться перші лекції з дискретної математики починати зі стислих лекцій про числа. А відповідна інформація відсутня у підручниках і посібниках з дискретної математики для вищих навчальних закладів. У них також, як правило, відсутні поняття базових математичних структур (наприклад, груп і полів) без знання яких і їх взаємозв'язку в даний час неможливо опанувати цілим рядом предметів (наприклад, з інформаційної безпеки і захисту інформації). Це й стало першим поштовхом до появи даного підручника.

Друга причина його появи полягає в тому, що на викладання дискретної математики нерідко відводиться дуже незначна кількість годин і лекційний матеріал доводиться подавати у доволі стислій і лаконічній формі, часто жертвуючи повним і строгим доведенням. Тож цілком розумно завжди мати під рукою математичний матеріал, підготовлений в однаковій формі, що забезпечує мінімумом необхідних знань, в першу чергу про числа, множини, функції та відношення, тобто знань з тих тем, які представлені у підручники і які викликали його написання.

У кожній природничій науці міститься стільки істини,
скільки в ній є математики.
Іммануїл Кант



ЗМІСТ

Вступ

Матеріали являють собою стислий зміст лекцій по тим розділам дискретної математики, без доброго володіння якими стає досить проблематичною можливість вивчення і розуміння теоретичних основ ряду дисциплін, що викладаються у вищих навчальних закладах та вимагають знання базових математичних понять і результатів. Вони можуть послужити хорошим довідковим матеріалом як для студентів, які вивчають математичні предмети в вищих навчальних закладах, так і для викладачів, які бажають використовувати досвід, накопичений автором у процесі його викладацької діяльності і відбитий в посібнику.

Лекційні матеріали складаються з чотирьох розділів.

Перший розділ присвячений розгляду чисел, що вивчаються в шкільних курсах математики, а саме: натуральних, цілих, раціональних, дійсних і комплексних. Даються їх визначення і наводяться властивості. Також розглядаються питання представлення чисел в різних системах числення і способи переведення чисел з однієї системи числення в іншу. У ході викладання матеріалу вводяться поняття основних математичних структур (таких, як групи, поля і тому подібне), без знання яких і їх взаємозв'язку в даний час неможливо опанувати низкою сучасних як математичних дисциплін, так і дисциплін з інформаційних технологій (наприклад, пов'язаних із захистом інформації та інформаційною безпекою).

Оскільки сучасна математика базується на теоретико-множинних побудовах, у другому розділі викладається наївна теорія множин, знання якої є необхідною для вирішення більшої частини теоретичних і прикладних задач, що виникають в математиці та інформатиці. Вводяться основні операції над множинами, наводяться їх властивості. Даються визначення алгебри множин і булевої алгебри множин. Проводиться вивчення скінченних, зличенних і незліченних множин в обсязі, достатньому для оволодіння рядом предметів, що вивчаються в вищих навчальних закладах і є необхідними для пояснення особливостей категорій "скінченний"і "нескінченний ".

До базових теоретико-множинним понять математики відносяться поняття відповідності, функції і відношення, котрим при-

свячений третій розділ. Даються їх загальні визначення, які в подальшому конкретизуються до певного рівня. Серед бінарних відношень особлива увага приділяється відношенням еквівалентності і часткового порядку. Розглядаються частково і цілком впорядковані множини, що дає можливість сформулювати і довести принципи математичної і повної індукції, а також ввести поняття булевих алгебр і решіток і описати деякі їх властивості. Спираючись на частковий порядок, дається, без залучення поняття графа, визначення дерева і супутніх йому понять, що широко використовуються в програмуванні та різних розділах прикладної інформатики.

Початкові кроки по теорії булевих функцій представлені в четвертому розділі. Після перелічення всіх бінарних булевих функцій показується, що будь-яка булева функція будь-якої арності може бути представлена у вигляді ряду стандартних форм (що містять тільки символи булевих операций кон'юнкції, диз'юнкції і заперечення), до числа яких відносяться мінімальні діз'юнктивна і кон'юнктивна нормальні форми. Обговорюються питання приведення будь-якої булевої функції до описаних мінімальних форм. Вводиться поняття повної системи булевих функцій. Доводиться критерій Поста, що дозволяє визначити, є чи ні розглянута система булевих функцій функціонально повною.

Єдине, що знадобиться для розуміння викладеного у нотатках, так це знання деяких розділів зі шкільного курсу алгебри. Крім того, у нотатках з самого початку використовується, найчастіше у прихованій формі, математичне поняття мови. Тому дамо тут їй визначення.

Якщо A — скінченний або нескінченний набір символів (так званий *алфавіт*), то *словом в алфавіті* A називається будь-який ланцюжок символів із A (можливо, пустий, тобто такий, що не містить жодного символу). Якщо A^* є сукупність усіх слів в алфавіті A, то будь-яка частина A^* називається *мовою в алфавіті* A.

1 Про числа

Існує п'ять видів чисел, що активно використовуються в повсякденному житті і науково-технічній практиці: натуральні (**N**), цілі (**Z**), раціональні (**Q**), дійсні (**R**) і комплексні (**C**).

Для позначення арифметичних операцій над числами у нотатках використовуються такі символи: "+" — для додавання, "∗" — для множення, "–" — для віднімання і ":" — для ділення.

1.1 Натуральні числа

Вважається, що вміння рахувати і розрізняти кількість предметів є вроджені здібності людини. Тому у повсякденному житті натуральними називаються числа, які використовуються при лічбі предметів або позначення номера предмета в ряду однорідних предметів. Звідси натуральне число є поняттям, яке однаково сприймається усіма людьми і задовольняє такому (рекурентному) визначенню, що використовує очевидну операцію "збільшення натурального числа n на одиницю", яка позначається Sn й інтерпретується як операція додавання одиниці $+1$ до натурального числа n.

Дотримуючись підходу Дж. Пеана, дамо індуктивне визначення натуральних чисел та дій (операцій) над ними:

(I) символ 0 (інтепретуємий як звичайний нуль) є *натуральним числом*;

(II) якщо n – натуральне число, то Sn також є *натуральним числом.*

(III) інших натуральних чисел, крім зазначених у (I) і (II), немає.

Тобто 0, $S0$, $SS0$, ..., $S\ldots SS0, \ldots$ – уся сукупність натуральних чисел.

Два натуральних числа є *рівними* тоді і тільки тоді, коли вони мають один і той самий запис зі використанням знаку S.

Число n *менше за число* m ($n < m$) в тому і тільки тому випадку, коли кількість символів S, що беруть участь у записі n, менше (у звичайному сенсі) за кількість символів S, що беруть участь у записі m.

Крім цього, нам треба постулювати ряд властивостей натуральних чисел, що дасть можливість виконувати їх формальне

порівняння, а також задати принцип індукції:

(IV) $0 = 0$ і $0 \neq Sn$ для будь-якого натурального числа n.

(V) якщо $Sn = Sm$ тоді і тільки тоді, коли $n = m$.

(VI) *Принцип індукції.*

Якщо P позначає властивість, яку, можливо, мають одні натуральні числа і не мають інші, і якщо:

(VI.1) натуральне число 0 володіє властивістю P і

(VI.2) для будь-якого натурального числа n виходячи з того, що n володіє властивістю P випливає, що і натуральне число Sn має властивість P, то всі натуральні числа мають властивість P.

Тому буде природним розташувати натуральні числа у звичайному порядку їх зростання: $0 < S0 < SS0 < \ldots < SS \ldots S0 \ldots < \ldots$, де $<$ – знак так званного строгого порядку.

Ми пишемо $n \leqslant m$ тоді і тільки тоді, коли $n = m$ або $n < m$

Введемо звичайні десяткові позначення для натуральних чисел, позначивши $S0$ як 1, $SS0$ як 2, ... і т. д.

Множина всіх натуральних чисел з нулем позначатися $\mathbf{N}$, а без нуля – $\mathbf{N}_+$. $\mathbf{N}_+$ часто називається *натуральним рядом.*

Натуральні числа від 1 до n називаються *початковим відрізком натуральних чисел* довжини n і позначаються $[n]$. За визначенням вважається, що $[0]$ є пустим відрізком, тобто сукупністю, що нічого не містить (або, іншими словами, є так званою пустою множиною).

1.1.1 Операції над натуральними числами

Тепер можна індуктивне задати операції додавання $(+)$ і множення $(*)$ на множині натуральних чисел $\mathbf{N}$. (При додаванні і множенні натуральних чисел знову породжується натуральне число.)

Операція додавання:

(I) $n + 0 = n$,

(II) $n + (m + 1) = S(n + m)$, де $S(n + m)$ позначає результат додавання зліва S до рядка $S \ldots S0$ з "раніше обчисленим" числом $(n + m)$ символів S.

Операція множення:

(I) $n * 1 = n$,

(II) $n * (m + 1) = (n * m) + n$.

Вважаємо, що за визначенням $n * 0 = 0 * n = 0$.

Нехай u і q – натуральні числа. Тоді число $u + q$ називається *сумою* u і q, а u і q називаються *доданками*; число $u * q$ називається *добутком* u і q, а u і q називаються *співмножниками*.

Додавання і множення натуральних чисел можуть бути застосовані до будь-яких натуральних чисел, і для них виконуються такі закони, доведення яких неважко отримати з визначень додавання і множення:

1. $a + b = b + a$ (*переставний закон, комутативність додавання*).

2. $(a + b) + c = a + (b + c)$ (*сполучний закон, асоціативність додавання*).

3. $a * b = b * a$ (*переставний закон, комутативність множення*).

4. $(a * b) * c = a * (b * c)$ (*сполучний закон, асоціативність множення*).

5. $a * (b + c) = a * b + a * c$ (*розподільний закон, дистрибутивність множення відносно додавання*).

Звертаємо увагу на те, що операції додавання і множення натуральних чисел володіють такими двома властивостями: по-перше, вони можуть бути застосовані до будь парі чисел і, по-друге, результатом їх застосування знову є натуральні числа.

На математичному мові перше властивість будь операції, діючої на деякій множині M, тобто властивість, згідно з якою операцію, що розглядається, можна застосувати до будь-яких елементів з M, називається її *всюдивизначеностю* (або ще кажуть, що розглядаєма операція є *всюди визначеною на* M). Якщо ж при наявності всюдивизначеності в результаті застосування операції завжди породжується елемент з M (друга властивість), M називається *замкненою множиною (замкненою сукупністю) відносно операції* (що розглядається).

Відмітимо, що операція, що не є на M всюди визначеною називається *частково визначеною на* M.

Якщо знову звернутися до $\mathbf{N}$, то у цих термінах отримуємо, що $\mathbf{N}$ є замкненою множиною відносно (всюди визначених) операцій додавання і множення.

Можна ввести операції, обернені до додавання і множення:

віднімання "$-$" і ділення "$:$", що дають результат рішення відповідних рівнянь в натуральних числах у певних, але не в будь-яких випадках.

Якщо m і n — натуральні числа, причому, $m \geqslant n$, x — змінна і $n + x = m$ — рівняння відносно змінної x, то його рішення в натуральних числах завжди існує і воно єдино. І це рішення, записуване у вигляді $m - n$, називається *різницею* чисел m і n і є результатом *операції віднімання* "$-$" (що виконується за правилами звичайного віднімання натуральних чисел). При цьому, m називається *зменшуваним*, а n – *від'ємником*.

Зауважимо, що з визначення "$-$" слідує, що $n - n = 0$ для будь-якого натурального n.

Віднімання $m - n$ може бути виконане тільки тоді, коли $m \geqslant n$, тобто воно є *частково визначеною операцією* на $\mathbf{N}$. Наприклад, для чисел 2 і 5 отримуємо, що $5 - 2 = 3$, але відсутня (натуральна) різниця $2 - 5$.

Зауважимо, що знак "$-$" буде далі завжди служити для позначення операції віднімання чисел (не обов'язково тільки натуральних).

Ще відзначимо, що з заданого вище впорядкування натуральних чисел за зростанням і визначення операції віднімання слідує, що для будь-яких натуральних чисел m і n, $m \leqslant n$ тоді і тільки тоді, коли $n - m \geqslant 0$.

Якщо m і n — натуральні числа, x — змінна і $n * x = m$ — рівняння відносно x, то рішення цього рівняння в натуральних числах, якщо воно існує, позначається $m : n$ і називається *часткою* чисел m і n, отриманою у результаті виконання *операції ділення* "$:$". При цьому, m називається *кратним* числа n, а n – *дільником* числа m.

Як і в випадку віднімання, операція (натурального) ділення є *частково визначеною*. Наприклад, для чисел 12 і 4 отримуємо, що $12 : 4 = 3$, але не існує (натуральної) частки від ділення 4 на 12.

Сказане вище показує, що $\mathbf{N}$ *не є замкненою множиною відносно операцій віднімання і ділення*.

Введемо ще поняття (натурального) степеня натурального числа.

Нехай m і n — натуральні числа, причому, $n \geqslant 2$. Тоді до-

буток числа m саме на себе n разів називається *n-ою степіню натурального числа m* і позначається m^n. При цьому m називається *основою степені*, а n — *показником степені*.

Вважається, що за визначенням $m^0 = 1$ і $m^1 = m$.

Легко доводиться (методом математичної індукції), що $m^n * m^k = m^{(n+k)}$ і $(m^n)^k = m^{(n*k)}$ для будь-яких натуральних m, n і k. Звідси, виходячи з визначення операції ділення, слідує, що у випадку, коли $n \geqslant k$, можна виконати (натуральне) ділення m^n на m^k і, при цьому $m^n : m^k = m^{(n-k)}$. Якщо ж $n < k$, то (натуральна) частка $m^n : m^k$ не існує.

Операції додавання, віднімання, множення і ділення називаються *арифметичними*.

Вираз (тобто послідовність деяких символів) називається *числовим*, якщо він складений із знаків арифметичних дій, включаючи піднесення до степеня, змінних (ідентифікаторів) і чисел. Якщо в числовому виразі виконати всі зазначені дії для конкретних значень усіх його змінних, то вийде число, яке називається *значенням* даного виразу.

Пріоритет арифметичних операцій у числовому виразі такий: спочатку виконуються дії в дужках; усередині дужок спочатку виконують піднесення до степеня, множення і ділення, після чого додавання і віднімання.

1.1.2 Ділення натуральних чисел із залишком

Кажуть, що натуральне число n *ділиться на натуральне число m із залишком r* ($r < m$) тоді і тільки тоді, коли для деякого натурального числа k число n можна представити у вигляді $m * k + r$ (тобто $n = m*k+r$). При цьому k називається (*неповною*) *часткою*.

Якщо у визначенні ділення із залишком $r = 0$, то говорять, що n *ділиться на m без залишку* і m є *дільником* n (пор. з відповідними визначеннями вище).

Для 0 отримуємо, що він завжди ділиться без залишку на будь-яке інше число, але ніяке ділення на 0, навіть із залишком, неможливе, оскільки у формулі $m * k + r$ число r повинно бути строго менше 0.

Твердження 1.1. Для будь-яких натуральних чисел n і

m ($m \neq 0$) завжди можна виконати операцію ділення n на m із залишком і одержувані при цьому неповна частка і залишок визначаються єдиним чином.

Простими і цікавими наслідками цієї теореми є факти про подання натуральних чисел у різних формах. Наприклад, будь-яке натуральне число має один із таких видів: $2*n$ або $2*n+1$ (наслідок того, що при діленні будь-якого натурального числа на 2 у залишку може залишатися тільки 0 або 1); $3*n, 3*n+1$ або $3*n+2$ (наслідок того, що при діленні будь-якого натурального числа на 3 у залишку може залишатися тільки $0, 1$ або 2) і т. д., де $n = 0, 1, 2, \ldots$

1.1.3 Деяка класифікація натуральних чисел

Будь-яке натуральне число, відмінне від 0, завжди ділиться без залишку на 1 і на себе.

Натуральне число n (n відмінне від 0 и 1) називається *простим*, якщо n має тільки два різних дільника, тобто коли n відмінно 1 і ділиться без залишку тільки на 1 і на себе. В інших випадках n називається *складеним* натуральним числом.

Числа 0 і 1 не є, за означенням, ані простими, ані складеними.

Для того, щоб довести, що дане натуральне число n просте, досить встановити, що воно не ділиться ні на одне з чисел від 2 до цілої частини від кореня квадратного з n включно. Інакше n – складене число.

Число називається *парним*, якщо воно ділиться на 2 без залишку. Інакше це числа називається *непарним*. Так, 1 є непарним числом, а 0 – парним.

Будь-яке непарне число має вигляд $2 * m + 1$, парне – $2 * m$ (m – деяке натуральне число). Це випливає з того, що ділення із залишком на 2 (та й на будь-яке інше натуральне число) завжди можна виконати, і тільки єдиним чином (див. вище).

Припустімо, що ми хочемо знайти всі прості числа від 2 до n. Давньогрецький математик Ератосфен запропонував такий метод, який нині носить його ім'я (*метод Ератосфена*).

Випишемо в рядок усі числа від 2 до n і викреслимо кожне друге число з наступних за числом 2 — всі вони складені, оскільки

кратні числу 2. Перше з решти невикреслених чисел — 3 є простим. Викреслимо кожне третє число з наступних за числом 3; наступне з невикреслених чисел — 5 також буде простим. За тим самим принципом викреслимо кожне п'яте число з наступних за числом 5 і взагалі кожне k-те з наступних за числом k. Усі числа, що залишилися невикресленими, будуть простими.

Твердження 1.2. Простих чисел нескінченно багато.

Доведення. Припустимо противне, тобто що їх скінченна кількість і нехай $u_1, \ldots, u_k$ — всі прості числа. Розглянемо число $u_1 * \ldots * u_k + 1$. Це число відмінно від будь-якого з чисел із $u_1, \ldots, u_k$ і воно, внаслідок припущення, повинно бути складеним, тобто ділитися без залишку хоча б на одне з чисел $u_1, \ldots, u_k$. Але, через вибір цього числа, при його діленні на будь-яке з чисел $u_1, \ldots, u_k$ завжди виходить залишок, рівний 1. Тобто серед $u_1, \ldots, u_k$ немає числа, на яке воно ділилося б без залишку. Отримали протиріччя з припущенням. *Кінець доведення.*

Прості числа відіграють важливу роль у багатьох математичних побудовах. Тут ми відзначимо тільки один із основних фактів щодо них, який має назву основної теореми арифметики, що може бути використана, наприклад, для обгрунтування певних властивостей операції множення раціональних чисел.

Твердження 1.3 (основна теорема арифметики). Будь-яке натуральне число n може бути єдиним чином подано у вигляді виразу $p_1 * p_2 * \ldots * p_r$, де $p_1, p_2, \ldots, p_r$ — прості числа і $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_r$.

1.1.4 Спільний дільник

Спільним дільником кількох натуральних чисел називається натуральне число, що ділить без залишку кожне з них. Серед усіх дільників завжди є найбільший. Такий дільник називається *найбільшим спільним дільником* і позначається НСД. Так, наприклад, числа $16, 24, 32$ мають найбільший спільний дільник — число 8. Цей факт коротко записується так: НСД $(16, 24, 32) = 8$. Якщо дані числа невеликі, то найбільший спільний дільник можна легко вгадати. Якщо ж дано великі числа, то НСД можна знайти розкладанням чисел на прості множники і виписуванням тих множників, які входять в усі дані числа. Після чого потрібно провести їх множення.

Отриманий результат і буде НСД.

Якщо НСД(a, b) двох натуральних чисел дорівнює 1, то a та b називають взаємно простими. Ця властивість не залежить від того, чи прості числа a та b. Наприклад, ні 6, ні 35 не є простими, оскільки їх можна розкласти на добутки $6 = 2 * 3$ та $35 = 5 * 7$. Однак, 6 та 35 взаємно прості. Жодне натуральне число, окрім 1, не ділить водночас 6 та 35, оскільки у них нема спільних дільників.

Нехай $g =$ НСД(a, b). Оскільки a та b є добутками g, їх можна записати як $a = m * g$ та $b = n * g$, і не існує числа більшого за g з такою ж властивістю. Натуральні числа m та n мають бути взаємно простими, оскільки інакше інший спільний дільник може бути виділений з m та n, що веде до збільшення g. Таким чином, будь-яке число, що ділить a та b, повинне ділити і g. Маємо, що найбільший спільний дільник g чисел a та b *може бути визначений* як спільний дільник, який можна поділити іншим спільним дільником.

Для обчислення найбільшого спільного дільника, як правило, використовується так званий алгоритм Евкліда (або евклідів алгоритм), названий на честь грецького математика Евкліда.

Алгоритм Евкліда має багато застосувань на практиці та в теорії. З його допомогою можна згенерувати практично всі найважливіші музичні ритми різних культур у всьому світі. Алгоритм Евкліда відіграє ключову роль в алгоритмі RSA, поширеному методі криптографії з відкритим ключем. Його також використовують для пошуку розв'язків діофантових рівнянь, наприклад, чисел, що задовольняють кільком умовам (див. так звану "Китайську теорему про залишки"), або пошуку зворотніх чисел в скінченному полі. Алгоритм Евкліда також застосовують для побудови ланцюгових дробів у методі Штурма для пошуку дійсних коренів полінома та в сучасних методах факторизації цілих чисел. Зрештою, він виступає простим інструментом для доведення теорем в теорії чисел, таких, як теорема Лагранжа про чотири квадрата та основної теореми арифметики.

Алгоритм Евкліда ітеративний. Пошук НСД відбувається в декілька кроків.

Для того, щоб знайти НСД(a, b), де a і b — натуральні числа та $a \geqslant b$, на 0-му кроці знаходять залишок r_0 від ділення a на

b. На 1-му кроці знаходять залишок r_1 від ділення b на r_0. На 2-му кроці знаходять залишок r_2 від ділення r_0 на r_1. І так далі. Оскільки залишки зменшуються на кожному кроці, але не можуть бути від'ємними, цю операцію виконують доти, поки на деякому n-му кроці не отримують залишок 0. Найбільшим спільним дільником є остання не нульовой залишок r_{n-1}. Кількість кроків в алгоритмі скінченна, оскільки існує лише скінченна кількість цілих чисел між початковим залишком r_0 та нулем.

Більш формально. Нехай a і b — натуральні числа та $a \geqslant b$. Тоді алгоритм Евкліда може бути заданий у такому вигляді.

$a = q_0 * b + r_0$, де $r_0 < b$ (0-ий крок);
$b = q_1 * r_0 + r_1$, де $r_1 < r_0$ (1-ий крок);
$r_0 = q_2 * r_1 + r_2$, де $r_2 < r_1$ (2-ий крок);
...
$r_{n-3} = q_{n-1} * r_{n-2} + r_{n-1}$, де $r_{n-1} < r_{n-2}$ ($(n-1)$-ий крок);
$r_{n-2} = q_n * r_{n-1} + 0$ (n-ий крок).

Правильність алгоритму Евкліда можна довести в два етапи. Спочатку доводиться, що r_{n-1} дійсно є дільником a та b, а потім — що це є найбільший спільний дільник.

1.1.5 Спільне кратне

Подвійним, в деякому сенсі, поняттям до спільного дільника є поняття спільного кратного.

Спільним кратним кількох натуральних чисел називається натуральне число, що ділиться без залишку на кожне з цих чисел. Наприклад, числа $14, 18, 7$ мають спільне кратне число 252, проте число 126 теж є спільним кратним цих чисел. Серед всіх спільних кратних завжди є найменше, яке називається *найменшим спільним кратним* (позначається НСК). У нашому прикладі найменшим спільним кратним перерахованих чисел буде число 126. Коротко цей факт записується так: НСК $(14, 18, 7) = 126$.

Якщо числа невеликі, то найменше спільне кратне можна легко вгадати. Якщо ж дано великі числа, то НСК можна знайти розкладанням чисел на прості множники і виписуванням тих множників, які входять хоча б в одне з даних чисел. Після цього кожен такий множник потрібно взяти з найбільшим показником, з

яким він входить в усі дані числа, а потім слід провести множення множників з найбільшими показниками.

Ми залишаємо осторонь подальше вивчення теорії (натуральних) чисел, зазначаючи насамкінець, що між НСК та НСД існує такий зв'язок:

$a * b =$ НСК $(a, b) *$ НСД (a, b),

який узагальнюється у разі будь-якої скінченної сукупності натуральних чисел.

1.2 Цілі числа та операції над ними

Спроба домогтися того, щоб операція віднімання була визначена для будь-яких натуральних чисел, призводить до появи так званих від'ємних чисел, які можуть бути введені в такий спосіб.

Натуральне число називається *додатним цілим числом.*

Будемо вважати, що для будь-якого натурального числа n існує єдине *від'ємне ціле число*, що позначається $(\text{-}n)$, для якого має місце: $n+(\text{-}n) = (\text{-}n)+n = 0$ і $0+(\text{-}n) = (\text{-}n) + 0 = (\text{-}n)$. (Тут префіксний знак "-" служить для позначення так званого *унарного мінуса.*)

При цьому дозволимо приписувати унарний мінус "-" і до від'ємних цілих чисел, вважаючи, що $(\text{-}(\text{-}n)) = n$.

Сукупність усіх додатних та від'ємних цілих чисел $\ldots$, -2, $\text{-}1, 0, 1, 2, \ldots$ позначається $\mathbf{Z}$.

Вважається, що всі цілі числа строго впорядковані за зростанням наступним природним чином: $\ldots < \text{-}2 < \text{-}1 < 0 < 1 < 2 < \ldots$.

Для цілих чисел m и n мы пишемо $n \leqslant m$ та кажемо, що "n менше або рівно m", тоді и тільки тоді, коли $n = m$ або $n < m$.

Якщо z — ціле число, то $(\text{-}z)$ називається *числом, протилежним до* z.

Операцію додавання "+", яка визначена для натуральних чисел, поширюється на множину цілих чисел наступним чином (в припущенні, що вона, за визначенням, є комутативною та асоціативною).

Нехай n і m — невід'ємні цілі числа і $n \leqslant m$. Тоді операція + для додатних і від'ємних цілих чисел визначається у відповідно-

сті з наступними правилами, що охоплюють всі випадки додавання цілих чисел:

(1) $n + m$ виконується у відповідності з наведеним раніше індуктивним визначенням операції додавання натуральних чисел;

(2) $(\text{-}n) + (\text{-}m) = (\text{-}(n + m))$;

(3) $(\text{-}n) + m = m + (\text{-}n) = m - n$ (де '$-$"є знак, введений для позначення віднімання натуральних чисел і, значить, $m+(\text{-}m) = 0$);

(4) $n + (\text{-}m) = (\text{-}m) + n = (\text{-}(m - n))$,

де "$-$" є операцією віднімання натуральних чисел, яка в (3) і (4) може бути виконана завдяки тому, що $n \leqslant m$.

Якщо звернутися до визначення числа $(\text{-}n)$, то можна сказати, що воно було введено для того, щоб дозволити йому бути (єдиним) коренем лінійного рівняння $n + x = 0$ у припущенні, що це рівняння має завжди мати рішення відносно змінної x для будь-якого натурального n.

Розглянемо рівняння $n + x = m$, де n і m — цілі числа. Для нього маємо $n + (\text{-}n) + x = m + (\text{-}n)$, тобто $x = m + (\text{-}n)$ є (єдиним) рішенням розглянутого рівняння, і це рішення називається *різницею цілих чисел* n і m, яка позначається $m - n$, де m називається *зменшуваним*, а n — *від'ємником* числом.

Таке визначення різниці призводить до того, що *операція віднімання* '$-$", введена вище для натуральних чисел, *поширюється* на випадок *будь-яких цілих чисел* n і m згідно з формулою $m-n = m+(\text{-}n)$. При цьому повинні виконуватися наступні *правила внесення знака віднімання всередину дужок*:

$(\text{-}(m + n)) = (\text{-}(n + m)) = (\text{-}m - n = (\text{-}n) - m$,

$(\text{-}(m - n)) = (\text{-}m) + n$.

Тобто ми отримуємо всі добре відомі з шкільного курсу математики правила внесення знака віднімання всередину дужок. А якщо ще врахувати, що $(\text{-}(\text{-}n)) = n$, то без виникнення будь-якої двозначності в усіх вже наведених формулах і будь-яких інших, які можуть з'явитися, ми можемо унарний мінус "-" замінити знаком "–", використовуваним у визначенні операції віднімання цілих чисел, тобто прийти до звичайного запису правил внесення знака "мінус" усередину дужок.

Отже маємо, що сукупність цілих чисел $\mathbf{Z}$ *замкнена відносно операцій додавання* та *віднімання*.

Як і у випадку натуральних чисел, є наступний зв'язок заданого впорядкування цілих чисел з операцією віднімання: для будь-яких цілих чисел p і q, $p \leqslant q$ тоді і тільки тоді, коли $q - p \geqslant 0$.

Що ж стосується поширення введеної вище операції множення натуральних чисел "$*$" на множину цілих чисел, то її можна задати наступним чином через натуральні числа m і n:

(1) $n*m$ обчислюється згідно з наведеним вище індуктивним визначенням операції $*$ для натуральних чисел;

(2) $(\text{-}n) * (\text{-}m) = (n * m)$;

(3) $(\text{-}n) * m = m * (\text{-}n) = (\text{-}(m * n))$.

Звідси неважко виводяться комутативність та асоціативність множення цілих чисел, а також дистрибутивність множення відносно додавання.

Відзначимо, що для будь-якого цілого числа z мають місце такі рівності: $0 * z = z * 0 = 0$ та $1 * z = z * 1 = z$.

Ми маємо, що множення цілих чисел є *всюди певною операцією* і що $\mathbf{Z}$ є *замкненою множиною відносно множення.*

Але, як і у випадку натуральних чисел, не можна ввести операцію ділення цілих чисел без залишку, яка завжди давала цілочисельний результат, оскільки легко підібрати цілі u і q (наприклад, 2 і 3), такі, що рівняння $u = q * z$ не має рішення відносно змінної z в цілих числах.

Це означає, що сукупність цілих чисел *не замкнута* відносно операції ділення, що приводить до задачі розширення поняття цілого числа таким чином, щоб такі рівняння вирішувалися при будь-яких цілих u і q ($q \neq 0$). (Цьому присвячений наступний розділ.)

Що ж стосується ділення із залишком, то ця операція, усюди певна для натуральних чисел, легко переноситься на цілі числа зі збереженням усіх властивостей.

Модулем цілого числа z, який позначається $|z|$, є z, коли z є невід'ємне число, і протилежне йому (додатне) число $\text{-}z$, коли z негативно.

Ціле число z *ділиться із залишком на ціле число* q ($q \neq 0$) тоді і тільки тоді, коли для деяких цілих чисел u і r, число z можна представити у вигляді $q * u + r$ і для r має місце: $0 \leqslant r < |q|$. При цьому u називається *неповною часткою*, q — *дільником* z, а r — *залишком від ділення* z *на* q.

Ділення із залишком завжди *здійснимо* і *однозначно*, тобто при виконанні ділення із залишком цілого числа z на ціле число q ($q \neq 0$) неповна частка u і залишок r завжди існують і єдині.

Звертаємо увагу на деякі особливості ділення із залишком цілих чисел, коли хоча б одне з них — від'ємне число.

Так, наприклад, при виконанні ділення із залишком цілого числа -5 на ціле число 2 отримуємо неповну частку, рівну -3, і залишок, що дорівнює 1 (-5 = 2∗(-3)+1); при діленні із залишком числа -5 на число -2 отримуємо частку, рівну 3, і залишок, що дорівнює 1 (-5 = (-2) ∗ 3 + 1); при діленні 5 на -2 отримуємо неповну частку, що дорівнює -2, і залишок, що дорівнює 1 ($5 = (\text{-}2) * (\text{-}2) + 1$) (в той же час, при діленні 5 на 2 отримуємо неповну частку, що дорівнює 2, і залишок, що дорівнює 1 ($5 = 2 * 2 + 1$)).

Як і випадку натуральних чисел, *піднесенням до n-го степеня цілого числа z* (n — натуральне число і $n \geqslant 2$) називається n-кратне множення цілого числа z само на себе, результат якого позначається z^n та називається *степінь цілого числа z*. При цьому z називається *основою степені*, а n — *показником степені*. За визначенням вважаємо, що $z^0 = 1$ і $z^1 = z$.

Очевидно, що $z^n * z^k = z^{(n+k)}$ і $(z^n)^k = z^{(n*k)}$ для будь-якого цілого z і натуральних n і k. Звідси, виходячи з визначення операції ділення, слідкує, що в разі, коли $n \geqslant k$, можна виконати (цілочисельне) ділення без залишку z^n на z^k і, при цьому, $z^n : m^k = z^{(n-k)}$. Якщо ж $n < k$, то виконати ділення без залишку z^n на z^k неможливо.

1.3 Раціональні числа та операції над ними

Раціональним числом називається вираз виду m/n, де $m \in \mathbf{Z}$ і $n \in \mathbf{N}_+$ (тобто $n \neq 0$). При цьому m називається його *чисельником*, а n — *знаменником*.

Це визначення відображає звичайне поняття дробового числа, при використанні якого такі дроби, як, наприклад, 1/2 і 5/10 співпадають. Тому ми повинні відобразити цей факт у вигляді відповідного рішення.

Якщо деяке раціональне число отримується із заданого раціонального числа за допомогою поділу його чисельника і знамен-

ника на їх певний спільний множник (або, як зазвичай кажуть, за допомогою *скорочення дробу на спільний множник*), то такі раціональні числа, і тільки вони, називаються *рівними*.

Або, що еквівалентно, два раціональних числа m/n і p/q ($n \neq 0$, $q \neq 0$) є *рівними* тоді і тільки тоді, коли $m * q = n * p$.

Якщо перед m ($m \neq 0$) у визначенні раціонального числа стоїть унарний мінус "-", то таке число називається *від'ємним*; інакше воно називається *додатним* і у цьому випадку замість m іноді пишуть $+m$ для того, щоб підкреслити, що m — позитивне число.

Множина усіх раціональних чисел позначається $\mathbf{Q}$. Вона *впорядковується за зростанням* через порядок, заданий на множині цілих чисел $\mathbf{Z}$, наступним чином: для будь-яких раціональних чисел m/n і p/g, $m/n \leqslant p/g$ тоді і тільки тоді, коли $m * q \leqslant p * n$ (очевидно, що $m * q$ і $p * n$ являють собою цілі числа).

З цього визначення впорядкування випливає, що порівнянними є будь-які раціональні числа, і що воно перебуває в повній відповідності з впорядкуванням цілих (і натуральних) чисел, наведеному у розділі про цілих числах.

Операції додавання і множення раціональних чисел задаються за допомогою вже введених операцій додавання і множення цілих чисел наступним чином.

Випадок, коли $n = 1$, розглядається як інша запис вже введених цілих чисел $\mathbf{Z}$. Якщо ж при цьому $m \in \mathbf{N}$, то отримуємо і інше подання всіх натуральних чисел у вигляді раціональних чисел.

Операції додавання і множення над раціональними числами задаються за допомогою вже введених операцій додавання і множення цілих чисел таким чином.

Нехай m/n і u/q — два раціональних числа.

Операція додавання: $m/n + u/q = (m * q + n * u)/(n * q)$.

Операція множення: $m/n * u/q = (m * u)/(n * q)$.

В операції додавання m/n і u/q називаються *доданками*, а $m/n + u/q$ — їх *сумою*. В операції множення m/n і u/q називаються *співмножниками*, а $(m/n) * (u/q)$ — їх *добутком*.

Легко перевіряється, що наведені операції додавання і множення раціональних чисел задовольняють законам комутативності, асоціативності та дистрибутивності множення відносно додавання.

Вони також збігаються зі своїми аналогами для цілих і натуральних чисел у припущенні, що u є скороченням запису $u/1$ у випадку, коли u є цілим (натуральним) числом. У зв'язку з цим, у всіх записах, що містять $u/1$, вираз $u/1$ зазвичай замінюється виразом u. Так, $u/1 + v/1$ і $u/1 * v/1$ зазвичай записуються як $u + v$ і $u * v$ (v — також ціле число); при цьому, $0/n$ завжди записується як 0, а n/n — як 1 для будь-якого натурального $n \neq 0$, які є (звичайними) нулем і одиницею в $\mathbf{Q}$: $0 + p/q = p/q + 0 = p/q$, $0 * p/q = p/q * 0 = 0$ та $1 * (p/q) = (p/q) * 1 = p/q$.

Зі сказаного вище отримуємо, що множина $\mathbf{Q}$ є *замкненою відносно додавання і множення раціональних чисел.*

Відносно додавання також відзначимо ще такий факт.

Оскільки добуток двох цілих чисел дорівнює добутку їх найбільшого спільного дільника на найменш спільне кратне, то, виходячи з визначення рівності раціональних чисел, отримуємо, що операція додавання двох раціональних чисел m/n і u/q може бути задана таким (еквівалентним) чином.

Нехай d — найбільший спільний дільник чисел n і q, k — їх найменше спільне кратне, а n' і q' — такі цілі числа, що $n = n' * d$ і $q = q' * d$ (тобто, n' і q' — так звані *додаткові співмножники*). Тоді сумою цих чисел називається число, яке обчислюється за такою формулою:

$$m/n + u/q = (m * q' + n' * u)/k.$$

Якщо m/n є раціональним числом, то *протилежним* до нього, що позначається $(\text{-}(m/n))$, називається число $(\text{-}m)/n$, де $(\text{-}m)$ — ціле число, протилежне до m.

Числа вигляду $\text{-}(m/n)$ при $m \geqslant 0$ та $n > 0$ називаються *від'ємними раціональними числами.* (При $n = 1$ це визначення " повторює " введене раніше визначення від'ємних цілих чисел.)

Модулем раціонального числа p/q, що позначається $|p/q|$, є p/q, коли p/q є невід'ємне число, і протилежне йому (додатне) число $(-p)/q$, коли p/q — від'ємне.

Операція віднімання раціональних чисел вводиться тим же способом, що був використаний у разі цілих чисел, тобто, через рішення рівняння $m/n + x = p/q$, де m/n і p/q — раціональні числа, а x — змінна.

Очевидно, що $x = p/q + (\text{-}m)/n = (p * n + (\text{-}m) * q)/(q * n)$ є

його (єдиним) рішенням. Число (-m)$*q$ можна переписати у вигляді числа (-($m*q$)), що є протилежним до цілого $m*q$. Тобто, ($p*n$+(-m)$*q$) являє собою цілочисельну різницю $p*n-m*q$ з операцією (звичайного) віднімання "–" для цілих чисел.

Останнє означає, що якщо ми визначимо *операцію відніманння раціональних чисел* m/n і p/q через (звичайне) віднімання цілих чисел за (шкільною) формулою $p/q-m/n$ =($p*n-m*q$)/($q*n$), то ця різниця буде збігатися з ($p*n$ + (-m)$*q$)/($q*n$), що і обґрунтовує коректність введеного визначення операції віднімання "–" для раціональних чисел. При цьому легко виявляється, що є справедливими наступні тотожності:

(-(m/n + p/q)) = (-(p/q + m/n)) = (-(m/n)) − p/q = (-p/q) − m/n,

(-($m/n-p/q$)) = (-m/n) + p/q,

(-(-(m/n))) = m/n.

Тобто ми можемо префіксний знак "-" замінити знаком "–", введеним для позначення операції віднімання раціональних чисел, тобто перейти до звичайних ("шкільних") правил внесення знака "мінус" всередину дужок.

Також з визначення множення раціональних чисел одержуємо такі очевидні тотожності: (m/n)$*$(-(p/q)) = (-(p/q))$*$(m/n) = (-((m/n) $*$ (p/q))) і (-(m/n)) $*$ (-(p/q)) = (m/n) $*$ (p/q).

Маючи операцію віднімання раціональних чисел ми можемо наступним (еквівалентним вже введеному) чином визначити порядок на множині **Q**: для будь-яких раціональних чисел m/n і p/g, $m/n \leqslant p/g$ тоді і тільки тоді, коли $p/g-m/n \geqslant 0$.

Очевидно, що при будь-якому раціональному $u = m/n$ ($u \neq 0$) рішення рівняння $u*z = 1$ відносно z завжди існує і воно є числом n/m, коли m додатне, і числом (-n)/(-m), коли m від'ємне. Це число називається *числом, зворотним до* u, яке часто позначається $1/u$.

Що ж стосується єдиності рішення рівняння $u*k = 1$, то воно буде таким, якщо вимагати, щоб рішення u завжди являло собою несократимий дріб m/n (тобто дріб з НСД$(m,n) = 1$), що слідує з основної теореми арифметики.

На основі введеного поняття зворотного числа, операція ділення (":") раціональних чисел v і u ($u \neq 0$) визначається наступним

чином: $v : u = v * (1/u)$. Отже, *завжди можна виконати ділення раціонального числа v (*діленого*) на раціональне число u (*дільник*), коли $u \neq 0$*, причому, результатом такого ділення завжди буде раціональне число, яке нає назву *частки*.

Тепер легко визначити поняття *цілочисельної степені будь-якого раціонального числа*.

Возведення (будь-якого) раціонального числа p/q в натуральну степінь n визначається тим же самим способом, який був використаний для випадку натуральних і цілих чисел, а саме, $(p/q)^n$ при $n \geqslant 2$ є результатом n-кратного множення числа p/q самого на себе, при цьому $(p/q)^1 = p/q$, а $(p/q)^0 = 1$. Очевидно, що при будь-якому натуральному n $(p/q)^n = p^n/q^n$ (p — будь-яке число), $(p/q)^{(n)} = q^n/p^n$ і, зокрема, $p^{(n)} = 1/p^n$ ($p \neq 0$).

Нехай z, p і q — цілі числа. Легко перевіряється справедливість таких тотожностей: $z^p * z^q = z^{(p+q)}$, $z^q * z^{-p} = z^{-p} * z^q = z^{(q-p)}$, $z^p : z^q = z^{(p-q)}$, $(z^p)^q = z^{(p*q)}$.

Сумуючи вищесказане, ми отримуємо, що сукупність раціональних чисел $\mathbf{Q}$ замкнена відносно усіх *чотирьох арифметичних операцій*: додавання, віднімання, множення та ділення. При цьому, операції *додавання* і *множення комутативні* і *асоціативні* та пов'язані між собою *дистрибутивностью* множення відносно додавання.

В математиці будь-яка сукупність чисел, що володіє всіма такими властивостями (включаючи *наявність* у ній *нуля* і *одиниці*), називається *полем* [1]. Значить, $\mathbf{Q}$ є *поле раціональних чисел*, в той час, як $\mathbf{N}$ і $\mathbf{Z}$ ніякого поля не утворюють: $\mathbf{N}$ не замкнена відносно віднімання та звичайного ділення, а $\mathbf{Z}$ не замкнена (тільки) відносно (звичайного) ділення.

[1] Більш строго. *Полем* називається *множина A с двома заданими на неї комутативними і асоціативними операціями — додаванням*, яке зазвичай позначається $+$, і *множенням*, яке зазвичай позначається $*$, і ці *операції пов'язані між собою законом дистрибутивности множення відносно додавання*. Поле має містити *нульовий елемент — нуль*, який звичайно позначається 0, для якого $0 + a = a + 0 = a$ для будь-якого $a \in A$, і *одиничний елемент — одиницю*, яка зазвичай позначається 1, для котрої $a * 1 = 1 * a = a$ для будь-якого ненульового $a \in A$. Поле для кожного елемента $a \in A$ також зобов'язано містити елемент, званий *протилежним до a* і позначуваний $-a$, для якого $a + (-a) = 0$, і для кожного ненульового елемента $a \in A$ — елемент, званий *зворотним* до a і позначуваний a^{-1} (або $1/a$), для якого $a * a^{-1} = 1$.

Далі ми встановимо, що дійсні та комплексні числа, що вводяться нижче, також утворюють *поле дійсних чисел* та *поле комплексних чисел*.

Окрім щойно перелічених полів, існують ще так звані *скінченні поля* (і ніяких інших полів, окромя вказаних, не існує). Ми в посібнику на них не зупиняємося, але зауважимо, що кожне з них являє собою сукупність натуральних чисел від 0 до p^n (де p — просте число, а n — будь-яке натуральне число) зі специфічно визначеними арифметичними операціями додавання, віднімання, множення і ділення.

Поля відіграють велику роль в різних розділах математики, наприклад, в теорії алгебраїчного кодування, яка має велике практичне значення. Ще відзначимо, що початок вивчення полів поклав французький математик Еваріст Галуа (1811-1832).

Також звертаємо увагу на те, що $\mathbf{Z}$ з зазначеними властивостями арифметичних операцій додавання, віднімання та множення утворюють структуру, маючу в математиці назву *кільця цілих чисел*.

Крім $\mathbf{Z}$, існують і інші кільця. Наприклад, сукупність всіх многочленів з цілими коефіцієнтами, додавання, віднімання та множення яких виконується за правилами, викладеними у курсі шкільної алгебри, являє собою *кільце многочленів з цілими коефіцієнтами*, а сукупність всіх многочленів з раціональнимі коефіцієнтами — *кільце многочленів з раціональнимі коефіцієнтами*.

1.4 Дійсні числа та операції над ними

Ще древні греки виявили, що рішення так званого *степенева рівняння* другого порядку (тобто *квадратного рівняння*) $x^2 = 2$, якщо воно існує, не може бути раціональним числом. Тому подальші кроки у розвитку поняття числа були спрямовані на те, щоб забезпечити можливість рішення по меншій мірі рівнянь такого типу (тобто рівнянь вигляду $x^n = r$, де n — натуральне число и r — ціле число), і це приводить до поняття дійсних чисел.

Ми вводимо поняття дійсного числа, спираючись на шкільний курс математики, для того, щоб не ускладнювати текст досить громіздкими і складними математичними побудовами. З цією ме-

тою звернемося до подання чисел у вигляді десяткового запису, тобто запису в системі числення з основою 10 (деталі див. у наступному розділі).

Як скінченний запис вигляду $+(-)a_n \ldots a_1a_0{,}b_1b_2\ldots b_r$ (включаючі цілочисельний випадок $+(-)a_n \ldots a_1a_0$), так і нескінченний запис вигляду $+(-)a_n \ldots a_1a_0{,}b_1b_2\ldots$, які відповідають обчисленням за формулою $+(-)(a_n * 10^n + \ldots + a_1 * 10 + a_0 + b_1 * 10^{-1} + b_2 * 10^{-2} + \ldots)$, називаються *дійсними числами*, де "+" використовується для позначення додатних чисел (причому, "+" може бути відсутнім), а "–" — для позначення від'ємних чисел.

Відмітимо, що в силу зауваження про унарний мінус з розділу про раціональні числах ми надалі використовуємо один і той же знак "–" як для позначення унарна мінуса, так і для позначення (бінарної) операції вирахування будь-яких чисел.

Ціле число (включаючи випадок 0), що стоїть перед так званою *десятковою комою*, називається *цілою частиною* числа, а після коми — його *дробовою частиною*.

Використовуючи алгоритм Евкліда, легко отримати, що будь-яке натуральне число m, а отже, і ціле, може бути подано у вигляді $a_n * 10^n + \ldots + a_1 * 10 + a_0$, де $a_n, \ldots, a_1, a_0$ - цифри від 0 до 9, що відповідають числам $0, \ldots, 9$ відповідно, причому $a_n \neq 0$.

Переходячи до позиційного подання чисел (див. наступний розділ), отримуємо *десятковий запис* натурального числа m у вигляді рядка цифр: $a_n \ldots a_1a_0$.

Якщо розглянути додатне дробове число u/q, у якому $u < q$, то при його поданні у вигляді десяткового дробу воно буде мати, в загальному вигляді, вигляд нескінченної суми $b_1 * 10^{-1} + b_2 * 10^{-2} + \ldots$, де b_i $(i = 1, 2, \ldots)$ позначає одну з цифр від 0 до 9. Тобто, у позиційному десятковому поданні дріб u/q може бути записана як $0, b_1b_2\ldots$.

Цей перехід від дробу u/q до його десяткового запису може бути отриманий у результаті звичайного алгоритму ділення u на q. Як наслідок такого ділення з однозначності результату ділення натуральних чисел з залишком отримуємо, що після виконання певного скінченого числа кроків цього алгоритму у нас або будуть з'являтися тільки b_i, рівні 0, або, починаючи з деякого b_r, буде утворена група цифр $b_rb_{r+1}\ldots b_{r+s}$, яка почне періодично повторюва-

тися в ході ділення. А це означає, що u/q має десяткове подання або у вигляді *десяткового скінченного дробу* (нескінченно повторювані нулі після b_{r-1} можна опустить), або у вигляді *нескінченного десяткового періодичного дробу* $0, b_1 \dots b_{r-1} b_r \dots b_{r+s} b_r \dots b_{r+s} \dots$ яка часто записується як $0, b_1 \dots b_{r-1}(b_r \dots b_{r+s})$ для того, щоб явно виділити циклічно повторювану групу цифр $b_r \dots b_{r+s}$.

Отже, при довільних додатних u і q, раціональне число u/q може бути записане або як $a_n \dots a_1 a_0$, або як $a_n \dots a_1 a_0, b_1 \dots b_{r-1}$, або як $a_n \dots a_1 a_0$, $b_1 \dots b_{r-1}(b_r \dots b_{r+s} b_r)$.

У випадку, коли від'ємне раціональне число $(\text{-}u)/q$, де u — додатне ціле число, має десятковий запис або у вигляді $a_n \dots a_1 a_0$, або у вигляді або $a_n \dots a_1 a_0, b_1 \dots b_{r-1}$, або у вигляді $a_n \dots a_1 a_0, b_1 \dots b_{r-1}(b_r \dots b_{r+s})$, *протилежне* до нього число в десятковому записі визначається або як $\text{-}a_n \dots a_1 a_0$, або як $\text{-}a_n \dots a_1 a_0, b_1 \dots b_{r-1}$, або як $\text{-}a_n \dots a_1 a_0$, $b_1 \dots b_{r-1}$ $(b_r \dots b_{r+s})$, відповідно.

Відзначимо, що вважається, що для будь-якого дійсного числа α має місце тотожність $\text{-}(\text{-}\alpha) = \alpha$.

Нехай тепер є нескінченний періодичний десятковий дріб $0, b_1 \dots b_{r-1} b_r \dots b_{r+s} b_r \dots b_{r+s} \dots$ $(r \geqslant 1)$. Тоді його можна переписати у вигляді нескінченної суми $b_1/10^1 + \dots + b_{r-1}/10^{(r-1)} + \sum_{k=0}^{\infty}((b_r/10^r + \dots + b_{r+s}/10^{(r+s)}) * 1/10^{(s*k+1)})$, де $\sum_{k=0}^{\infty}((b_r/10^r + \dots + b_{r+s}/10^{(r+s)}) * 1/10^{(s+1)*k})$ є сума членів нескінченно спадної геометричної прогресії зі знаменником $1/10^{(s+1)}$, яка дорівнює $(b_r/10^r + \dots + b_{r+s}/10^{(r+s)}) * (10^{(s+1)}/(10^{(s+1)} - 1))$. А це говорить про те, що ця сума є раціональним числом. Оскільки ціла частина (додатна або від'ємна) будь-якого дійсного числа є ціле раціональне число, то отримуємо, що будь-який нескінченний періодичний десятковий дріб являє собою деяке раціональне число. Тобто має місце наступне твердження.

Твердження 1.4. Будь-яке раціональне число, і тільки воно, може бути подано у вигляді дійсного числа з скінченним або нескінченним періодичним десятковим дробом.

Відзначимо, що *деякі раціональні числа можуть мати два різних подання у вигляді дійсного числа у десятковому запису.* Це завжди спостерігається у тих і тільки тих випадках, коли розглядаємо раціональне число може бути подано у вигляді скінченного рядка символів, що складається лише з цифр і, бути може, містить

у своєму складі ще кому. Тоді воно допускає інше своє десяткове подання з дрібною частиною у вигляді нескінченного періодичного десяткового запису.

Наприклад, раціональне число 13/10 має таки дійсні подання у вигляді десяткового запису: $1,3$ і $1,2999\ldots$. А натуральне число 123 має таке друге подання у десятковому запису — $122,999\ldots$.

Для таких чисел, суто для технічних цілей, ми завжди будемо віддавати перевагу першому (скінченному) запису, за *умовчанням маючи на увазі*, що у цьому записі після останньої цифри праворуч *розташоване нескінченна кількість* 0. Так, $1,3$ служить звичайним і зручним позначенням $1,30\ldots0\ldots$. Таким чином, ми можемо вважати, що *ми завжди оперуємо з дійсними числами, що мають вигляд нескінченного десяткового запису.*

Виходячи з твердження 1.4 і визначення, що будь-яка скінченний або нескінченний запис вигляду $+(-)a_n\ \ldots\ a_1a_0{,}b_1b_2\ \ldots$ визначає дійсне число і тільки його, отримуємо, що, наприклад, запис $0,1010010001\ldots$, який являє собою дійсне число та задає обчислення $10^{-1}+10^{-3}+10^{-6}+\ldots$, не може бути раціональним числом (так само як і число $-0,1010010001\ldots$), оскільки у записи відсутня періодично повторювана група цифр. Тому додатні і від'ємні числа, яки не є раціональними, отримали назву *ірраціональних.*

Поняття модуля дійсного числа вводиться тим же самим способом, що і поняття модуля раціонального числа.

Модулем дійсного числа α, що позначається $|\alpha|$, є α, коли α є невід'ємне число, і протилежне йому (додатне) число $-\alpha$, коли α від'ємне.

Сукупність усіх раціональних і ірраціональних чисел називається *множиною дійсних чисел* та позначається $\mathbf{R}$.

Як ми бачимо, дійсне число є скінченною або нескінченною послідовністю десяткових цифр, розділених, бути може, в якомусь одному місці комою. Тому для визначення операцій додавання і множення дійсних чисел потрібно задати правила оперування з нескінченними послідовностями цифр, що, в принципі, для нашого підходу є неможливим. У зв'язку з цим ми будемо будь-яке дійсне число (раціональний чи ірраціональний), яке має нескінченний десятковий запис, замінювати його скінченним записом за допомогою операції округлення чисел і *виконувати додавання і множення*

округлених чисел за добре відомим правилам додавання і множення скінченних десяткових дробів, вважаючи, що отриманий результат і є округлене значення шуканої суми (добутку) дійсних чисел. В результаті ми отримуємо, що *операції додавання і множення дійсних чисел є комутативними і асоціативними і що для них також має місце дистрибутивность множення відносно додавання.*

Аналогічно (тобто, *використовуючи операцію округлення*) *визначаються операції віднімання і ділення дійсних чисел.* При цьому вважається, що для будь-якого дійсного числа α існує йому *протилежне*, яке позначається $-\alpha$ і служить (єдиним) коренем рівняння $\alpha + z = 0$ відносно z. Також вважається, що для будь-якого дійсного числа $\alpha \neq 0$ рівняння $\alpha * z = 1$ (відносно z) завжди має єдине рішення, яке позначається $1/\alpha$ і називається числом, *зворотним до* α.

В результаті маємо, що оскільки у нас є нуль (0) та одиниця (1), сукупність $\mathbf{R}$ *являє собою поле дійсних чисел.*

Оскільки у нас арифметичні операції над $\mathbf{R}$ задано через арифметичні операції над $\mathbf{Q}$, то можна вважати, що у нас є однозначна операція зведення будь-якого дійсного числа α в будь-яку цілу степінь q, результат виконання якої позначається α^q і для якої виконуються всі властивості операції зведення в степінь, що мають місце для випадку раціональних чисел.

Знову розглянемо рівняння $x^2 = 2$. Воно має додатне рішення в полі дійсних чисел (тобто його коренем є *додатне* дійсне число), яке позначається $\sqrt[2]{2}$. Згідно з нашим підходом існування цього рішення слідує з того, що подання $\sqrt[2]{2}$ у вигляді десяткового запису може бути згенеровано, використовуючи, наприклад, шкільний алгоритм вилучення квадратного кореня з додатного цілого числа, нескінченне виконання якого веде до породження нескінченною *непериодической* послідовності цифр, яка і буде являть собою $\sqrt[2]{2}$. Неперіодичність випливає з твердження 1.4, оскільки, як було сказано на самому початку цього розділу, $\sqrt[2]{2}$ не є раціональним числом.

Подібним же чином (тобто через корінь n-ої степеня з натурального числа m), який позначається $\sqrt[n]{m}$) і є (додатним) коренем рішенням рівняння $x^n = m$, де n і m — будь-які натуральні числа)

ми можемо отримати дійсні числа $\sqrt[2]{2}$, $\sqrt[2]{3}, \ldots$, $\sqrt[3]{2}$, $\sqrt[3]{3}, \ldots$ і т. д, одна частина яких буде раціональними числами (більше того, натуральними числами, наприклад, $\sqrt[2]{4}$ або $\sqrt[4]{256}$), а вся інша частина — ірраціональними (наприклад, вже згадуване число $\sqrt[2]{2}$ або число $\sqrt[4]{257}$).

Оскільки саме операція добування кореня потребувала введення поняття ірраціонального числа, розглянемо ще один (зручний) засіб подання коріння з дійсного числа, який веде до поняття *раціонального степеня дійсного числа.*

Нехай $\sqrt[n]{\alpha}$ позначає єдине (при можливості, додатне) дійсне число, якщо таке існує, n-ая степінь якого дорівнює α, тобто якщо $(\sqrt[n]{\alpha})^n = \alpha$ (α — дійсне число, а n — натуральне число, причому $n \geqslant 2$).

Відразу відзначимо наступний факт, відомий ще з шкільної математики. Якщо n — непарне число, то $\sqrt[n]{\alpha}$ існує для будь-якого α, як додатного, так і від'ємного. Якщо ж n — парне число, то $\sqrt[n]{\alpha}$ існує тільки для невід'ємних дійсних α, так як парна степінь будь-якого числа завжди є невід'ємне число.

Якщо у нас є вираз, що складається зі знаків арифметичних операцій (усіх, або деяких) і знаків добування кореня (будь-якого степеня), то воно називається *виразом зі знаками радикалів.*

Оскільки $(\sqrt[n]{\alpha})^n = \alpha$, то для $\sqrt[n]{\alpha}$ виявляється дуже зручною запис цього числа у вигляді $\alpha^{1/n}$, оскільки ми можемо визначити *операцію зведення дійсного числа α в раціональну степінь m/n* наступним чином: $\alpha^{m/n} = (\alpha^{1/n})^m$ $(= (\sqrt[n]{\alpha})^m)$. Ясно, що не при всяких α, m і n ця операція здійсненна, але в разі її застосовності вона веде до єдиного результату. При цьому $\alpha^{m/n}$ називається (раціональної) *степенем числа α*, а m/n — її *показником.*

Для раціональних чисел m/n і p/q і дійсного числа α ми постулюємо, що $(\alpha^{m/n})^{p/q} = \alpha^{(m/n)*(p/q)}$, $\alpha^{m/n} * \alpha^{p/q} = \alpha^{(m/n+p/q)}$ і $\alpha^{m/n} : \alpha^{p/q} = \alpha^{(m/n-p/q)}$, а також те, що $\alpha^0 = 1$ і $\alpha^1 = \alpha$. Це добре узгоджується з тими ж самими тождествами для операції зведення раціональних чисел у цілу степінь. Отже, у нас з'являється можливість проводити з раціональними показниками степенів дійсних чисел деякі арифметичні дії, що часто виконується на практиці.

У курсі вищої алгебри розглядається питання про те, коли і скільки дійсних рішень відносно змінної x має многочлен

$\sum_{k=0}^{n} a_k * x^k$ степеня n з дійсними коефіцієнтами $a_0, \ldots, a_n$. (Число α є коренем многочлена $\sum_{k=0}^{n} a_k * x^k$ тоді і тільки тоді, коли $\sum_{k=0}^{n}(a_k * \alpha^k) = 0$.) Виявляється, що для непарних n завжди існує принаймні один дійсний корінь. Але існують многочлени, наприклад $x^2 + 1$, у яких немає ні одного кореня. Проте при розширенні дійсних чисел на випадок так званих комплексних чисел ця ситуація різко змінюється на краще (див. наступний розділ).

На закінчення скажемо декілька слів про впорядкування дійсних чисел.

Підхід, запропонований до визначення дійсного числа у вигляді десяткового запису, не дає можливості дати достатньо чітке визначення того, що одне з розглядаємих дійсних чисел є більше або менше іншого.

Це викликано тим, що для того, щоб проводити впорядкування і порівняння дійсних чисел на рівні їх десяткових записів, ми повинні припускати, що, коли ми говоримо про деяке дійсне число, ми знаємо повністю його десятковий запис і можемо вибирати з будь-якого десяткового запису числа будь-яку її цифру (що, на жаль, не може бути зроблено на формальному рівні при нашому підході). На додаток до цього, кожну скінченний десятковий запис дійсного числа ми перетворюємо в нескінченний десятковий запис цього числа, додаючи нескінченне число нулів праворуч від останньої правої цифри в дробової частини цього числа, якщо число дробове, і додаючи кому і нескінченне число нулів праворуч від останньої правої цифри в цілу частину цього числа, якщо число ціле. Наприклад, $0,1$ перетворюється в $0,10\ldots0\ldots$, а 0 у $0,0\ldots0\ldots$.

Два дійсних числа вважаються *рівними* тоді і тільки тоді, коли вони є числами одного знака і їх нескінченні десяткові записи (без знака) збігаються (як нескінченні послідовності) в припущенні, що цілі частини цих десяткових записів не починаються з 0 (за винятком числа 0, поданого у вигляді $0,0\ldots0\ldots$).

Впорядкуємо множину всіх дійсних чисел $\mathbf{R}$.

Нехай α і β є двома *додатними дійсними числами* (поданими у вигляді нескінченних послідовностей), які мають різні десяткові записи.

У разі, коли α і β *є раціональними числами*, вважається, що ці числа в множині $\mathbf{R}$ знаходяться в тому порядку (який позна-

чається $\leqslant$), в якому вони знаходяться в множині всіх раціональних чисел $\mathbf{Q}$ (Тобто $\alpha \leqslant \beta$ має місце в множині $\mathbf{R}$ тоді і тільки тоді, коли в множині $\mathbf{Q}$ виконується $\alpha \leqslant \beta$).

Нехай тепер хоч би *одне з двох різних (додатних) чисел* α *і* β *є ірраціональним*. Не порушуючи спільності, можна вважати, що цілі частини цих чисел містять однакову кількість цифр, так як в противному випадку ми можемо вирівняти кількість цифр в цілих частинах α і β, дописуючи зліва необхідне число нулів до числа, що містить менше число цифр у своїй цілої частини. (Наприклад, якщо α є ірраціональним числом $432,1010010001\ldots$ і β є (раціональним або ірраціональним) числом $5,6789\ldots$, то вважається, що β має вигляд $005,6789\ldots$.)

Переглядаючи α і β зліва направо і порівнюючи їх цифри, що займають одні й ті ж позиції в α і β (тобто стоять на однакової "відстані" праворуч від перших цифр α і β), ми рано чи пізно знайдемо дві різні цифри, скажімо, a в числі α і b в числі β, які являють собою натуральні числа a і b. Якщо $a \leqslant b$ ($b \leqslant a$) як натуральні числа, то вважаємо, що за визначенням $\alpha \leqslant \beta$ ($\beta \leqslant \alpha$).

Наприклад, $5,16789\ldots \leqslant 432,1010010001\ldots$ (що є ірраціональним числом), у той час як $5,1010010001\ldots \leqslant 5,16789\ldots$.

Тепер введений для додатних дійсних чисел порядок $\leqslant$ поширюється на довільні (додатні та від'ємні) числа α і β наступним чином. Вважається, що за визначенням *будь-яке від'ємне дійсне число не більш будь-якого невід'ємного числа*, а для будь-яких від'ємних чисел α і β *нерівність* $\alpha \leqslant \beta$ *має місце тоді і тільки тоді,коли* $-\beta \leqslant -\alpha$, де $-\alpha$ і $-\beta$ позначають додатні числа, одержувані видаленням в α і β знака мінуса.

Ми бачимо, що будь-яки два дійсних числа є порівняннимі, а множина $\mathbf{R}$ є впорядкуваною (відносно $\leqslant$). Також зазначемо, що введене визначення порядку на $\mathbf{R}$ знаходиться у повній відповідності з інтуїтивно ясним його визначенням через те, що кожне дійсне число відповідає одній точці дійсної прямої (осі) і тільки їй, а точки прямої впорядковані за зростання згідно з переглядом точок на прямий зліва направо.

Надалі, будуть використовуватися такі позначення, що торкаються дійсних чисел:

(a, b) — для позначення *відкритого інтервалу*, тобто сукуп-

ності всіх точок x дійсної прямої, які задовольняють нерівностям $a < x < b$, де a і b — дійсні числа, і

$[a, b]$ — для позначення *закритого інтервалу*, тобто сукупності всіх точок x дійсної прямої, що задовольняють нерівностям $a \leqslant x \leqslant b$, де a і b — дійсні числа.

$(a, b]$ і $[a, b)$ — для позначення *напіввідкритих інтервалів*, тобто сукупностей всіх точок x дійсної прямої, що задовольняють нерівностям $a < x \leqslant b$ і $a \leqslant x < b$ відповідно, де a і b — дійсні числа.

Отже, використовуючи символи нескінченності, дійсна ось може бути записана як відкритий інтервал $(-\infty, +\infty)$.

1.5 Комплексні числа та операції над ними

На практиці іноді виникають задачі, вирішення яких зводиться до вирішення алгебраїчних рівнянь, що вимагають добування кореня парного степеня з від'ємного дійсного числа — операції, виконання якої неможливо в області дійсних чисел, оскільки парний степінь будь-якого (додатного чи від'ємного) дійсного числа є додатним числом. Тому природно постає питання: Чи можна так розширити поняття дійсного числа, щоб операція добування кореня парного степеня завжди була визначеною? Нижче показується, як це можна зробити тільки за допомогою так званої уявної одиниці, яка служить коренем рівняння $x^2 = -1$, яке, таким чином, завжди має розв'язок.

Відразу зазначимо, що таке, здається, чисто теоретичне розширення знайшло численні застосування в різноманітних природно-наукових галузях, наприклад, у фізиці, і зіграло велику роль у їх розвитку.

Вважатимемо, що, за визначенням, у нас є число i, яке являється рішенням рівняння $x^2 = -1$, у зв'язку з чим воно називається *уявною одиницею* (i — перша літера латинського слова imaginarius — «уявний»). Тому квадрат уявної одиниці дорівнює мінус одиниці ($i^2 = -1$); куб уявної одиниці дорівнює уявній одиниці, взятій із протилежним знаком ($i^3 = -i$); четвертий степінь уявної одиниці дорівнює одиниці ($i^4 = 1$).

Комплексними називаються числа виду $a + i * b$, де a, b —

дійсні числа. Число a називається *дійсною частиною* комплексного числа, а $i*b$ називається його *уявною частиною*, де b — *коефіцієнт уявної частини*.

Зауважимо, що поряд із записом $a + i * b$ для комплексних чисел також використовується запис $a + b * i$. У разі, коли $b = -c$, замість $a + i * (-c)$ також пишуть $a - i * c$ або $a - c * i$.

Дійсні числа є окремим випадком комплексних чисел, коли $b = 0$, у зв'язку з чим уявні частини таких чисел опускаються. Тому *комплексний нуль* $0 + i * 0$ записується як дійсний нуль 0, а *комплексна одиниця* $1 + i * 0$ — як дійсна одиниця 1.

Сукупність усіх комплексних чисел називається *множиною комплексних чисел* і позначається $\mathbf{C}$.

Два комплексні числа *рівні* тоді і тільки тоді, коли рівні їх дійсні частини і рівні коефіцієнти їх уявних частин.

Відмітимо, що для комплексних чисел не існує таких понять "більше" і "менше", яки дозволяли б впорядкувати їх природним чином (тобто таким чином, при якому запроваджений порядок був би узгоджений з порядком дійсних чисел і, при цьому, був б інваріантним відносно арифметичних дій над комплексними числами.

Ще відзначимо, що модуль комплексного числа $a+i*b$ визначається як дійсне число $\sqrt{a^2 + b^2}$, що позначається $|a + i * b|$, і він є довжиною вектора при використанні геометричного подання комплексного числа на площині (див. відповідну літературу). (Випадок $b = 0$ призводить до звичайного визначення модуля дійсного числа.)

Визначимо формально (всюди визначені) операції додавання $(+)$ і множення $(*)$ комплексних чисел через арифметичні операції, які були введені для дійсних чисел:

$(a + i * b) + (c + i * d) = (a + c) + i * (b + d)$,

$(a + i * b) * (c + i * d) = (a * c - b * d) + i * (a * d + b * c)$.

Оскільки результат виконання цих операцій являє собою комплексне число, одержуємо, що множина комплексних чисел $\mathbf{C}$ *є замкненою відносно додавання та множення*.

Два комплексні числа $a + i * b$ і $-a - i * b$ називаються *протилежними* числами, де $-a-i*b$ служить зручним записом числа $(-a) + i * (-b)$, яке часто ще позначується $-(a + i * b)$. (a і b є раціональні числа, протилежні a і b відповідно.)

Звідси випливає, що $-(-(a+i*b)) = -(-a-i*b) = (a+i*b)$. Тому рівняння $\theta + x = 0$ (с комплексним θ) щодо змінної x завжди має єдине рішення, і їм є число $-\theta$. Значить, і рівняння $\theta + x = \omega$ (θ і ω — комплексні числа) завжди має єдине рішення, яким є число $\omega + (-\theta)$, або, в іншому записі, $\omega - \theta$, яке називається *різницею комплексних чисел* ω та θ (ω — *зменьшуване*, а θ — *від'ємник*).

Це дозволяє вважати, що *операція віднімання комплексних чисел* (тобто операція, обернена до операції додавання) визначається за такою формулою (що використовує операцію віднімання дійсних чисел):

$(a + i * b) - (c + i * d) = (a - c) + i * (b - d)$.

Два комплексні числа $a + i * b$ і $a - i * b$ називаються *спряженими числами*, де $a - i * b$ є те ж саме, що і $a + i * (-b)$.

Використовуючи арифметичні операції над дійсними числами,таким чином визначаємо *частка двох комплексних чисел* (":" позначає операцію ділення як над дійсними, так і комплексними числами):

$(c+i*d) : (a+i*b) = ((c*a+d*b) : (a^2+b^2)) + i*((c*(-b)+ d*a) : (a^2+b^2))$.

При цьому $a+i*b$ називається *діленим*, а $c+i*d$ — *дільником*.

Легко перевіряється, що частка є (єдиним) коренем рівняння $(a+i*b)*x = c+i*d$ відносно змінної x у разі, коли $a+i*b$, а, значить, і a або b відмінне від 0. (Якщо $a = b = 0$, то вважається, що рівняння не має сенсу.) Ця частка часто позначається $(c + i * d)/(a + i * b)$.

Для випадку рівняння $(a + i * b) * x = 1$ отримуємо, що воно завжди має єдине рішення (a і b відмінні від 0). Його рішення $1/(a + i * b)$ $(= (a - i * b)/(a^2 + b^2))$ називається комплексним числом, що є *зворотним* до $(a + i * b)$. Отримуємо, що введена (всюди визначена) операція ділення є *зворотною* до операції множення.

Спосіб визначення віднімання і ділення комплексних чисел показує, що множина $\mathbf{C}$ *є замкненою відносно віднімання та ділення.*

Якщо повернутися до операцій додавання і множення, то легко перевіряється, що для них виконуються закони асоціативності та комутативності. Крім того, ці операції пов'язані дистрибутивностью множення відносно додавання. Тому, враховуючи існування для них зворотних операцій (віднімання і ділення), а також наяв-

ність у $\mathbf{C}$ комплексних 0 і 1, приходимо до висновку, що $\mathbf{C}$ являє собою *поле комплексних чисел* (без дільників нуля).

Діючи таким же чином, що і у випадку дійсних чисел, ми можемо визначити цілочисельні і раціональні спепени комплексного числа, скажімо, θ, послідовно вводячи очевидні визначення для виразів: θ^m, $\sqrt[n]{\theta}$, $\theta^{1/n}$, $\theta^{m/n}(=(\theta^{1/n})^m)$, де m — ціле число, а n — натуральне, відмінне від 0.

Раніше ми відзначали, що при роботі тільки в області дійсних чисел при певних значеннях θ, m і n деякі з цих виразів стають безглуздими, так як вони не являють собою ніякого дійсного числа (наприклад, $\sqrt[2]{-1}$). Однак у випадку комплексних чисел кожен з наведених виразів завжди є хоча б одним комплексним числом при будь-яких θ, m і n ($n \neq 0$). Більш того, в теорії комплексних чисел має місце такий факт:

Для будь-яких θ і n вираз $\sqrt[n]{\theta}$ має сенс і *існує в точності* n *різних комплексних чисел,* n*-тая степінь кожного з яких дорівнює* θ.

Наприклад, $\sqrt[4]{1}$ має сенс і в області комплексних чисел, і в області дійсних чисел. Але в області комплексних чисел існує чотирі різних комплексних числа $i, -i, 1$ та -1, четверта степінь кожного з яких дорівнює 1, у той час як в області дійсних чисел є тільки два таких числа, а саме: 1 та -1. Вираз $\sqrt[2]{-1}$ не має сенсу в області дійсних чисел, але в області комплексних чисел для уявної одиниці i маємо: $i^2 = (-i)^2 = -1$.

У більш загальному вигляді цей факт набуває форму наслідку з основної теореми алгебри.

Сама ж основна теорема алгебри формулюється наступним чином.

Твердження 1.5 (основна теорема алгебри). Будь-який відмінний від константи многочлен $\sum_{k=0}^{n} a_k * x^k$ степеня n із комплексними (дійсними, раціональними або натуральними) коефіцієнтами $a_0, \ldots, a_n$ має хоча б один комплексний корінь.

Враховуючи *теорему Безу* про те, що якщо θ є корінь відмінного від константи многочлена $\sum_{k=0}^{n} a_k * x^k$ степеня n, то цей многочлен можна представити у вигляді добутку лінійного двочлена $x - \theta$ на многочлен, степінь якого дорівнює $n - 1$, одержуємо наступне твердження (яке також, іноді, називається основною тео-

ремою алгебри).

Наслідок 1.1. Будь відмінний від константи многочлен $\sum_{k=0}^{n} a_k * x^k$ степеня n з комплексними (дійсними, раціональними або натуральними) коефіцієнтами $a_0, \ldots, a_n$ має в точності n комплексних коренів з урахуванням їх кратності.

Природно поставити питання: Можна ли узагальнити поняття комплексного числа таким чином, щоб сукупність всіх нових чисел включала б у свій склад всі комплексні (а, значить, дійсні, раціональні, цілі та натуральні) числа й утворювала б поле після введення відповідних арифметичних операцій? Відповідь на нього негативна. Єдине, чого вдалося досягти, так це узагальнити комплексні числа до так званих *кватерніонів*, але введення відповідних арифметичних операцій веде до того, що *сукупність всіх кватерніонів являє собою тільки кільце з діленням*, а не поле.

1.6 Деякі алгебраїчні структури

Раніше ми познайомилися з такими поняттями, як кільця і поля. У даному розділі ми завершуємо знайомство з основними алгебраїчними конструкціями, що грають велику роль у математиці.

Найпростішим серед них є *групоїд*, під під яким розуміється впорядкована пара $\langle G, \cdot \rangle$, де G являє собою множину елементів (*носій* групоїда), на якому задана всюди визначена бінарна операція "$\cdot$", що як правило, називається *множенням* (в окремих випадках — *додаванням*, коли вона позначається "+").

Відзначимо, що в групоїді на бінарну операцію "$\cdot$" не накладаються ніякі обмеження.

Групоїд $\langle G, \cdot \rangle$ називають *напівгрупою*, якщо його операція "$\cdot$" асоціативна, тобто для будь-яких елементів a, c носія G виконується рівність $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Групоїд $\langle G, \cdot \rangle$ називають *моноїдом*, якщо його операція "$\cdot$" асоціативна і відносно "$\cdot$" існує *нейтральний елемент* (*одиниця*), тобто елемент, скажімо, $\mathbf{1}$, з наступною властивістю: $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$ для будь-якого $a \in G$. Тому моноїд ще називають *напівгрупою з одиницею*.

Серед напівгруп виділяють напівгрупи з комутативною операцією '$\cdot$'— *коммутативные напівгрупи*.

Групоїд $\langle G, \cdot \rangle$ називають *групою*, якщо його операція "$\cdot$" асоціативна, існує нейтральний елемент (одиниця) $\mathbf{1}$ відносно операції "$\cdot$" і для кожного $a \in G$ існує такий елемент $a' \in G$, званий *оберненим до* a, що $a \cdot a' = a' \cdot a = \mathbf{1}$. Як правило, зворотний елемент a' позначається a^{-1}, і, як можна показати, цей зворотний елемент єдиний.

Іншими словами, група — це моноїд, в якому для кожного елемента існує йому зворотний. Або інакше, група — це напівгрупа з одиницею і оберненим елементом.

Серед усіх груп важливе місце займають групи з комутативнівною операцією "$\cdot$", так звані *комутативні*, або *абелеві групи*.

Приклади. Проілюструємо введені алгебраїчні конструкції на ряді прикладів.

– Введемо операцію "$\setminus$" на множині натуральних чисел $\mathbf{N}$ наступним чином: $n \setminus m = n - m$, якщо $n \geqslant m$, і $n \setminus m = 0$ в інших випадках. Ця операція всюди визначена, але не асоціативна, оскільки наприклад, $2 \setminus (3 \setminus 2) = 1$, у той час як $(2 \setminus 3) \setminus 2 = 0$. Отже, множина $\mathbf{N}$ відносно введеної операції '$\setminus$"являє собою групоїд і тільки його.

– Множина натуральних чисел $\mathbf{N}_+$ відносно звичайної операції додавання натуральних чисел буде (комутативною) напівгрупою без нейтрального елемента (але не буде моноїдом із-за відсутності нейтрального елемента), у той час як $\mathbf{N}_+$ відносно операції множення натуральних чисел вже буде (комутативним) моноїдом, тобто комутативною полугруппой з одиницею, якою є звичайна одиниця 1.

– Множина цілих чисел $\mathbf{Z}$ відносно звичайного додавання буде комутативною групою, у якій 0 є нейтральний елемент, а в якості зворотного елемента до цілого числа z виступає протилежне йому число $-z$. Стосовно ж звичайного множення $\mathbf{Z}$ являє собою не більш ніж комутативний моноїд, у якого 1 є нейтральним елементом. Беручи до уваги, що виконується закон дистрибутивності множення відносно додавання, отримуємо іншу формулировку того, що $\mathbf{Z}$ утворює кільце (але не поле) цілих чисел.

– Множини раціональних і дійсних чисел ($\mathbf{Q}$ і $\mathbf{R}$) є комутативними групами як відносно додавання, так і відносно множен-

ня. Більше того, вони є полями. У цьому зв'язку цікаво зазначити, що *поле можна ще визначити* як множину з двома діючими на ньому операціями — додаванням і множенням, відносно яких ця множина являє собою дві абелевы групи, одна з нулем, а інша з одиницею, які являють собою їх нейтральні елементи; при цьому операції пов'язані одна з одною законом дистрибутивності множення відносно додавання.

1.7 Системи числення. Позиційні системи числення

Для того, щоб мати можливість говорити про числа, записувати їх та виконувати обчислення та операції з ними, необхідно мати засоби запису чисел. І ці засоби мають назву систем числення. (Вище ми у скритій формі використовували десяткову систему числення.)

Розрізняють такі типи систем числення: позиційні, непозиційні і змішані.

Запис чисел в тій чи іншій системі числення проводиться за допомогою спеціальних знаків, званих *цифрами*. Як правило, запис числа є лінійною послідовністю цифр (тобто слово, що складається з цифр), в якій можуть зустрічатися спеціальні розділові знаки, наприклад, кома або крапка.

У позиційних системах числення одна і та сама цифра набуває різних значень залежно від своєї позиції при запису чисел у вигдяді (лінійної) послідовності цифр. Таким чином, позиція цифри має "вагу" у числі. Здебільшого вага кожної позиції кратна деякому натуральному числу p, $p > 1$, яке називається *основою* системи числення.

У непозиційних системах числення величина, яку позначає цифра, не залежить від позиції її у числі, хоч система може накладати обмеження на позиції цифр та їх порядок, наприклад, щоб вони були розташовані за спаданням чи згруповані за значенням, що не є принциповою умовою для розуміння чисел, що записані у таких системах. Типовим прикладом непозиційної системи числення є римська система числення, в якій у якості цифр використовуються латинські літери.

Змішана система числення є узагальненням системи числен-

ня з основою p і її часто відносять до позиційних систем числення. У подальшому нас будуть цікавити тільки позиційні системи числення.

Винахід позиційної системи числення, заснованої на помісному значенні цифр, приписують шумерам і вавилонянам. Її було розвинуто індусами.

Будь-яка позиційна система числення, що розглядається нижче, визначається числом $p > 1$, званим основою системи числення. Система числення з основою p також називається p-ичною (зокрема, вона може бути четверичною, двійковою, вісімковою, десятковою або шістнадцятковою).

Основа позиційної системи числення не зобов'язана бути натуральним числом, узгоджену систему числення можна створити з основою. яким являється від'ємне ціле, раціональне або ірраціональне число (наприклад, нею може бути так званий "золотий перетин" або число π). Але надалі ми будемо розглядати системи числення тільки з натуральною основою.

Для задання будь-якого числа в p-ичній системі числення необхідно мати p цифр, починаючи з 0 для нуля і 1 для одиниці. Для позначення чисел в системах числення з основою від двох до шістнадцяті існують такі узгодження: цифра 0 використовується для позначення числа "нуль", цифра 1 — для позначення числа "один", ..., цифра 9 — для позначення числа "дев'ять", заглавна латинська літера (цифра) A — для позначення числа "десять", заглавна латинська літера (цифра) B — для позначення числа "одинадцять", ..., заглавна латинська літера (цифра) F — для позначення числа "п'ятнадцять".

Наприклад, у двійковій системі числення використовуються цифрі 0 і 1, у сімковій системі використовуються цифри від 0 до 6 включно, у десятковій системі використовуються цифри від 0 до 9 включно, у дванадцятиричній системі використовуються цифри від 0 до 9 включно та цифри-літери A і B, у шіснадцятковій системі використовуються цифри від 0 до 9 включно та цифри-літери від A до F включно.

Натуральне число x в p-ичній системі числення задається у вигляді деякої скінченної лінійної комбінації степенів числа p: $x = (+)\sum_{k=0}^{n-1} a_k * p^k$, де кожна a_k — одна з цифр p-ичної системи

числення.

Існування та єдиність такого подання натурального числа забезпечують відповідні властивості ділення натуральних чисел із залишком.

Очевидно, що *від'ємні цілі числа* мають аналогічну форму подання в p-ичній системі числення: $x = -\sum_{k=0}^{n-1} a_k * p^k$, де кожна a_k — одна з цифр p-ичної системи числення. Тобто *будь-яке ціле число* має вигляд $\pm\sum_{k=0}^{n-1} a_k * p^k$.

Кожний степінь p^k у такому записі називається *розрядом* (*позицією*). Старшинство розрядів та відповідних їм цифр визначається значенням показника степеня k. Зазвичай для ненульового числа x вимагають, щоб старша цифра a_{n-1} у p-ичному поданні x була також ненульовою.

Якщо не виникає різночитань, *натуральне* (тобто *невід'ємне ціле*) число x записують у вигляді послідовності його p-ичних цифр, що перераховуються за зменшенням старшинства розрядів зліва направо: $x = (+)a_{n-1} \dots a_1 a_0$.

Очевидно, що *від'ємні цілі числа* мають наступний вигляд у формі послідовності: $x = -a_{n-1} \dots a_1 a_0$.

Побудову (позиційного) запису числа називають *позиційним кодуванням* числа, а сам запис — *позиційним кодом* числа.

Наприклад, число *сто дев'ять* задається в десятковій системі числення у вигляді: $109 = 1 * 10^2 + 0 * 10^1 + 9 * 10^0$.

Щоб уникнути плутанини при одночасній роботі з кількома системами числення, основа (p) системи числення вказується в якості нижнього індексу. Наприклад, 109_{10}.

Так, для числа *сто дев'ять* маємо таке його подання у шістнадцятковій системі: $6D_{16}$. У двійковій системі воно записується як 1101101_2.

Зауважимо, що використовуючи n позицій, у p-ічної системі числення можна записати тільки p^n різних натуральних чисел, а саме, числа від 0 до $p^n - 1$.

Тепер перейдемо до подання *раціональніх і дійсних чисел* в позиційних системах числення.

Вважається, що будь-яка (нескінченна) сума виду $\sum_{j=1}^{\infty} b_j * p^{-j}$,
де $b_1, b_2, \dots$ — цифри p-ичній системі числення, задає у p-ичній

системі числення деяке додатне (дробове) дійсне число x, не більше за одиницю, і навпаки, будь-яке додатне (дробове) дійсне число x, не більше за одиницю, має це подання у p-ичній системі числення.

Якщо у сумі вище, починаючи з деякого q, усі $b_{q+i} = 0$, то можна вважати, що сума має вигляд скінченного виразу.

Переходячи до подання x у вигляді послідовності його p-ичних цифр, маємо (можливо, скінченний) запис для x: $0, b_1 b_2 \ldots$.

Тому будь-яке *невід'ємне дійсне число* x має вигляд $\sum_{k=0}^{n-1} a_k * p^k + \sum_{j=1}^{\infty} b_j * p^{-j}$.

Переходячи до запису x у вигляді послідовності його p-ичних цифр, маємо (скінченну або нескінченну) строку цифр $a_{n-1} \ldots a_1 a_0, b_1 b_2 \ldots$.

Від'ємні дійсні числа мають вигляд: $-(\sum_{k=0}^{n-1} a_k * p^k + \sum_{j=1}^{\infty} b_j * p^{-j})$, або $-a_{n-1} \ldots a_1 a_0, b_1 b_2 \ldots$.

Арифметичні операції додавання, віднімання, множення й ділення у p-ичній системі числення можна виконувати тим самим чином, що й у разі десяткової системи числення, тобто задавши таблиці додавання і множення чисел, що відповідають цифрам системи. При цьому треба пам'ятати, що дійсне число є скінченним або нескінченним десятковим дробом. Тому для визначення арифметичних операцій над дійсними числами у будь-якій p-ичній системі числення потрібно, як і у випадку десяткової системи, нескінченне подання числа замінювати його скінченним поданням за допомогою операції округлення чисел і виконувати арифметичні дії вже з округленими числами.

В силу твердження 1.4 все сказане вище про подання дійсних чисел в системі числення з основою p має місце і для раціональних чисел. Значить, арифметичні операції над раціональними числами, що були введені в розділі про раціональні числа, можна замінити арифметичними діями з скінченими послідовностями чисел, що подають раціональні числа в тій чи іншій p-ичній системі числення. Правда, при цьому може виявитися, що результат, який був би точним раціональним числом при використанні раціональних чисел і арифметичних операцій над ними у формі вихідних визначень із розділу про раціональні числа, стає його наближеним виразом.

Відмітимо, що додавання і множення дійсних чисел є комутативними і асоціативними операціями у будь-якій p-ичній си-

стемі числення. Для них також має місце дистрибутивність множення відносно додавання. Крім цього, в будь-який p-ічной системі числення для додавання і множення існують усюди певні зворотні операції — віднімання і ділення. Тобто те, що $\mathbf{Q}$ і $\mathbf{R}$ є полями, не залежить від вибору основи p системи числення для подання раціональних і дійсних чисел у вигляді p-ічніх записів.

1.8 Переведення із одної системи числення у другу

Ми дамо тільки правила переведення чисел із одної системи числення у другу, не зупиняючись на обгрунтуванні їх правильності.

1.8.1 Переведення в десяткову систему числення

Якщо дано таке число в p-ичній системі числення:

$$\pm a_{n-1} \dots a_1 a_0, b_1 b_2 \dots b_m,$$

то для переведення в десяткову систему обчислюємо таку суму:

$$\pm(\sum_{k=0}^{n-1} a_k * p^k + \sum_{j=1}^{m} b_j * p^{-j})$$

або, в більш наочному вигляді:

$$\pm(a_{n-1} * p^{n-1} + \dots + a_1 * p + a_0 + b_1 * p^{-1} + b_2 * p^{-2} + \dots + b_m * p^{-m}).$$

Наприклад: $101100,001_2 = 1 * 2^5 + 0 * 2^4 + 1 * 2^3 + 1 * 2^2 + 0 * 2^1 + 0 * 2^0 + 0 * 2^{-1} + 0 * 2^{-2} + 1 * 2^{-3} = 32 + 8 + 4 + 1/8 = 44,125_{10}$.

1.8.2 Переведення з десяткової системи числення у іншу систему

Окремо переводяться ціла та дрібна частини.

Для переведення цілої частини потрібно спочатку на основу поділити з залишком вихідне ціле число, потім потрібно на основу поділити з залишком отримане неповну частку і так поступати до тих пір, поки неповна частка не стане рівною нулю.

Отримані при ділінні залишки є цифрами цілої частини вихідного числа у новій системі, які записують, починаючи з останнього ненульового залишку.

Для переведення дробової частини потрібно виконати наступне. Дробову частину вихідного десяткового числа помножити

на основу системи, в яку потрібно перевести. Виділити в ньому дробову частину. Продовжувати послідовно множити одержувані дробові частини на основу нової системи до тих пір, поки чергова дробова частина не стане рівною 0, або зупинитися після досягнення необхідної точності подання числа (процес множення може бути нескінченним).

Дробову частину вихідного числа в новій системі складають цифри, яки послідовно з'являються в цілій частині результату множення проміжних дробових частин на основу і яки записуються в порядку, відповідному їх отриманню.

Нариклад, переведемо $44,125_{10}$ у четверичну систему.

Для цілої частини маємо: 44 ділимо на 4: неповна частка — 11, залишок — 0; 11 ділимо на 4: неповна частка — 2, залишок — 3; 2 ділимо на 4: неповна частка — 0, залишок — 2; Ділення закінчено.

Тепер, записавши залишки у зворотному порядку відносно їх появи, отримаємо число 230_4.

Для дробової частини $0,125_{10}$ маємо: $0,125$ множимо на 4: добуток — $0,5$, ціла частина — 0, дробова частина — $0,5$; $0,5$ множимо на 4: добуток — $2,0$, ціла частина — 2, дробова частина — 0; множення закінчено.

Тепер, записуючи після нуля з комою цілі частини в порядку їх появи, отримаємо число $0,02_4$, яке є дробовою частиною вихідного числа у четверичной системі числення.

Тобто, вихідне число $44,125_{10}$ є $230,02_4$.

1.8.3 Переведення з двійкової у четверичну, вісімкову і шістнадцяткову системи

Для цього типу операцій існує спрощений алгоритм. Для його наочності розглянемо переведення з двійкової у вісімкову систему.

По-перше, розбиваємо двійковий запис числа, що переводиться, на трійки цифр: для цілої частини — зправа наліво, дописуючі нулі для створення трійки на початку цілої частини, у разі такої потреби, і для дробової частини — зліва направо, дописуючи нулі для створення трійки у кінці дробової частини, у разі такої потреби. (У випадку четверичної і шістнадцяткової систем двійковий запис розбивається на двійки і четвірки цифр.)

Перетворимо трійки цифр у вісімкові цифри за такою таблицею: $000-0$, $001-1$, $010-2$, $011-3$, $100-4$, $101-5$, $110-6$, $111-7$. (У випадку шістнадцяткової системи маємо таку таблицю: $0000-0$, $0001-1$, $0010-2$, $0011-3$, $0100-4$, $0101-5$, $0110-6$, $0111-7$, $1000-8$, $1001-9$, $1010-A$, $1011-B$, $1100-C$, $1101-D$, $1110-E$, $1111-F$. А для четверичної системи таблиця має вигляд: $00-0$, $01-1$, $10-2$, $11-3$.)

Наприклад, $1101100,01_2$ спочатку перетворюється на такі трійки: 001 101 100,010. Після заміни трійок цифрами отримаємо вісімковий запис: $154,2_8$.

Для шістнадцяткової системи зпочатку "генеруємо" четвірки: 0110 1100,0100, які потім "трансформуємо" у шістандцяткове число $6C,4_{16}$.

Для четверичної системи числення маємо число $1230,1_4$.

Діючи зворотним чином, тобто замінюючи шістнадцяткові, вісімкові або четверичні цифри розглядаємого числі їх двійковими кодами, ми легко переходимо від шістнадцяткового, вісімкового або четверичного запису цього числа до його двійкового подання. Наприклад, число $74F,C_{16}$ є 0111 0100 1111,1100$_2$ (= 11101001111,11$_2$), $341,12_8$ — 011 100 001,001 010$_2$ (= 11100001,00101$_2$), а $132,12_4$ — 01 11 10,01 10$_2$ (= 11110,011$_2$).

2 Про множини

Досвід сучасної математики та її аналіз її показують, що множини служать тим основним елементарним матеріалом, на базі якого будуються всі основні математичні теорії. Звідси випливає універсальність ідеї множини і мови теорії множин для математики, як неперервної, так і дискретної.

Основи теорії множин були закладені відомим німецьким математиком Георгом Кантором у другій половині 19-го століття. Поява теорії множин була зустрінута з ентузіазмом багатьма авторитетними математиками. Вони побачили в ній можливість створення метамови математики, тобто формальної одностайної системи понять і принципів, за допомогою якої можна було б викласти з єдиних позицій зміст різноманітних традиційно далеких один від одного розділів математики. Перші такі досить успішні спроби були виконані вже незабаром після виникнення канторівської теорії множин.

Однак пізніші дослідники виявили в теорії Кантора чимало суперечностей: так званих парадоксів, або антиномій. Виникла кризова ситуація. Одна частина математиків, посилаючись на штучність сформульованих антиномій, вважала за краще не помічати ці суперечності або не надавати їм великого значення. У той час як інша група математиків зосередила свої зусилля на пошуках більш обгрунтованих та точних принципів і концепцій, на яких могла б бути побудована несуперечлива теорія множин. У результаті було запропоновано декілька формальних (або аксіоматичних) систем, які служать фундаментом сучасної теорії множин, а значить, фундаментом всієї класичної математики. Важливість цих досліджень серед іншого підкреслює той факт, що значний внесок у становлення аксіоматичної теорії множин зробили такі видатні математики і мислителі, як Б.Рассел, Д.Гільберт, К.Гедель, П.Бернайс та ін.

Докладніше з історією виникнення та розвитку теорії множин можна ознайомитись, прочитавши цікаву монографію А.Френкеля і І.Бар-Хіллела “Основания теории множеств” або книгу М.Клайна “Математика. Утрата определенности”.

2.1 Елементи і множини

Для наших цілей достатньо буде викладення основ так званої інтуїтивної, або наївної теорії множин, яка в головних своїх положеннях зберігає ідеї та результати засновника теорії Г.Кантора.

В інтуїтивній теорії множин поняття "елемент" та "множина" належить до первинних невизначальних понять, тобто вони не можуть бути означено через інші більш прості терміни або об'єкти, а пояснюються на прикладах, апелюючи до нашої уяви та інтуїції. Такими поняттями в математиці є також поняття "число", "пряма", "точка", "площина" тощо.

Канторівське речення: "Множина — це зібрання в єдине ціле визначених об'єктів, які чітко розрізняються нашою інтуіцією або нашою думкою" — безумовно не може вважатися строгим математичним означенням, а є скоріше поясненням поняття множини, яке заміняє термін "множина" на термін "зібрання". Іншими синонімами основного слова "множина" є "сукупність", "набір", "колекція", "об'єднання" (так званих елементів, тобто об'єктів) тощо. Наприклад, сукупність цілих чисел, множина студентів, колекція картин і т. д.

При написанні множини позначаються, як правило, великими літерами. Об'єкти, з яких складається задана множина, називаються її елементами, яки позначаються малими літерами латинського алфавіту.

Теорія множин спирається на поняття "бути елементом множини", яке вважається однозначно трактованим. Той факт, що об'єкт a є елементом множини X записується так: $a \in X$ (читається: "a належить (множині) X" або "a є елементом (членом) X"), де $\in$ служить для позначення так званого *відношення* (*предиката*) *приналежності*. Для того, щоб підкреслити, що деякий елемент a не належить множині X, вживають позначення $a \notin X$ або $a \bar{\in} X$.

Запис $a, b, c, \ldots \in X$ використовують для скорочення запису $a \in X$, $b \in X$, $c \in X$, ...

Якщо кожен елемент множини Y є елементом множини X, множину Y називають *підмножиною* множини X, що позначається $Y \subseteq X$. У цьому випадку також кажуть, що Y *включається в* X або X *включає* Y, і пишуть $X \supseteq Y$.

Очевидно, що для будь-якої множини X виконується $X \subseteq X$. Також очевидно, що в теорії множин має місто так звана *транзитивність включення* $\subseteq$: для будь-яких множин X, Y і Z з того, що $Z \subseteq Y$ і $Y \subseteq X$, слідкує, що $Z \subseteq X$.

Дві множини X і Y *є рівними* (*співпадають*) в тому і тільки тому випадку, коли вони складаються з одних і тих самих елементів; запис $X = Y$ означає, що множини X і Y рівні.

З цього визначення випливає, що $X = Y$ в тому і тільки тому випадку, коли $X \subseteq Y$ і $Y \subseteq X$, що часто використовується для доведення рівності двох множин.

Підмножина Y множини X називається *власною підмножиною* множини X (позначення — $Y \subset X$), якщо $Y \subseteq X$ і $Y \neq X$.

Пустою множиною називається множина, яка не містить жодного елемента. Вона позначається $\varnothing$. Вважається, що для будь-якої множини X має місце $\varnothing \subseteq X$.

Слід чітко розуміти різницю між знаками $\in$ і $\subseteq$ і не плутати ситуації їхнього вживання. Якщо $\{a\} \subseteq X$, то $a \in X$, і навпаки. Однак із включення $\{a\} \subseteq X$, взагалі кажучи, не випливає $\{a\} \in X$. Наприклад, $\{a\} \subseteq \{a, b\}$, но не вірно, що $\{a\} \in \{a, b\}$.

Крім пустої множини, стандартні назви і позначення мають такі множини (які вже розглядалися):

$\mathbf{N} = \{0, 1, 2, \ldots\}$ — множина натуральних чисел;

$\mathbf{Z} = \{\ldots, -2, -1, 0, +1, +2, \ldots\}$ — множина цілих чисел;

$\mathbf{Q} = \{p/q |\ p \in Z, q \in N_+\}$ — множина раціональних чисел;

$\mathbf{R} = \{$*Всі десяткові (скінченні та нескінченні) дроби*$\}$ — множина дійних чисел;

$\mathbf{C} = \{a + i * b |\ a \in R, b \in R, i$ — уявна одиниця, тобто $i^2 = -1\}$ — множина комплексних чисел.

2.2 Способи задання множин

Існує три основних способи задання множин.

2.2.1 Задання через перелік елементів

Цей спосіб полягає у конкретному зазначенні всіх елементів множини. Він застосовується лише для скінченних множин елементів, таких, наприклад, як множина усіх континентів = {Європа,

Азія, Америка, Африка, Австралія, Антарктида} та множина всіх російських голосних літер = {а, е, и, о, у, э, ю, я}.

2.2.2 Задання через характеристичні властивости

Завдання множини через характеристичні властивості — це конкретне зазначення набору властивостей/властивості, якої повинен задовольняти всі елементи множини, що задається.

Якщо множину A задано характеристичною властивістю P, то це зазвичай позначається як $A = \{x \mid P(x)\}$. (Тобто $x \in A$ тоді і тільки тоді, коли x задовольняє властивості P).

Наприклад, множина всіх парних натуральних чисел може бути задана як множина $\mathbf{N}_2 = \{x \mid x \in \mathbf{N}$ і "x ділиться без залишку на 2"$\}$.

2.2.3 Задання через породжуючу процедуру

Породжуюча процедура — це певний алгоритм (наприклад, заданий у вигляді сукупності правил або обчислюваної формули), виконання якого призводить до (послідовного) породження елементів множини.

Так, елементи вищезазначеної множини $\mathbf{N}_2$ можуть розглядатися як значення функції $m = 2 * n$, що обчислюється для $n = 0, 1, 2, \ldots$

Іншим прикладом служать числа Фібоначчі, породження яких відбувається за такими правилами: $a_1 = 1, a_2 = 2$ і $a_n = a_{n_1} + a_{n_2}$ для $n > 2$. Останнє правило дозволяє послідовно обчислювати значення $a_3 = a_2 + a_1 = 3, a_4 = 5, a_5 = 8$ і т. д.

2.3 Теоретико-множинні операції

У подальших наших міркуваннях про множини передбачатиметься (якщо не зазначено інше), що вони є підмножинами деякої фіксованої множини U, яка, як правило, називається *універсумом*. На практиці цю множину часто явно не вказують, припускаючи, що в разі необхідності вона однозначно визначаєеться з контексту.

2.3.1 Перетин множин

Перетином множин A і B називається множина, що позначається $A \cap B$ і складається з усіх тих і тільки тих елементів, які одночасно належать обом множинам —A і B.

Формально перетин множин визначається так:

$A \cap B = \{x \mid x \in A \text{ і } x \in B\}$.

Наприклад, $\{a, b, c\} \cap \{a, c, d\} = \{a, c\}$.

2.3.2 Об'єднання множин

Об'єднанням множин A і B називається множина, що позначається $A \cup B$ і складається з усіх тих і тільки тих елементів, які належать хоча б одній множині — A або B.

Формально об'єднання множин визначається так: $A \cup B = \{x \mid x \in A \text{ или } x \in B\}$.

Наприклад, $\{a, b, c\} \cup \{a, c, d\} = \{a, b, c, d\}$.

2.3.3 Різниця множин

Різницею множин B і A називається множина, яка позначається $B \dot{-} A$ і складається з усіх тих і тільки тих елементів з B, які не належать A.

Формально різниця множин визначається так:

$B \dot{-} A = \{x \mid x \in B \text{ и } x \notin A\}$.

Наприклад, $\{a, b, c\} \dot{-} \{a, c, d\} = \{b\}$.

2.3.4 Симетрична різниця множин

Симетрична різниця множин B і A позначається $B \div A$ і містить всі елементи з $A \cup B$, які належать тільки A або тільки B.

Формально симетрична різниця множин може бути визначена таким чином:

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

Очевидно, що вираз $(B \dot{-} A) \cup (A \dot{-} B)$ задає ту ж саму множину, що і $(B \cup A) \dot{-} (B \cap A)$. Тому він також може виступати в якості визначення симетричної різниці. Зауважимо, що $B \div A = A \div B$.

Наприклад, $\{a, b, c\} \div \{a, c, d\} = \{b, d\}$.

2.3.5 Доповнення множини

Операція доповнення передбачає наявність деякого універсуму, скажімо, U, який включає всі розглядувані множини. Тоді *доповнення* $\overline{A}$ множини A задається виразом $\overline{A} = U \dot{-} A$.

Тобто, $\overline{A}$ містить всі елементи з універсуму U, які не належать A. Тому $\overline{U} = \varnothing$ і $\overline{\varnothing} = U$.

Наприклад, якщо унінерсум $U = \{a, b, c, d\}$, то
$\overline{\{a, b, c\}} = \{d\}$.

2.4 Властивості операцій над множинами

Нехай задано універсум U. Тоді для множин $A, B, C \in U$ виконуються такі тотожності:

1) *ідемпотентність*: $A \cup A = A, A \cap A = A$;
2) *комутативність*: $A \cup B = B \cup A, A \cap B = B \cap A$;
3) *асоціативність*: $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$;
4) *поглинання*: $(A \cap B) \cup A = A, (A \cup B) \cap A = A$;
5) *дистрибутивність*: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
6) *закони де Моргана*: $\overline{A \cup B} = \overline{A} \cap \overline{B}, \overline{A \cap B} = \overline{A} \cup \overline{B}$;
7) *властивості нуля (пустої множини)*: $A \cup \varnothing = A$, $A \cap \varnothing = \varnothing$, $\overline{\varnothing} = U$;
8) *властивості одиниці (універсума)*: $A \cup U = U$, $A \cap U = A, \overline{U} = \varnothing$;
9) *інволютивність*: $\overline{\overline{A}} = A$;
10) *властивості доповнення*: $A \cup \overline{A} = U, A \cap \overline{A} = \varnothing$;
11) *вирази для різниці*: $A \dot{-} B = A \cap \overline{B}$, $A \dot{-} B = \overline{\overline{A} \cup B}$.

Формальне доведення перерахованих тотожностей повинно базуватися на визначенні рівності множин, оскільки досі жодну тотожність, якою можна було б скористатися, ще не було доведено. Як приклад доведемо перший закон де Моргана, показавши, що його ліва частина включається в праву, і навпаки.

Нехай $x \in \overline{A \cup B}$. Тоді $x \notin (A \cup B)$ і, отже, $x \notin A$ і $x \notin B$, що означає, що $x \in \overline{A}$ і $x \in \overline{B}$. Тобто, $x \in (\overline{A} \cap \overline{B})$ і, тим самим, $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$.

У зворотний бік. Нехай $x \in \overline{A} \cap \overline{B}$, тобто $x \in \overline{A}$ і $x \in \overline{B}$. Останнє означає, що $x \notin A$ і $x \notin B$. Тому $x \notin (A \cup B)$. Тобто,

$x \in \overline{A \cup B}$ і, тим самим, $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$.

Остаточно маємо $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Встановивши тотожності (1)-(11), тепер можна послідовно користуватися ними для проведення *тотожних теоретико-множинних перетворень одного виразу*, що складається з символів, що позначають множини, деяких знаків, що позначають теоретико-множинні операції, і, можливо, символів пустої множини і універсуму, та *задає деяку множину, в інший вираз, що задає ту ж саму множину.* Тобто, використовуючи (1)–(11), для одній і тій же множини можна отримувати різні теоретико-множинні вирази, що задають цю множину. Значить, можна вирішувати *задачу спрощення вихідного виразу* з метою отримання найпростішого в якомусь сенсі теоретико-множинного виразу, що задає ту саму множину, що і вихідний вираз.

Як приклад розглянемо наступний ланцюжок застосувань деяких з тотожностей (1)–(11): $\overline{(A \cup \overline{B}) \cap B} \div A =$ ⟨на підставі (11)⟩ $(A \cup \overline{B}) \cap B \cap \overline{A} =$ ⟨на підставі (6)⟩ $((A \cup \overline{B}) \cup \overline{B}) \cap \overline{A} =$ ⟨на підставі (6)⟩ $((\overline{A} \cap \overline{\overline{B}}) \cup \overline{B}) \cap \overline{A} =$ ⟨на підставі (9)⟩ $((\overline{A} \cap B) \cup \overline{B}) \cap \overline{A} =$ ⟨на підставі (2)⟩ $(\overline{B} \cup (\overline{A} \cap B)) \cap \overline{A} =$ ⟨на підставі (5)⟩ $((\overline{B} \cup \overline{A}) \cap (\overline{B} \cup B)) \cap \overline{A} =$ ⟨на підставі (10)⟩ $((\overline{B} \cup \overline{A}) \cap U) \cap \overline{A} =$ ⟨на підставі (8)⟩ $(\overline{B} \cup \overline{A}) \cap \overline{A} =$ ⟨на підставі (4)⟩ $\overline{A}$. (Очевидно, що $\overline{A}$ не може бути далі спрощеним.)

Маємо, що вирази $\overline{(A \cup \overline{B}) \cap B} \div A$ і $\overline{A}$ визначають одну і ту ж множину. (Те ж саме можна сказати і про всі проміжні вирази, отримані в процесі переходу від $\overline{(A \cup \overline{B}) \cap B} \div A$ до $\overline{A}$.)

Також зазначимо, що, виходячи з (7), першого закону де Моргана і (11) ((7), другого закону де Моргана і (11)), будь-який теоретико-множинний вираз, побудований зі змінних, символів для універсуму і пустої множини, а також із будь-яких знаків теоретико-множинних операцій, може бути подано у вигляді тотожно рівного йому виразу, побудованого з тих самих змінних, символу для універсуму або символу пустої множини і знаків тільки двох операцій — об'єднання та доповнення (перетину та доповнення).

Якщо уважно проаналізувати операції над множинами, введені до цього, можна побачити, що вони мають таку особливість: результат їх застосування до одної множини A (взяття доповнення) або до двох множин A і B (інші операції) є множиною, яка

містить всі або деякі елементи, що утворюють A та/або B та/або їх доповнення. Однак у теорії множин є дві операції, що відіграють дуже важливу роль у багатьох математичних побудовах, які (у загальному випадку) такої властивості не мають. Саме їх розгляду присвячені два наступні розділи.

2.5 Декартів (прямий) добуток множин

Декартовим (прямим) добутком множин A і B (записується $A \times B$) називається множина всіх впорядкованих пар $\langle a, b\rangle$, в яких перший компонент належить множині A ($a \in A$), а другий - множині B ($b \in B$). Тобто $A \times B = \{\langle a, b\rangle \mid a \in A \text{ і } b \in B\}$.

Бінарна операція декартового добутку неасоціативна і некомутативна, тобто множини $(A \times B) \times C$ і $A \times (B \times C)$, а також множини $A \times B$ і $B \times A$, взагалі кажучи, нерівні між собою.

Декартів добуток природно узагальнюється на випадок довільної скінченної сукупності множин. Якщо $A_1, A_2, \ldots, A_n$ — множини, то їхнім *декартовим (прямим) добутком* називається множина

$$D = \{\langle a_1, a_2, \ldots, a_n\rangle \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\},$$

яка складається з усіх наборів (n-ок) $\langle a_1, a_2, \ldots, a_n\rangle$, в кожному з яких i-й член, що називається *i-ю координатою*, або *i-м компонентом* набору, належить множині A_i, $i = 1, 2, \ldots, n$. Декартів добуток позначається через $A_1 \times A_2 \times \ldots \times A_n$.

Набір $\langle a_1, a_2, \ldots, a_n\rangle$, щоб відрізнити його від множини, яка складається з елементів $a_1, a_2, \ldots, a_n$, записують не у фігурних, а в кутових дужках і називають *кортежем, вектором*, або *впорядкованим набором. Довжиною* кортежу називають кількість його координат. Два кортежі $\langle a_1, a_2, \ldots, a_n\rangle$ і $\langle b_1, b_2, \ldots, b_n\rangle$ однакової довжини вважаються рівними тоді і тільки тоді, коли рівні їхні відповідні координати, тобто $a_i = b_i$, $i = 1, 2, \ldots, n$. Отже, кортежі $\langle a, b, c\rangle$ і $\langle a, c, b\rangle$ вважаються різними, в той час як множини $\{a, b, c\}$ і $\{a, c, b\}$ — рівні між собою.

Проекцією на i-у вісь (або *i-ою проекцією*) кортежу $w = \langle a_1, a_2, \ldots, a_n\rangle$ називається i-а координата a_i кортежу w; позначається $Pr_i(w) = a_i$.

Декартів добуток множини A на себе n разів, тобто множи-

ну $A \times A \times \ldots \times A$ (тут A зустрічається n разів) називають n-*м декартовим* (або *прямим*) *степенем* множини A і позначають A^n.

Прийнято вважати, що за визначенням, коли $n = 0$, $A^0 = \varnothing$, і що коли $n = 1$, $A^1 = A$.

Наприклад, якщо $A = \{a, b\}$ і $B = \{b, c, d\}$, то

$A \times B = \{\langle a, b\rangle, \langle a, c\rangle, \langle a, d\rangle, \langle b, b\rangle, \langle b, c\rangle, \langle b, d\rangle\}$,

$A^2 = \{\langle a, a\rangle, \langle a, b\rangle, \langle b, a\rangle, \langle b, b\rangle\}$.

Якщо $\mathbf{R}$ — множина дійсних чисел, або,іншими словами, множина точок координатної прямої, то $\mathbf{R}^2$, тобто множина $\{\langle a, b\rangle \mid a, b \in \mathbf{R}\}$, є множина точок *координатної* (*декартовій*) площині.

Координатне зображення точок площини вперше було запропоновано французьким математиком і філософом Рене Декартом, тому введена теоретико-множинна операція і називається декартовим добутком.

2.6 Булеан і алгебри множин

Інший операцією, яка, виходячи з наявної множини A, будує нову множину, так званий булеан 2^A, що містить елементи, відмінні від елементів A, є взяття всіх підмножин множини A.

Формально 2^A задається так:

$2^A = \{B \mid B \subseteq A\}$.

З цього визначення випливає, що $\varnothing \in 2^A$ і $A \in 2^A$.

Так, для множини $A = \{a, b\}$ маємо, що 2^A містить 4 елементи: $\varnothing, \{a\}, \{b\}, \{a, b\}$. Тобто $2^A = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$.

Загальніше. Якщо множина A містить n елементів, де n — будь-яке натуральне число, то 2^A містить 2^n елементів.

Саме останній факт "виправдовує" те, що 2^A використовується для позначення булеану будь-якої множини A безвідносно до кількості елементів у A.

Для того, щоб довести вищеозначену формулу про кількість всіх підмножин (скінченної) множини A з n елементами, довільній множині $B \subseteq A$ поставимо у відповідність впорядкований двійковий кортеж $\langle b_1, b_2, \ldots, b_n\rangle$, для якого $b_i \in \{0, 1\}$ та $b_i = 1$ тоді і тільки тоді, коли $a_i \in B$, $i = 1, \ldots, n$. Очевидно, що кожній підмножині $B \subseteq A$ відповідає один і тільки один такий кортеж (наприклад, пу-

стій множині $\varnothing$ відповідає $\langle 0, 0, \ldots, 0\rangle$, а множині A — $\langle 1, 1, \ldots, 1\rangle$, і навпаки. Оскільки b_i приймає 0 або 1, то кількість всіх впорядкованих наборів з n елементів зазначеного виду дорівнює 2^n. Значить, 2^A містить в точності 2^n елементів.

Як бачимо, у випадку будь-якого натурального числа n кількість елементів у множині A (із n елементами) завжди менше за кількість елементів у 2^A ($n < 2^n$). Ця ситуація зберігається і в разі множини з довільним числом елементів, про що свідчить теорема Кантора з розділу, наведеного нижче і присвяченого порівнянню множин (що вимагає уточнення, яке і робиться далі) з довільною кількістю елементів.

Алгеброю множин називається будь-яка непуста сукупність множин, замкнена відносно операцій об'єднання і взяття доповнення (і, як наслідок, відносно всіх теоретико-множинних операцій) у припущенні, що зафіксований деякий універсум U, який включає в себе всі множини сукупності. (Замкненість означає, що об'єднання двох множин із сукупності і доповнення множини із сукупності належать цій сукупності.)

Алгебра множин на булеані 2^A множини A, коли A розглядається як універсум, називається *булевою алгеброю підмножин* множини A. Вона відіграє важливу роль у багатьох математичних теоріях.

2.7 Порівняння множин

Одним із основних досягнень канторівської теорії множин є поширення поняття "кількість елементів" зі скінченних множин на нескінченні та формулювання принципу, за яким можна порівнювати за "кількістю елементів" нескінченні множини. Зокрема, несподіваним та незвичайним виявився той факт, що різні нескінченні множини можуть мати різну "кількість елементів", тобто для нескінченностей також існує своя ієрархія.

Канторівська ідея грунтується на такому спостереженні: для того, щоб порівняти за кількістю елементів дві скінченні множини, зовсім не обов'язково перераховувати кількість елементів у кожної з них. Можна діяти таким чином. Наприклад, нехай необхідно порівняти за кількістю дві множини — множину S студентів та множи-

ну M всіх місць в аудиторіях університету. Запропонуємо кожному студентові зайняти одне місце. Якщо кожен студент отримає місце і при цьому в аудиторіях не залишиться жодного вільного місця, то очевидно, що кількість елементів в обох множинах S і M однакова. В іншому випадку множина S містить більше елементів, ніж множина M, або навпаки. Очевидно, що запропонована процедура встановлює деяку функціональну відповідність між множинами S і M. У першому випадку ця відповідність вказує на рівність елементів у множинах (без їх перерахування), в той час як у другому і третьому випадках або порушується умова повної визначеності (принаймні один студент не дістав місця), або порушується умова так званої сюр'єктивності відповідності (хоча б одне місце залишилося вільним).

У математиці ця ідея реалізується таким чином.

Будемо говорити, що між множинами A і B можна встановити *взаємно однозначну відповідність* f, якщо кожному елементу множини A можна співвіднести один і тільки один елемент множини B, і навпаки, якщо кожному елементу множини B можна співвіднести один і тільки один елемент множини A. При цьому f зручно подати у вигляді декартового добутку $A \times B$ із зазначеними вище обмеженнями на елементи множин A і B.

Якщо f — взаємно однозначна відповідність між A і B ($f = A \times B$) та $C \subseteq A$, то $f(C) = \{\langle c, b\rangle \mid c \in C\}$.

Множини A і B називаються *рівнопотужними*, або *однакової потужності* ($A \backsim B$) тоді і тільки тоді, коли існує взаємно однозначна відповідність між множинами A і B.

Безпосередньо з визначення рівнопотужності випливають такі її властивості:

1) $A \backsim A$ (рефлексивність рівнопотужності);

2) Якщо $A \backsim B$, то $B \backsim A$ (симетричність рівнопотужності);

3) Якщо $A \backsim B$ і $B \backsim C$, то $A \backsim C$ (транзитивність рівнопотужності).

Наведемо декілька прикладів рівнопотужних нескінченних множин.

– Множина натуральних чисел $\mathbf{N}$ рівнопотужна множині $\mathbf{N}_2 = \{0, 1, 4, 9, 16, \ldots\}$, яка складається з квадратів натуральних чисел. Необхідна взаємно однозначна відповідність встановлюєть-

ся за законом, що числу n відповідає число n^2 ($n \in N$, $n^2 \in \mathbf{N}_2$).

– Множина $\mathbf{Z}$ всіх цілих чисел рівнопотужна множині P всіх парних чисел. Тут взаємно однозначна відповідність встановлюється таким чином: числу n відповідає $2n$, ($n \in \mathbf{Z}$, $2n \in P$).

– Множина усіх точок інтервалу $(-\pi/2, +\pi/2)$ рівнопотужна множині точок дійсної прямої. Шукана взаємно однозначна відповідність встановлюється за допомогою тригонометричної функції tg: числу x відповідає $tg(x)$, ($x \in (-\pi/2, +\pi/2), tg(x) \in (-\infty, +\infty)$).

– Неважко встановити рівнопотужність двох довільних відкритих інтервалів) дійсної прямої, звідки можна зробити висновок, що будь-який відкритий інтервал рівнопотужний інтервалу $(-\pi/2, +\pi/2)$ і, отже, з використанням транзитивності рівнопотужності, рівнопотужний усій прямій.

2.7.1 Скінченні і нескінченні множини

Маючи засіб для порівняння множин з точки зору їх рівнопотужності, можна дати таки визначення скінченності і нескінченності, беручи до уваги, що звичайна людина вважає деяку сукупність об'єктів скінченною, якщо вона може всі об'єкти послідовно перерахувати за скінченний відрізок часу.

Множина є *скінченною* тоді і тільки тоді, коли для деякого натурального числа n вона рівнопотужна початковому відрізку натурального ряду $[n]$. В цьому випадку n називається *потужністю скінченної множини* та говориться, що *множина має скінченну потужність* n. В інших випадках множина, що розглядається, вважається *нескінченною*.

Серед інших визначень скінченності і нескінченності відмітимо те, яке не суперечить введеному і належить Р. Дедекінду, який пропонував *вважати нескінченною множиною таку множину, яка рівнопотужна своїй деякої власній підмножині*, спираючись на те, що тільки скінченні, в життєвому розумінні, множини не задовольняють цій властивості.

Прикладами скінченних множин можуть бути будь-які сукупності об'єктів реального світу, оскільки, відповідно до сучасних космологічних моделей, вважається, що ми живемо в скінченному, з фізичної точки зору, Всесвіту.

Прикладами нескінченних сукупностей є множини натуральних чисел ($\mathbf{N}$), цілих чисел ($\mathbf{Z}$), раціональних чисел ($\mathbf{Q}$), дійсних чисел ($\mathbf{R}$), комплексних чисел ($\mathbf{C}$), будь-які інтервали дійсних чисел, вся дійсна пряма і т. д.

Очевидно, що множина натуральних чисел $\mathbf{N}$ рівнопотужна будь-якої своєї підмножині, яка утворюється видаленням з $\mathbf{N}$ якого початкового відрізка. Множина $\mathbf{N}$ нескінченна. Значить, і множина натуральних чисел без нуля $\mathbf{N}_+$ нескінченна. Оскільки будь-який початковий відрізок натурального ряду має власне включення в нескінченну кількість інших попарно різних початкових відрізків натурального ряду, отримуємо, що існує нескінченна сукупність скінченних множин, і між цією сукупністю і $\mathbf{N}_+$ очевидним чином встановлюється взаємооднозначна відповідність. Тому природно постає питання: чи всі нескінченні множини рівнопотужні? Далі буде дано негативну відповідь на нього з дуже цікавими наслідками.

2.7.2 Властивості операцій над скінченними множинами

Цей розділ присвячений найпростішим властивостями скінченних множин, які виникають при виконанні основних теоретико-множинних операцій. Нас буде цікавити питання про те, виводять чи ні розглянуті вище операції над скінченними множинами з класу скінченних множин (який містить універсум U).

Оскільки довільна підмножина скінченної множини також скінченна, то результатом операції, яка призводить до породження підмножини деякої скінченної множини, є скінченна множина. Значить, перетин і теоретико-множинна різниця множин є скінченною множиною: ми маємо, що $(A \cap B) \subseteq A$ і $(A \dot{-} B) \subseteq A$.

Звідси випливає, що для будь-якої скінченної множин A її доповнення $\overline{A} = U \dot{-} A$ скінченне.

Для скінченних множин A і B, що не перетинаються, можна вказати таки натуральні числа n і m, що $A \sim [n]$ і $B \sim [m]$. Це означає, що елементи A і B можна перенумерувати натуральними числами, починаючи з 1, і, наприклад, написати, що $A = \{a_1, \ldots, a_n\}$ і $B = \{b_1, \ldots, b_m\}$. Так як A і B не перетинаються, то $A \cup B = \{a_1, \ldots, a_n, b_1, \ldots, b_m\}$, де $a_1, \ldots, a_n, b_1, \ldots, b_m$ є попарно

різними елементами. Значить, $A \cup B \sim [n+m]$, тобто множина $A \cup B$ скінченна в цьому випадку.

Нехай $A \cap B \neq \varnothing$. Покладемо $C = A \cap B$. Тоді $A \cup B = A \cup (B \dot{-} C)$ і $A \cap (B \dot{-} C) = \varnothing$. Множина C скінченна, як і множина $B \dot{-} C$ (див. вище), і в силу попереднього абзацу маємо, що множина $A \cup (B \dot{-} C) = A \cup B$ також скінченна.

Остаточно маємо, що об'єднання $A \cup B$ скінченне незалежно від того, перетинаються чи ні множини A і B.

Симетрична різниця задається формулою $A \div B = (A \cup B) \dot{-} (A \cap B)$, з якої, з урахуванням вищенаведених результатів, отримуємо її скінченність в разі скінченності A і B.

Нехай $A = \{a_1, \ldots, a_n\}$ і $B = \{b_1, \ldots, b_m\}$ — скінченні множини. тоді їх декартів добуток $A \times B = \{\langle a_1, b_1\rangle, \ldots \langle a_1, b_m\rangle, \ldots, \langle a_n, b_1\rangle, \ldots, \langle a_n, b_m\rangle\}$. Цей запис $A \times B$ показує, що $(A \times B) \sim [n * m]$. значить, множина $A \times B$ скінченна. Звідси автоматично випливає скінченність будь-якого скінченного декартова добутка множин.

Раніше в розділі про булеан і алгебри множин було показано, що якщо A складається з n елементів, то 2^A містить в точності 2^n елементів. Значить, $2^A \sim [2^n]$ і, отже, множина 2^A скінченна.

Ми показали, що всі введені *теоретико-множинні операції над множинами не виводять з класу скінченних множин, якщо вони застосовуються тільки до скінченних множин.* У разі ж нескінченних множин ситуація дещо інша.

2.7.3 Зліченні множини

Множина A, рівнопотужна множині $\mathbf{N}_+$ натуральних чисел, називається *зліченною множиною*. Множина, відмінна від скінченної або зліченної множини, є *незліченною*.

Тобто, зліченна множина A — це така множина, всі елементи якої можна пронумерувати числами $1, 2, 3, \ldots$, тобто можна вказати спосіб, за яким першому елементу множини A ставиться у відповідність число 1, другому — число 2 і т. д. Отже, будь-яку зліченну множину A можна подати у вигляді послідовності

$A = a_1, a_2, a_3, \ldots, a_n, \ldots$

Неважко переконатися, що множина $\mathbf{N}$, а також множини квадратів натуральних чисел, усіх парних чисел, усіх непарних чи-

сел, чисел, кратних деякому числу k, простих чисел тощо є зліченними множинами.

Перейдемо до формулювання деяких властивостей злічених множин.

Твердження 2.1. Будь-яка нескінченна множина включає зліченну підмножину.

Доведення. Нехай M — нескінченна множина. Тоді в M можна взяти два різних елементи a_1, b_1. Очевидно, множина $M \dot{-} \{a_1, b_1\}$ є нескінченною. Тоді візьмемо наступні два нові елементи $a_2, b_2 \in (M \dot{-} \{a_2, b_2\})$, де $a_2 \neq b_2$, і т. д. Т аким чином, ми виділимо з множини M дві злічені (рівнопотужні) множини $A = \{a_1, a_2, \ldots, a_n, \ldots\} \in M$ і $B = \{b_1, b_2, \ldots, b_n, \ldots\} \in M$. Це не тільки завершує доведення, а і дозволяє підсилити властивість нескінченних множин із твердження. А саме: будь-яка нескінченна множина M включає в себе таку зліченну підмножину A, що $M \dot{-} A$ є нескінченною множиною (оскільки $B \subseteq (M \dot{-} A)$). *Кінець доведення.*

Твердження 2.2. Будь-яка підмножина зліченної множини є або скінченною, або зліченною множиною.

Доведення. Нехай $A = \{a_1, \ldots, a_n, \ldots\}$ — зліченна множина і $B \subseteq A$. Отже, B можна записати у вигляді множини $\{a_{i_1}, a_{i_2}, \ldots, a_{i_n}, \ldots\}$ і можливі дві ситуації: або послідовність у фігурних дужках уривається на деякому елементі, тоді B — скінченна множина, або послідовність у дужках нескінченна, для якої, встановлюючи відповідність між a_j та a_{i_j}, одержуємо, що B — зліченна множина. *Кінець доведення.*

З цього твердження, зокрема, випливає, що злічені множини є певною мірою найпростішими нескінченними множинами, бо, з одного боку, вони можуть включатися в інші нескінченні множини, а з другого — вони містять в собі тільки скінченні або злічені множини.

Надалі, в доведеннях деяких важливих тверджень, ми не зможемо обійтися без застосування так званої аксіоми вибору, яка відіграє важливу роль не тільки в теорії множин, а і у математичному аналізу та теорії міри. Розглянемо її.

2.7.4 Аксіома вибору

У математичних доведеннях нерідко доводиться вдаватися до "ідеалізованої" побудови функції наступного типу. Нехай для кожного елемента i скінченної або нескінченної множині (індексів) I задано непуста множина S_i. Вибравши в кожному з множин S_i певний елемент s_i, ми можемо наступним чином задати функцію f, визначену на множині I і таку, що $f(i) \in S_i$ для всіх $i \in I$: $f(i) = s_i$.

Ця функція f називається *функцією вибору* для сімейства множин S_i з індексами $i \in I$ і, по суті, у наведеної побудові використаний наступний загальний принцип – знаменита аксіома вибору:

Аксіома вибору (AC). До всякого сімейства $\{S_i \mid i \in I\}$ непустих множин S_i будь-якої природи існує функція вибору.

Цей принцип, вперше явно сформульований Е. Цермело в 1904 р. для доведення теореми про можливість цілком впорядкувати будь-ку множину (див. розділ про відношення), було новим для математики того часу, бо існування математичних об'єктів зазвичай розумілося як можливість пред'явити конкретний об'єкт з необхідними властивостями. А у випадку функції вибору f, існування якої постулюється аксіомою вибору, у загальному випадку рівно нічого не відомо, і навіть в принципі не можна поставити питання, чому дорівнює значення $f(i)$ для конкретних індексів i. Тому аксіома вибору негайно стала об'єктом критики з боку багатьох видатних математиків, наприклад Е. Бореля та А. Лебега. Пізніше (Л. Брауер, Н. Н. Лузін та ін.) головною причиною критики аксіоми почав виступати її неконструктивний характер, тобто те, що її формулювання не містить ніяких вказівок на закон, згідно з яким здійснюється конкретний вибір елемента $f(i) = s_i$ в кожному з множин S_i, що складають сімейство, яке розглядається.

Втім, в деяких спеціальних випадках для побудови функції вибору немає потреби вдаватися до (AC). Наприклад, якщо кожна множина S_i містить всього один елемент s_i, то візьмемо цей елемент в якості $f(i)$ і отримаємо єдину в даному випадку функцію вибору. Інший випадок: якщо всі множини S_i є непустими скінченними множинами дійсних чисел або довільними непустими множинами натуральних чисел, то в якості $f(i)$ можна взяти найменший елемент множини S_i.

Існування функції вибору не викликає заперечень і в тому випадку, коли множина індексів I є скінченною. Один з аргументів проти необмеженого використання аксіоми вибору (при нескінченної множині I індексів) полягав у тому, що "людський розум" не в змозі здійснити нескінченне число актів вибору елементів у непустих множинах даного сімейства, не маючи закону, по якому слід вибирати елементи. Щоб зрозуміти роль і місце аксіоми вибору (AC) в будівлі сучасної математики, найкраще розглянути ті математичні міркування, в яких використовується ця аксіома.

Фахівці, інтереси яких лежать далеко від теорії множин або теоретико-множинної топології, часто асоціюють роль аксіоми вибору з побудовою різного роду "парадоксальних" множин, начебто невимірної за Лебегом множини дійсних чисел або розбиття кулі на скінченне число частин, з яких без накладень і пустот складаються дві кулі того ж радіуса. На цей підставі іноді робиться висновок, що аксіома вибору, по суті, не потрібна в "справжній" математики, а всі пов'язані з цією аксіомою дискусії носять чисто схоластичний, кабінетний характер. Насправді ж ми не можемо обійтися без її застосування у багатьох доведеннях, наприклад, у доведеннях таких важливих тверджень з теорії множин, що наведені нижче.

2.7.5 Властивості зліченних множин

Наступна властивість, яку неможливо довести без аксіоми вибору, дозволяє отримати зліченність ряду важливих множин.

Твердження 2.3. Об'єднання скінченної або зліченної сукупності зліченних множин є зліченною множиною.

Доведення. Розглянемо не більше ніж зліченне сімейство зліченних множин:

$X_1 = \{x_{1,1}, x_{1,2}, x_{1,3}, \ldots\}$,
$X_2 = \{x_{2,1}, x_{2,2}, x_{2,3}, \ldots\}$,
$\ldots$,
$X_n = \{x_{n,1}, x_{n,2}, x_{n,3}, \ldots\}$,
$\ldots$

Елементи об'єднання X всіх множин X_i можна розташувати в послідовність наступним простим способом:

$$x_{1,1}, x_{1,2}, x_{2,1}, x_{1,3}, x_{2,2}, x_{3,1}, \ldots, x_{1,n}, x_{2,n-1}, \ldots, x_{n,1}, \ldots$$

(Тобто, елементи $x_{i,j}$ множини X організуються в блоки з однаковою сумою індексів $i+j$, що слідують один за одним у порядку зростання $i+j$; при цьому, порядок усередині кожного блоку відповідає зростанню індексу i.) Значить, ми маємо можливість перенумерувати натуральними числами з $\mathbf{N}_+$ всі елементи множини X, що говорить про те, що множини $\mathbf{N}_+$ і X рівнопотужні. Тобто, X - зліченна множина. *Кінець доведення.*

Аналізуючи це доведення, ми бачимо, що кожна множина X_i допускає нескінченно багато засобів перерахування своїх елементів наведеного вигляду. У той же час, зазначений запис множини X передбачає, що для кожної множини X_i зафіксовано якраз *одне*, конкретне перерахування вказаного вигляду, яке і вибирає "потрібний" елемент з X_i. Таким чином, тут, по-суті, йдеться про використання функції вибору для сімейства $X_1, X_2, \ldots$, і, таким чином, аксіома вибору відіграє визначальну роль у доведенні твердження.

З нього випливає низка цікавих наслідків.

Твердження 2.4. Скінченний декартів добуток $A_1 \times \ldots \times A_n$ зліченних множин $A_1, \ldots, A_n$ $(n \geqslant 2)$ є зліченною множиною.

Доведення. Індукція по n. В силу очевидного індукційного переходу справедливість даного твердження досить встановити для $n = 2$. Його ж істинність випливає з того, що множину всіх пар $(a_i, b_j) \in A_1 \times A_2$, де $A_1 = \{a_1, a_2, \ldots, a_m, \ldots\}$ і $A_2 = \{b_1, b_2, \ldots, b_k, \ldots\}$ можна подати як об'єднання такої зліченної сукупності зліченних множин

$$B_1 = \{(a_1, b_1), (a_1, b_2), \ldots, (a_1, b_k), \ldots\},$$
$$B_2 = \{(a_2, b_1), (a_2, b_2), \ldots, (a_2, b_k), \ldots\},$$
$$\ldots$$
$$B_m = \{(a_m, b_1), (a_m, b_2), \ldots, (a_m, b_k), \ldots\},$$
$$\ldots$$

яка є зліченною множиною у силу твердження 2.3. *Кінець доведення.*

Як наслідок маємо, що, множина всіх точок координатної площини з раціональними координатами зліченна.

Також на базі твердження 2.3 нетрудне довести, що множина Σ^* всіх слів у заданому скінченному алфавіті Σ зліченна.

Дійсно, $\Sigma^* = \{e\} \cup \Sigma_1^* \cup \ldots \cup \Sigma_m^* \cup \ldots$, де e – пусте слово і

Σ_m^* – множина всіх слів із m символів алфавіта Σ ($m = 1, 2, \ldots$).

Твердження 2.5. Множина $\mathbf{Z}$ всіх цілих чисел зліченна.

Доведення. Подамо множину $\mathbf{Z}$ у вигляді об'єднення $\mathbf{N} \cup \{-1, -2, -3, \ldots\}$. Множина $\mathbf{N}$ зліченна. Очевидно, що і множина $\{-1, -2, -3, \ldots\}$ зліченна. Тому, у силу твердження 2.3, $\mathbf{Z}$ є зліченною множиною. *Кінець доведення.*

Числова множина W називається *щільною* тоді і тільки тоді, коли для будь-якої пари чисел $a, b \in W$ $(a < b)$ завжди існує число $c \in W$ таке, що $a < c < b$.

Безпосередньо з означення випливає, що щільна множина W завжди є нескінченною. Більш того, для кожної пари чисел $a, b \in W$ існує безліч чисел $c \in W$, для яких виконується $a < c < b$.

Очевидно, що множина $\mathbf{Z}$ цілих чисел, а також будь-яка її підмножина (зокрема, множина $\mathbf{N}$ натуральних чисел з нулем) — не щільні. У той же час множина $\mathbf{Q}$ раціональних чисел є щільною множиною. Справді, для будь-яких раціональних чисел r_1 і r_2 $(r_1 < r_2)$ число $r = (r_1 + r_2)/2$ задовольняє нерівності $r_1 < r < r_2$. Зокрема, для всіх чисел r' з нескінченної множини раціональних чисел $\{r_1 + (r_2 - r_1)/2^i \mid i = 1, 2, \ldots\}$ виконуються нерівності $r_1 < r' < r_2$.

Здавалося б, зі щільності множини раціональних чисел повинно було б випливати, що ця множина має більшу потужність, ніж множина $\mathbf{N}$ або множина $\mathbf{Z}$. Однак має місце таке твердження, яке є наслідок твердження 2.3.

Твердження 2.6. Множина $\mathbf{Q}$ всіх раціональних чисел зліченна.

Доведення. Множину $\mathbf{Q}$ можна подати як об'єднання таких зліченних множин:

$A_1 = \{0, -1, 1, -2, 2, -3, 3, \ldots\}$ – дроби вигляду $q/1 (= q), q \in \mathbf{Z}$ (тобто усі цілі числа),

$A_2 = \{0/2, -1/2, 1/2, -2/2, 2/2, -3/2, 3/2, \ldots\}$ – дроби вигляду $q/2, q \in \mathbf{Z}$,

$A_3 = \{0/3, -1/3, 1/3, -2/3, 2/3, -3/3, 3/3, \ldots\}$ – дроби вигляду $q/3, q \in \mathbf{Z}$,

$\ldots$,

$A_k = \{0/k, -1/k, 1/k, -2/k, 2/k, -3/k, 3/k, \ldots\}$ – дроби вигляду $q/k, q \in \mathbf{Z}$,

...

У силу твердження 2.3 маємо зліченность $\mathbf{Q}$. *Кінець доведення.*

Розглянемо множину P усіх многочленів $p(x) = a_n * x^n + a_{n-1} * x^{n-1} + \ldots + a_1 * x + a_0$ з раціональними коефіцієнтами ($a_i \in \mathbf{Q}$, $i = 0, 1, \ldots, n$, $n = 0, 1, 2, \ldots$).

Множину P можна подати у вигляді об'єднання зліченної сукупності множин P_n, де P_n — це множина многочленів з раціональними коефіцієнтами, степінь яких не перевищує n, $n = 0, 1, 2, \ldots$ Разом тим, будь-якому многочлену $p(x) = a_n * x^n + a_{n-1} * x^{n-1} + \ldots + a_1 * x + a_0$ з множини P_n можна поставити у відповідність кортеж $\langle a_n, a_{n-1}, \ldots, a_1, a_0 \rangle$, який складається з раціональних чисел a_i — коефіцієнтів цього многочлена. Очевидно, ця відповідність є взаємно однозначною. Тобто, $P_n \backsim \mathbf{Q}^{n+1}$. Тоді з твердження 2.4 випливає, що множина P_n — зліченна, а тому зліченною є і множина P.

Назвемо число *алгебраїчним*, якщо воно є коренем деякого многочлена з раціональними коефіцієнтами. Відомо, що кожен такий многочлен має скінченну кількість коренів (не більшу від степеня многочлена). Таким чином, множину всіх алгебраїчних чисел можна подати у вигляді об'єднання зліченної сукупності скінченних множин. Отже, має місце наступний факт.

Твердження 2.7. Множина всіх алгебраїчних чисел зліченна.

Після розгляду зліченности множин і деяких прикладів зліченних множин логічне випливає припущення про рівнопотужність усіх нескіченних множин: чи всі нескінченні множини зліченні, або чи існують нескінченні множини, які не будуть зліченними? Дослідженню цього питання присвячено наступній розділ.

2.7.6 Незліченні множини

Факт існування множин, які не є зліченними (незліченних множин), вперше був встановлений Г. Кантором за допомогою запропонованого ним діагонального методу, який набув згодом фундаментального значення в різних розділах математики. Зокрема, цей метод лежить в основі доведення такого твердження про існування незліченних множин, яке належить Г. Кантору.

Твердження 2.8. Множина всіх чисел x, таких, що $0 < x < 1$ (тобто тих, що належать відкритому інтервалу $(0,1)$) є незліченною.

Доведення. Припустімо, що це твердження хибне і множина всіх дійсних чисел, що розглядаються, зліченна. Значить, можна встановити взаємно однозначну відповідність між ними і натуральними числами $1, 2, 3, \ldots$. Тобто, іншими словами, існує нумерація цих чисел, скажімо, $x_1, x_2, \ldots, x_n, \ldots$. Перепишемо їх у вигляді нескінченних десяткових дробів в порядку їх нумерації:

$$x_1 = 0, a_{11}a_{12}a_{13}\ldots a_{1n}\ldots$$
$$x_2 = 0, a_{21}a_{22}a_{13}\ldots a_{2n}\ldots$$
$$x_3 = 0, a_{31}a_{32}a_{33}\ldots a_{3n}\ldots$$
$$\ldots$$
$$x_n = 0, a_{n1}a_{n2}a_{n3}\ldots a_{nn}\ldots$$
$$\ldots$$

Звертаємо увагу на те, що при цьому використовується угода, яка наведена в розділі про дійсні числа після твердження 1.4, згідно з якою можна вважати, що всі дійсні числа мають вигляд нескінченного десяткового запису і зустрічаються у зазначеному вище перелику тільки один раз.

Тепер, рухаючись по діагоналі від a_{11} до a_{22}, від a_{22} до a_{33} і т. д., утворимо новий нескінченний десятковий дріб $y = 0, b_1b_2\ldots b_n\ldots$, вибираючи цифри $b_1, b_2, \ldots, b_n, \ldots$ довільним чином, але з додержанням таких умов: $b_1 \neq a_{11}, b_2 \neq a_{22}, \ldots, b_n \neq a_{nn}, \ldots$. Додатково, щоб уникнути ситуації з можливістю зображення одного й того ж раціонального числа у двох формах, будемо вибирати цифри b_i так, щоб $b_i \neq 0$ і $b_i \neq 9$, $i = 1, 2, \ldots$ (що легко зробити тому, що у нас є десять цифр для зображення дійсних чисел у десятковому запису).

Утворений дріб y є записом деякого дійсного числа між 0 і 1. З побудови y дроби y і x_n відрізняються принаймні n-ю цифрою після коми ($n = 1, 2, \ldots$). Тому y не належить розглядуваній зліченної множені $\{x_1, \ldots, x_n, \ldots\}$. Отримуємо протиріччя з припущенням. Отже, множина всіх розглядаємих дійсних чисел незліченна. *Кінець доведення.*

Будь-яка множина, рівнопотужна множині всіх дійсних чисел x, що знаходяться між числами 0 і 1 ($0 < x < 1$), називається

континуальною, або *множиною потужності континуум.*

З наведених вище прикладів і зауваження про рівнопотужність усіх відкритих інтервалів дійсної прямої, а також з твердження про рівнопотужність будь-якого відкритого інтервалу і всієї дійсної прямої випливає, що всі *ці множини точок будуть континуальними.*

Продовжимо вивчення незліченних множин.

Твердження 2.9. Якщо S — незліченна множина, а A — скінченна або зліченна підмножина множини S, то множини S і $S \dot{-} A$ рівнопотужні, тобто $S \backsim (S \dot{-} A)$.

Доведення. Множина $S \dot{-} A$ незліченна. Якби множина $S' = S \dot{-} A$ була зліченною, то за твердженням 2.3 множина $S = S' \cup A$ була б також зліченною, що суперечить умові твердження.

За твердженням 2.1 множина S' включає в себе зліченну підмножину B $(B \subseteq (S \dot{-} A))$.

Розглянемо множину $C = (S \dot{-} A) \dot{-} B$, для якої маємо $S \dot{-} A = B \cup C$ і $S = (A \cup B) \cup C$. Множина $A \cup B$ зліченна. Тоді з того, що $B \backsim (A \cup B)$, а також того, що $C \cap B = \varnothing$ і $C \cap (A \cup B) = \varnothing$, випливає співвідношення $((A \cup B) \cup C) \backsim (B \cup C)$, тобто $S \backsim (S \dot{-} A)$. *Кінець доведення.*

Сформулюємо декілька тверджень, які досить просто виводяться із вищенаведених фактів.

Твердження 2.10. Якщо S — нескінченна множина, а множина A — скінченна або зліченна, то $S \backsim (S \cup A)$.

Доведення. Очевидно, що можна вважати, що $S \cap A = \varnothing$.

Якщо S — зліченна множина, то $S \cup A$ — також зліченна множина (твердження 2.3), отже $(S \cup A) \dot{-} S$.

Якщо S — незліченна множина, то $S \cup A$ — також незліченна множина. Тоді за твердженням 2.9 $((S \cup A) \dot{-} A) \backsim (S \cup A)$. Оскільки $(S \cup A) \dot{-} A = S$, маємо $S \backsim (S \cup A)$. *Кінець доведення.*

Безпосередньо з цього твердження випливає, що $\mathbf{N} \backsim \mathbf{N}_+$. Тобто будь-яку зліченну множину A можна послідовно перенумерувати натуральними числами, починаючи як з нуля, так і з одиниці, оскільки $A \backsim \mathbf{N} \backsim \mathbf{N}_+$.

Твердження 2.11. Множина всіх ірраціональних чисел континуальна.

Доведення. Множина всіх ірраціональних чисел є теоретико-множинною різницею між незліченною (континуальною) множиною всіх дійсних чисел і зліченною множиною всіх раціональних чисел. Залишається застосувати попереднє твердження. *Кінець доведення.*

Число, яке не є коренем жодного многочлена з раціональними коефіцієнтами, називається *трансцендентним.*

Твердження 2.12. Множина всіх трансцендентних чисел континуальна.

Доведення. Множина всіх трансцендентних чисел є теоретико-множинною різницею між незліченною множиною всіх дійсних чисел і зліченною множиною всіх алгебраїчних чисел (твердження 2.7). Залишається застосувати твердження 2.9. *Кінець доведення.*

Що ж до операції побудови булеана, то зараз ми доведемо, що її застосування до зліченніх множин породжує континуальні множини.

Твердження 2.13. Множина 2^A усіх підмножин зліченної множини A є континуальною.

Доведення. Оскільки всі зліченні множини рівнопотужні множині $\mathbf{N}_+$ натуральних чисел, то достатньо довести континуальність булеана $2^{\mathbf{N}_+}$ множини $\mathbf{N}_+$.

З цією метою поставимо у відповідність кожній множині A_k з $2^{\mathbf{N}_+}$ нескінченну послідовність з нулів і одиниць $m_1^k m_2^k \dots m_i^k \dots$ за наступним законом: $m_i^k = 1$, якщо $i \in A_k$ і $m_i^k = 0$, якщо $i \notin A_k$.

Очевидно, ця відповідність є взаємно однозначною. Більш того, для кожної такої послідовності існує множина з $2^{\mathbf{N}_+}$, яка кодується нею, і навпаки, кожна множина з $2^{\mathbf{N}_+}$ кодується певною такою послідовністю.

Перетворимо $m_1^k m_2^k \dots m_i^k \dots$ в дробове число між 0 і 1 в двійковій системі числення, дописавши перед $m_1^k m_2^k \dots m_i^k \dots$ нуль з комою: $0, m_1^k m_2^k \dots m_i^k \dots$.

Тим самим, ми кожної множині A_k з $2^{\mathbf{N}_+}$ ставимо у відповідність деяке дійсне число з відкритого інтервалу $(0, 1)$, яке подано у двійковій системі числення, і тільки його, і навпаки, кожному такому числу ставимо у відповідність деяку множину з $2^{\mathbf{N}_+}$ і тільки її. А це означає рівнопотужність булеана $2^{\mathbf{N}_+}$ і множини всіх дійсних

чисел з відкритого інтервалу $(0, 1)$, тобто говорить про континуальність булеана $2^{\mathbf{N}_+}$. *Кінець доведення.*

Це твердження вказує на те, що взяття булеану від зліченних множин, як і у випадку скінченних множин, є дуже "потужною" операцією і веде до побудови значно "більшої" множини. (Всі інші введені теоретико-множинні операції або відносять результат свого застосування до типу нескінченності свого аргументу або одного зі своїх аргументів, коли їх декілька, або "спрощують" його в сенсі, що, наприклад, аргументи були зліченними множинами, а результат виявився скінченною множиною.) Тому природно спитати, а що буде, якщо взяти булеан від континуальної множини? Для отримання відповіді на це питання нам потрібно ввести поняття "розміру" множин.

2.8 Потужність множин

Перші ж дослідження в теорії множин показали, що, спираючись на аксіому вибору, можна довести що для будь-яких множин A і B або *існує взаємно однозначна відповідність між множиною A і деякою підмножиною множини B*, *або* навпаки, *існує взаємно однозначна відповідність між множиною B і деякою підмножиною множини A*. Тобто A і B завжди можна "порівняти" щодо взаємно однозначної відповідності. Цей факт веде до таких визначень.

Нехай A є деяка множина і $S = \{C \mid C \backsim A\}$, тобто S є сукупність усіх множин, рівнопотужних множині A (S, звичайно, містіть A). *Потужністю*, або *кардинальним числом* множини A, що позначається $|A|$, називається деяка абстракція, яка приписується у вигляді "міри однієї і тієї ж кількості елементів" будь-якої множині C із сукупності S. При цьому вважається, що $|C| = |A|$ для будь-якого $C \in M$.

Для скінченних множин потужність уточнюється таким чином.

Для будь-якої *скінченної множини* A і сукупності $S = \{C \mid C \backsim A\}$, яка, звичайно, містить деякий (єдиний) початковий відрізок натуральних чисел, скажімо, $[n]$, *потужністю* множини A (її (скінченним) *кардинальним числом* $|A|$) називається натуральне число n (яке позначає кількість елементів у будь-якої мно-

жині з сукупності S у звичайному сенсі). За визначенням покладаємо, що $|\varnothing| = 0$.

Таким чином, можна вважати, що кардинальне число є узагальненням звичайного поняття числа елементів.

У випадку, коли множина A знаходиться у взаємно однозначної відповідності з деякою підмножиною множини B, говорять, що потужність A *не більш потужності* B та пишуть $|A| \leqslant |B|$. Якщо при цьому множини A і B рівнопотужні, тобто існує взаємно однозначна відповідність між A і B ($A \backsim B$), то вважається, що потужності множин A і B *є рівними* ($|A| = |B|$), а якщо такої відповідності немає, то пишуть $|A| < |B|$ та говорять, що потужність множини A *строго менше* потужності множини B.

Оскільки множини завжди можна "порівняти" щодо взаємно однозначної відповідності, то виходячи з цих визначень, нам хотілося б, щоб для введеного порядку на потужностях мало місце, що $|A| = |B|$ тоді і тільки тоді, коли $|B| \leqslant |A|$ та $|A| \leqslant |B|$. Тобто, щоб для потужностей $|A|$ і $|B|$ довільних множин A і B виконувалося б одне з трьох співвідношень: $|A| < |B|$, $|A| = |B|$ або $|B| < |A|$. Теорема Кантора-Бернштейна, що приведена нижче, як раз і забезпечує виконання цих співвідношень.

Якщо A і B — множини і f — деяка взаємно однозначна відповідність між A та деякою підмножиною B' множини B, то $f(A)$ позначає підмножину B'.

Для розуміння подальшого, нам будуть потрібні поняття перетину та об'єднання нескінченної кількості множин, які вводяться таким чином.

Перетином нескінченної сукупності множин $A_0, \ldots, A_i, \ldots$ є множина $\{a \mid a$ належить кожної з множин $A_0, \ldots, A_i, \ldots\}$, яка позначається $\bigcap_{n=0}^{\infty} A_n$.

Об'єднанням нескінченної сукупності множин $A_0, \ldots, A_i, \ldots$ є множина $\{a \mid a$ належить хоча б одній з множин $A_0, \ldots, A_i, \ldots\}$, яка позначається $\bigcup_{n=0}^{\infty} A_n$.

Твердження 2.14 (теорема Кантора-Бернштейна). Якщо множина A рівнопотужна деякій підмножині B' множини B ($|A| \leqslant |B|$) і, одночасно, множина B рівнопотужна деякій підмножині A' множини A ($|B| \leqslant |A|$), то множини A і B рівнопотужні, тобто $|A| = |B|$.

Доведення. Нехай f — взаємно однозначна відповідність між A і B', а g — взаємно однозначна відповідність між B і A'.

Покладемо $A_0 = A$, $A_1 = g(B) = A'$, $A_2 = g(f(A_0)) = g(B')$ і $A_{n+2} = g(f(A_n))$ для $n \geqslant 1$. Індукцією по n легко довести, що $A_{n+1} \subseteq A_n$.

Нехай $D = \bigcap_{n=0}^{\infty} A_n$ і $C_i = A_i \dot{-} A_{i+1}$. Очевидно, що $A_k = (\bigcup_{i=k}^{\infty} C_i) \cup D$ і $C_i \cap C_j = \varnothing$ при $i \neq j$.

Визначимо відображення h таким чином:

$h(a) = a$, якщо $a \in (\bigcup_{i=k}^{\infty} C_{2*i+1}) \cup D$, і $h(a) = g(f(a))$, якщо $a \in \bigcup_{i=k}^{\infty} C_{2*i}$.

Неважко перевірити, що h є взаємно однозначною відповідністю між A і $A_1 = A'$, тобто $A \backsim A'$. Оскільки $B \backsim A'$, остаточно маємо $A \backsim B$. *Кінець доведення.*

Відмітимо, що первісне доведення цього твердження використовувало аксіому вибору.

Якщо повернуться до операції побудови булеана, то Г. Кантор довів важливе, вже згадуване твердження щодо кардинальних чисел, відому як теорема Кантора, яку неможливо довести без використання аксіоми вибору.

Зауважимо, що на відміну від первісного доведення цього твердження наведене доведення не використовує аксіому вибору.

Якщо повернуться до операції побудови булеана, то Г. Кантор довів важливе, вже згадуване твердження, що стосується кардинальних чисел, і відоме як теорема Кантора, яку неможливо довести без використання аксіоми вибору. Крім того зауважимо, що вважається, що потужність пустої множини дорівнює 0, у той час як булеан пустої множини містить пусту множину як свій єдиний елемент.

Твердження 2.15 (теорема Кантора). Потужність будь-якої множини A строго менше потужності її булеану 2^A ($|A| < |2^A|$).

Доведення. Для випадку пустої множини A доводити нічого.

Нехай A — непуста множина. Оскільки існує тривіальна взаємно однозначна відповідність між множиною A і підмножиною $\{\{a\} \mid a \in A\}$ множини 2^A, яка кожному $a \in A$ ставить у взаємно однозначну відповідність $\{a\} \in 2^A$, то $|A| \leqslant |2^A|$. Тому достатньо довести, що множини A та 2^A нерівнопотужні.

Доведення останнього буде проводитися від протилежного,

використовуючи відомий діагональний метод Кантора (в якому і "захована" аксіома вибору).

Припустимо, що існує взаємно однозначна відповідність g між множинами A і 2^A, задане у вигляді $g = \{\langle b, B\rangle \mid b \in A$ і $B \in 2^A\}$, де у кожній парі відповідності g перша координата b — це елемент множини A, а друга координата B — деяка підмножина множини A. Ясно, що для кожної пари $\langle b, B\rangle \in g$ виконується тільки одна з двох умов: або $b \in B$, або $b \notin B$.

Побудуємо нову множину $K = \{b \mid b \in A$ і $b \notin B$ для $\langle b, B\rangle \in g\}$. Зауважимо, що з того, що $\varnothing \in 2^A$ слідує, що $K \neq \varnothing$.

Оскільки від K є підмножиною множини A ($K \in 2^A$), то g підмножині K ставить у відповідність певний елемент $k \in A$, тобто $\langle k, K\rangle \in g$. Тоді відносно елемента $k \in A$ і підмножини $K \subseteq A$ можливі два випадки: або $k \in K$, або $k \notin K$.

Нехай $k \in K$. З умови $\langle k, K\rangle \in g$ і способу побудови множини K випливає, що $k \notin K$. Протиріччя.

З іншого боку, якщо припустити, що $k \notin K$, то на підставі того, що $\langle k, K\rangle \in g$, і способу побудови множини K повинно виконуватися $k \in K$. Знову протиріччя.

Отже, неможливо встановити взаємно однозначне відповідність між A і 2^A.

Остаточно маємо $|A| < |2^A|$. *Кінець доведення.*

Теорема Кантора показує, що не існує множини найбільшої потужності, або, іншими словами, не існує найбільшого кардинального числа. Справді, розглянувши множини $\varnothing$, $[1]$, $[2]$, $\ldots, [n], \ldots$, $\mathbf{N}$, $2^{\mathbf{N}}$, $2^{2^{\mathbf{N}}}, \ldots$, одержимо нескінченно зростаючу послідовність відповідних кардинальних чисел $|\varnothing| < |[1]| < |[2]| < \ldots < |[n]| < \ldots < |\mathbf{N}| < |2^{\mathbf{N}}| < |2^{2^{\mathbf{N}}}| < \ldots$ (де $|\varnothing|$ — наименьший кардинал, який, як бачимо, існує). Ще звертаємо увагу на те, що у сенсі кардиналів зліченні множини є самими "маленькими" серед нескінченних множин.

Ще відзначимо, що звичайні арифметичні операції над числами натурального ряду можна узагальнити на випадок кардинальних чисел. Можна показати, що в разі скінченних кардинальних чисел ці операції збігаються з відповідними арифметичними діями над числами. Крім цього, операції над кардинальними числами зберігають багато властивостей звичайних арифметичних операцій.

Також бігло торкнемося ще одній цікавої класичної проблеми теорії множин, сформульований ще у 1884 році Г. Кантором і відомої як *гіпотеза континуума*, яка стверджує, що не існує множини, кардинальне число якої розташоване між кардинальним числом зліченних множин і кардинальним числом континуальних множин.

Проблему гіпотези континуума, після її появи, майже вісім десятків років намагалися розв'язати або спростувати багато математиків світу. І лише у 1963 році тридцятирічний американський математик Пол Коен отримав результат, з якого випливає, що гіпотезу континуума не можна ні довести, ні спростувати, виходячи з аксіом так званої аксіоматичної теорії множин Цермело-Френкеля з аксіомою вибору. Отже, прийняття або відхилення гіпотези континуума є однаково законними, що веде до можливості побудови двох різних несуперечливих теорій множин у рамках аксіоматичного підходу до теорії множин, розвитого Е. Цермелом і А. Френкелім.

На закінчення просто згадаємо одне з важливих узагальнень поняття натурального числа, що веде за "межі нескінченності" — так звані *порядкові числа*, або *трансфінітні числа*, або *ординали*. Вперше введені Георгом Кантором у 1897 році з метою класифікації цілком впорядкованих множин (див. розділ про відношення), вони грають ключову роль в доведеннях багатьох теорем теорії множин, особливо у зв'язку зі зв'язаним з ними принципом трансфинитной індукції. Як і інші типи чисел, їх можна додавати, перемножувати та підносити до степеня.

2.9 Парадокси

Якщо проаналізувати матеріал з наївної теорії множин, наведений у попередніх розділах, то можна виявити відсутність будь-яких обмежень як на поняття множин, так і на операції над ними. Така повна свобода (за висловом Г. Кантора "суть математики полягає в її свободі") спочатку ніяк не впливала на розвиток теорії множин, але на рубежі 19-го і 20-го століть несподівано виявилося, що будинок математики, зведений до того часу на базі наявної теорії множин, є недосконалим — в ньому присутні так звані парадокси, або антиномії. Це привернуло увагу до того, які теоретико-множинні побудови повинні лежати в основі математики.

Взагалі говориться, що будь-яка теорія містить антиномію, якщо в цій теорії можна довести два речення, що суперечать один одному, або одне складне речення, що має вигляд еквівалентності між двома взаємно суперечливими реченнями.

У першому випадку це свідчить про невдало вибрані вихідні положення теорії та/або використування в теорії некоректних правил виведення, що призвело до суперечливої теорії. І цю ситуацію часто можна виправити, якщо підправити вихідні положення та/або змінити певним чином правила виведення. Другий же випадок говорить про те, що, схоже, з самого початку не дуже вдало був обраний понятійний апарат теорії та/або недостатньо повно була проведена його (можливо, часткова) формалізація, навіть якщо аксіоми теорії виглядають справжніми, а правила виведення — вірними. Саме з цим другим випадком і зіткнулися розробники теорії множин на початку 20-го століття.

Зупинимося на деяких найбільш відомих парадоксах, які показали, що інтуїтивна теорія множин недосконала, і її виправлення потребує суттєвого коригування, що призвело, зрештою, до появи цілого ряду аксіоматичних теорій множин. Відразу зауважимо, що ми залишаємо осторонь опис цих аксіоматичних теорій, і просто наводимо ті парадокси, які надали найбільш істотний вплив на розвиток теорії множин і логіки в напрямку їх подолання.

Парадокс Кантора. За теоремою Кантора, множина 2^A всіх підмножин даної множини A має більшу потужність, ніж сама множина A. Розглянемо тепер множину всіх множин, яку назвемо U. Його множина 2^U всіх підмножин U, має тоді більшу потужність, ніж саме U, що парадоксально в силу того факту, що U, за визначенням, є множиною, що включає в себе всі множини.

Ця антиномія була відома самому Георгу Кантору ще в 1899 р.; цікаво, однак, що опублікована вона була лише в 1932 р. У 1901 вона привернула увагу Бертрана Рассела, який під її впливом побудував власну антиномію.

Парадокс Рассела. Для довільної множини видається цілком осмисленим з'ясувати, є воно своїм власним елементом чи ні. По відношенню до деяких множин важко засумніватися в тому, що вони не є власними елементами: множина планет, наприклад, не є, звичайно, планетою і тому не є власним елементом. Інші множини

настільки ж природно без вагань вважати власними елементами: очевидний приклад — множина всіх множин. Тому здається цілком природним поставити те ж питання щодо множини всіх множин, які не є власними елементами. Відповідь на це питання, однак, бентежить: позначивши останню множину через S, ми відразу бачимо, що якщо S є елементом S, то S належить множині всіх множин, які не є власними елементами, тобто S не є власним елементом. З іншого боку, якщо S не є елементом S, S не належить множині всіх множин, які не є власними елементами, а тому є власним елементом. Зіставляючи сказане, ми переконуємося, що S є елементом S в тому і тільки в тому випадку, коли S не є елементом S, — очевидна тупикова ситуація, що отримана на підставі правдоподібних припущень ланцюгом безперечних на вигляд міркувань.

Вище ми привели парадокси, що виникають у зв'язку з "необмеженим" використанням наївною теорії множин. Однак в математиці, переважно пов'язаної з теорією алгоритмів, значну роль грають парадокси наданого нижче типу.

Парадокс брадобрея. Припустимо, що в деякому селищі немає бородатих людей і всі чоловіки голяться або самі, або у місцевого брадобрея. Відомо, що в цьому селищі брадобрей голить тих і тільки тих, хто не голиться сам. Чи голить брадобрей самого себе? Якщо він голить самого себе, то він відноситься до тих, хто голиться сам, а людей цієї категорії він не повинен голити. Якщо ж він не буде голити самого себе, то він відноситься до тих, хто не голиться сам, а таких людей він якраз і повинен голити. Тупикова ситуація. І, як правило, саме за допомогою використання таких тупикових ситуацій або зведення до однієї з них проводиться доведення алгоритмічної нерозв'язаності цілого ряду математичних проблем, тобто до встановлення того, що не можна побудувати сукупність правил дій, що задають загальний алгоритм вирішення будь-якої задачи із заздалегідь заданого (нескінченного) класу задач.

Наведені парадокси зазвичай відносять до розряду логіко-математичних, поряд з якими є так звані семантичні парадокси, пов'язані з семантичної замкнутістю природних мов, приклади яких даються нижче.

Парадокс Греллінга–Нельсона. Антиномія Греллінга–Нельсона формулюється дуже просто. Деякі українські прик-

метники, наприклад, "український" і "багатоскладовий", мають ті самі властивості, які вони називають: прикметник "український" сам є українським, а прикметник "багатоскладовий" сам є багатоскладовим, в той час як величезна більшість прикметників, такі як "французький", "односкладовий" і "гарячий", не володіють властивістю, названою кожним з них. Називаючи прикметники другого роду гетерологічними, ми відразу ж виявляємо до свого жаху, що прикметник "гетерологічний" є гетерологічним в тому і тільки в тому випадку, якщо він не є гетерологічним.

Парадокс брехуна. Припустимо, що Іван Іванко виголосив 1 січня 2013 наступне (і нічого іншого за весь цей день не вимовляв): «Єдине висловлення, вимовлене Іваном Іванком 1 січня 2013, хибне». Слушно поставити питання про істинність чи хибність цього вислювання. Але відразу ж з'ясовується, що це висловлення істинне в тому і тільки в тому випадку, коли воно хибне.

Всі парадокси, як логічні, так і семантичні, мають загальну властивість, яку нестрого можна визначити як самозастосовність (або самовідносність). У будь-якому з цих парадоксів сутність, про яку в ньому йдеться, сама може бути віднесена до об'єктів, які визначаються або характеризуються за допомогою певної сукупності признаків. Мабуть, у всіх міркуваннях, що призводять до таких парадоксів, є деяке коло; і цілком зрозуміло прагнення саме в цьому бачити корінь зла. Проте рішуче вилучення всіх міркувань, що включають будь-який вид самозастосовності, є явно занадто сильний засіб боротьби з протиріччями. Не всяке поняття самозастосовності веде до них, і деякі такі поняття є необхідними (наприклад, для побудови сучасної теорії рекурсивних обчислень). Тому спроби обійти ці труднощі привели до появи ряду аксіоматичних систем для теорії множин, серед яких найбільш популярними є вже згадувана система Цермело-Френкеля з аксіомою вибору, а також системи фон Неймана-Бернайса-Геделя і Рассела-Уайтхеда.

На закінчення зупинимося ще на одному типі парадоксів, що відносяться до використання природних мов.

Парадокс Беррі. Множина натуральних чисел нескінченна. Множина же імен цих чисел, які є в української мові і містять, припустимо, менше ніж ста слів, є скінченною. Це означає, що існують такі натуральні числа, для яких в української мові немає імен мен-

ше ніж ста слів. Серед цих чисел є, очевидно, найменше число. Його, начебто, не можна назвати за допомогою українського речення, що містить менше ніж ста слів. Але фраза “найменше натуральне число, для якого не існує в українській мові його складного імені, що містіть менше ніж ста слів” є, як раз, ім’ям цього числа. Це ім’я сформульовано українською мовою і містить тільки дев’ятнадцять слів. Очевидний парадокс: названим виявилося те число, для якого немає імені.

Цей парадокс зникає, якщо розрізняти предметну (вихідну) мову і метамову, тобто мову, на якої задається предметна мова і описуються властивості його фраз). Справді, розглянута фраза дає характеристику названого числа, яка може бути описана деякою предметною мовою, і в цій фразі стверджується, що такий опис повинен містити не менше ста слів предметної мови; сама ж ця фраза відноситься до метамови і тому може містити і меншу кількість слів.

Парадокс Беррі говорять про необхідність чіткого розрізнення предметної мови і метамови, що, однак, не завжди можливо.

3 Про відповідності, функції та відношення

Розділ присвячено деяким необхідним математичним відомостям, які належать до основ інформатики. Він досить повний і містить доведення найбільш важливих фактів для людей, що вже мають навички проводити досить прості міркування в термінах логіки першого порядку. Читач, не знайомий з такими логічними побудовами, ці доведення може пропустити.

Розділ починається з відомостей про відповідності, а закінчується описом деревовидних структур і дій над ними, спираючись на списковий підхід, а не на графовий, як це зазвичай робиться у стандартних підручниках з дискретної математики, що викликано відсутністю у цих нотатках якого б не було матеріалу з теорії графів.

3.1 Відповідності та функції

У розділі про порівняння множин ми вже використовували частковий випадок поняття відповідності — так звану взаємно однозначну відповідність. Перейдемо тепер до розгляду цього поняття у загальному випадку.

3.1.1 Відповідності

Нехай задано дві (непусті) множини A і B. Тоді будь-яка (можливо, пуста) підмножина R бінарного декартового добутку $A \times B$ називається *відповідністю* між A і B та позначається $\langle A, R, B\rangle$.

У випадку, якщо A і B відомі або не має значення, що вони позначають, замість $\langle A, R, B\rangle$ часто пишеться просто R.

Якщо R — бінарна відповідність між A і B, то множина $\{x \mid x \in A$ й існує елемент $y \in B$, такий, що $\langle x, y\rangle \in R\}$, називається *областю визначення відповідності* R та позначається $dom(R)$, а множина $\{y \mid y \in B$ і існує елемент $x \in A$, такий, що $\langle x, y\rangle \in R\}$ називається *областю значень відповідності* R та позначається $ran(R)$.

Якщо $dom(R) = A$, то відповідність R називається *всюди*, або *повністю визначеною*. У протилежному випадку відповідність R називається *частково визначеною*.

Для відповідності R *образом елемента* $a \in dom(R)$ називається множина всіх елементів $b \in ran(R)$, які відповідають елементу a.

Для відповідності R *прообразом елемента* $b \in ran(R)$ називається множина всіх елементів $a \in dom(R)$, яким відповідає елемент b.

Якщо $C \subseteq dom(R)$, то *образом множини* C при відповідності R називається об'єднання образів усіх елементів з C.

Якщо $D \subseteq ran(R)$, то *прообразом множини* D при відповідності R називається об'єднання прообразів усіх елементів з D.

Оскільки відповідності є множинами, то до довільних відповідностей можуть бути застосовані всі відомі теоретико-множинні операції: об'єднання, перетин, різниця тощо.

Якщо задано відповідність R між A і B, то *обернена відповідність* до R визначається як така підмножина, яка позначається R^{-1}, множини $B \times A$, що $\langle b, a\rangle \in R^{-1}$ тоді і тільки тоді, коли $\langle a, b\rangle \in R$.

3.1.2 Частково і всюди визначені функції

Відповідність f між A і B називається *функціональною* (*функцією з A в B*) тоді і тільки тоді, коли для будь-яких $x \in A$ і $y, z \in B$, таких, що $\langle x, y\rangle \in f$ і $\langle x, z\rangle \in f$, має місце $y = z$.

Зокрема, всі функції, які вивчаються в шкільної елементарний математиці, є окремими випадками функціональних відповідностей, коли $A = B = \mathbf{R}$, де $\mathbf{R}$ — множина дійсних чисел, тобто ті, які, як ще кажуть, є дійсними функціями дійсного змінного.

Функція f з A в B зазвичай записується у вигляді $f : A \mapsto B$. В зв'язку з цим функція f іноді називається *відображенням* з A в B.

Графіком функції f з A в B, позначеним $graph(f)$, є найменша множина $R \subseteq A \times B$, така, що $\langle a, b\rangle \in R$ тоді і тільки, коли $\langle a, b\rangle \in f$.

Для кожного a з області визначення функції f (тобто з $dom(graph(f))$) єдиний елемент з області значень f (тобто з $ran(graph(f))$), який відповідає обраному a, позначається $f(a)$. Тому функцію f також записують у вигляді $y = f(x)$, де x являє

собою змінну.

Функція $f : A \mapsto B$ називається *всюди визначеною* тоді і тільки тоді, якщо $A = dom(graph(f))$. Функція, яка не є всюди визначеною, називається *частково визначеною*.

Якщо для функцій f і g, що діють з A в B, виконується $graph(f) \subseteq graph(g)$, то говориться, що g є *розширенням* функції f, а f — *звуженням* функції g.

3.1.3 Композиція відповідностей і функцій

Нехай задано дві бінарні відповідності: R між A і B та S між B і C. Їх *композицією (добутком)*, що позначається $R \circ S$, є відповідність між A і C, яка визначається як така множина впорядкованих пар: $\{\langle a, c\rangle \mid$ існує таке $b \in B$, що $\langle a, b\rangle \in R$ і $\langle b, c\rangle \in S\}$.

Тобто для двох заданих частково або всюди визначених функцій $f : A \mapsto B$ і $g : B \mapsto C$ їх *композицією* (або *добутком)*, що позначається як $f \circ g$ (або $f \cdot g$, або fg), є частково або всюди визначена функція з A в C, яка має графік $graph(f) \circ graph(g)$.

Нехай задано множину A. *Одиничною відповідністю* (*одиничним відношенням*, *діагоналлю*, або просто *рівністю*), яка позначається I_A (або просто I, коли A відомо), є відповідність з A в A, що дорівнює $\{\langle a, a\rangle \mid a \in A\}$.

Відмітимо, що I_A є всюди визначена функція.

Зауважимо, що відповідно до визначення, $(f \circ g)(x)$ є іншою формою звичайного запису композиції $g(f(x))$, що підкреслює, що функція f застосовується першою. Також відзначимо, що композиція є асоціативною операцією: $((f \circ g) \circ h)(x) = (f \circ (g \circ h))(x)$.

Оскільки функція і відображення є окремими випадками відповідності, то для них мають місце всі наведені вище визначення: поняття областей визначення та значень, поняття образу та прообразу елементів і множин та ін. Зокрема, для функції f елементи множини $dom(f)$ називають *аргументами* функції, образ елемента $a \in dom(f)$ позначають через $f(a)$ і називають *значенням* функції f на a. Прообраз елемента $b \in ran(f)$ позначають через $f^{-1}(b)$. Аналогічно позначаються (функціональний) образ і прообраз множини.

3.1.4 Ін'єкції, сюр'єкції, бієкції

Всюди визначена функція $f : A \mapsto B$ називається *ін'єктивною* тоді і тільки тоді, коли для всяких $a, b \in A$ з $f(a) = f(b)$ випливає, що $a = b$.

Функція $f : A \mapsto B$ називається *сюр'єктивною* (або *функцією "на"*) тоді і тільки тоді, коли для всякого $b \in B$ існує деякий $a \in A$, такий, що $f(a) = b$ (або, що еквівалентно, коли область значень функції f збігається з B).

Функція $f : A \mapsto B$ називається *бієктивною* тоді і тільки тоді, коли f є ін'єктивною і сюр'єктивною.

Можна показати, що функція $f : A \mapsto B$ є сюр'єктивною тоді і тільки тоді, коли існує функція $g : B \mapsto A$, така, що $g \circ f = I_B$. Якщо існує функція $g : B \mapsto A$, така, що $f \circ g = I_A$, то функція $f : A \mapsto B$ ін'єктивна. Якщо $f : A \mapsto B$ — ін'єктівна функція і $A \neq \varnothing$, то існує функція $g : B \mapsto A$, така, що $f \circ g = I_A$. Як наслідок отримуємо, що функція $f : A \mapsto B$ бієктивна тоді і тільки тоді, коли існує єдина функція $f^{-1} : B \mapsto A$, названа *оберненою*, така, що $f \circ f^{-1} = I_A$ і $f^{-1} \circ f = I_B$.

При порівнянні множин ми використовували поняття взаємно однозначної відповідності. У термінах, які щойно були введені, воно може бути визначено таким чином.

Відповідність R між A і B *є взаємно однозначною* тоді і лише тоді, коли вона *функціональна, всюди визначена, ін'єктивна* та *сюр'єктивна*.

Наведемо деякі приклади відповідностей та відображень.

– Відповідність між клітинками і фігурами на шахівниці в будь-який момент гри є функціональною, але не є всюди визначеним відображенням, оскільки не всі поля шахівниці зайняті фігурами.

– Відповідність між натуральними числами і сумами цифр їх десяткового запису є відображенням. Це відображення не є ін'єктивним, оскільки йому належать, наприклад, такі пари, як $\langle 17, 8\rangle$ і $\langle 26, 8\rangle$.

– Відповідність, за якою кожному натуральному числу $n \in \mathbf{N}$ відповідає число $3 * n$, очевидно, є взаємно однозначною відповідністю між множиною всіх натуральних чисел і множиною нату-

ральних чисел, кратних 3.

3.1.5 Прямий і обернений образи

Нехай задано функція $f : A \mapsto B$. Для кожної підмножини X з A *прямим образом* X (або просто *образом* X) відносно f є множина $\{b \in B \mid$ існує $a \in X$ таке, що $f(a) = b\}$, що позначається $f(X)$.

Для кожної підмножини Y з B *оберненим образом* Y відносно f є множина $\{a \in A \mid$ існує $b \in Y$ таке, що $f(a) = b\}$, що позначається $f^{-1}(Y)$.

Відмітимо, що функція f може не мати оберненої. Тому $f^{-1}(Y)$ не слід плутати з $f^{-1}(b)$ для $b \in B$. Оберненість спостерігається тільки у випадку, коли f є бієкцією.

3.1.6 Послідовності і перелічуваність

Для двох будь-яких множин I і A будь-яка функція $h : I \mapsto A$, що зазвичай позначається $(h_i)_{i \in I}$, називається *I-індексованою послідовністю* (або просто *послідовністю*, коли I відомо або є $\mathbf{N}$).

Якщо для отримання елементів послідовності деякий початковий відрізок $[n]$ натурального ряду може виступати як I, то послідовність $(h_i)_{i \in I}$ називається *скінченною*. Якщо ж для отримання елементів послідовності натуральний ряд $\mathbf{N}_+$ може виступати як I, то $(h_i)_{i \in I}$ називається *перелічуваною послідовністю*. У всіх інших випадках розглядаєма послідовність вважається *неперелічуваною послідовністю*.

3.2 Відношення, еквівалентність, частковий порядок

Довільна підмножина R n–кратного декартового добутку $A \times \ldots \times A$ множини A на себе ($R \subseteq A \times \ldots \times A$) називається n–арним відношенням на множині A.

Надалі нас будуть цікавити тільки бінарні відношення, які можна розглядати як окремий випадок відповідностей між двома множинами у разі, коли ці множини співпадають. Тобто відповідність R між A і B називається *бінарним відношенням на A*, або *бінарним відношенням, що задане на A*, якщо $A = B$.

Для бінарних відношень замість $\langle a, b\rangle \in R$ також використовується запис aRb.

З бінарними відношеннями можна проводити всі ті операції, які мають місце для відповідностей, зокрема, виконувати теоретико-множинні операції, а також здійснювати операцію композиції.

Якщо R — бінарне відношення на A, то множина $R^{-1} = \{\langle b, a\rangle \mid \langle a, b\rangle \in R\}$ називається *відношенням, оберненим до* R.

Тепер перейдемо до визначення деяких бінарних відношень, що грають важливу роль в математичних побудовах і теоріях, і вивчення їх властивостей.

3.2.1 Рефлексівне, симетричне і транзитивне відношення та відношення еквівалентності

Нехай R є бінарне відношення на множині A, тобто $R \subseteq A \times A$.

Бінарне відношення R на A називається *повним* тоді і тільки тоді, коли $\langle a, b\rangle \in R$ або $\langle b, a\rangle \in R$ має місце для будь-яких двох елементів $a, b \in A$.

Бінарне відношення R на A називається *рефлексивним* тоді і тільки тоді, коли для всіх $a \in A$ має місце $\langle a, a\rangle \in R$. (В теоретико-множинних термінах бінарне відношення R на A називається *рефлексивним* тоді і тільки тоді, коли $I_A \subseteq R$.)

У випадку, коли для всілякого $a \in A$ *не має місце* $\langle a, a\rangle \in R$ (тобто коли $I_A \cap R = \varnothing$), бінарне відношення R над A називається *іррефлексивним*.

Бінарне відношення R на A називається *симетричним* тоді і тільки тоді, коли для всіх $a, b \in A$ з $\langle a, b\rangle \in R$ випливає $\langle b, a\rangle \in R$. (В теоретико-множинних термінах бінарне відношення R на A називається *симетричним* тоді і тільки тоді, коли $R = R^{-1}$.)

Бінарне відношення R на A називається *транзитивним* тоді і тільки тоді, коли для всяких $a, b, c \in A$ з $\langle a, b\rangle \in R$ і $\langle b, c\rangle \in R$ випливає $\langle a, c\rangle \in R$. (В теоретико-множинних термінах бінарне відношення R на A називається *транзитивним* тоді і тільки тоді, коли $(R \circ R) \subseteq R$.)

Бінарне відношення R на A називається *відношенням еквівалентності* тоді і тільки тоді, коли R рефлексивне, симетричне і

транзитивне.

Діагональ I_A (тобто відношення рівності) на будь-якої множині A є відношенням еквівалентності. Рівність — це найменше (відносно включення $\subseteq$) відношення еквівалентності, бо при видаленні бодай одного елемента з I_A відношення I_A перестає бути рефлексивним, а отже, перестає бути і відношенням еквівалентності.

Другим прикладом відношення еквівалентності служить рівнопотужность множин.

Якщо R — відношення еквівалентності на A, то для кожного $a \in A$ множина $\{x \mid x \in A \text{ і } \langle a, x\rangle \in R\}$ називається *класом еквівалентності елемента x за модулем R* і позначається x/R, $[x]_R$, або просто $[x]$.

Множина $\{a/R \mid a \in A\}$, де R — відношення еквівалентності на множині A, називається *фактором* (*фактор-множиною*) *множини A за відношенням еквівалентності R* і позначається A/R.

Отримуємо, що будь-які два елементи з одного класу A/R еквівалентні між собою, у той час як два елементи з різних класів фактор-множини A/R неэквивалентны. Отже, класи еквівалентності фактор-множини A/R непусті та попарно не перетинаються, A/R задається відношенням R єдиним чином і об'єднання всіх класів еквівалентності за модулем R дає всю множину A. Іншими словами, *множина A розбивається відношенням еквівалентності R на непусті класи, яки попарно не перетинаються і об'єднання яких збігається з множиною A.*

Сукупність непустих множин $A_1, \ldots, A_n$ називається *розбиттям множини A* тоді і тільки тоді, коли $A_1, \ldots, A_n$ попарно не перетинаються і $A_1 \cup \ldots \cup A_n = A$.

Твердження 3.1. Кожне відношення еквівалентності R на множині A однозначно визначає деяке розбиття множини A, і навпаки, кожне розбиття $A_1, \ldots, A_n$ множини A однозначно задає таке відношення еквівалентності R над A, що $A/R = \{A_1, \ldots, A_n\}$.

Доведення. Раніше ми відзначали, що множина A розбивається відношенням еквівалентності R на непусті класи, яки попарно не перетинаються і об'єднання яких збігається з множиною A. Значить, ці класи, згідно з визначенням, утворюють розбиття множини A.

Нехай сукупність непустих множин $A_1, \ldots, A_n$ утворює роз-

биття множини A. Визначимо відношення R наступним чином: $\langle a, b\rangle \in R$ тоді і тільки тоді, коли $a, b \in A_i$ для деякого i $(1 \leqslant i \leqslant n)$. Легко перевіряється, що R є відношенням еквівалентності (тобто що R рефлексивно, симетрично і транзитивно). Тому з способу визначення R отримуємо, що $A/R = \{A_1, \ldots, A_n\}$. *Кінець доведення.*

Сюр'єктивна функція $h_R : A \mapsto A/R$, така, що $h_R(x) = [x]_R$, називається *канонічною функцією*, пов'язаною з R.

Степені відношення R на множині A визначаються так.

Для кожного $n \geqslant 0$: $R^0 = I_A, R^1 = R, R^2 = R \circ R, \ldots, R^{n+1} = R \circ R^n$.

Об'єднання $R^+ = \bigcup_{n \geqslant 1} R^n$, яке називається *транзитивним замиканням* (бінарного) відношення R на A, є найменшим транзитивним відношенням на A, що включає в себе R, а об'єднання $R^* = \bigcup_{n \geqslant 0} R^n$, яке називається *рефлексивно-транзитивним замиканням* відношення R на A, є найменшим рефлексивним і транзитивним відношенням на A, що включає в себе R.

Очевидно, що $R^+ = R \circ R^*$ і $R^* = (I_A \cup R^1)^+$. Використовуючи це, легко показати, що для будь-якого бінарного відношення R на A, $(R \cup R^{-1})^*$ є найменшим відношенням еквівалентності, що включає в себе R.

3.2.2 Частково впорядковані множини

Відношення R на A називається *антисиметричним* тоді і тільки тоді, коли для всяких $x, y \in A$ з того, що $\langle x, y\rangle \in R$ і $\langle y, x\rangle \in R$ випливає, що $x = y$.

Відношення R на A називається *відношенням часткового порядку (частковим порядком)* тоді і тільки тоді, коли R є рефлексивним, антисиметричним і транзитивним.

Якщо задано частковий порядок R на A, то пара $\langle A, R\rangle$ називається *частково впорядкованою множиною* (з абревіатурою *ч.в.м.*, або *poset* англійською). Як правило, частковий порядок R позначається символом $\preceq_A$, або просто $\preceq$, коли множина A відома.

Для заданого часткового порядку $\preceq$ на множині A, *строгий порядок* $\prec$, пов'язаний з $\preceq$, визначається так: $x \prec y$ тоді і тільки тоді, коли $x \preceq y$ и $x \neq y$.

Строгий порядок на множині A можна визначити по-іншому

— а саме як таке відношення $\prec$, яке *асиметричне* і *транзитивне*, де *асиметричність* означає, що якщо $a \prec b$, то не виконується, що $b \prec a$ (у теоретико-множинних термінах: $\prec \circ \prec^{-1} = \varnothing$).

Так незалежно визначений строгий порядок $\prec$ на A індукує пов'язане з ним відношення часткового порядку $\preceq$ на A: $a \preceq b$ тоді і тільки тоді, коли $a \prec b$ або $a = b$ $(a, b \in A)$. (Звертаємо увагу на те, що це визначення $\preceq$ тягне його рефлексивність і антисиметричність, тобто те, що $I_A \subseteq \preceq$ та $(\prec \circ \prec^{-1}) \subseteq I_A$.)

Нехай задано частковий порядок $\preceq_A$ на множині A і B — підмножина множини A. B називається *ланцюгом* тоді і тільки тоді, коли для будь-яких двох елементів $a, b \in B$ або $a \preceq_A b$, або $b \preceq_A a$.

Частковий порядок $\preceq_A$ на множині A називається *лінійним* (або *досконалим*) тоді і тільки тоді, коли вся множина A є ланцюгом.

Нехай задано частковий порядок $\preceq_A$ на множині A і B є підмножиною множини A. Елемент $b \in A$ називається *нижньою гранню* множини B тоді і тільки тоді, коли для всіх $a \in B$ має місце $b \preceq_A a$. Елемент $c \in A$ називається *верхньою гранню* множини B тоді і тільки тоді, коли для всіх $a \in B$ має місце $a \preceq_A c$.

Звертаємо увагу на те, що як верхня грань m, так і нижня грань b можуть належати і не належати X (якщо вони існують). Наприклад, якщо A є дійсна пряма $(-\infty, +\infty)$, то у відкритого променя $(-\infty, 2)$ немає нижньої грані, а його верхня грань, 2 (якої також є будь інше число, яке більше 2), не належить променю. Далі, у напівзакритого променя $[2, +\infty)$ верхня грань відсутня, а 2 є його нижньою гранню, яка належить цьому променю (будь-яке число, що менше 2, також є нижньою гранню променя, але воно не належить йому). Дійсна пряма $(-\infty, +\infty)$ не має ні нижньої, ні верхньої граней.

Елемент $b \in A$ називається *найменшим елементом* частково впорядкованої множини $\langle A, \preceq \rangle$ тоді і тільки тоді, коли для всіх $a \in A$ має місце $b \preceq_A a$. Елемент $c \in A$ називається *найбільшим елементом* множини $\langle A, \preceq \rangle$ тоді і тільки тоді, коли для всіх $a \in A$ має місце $a \preceq_A c$.

З цих визначень випливає єдиність найбільшого та найменшого елементів у розглядуваної множині у випадку їх існування.

У прикладах вище, $(-\infty, 2)$ та $(-\infty, +\infty)$ не мають ні най-

меншого, ні найбільшого елементів. У $[2, +\infty)$ немає найбільшого елемента, але є найменший — число 2. У напіввідкритому інтервалі $(-2, 2]$ число 2 є найбільшим елементом, але немає найменшого елемента.

Елемент $b \in A$ називається *мінімальним* у частково впорядкованої множини $\langle A, \preceq \rangle$ тоді і тільки тоді, коли для будь-якого $a \in A$ з $a \preceq_X b$ випливає, що $a = b$. Елемент $c \in A$ називається *максимальним* у частково впорядкованої множини $\langle A, \preceq \rangle$ тоді і тільки тоді, коли для будь-якого $a \in A$ з $c \preceq_A a$ випливає, що $a = c$.

На відміну від найбільшого і найменшого елементів, мінімальних і максимальних елементів у частково впорядкованої множини A може бути понад один.

Ще відзначимо, що в разі наявності у частково впорядкованої множини $\langle A, \preceq \rangle$ найбільшого (найменшого) елемента цей елемент служить єдиним максимальним (мінімальним) елементом множини A. У зворотний бік твердження не завжди вірно. Легко побудувати частково впорядковану множину $\langle A, \preceq \rangle$, яке містить два максимальних елемента (два мінімальних елемента), і, отже, жоден з них не буде найбільшим (найменшим). У лінійно впорядкованої множині поняття найбільшого і максимального (найменшого і мінімального) елементів збігаються.

Розглянемо деякі приклади.

У довільній множині A з тривіальним порядком, яким являється діагональ I_A (тобто відношення рівності), кожен елемент $a \in A$ є одночасно максимальним і мінімальним. Найбільший і найменший елементи відносно цього порядку в множині A відсутні.

Булеан 2^A множини A з включенням $\subseteq$ як відношенням часткового порядку містить найменший елемент — пусту множину $\varnothing$ і найбільший елемент — саму множину A. У множині $2^A \div \{\varnothing\}$ всіх непустих підмножин множини A не існує найменшого елемента, але всі одноелементні множини $\{a\}$, $a \in A$, є її мінімальними елементами.

У множині $\mathbf{N}_+$ натуральних чисел, частково впорядкованої за відношенням "ділить без залишку" ($m \preceq n$ тоді і тільки тоді, коли натуральне m ділить натуральне n без залишку), число 1 є найменшим елементом, а найбільшого елемента не існує. Якщо ж розглянути $\mathbf{N}$ із відношенням часткового порядку "ділить без залишку",

то окрім найменшого елемента (як і раніше, число 1) з'являється найбільший елемент — число 0.

Нехай B є підмножиною частково впорядкованої множини $\langle A, \leq \rangle$. Елемент $b \in A$ називається *точною нижньою гранню* множини B ($infimum\ B$, $inf\ B$) в A тоді і тільки тоді, коли множина нижніх граней B в A не є пустою і b є найбільшим елементом цієї множини. Елемент $c \in A$ називається *точною верхньою гранню* множини B ($supremum\ B$, $sup\ B$) в A тоді і тільки тоді, коли множина верхніх граней B в A не є пустою і c є найменшим елементом цієї множини.

У вже розглянутих прикладах з інтервалів, у $(-\infty, +\infty)$ немає ні точної верхньої грані, ні точної нижньої грані. У $(-\infty, 2)$ є тільки точна верхня грань — число 2, яке є точною нижньою гранню інтервалу $[2, +\infty)$, який не має точної верхньої грані. Напіввідкритий інтервал $(-2, 2]$ має як точну нижню грань — число -2, так і точну верхню грань — число 2.

Наступний важливий факт, відомий як *лема Цорна* (або *теорема Куратовського-Цорна*) і еквівалентний аксіомі вибору, наводитися без доведення.

Твердження 3.2 (*лема Цорна*). Нехай задано часткову впорядковану множину $\langle A, \leq \rangle$. Якщо кожний непустий ланцюг в A має верхню (нижню) грань в A, то A має хоча б один максимальний (мінімальний) елемент.

Також наведемо теорему, еквівалентну лемі Цорна і, таким чином, еквівалентну аксіомі вибору.

Твердження 3.3 (*теорема Хаусдорфа*). Будь-який ланцюг частково впорядкованої множини A включається в деякий максимальний ланцюг множини A.

Лема Цорна (або яка-нибудь з її можливих переформулировок) виявляється більш зручною для використання її замість аксіоми вибору у доведеннях ряду важливих теорем з вищої алгебри, математичного аналізу, топології та інших розділах сучасної математики. Прикладами можуть бути теорема існування алгебраїчного замикання довільного поля, теорема Хана – Банаха про продовження лінійного функціоналу, теорема про існування максимального ідеалу у кільці з одиницею, теореми Тихонова.

3.3 Повністю впорядковані множини

Найбільший загальний принцип індукції належить до частково впорядкованих множин, яки задовольняють так званої властивості повної впорядкованості.

Частково впорядкована множина $\langle A, \preceq \rangle$ називається *фундованою* тоді і тільки тоді, коли будь-яка її підмножина має мінімальний елемент.

Фундована лінійно впорядкована множина називається *повністю впорядкованою*, а відповідний порядок — *повним*.

За умови використання аксіоми вибору, еквівалентне визначення фундованості полягає в тому, що множина A з відношенням порядку $\preceq$ є фундованою тоді і тільки тоді, коли воно *задовольняє умові обриву строго спадної послідовності*, тобто коли у A не існує такої нескінченної послідовності, $(a_j)_{j\in\mathbf{N}}$, що $a_{j+1} \prec a_j$ для усіх $j \geqslant 0$.

Для лінійних порядків поняття найменшого і мінімального (найбільшого і максимального) елементів збігаються, такщо в усякої повністю впорядкованої множині всяка непуста підмножина має найменший елемент. Тобто повністю впорядкована множина завжди містить найменший елемент.

Ще зауважимо, що частково впорядкована множина, у якої всяка непуста підмножина має найменший елемент, автоматично є лінійно впорядкованою. (Дійсно, будь-яка двоелементна множина має найменший елемент, тому будь-які два елемента порівняні між собою.)

З сказаного слідує, що частково впорядкована множина $\langle A, \preceq \rangle$ є повністю впорядкованою тоді і тільки тоді, коли будь-яка непуста підмножина множини A має найменший елемент.

Використовуючи аксіому вибору, можна довести *рівносильне* їй (а, значить, лемі Цорна і теоремі Хаусдорфа) таке твердження.

Твердження 3.4 (*теорема Цермело*). Будь-яку множину можна повністю впорядкувати.

Ще відмітимо, що якщо X та Y — два повністю впорядковані множини, то можна встановити взаємно однозначну відповідність або між ними, або між одним з них і рівно початковим відрізком

іншого (із збереженням порядків на X та Y в обох випадках). Це властивість повністю впорядкованих множин "веде" до побудови теорії так званих *порядкових чисел* (*ординалів*), розгляд яких тут опущено.

Прикладом скінченної повністю впорядкованої множини може служити будь-який початковий відрізок натуральних чисел $[n]$ ($n \geqslant 0$) з природним впорядкуванням (включаючи випадок пустої множини, коли $n = 0$). Найпростіший приклад нескінченної повністю впорядкованої множини — це зліченна множина натуральних чисел $\mathbf{N}$ з природним порядком, у той час як множина цілих чисел $\mathbf{Z}$ та множина дійсних чисел $\mathbf{R}$ (обидві з природним порядком) не є повністю впорядкованими — у обох немає найменшого елемента. $\mathbf{Z}$ легко повністю впорядкувати, наприклад, таким чином: $0 \prec -1 \prec 1 \prec -2 \prec 2 \prec \ldots$. Звичайно, $\mathbf{R}$ також можна повністю впорядкувати, але ця справа є складнішою, і тут ми на цьому зупинятися не будемо.

3.4 Математична і трансфінітна (повна) індукція

У шкільному курсі математики вивчається спосіб доведення, названий методом *математичної індукції*, але не проводиться доведення його *коректності*, тобто того, що він веде до вірних (*істинних*) тверджень у випадках його правильного застосування. Даний розділ покликаний не тільки щоб заповнити цей пробіл, але і дати опис та обгрунтування більш загального прийому доведення, відомого як метод, або принцип трансфінітної (повної) індукції (окремим випадком якого є метод математичної індукції).

Метод математичної індукції полягає в наступному.

Нехай є деяке твердження $P(n)$, що формулюється для будь-якого натурального числа n, і нехай відомо, що:

(I) затвердження P вірно для 1 (або для 0), тобто $P(n)$ *має місце при* $n = 1$ (при $n = 0$) та

(II) з того, що для всіх $k \leqslant n$ *припущення* $P(k)$ *має місце*, випливає, що і $P(n+1)$ *має місце*.

Тоді $P(n)$ *має місце для усіх* $n = 1, 2, \ldots$.

Той ж самий прийом доведення може бути використаний з заміною у формулюванні математичної індукції натурального ряду

будь-якою повністю впорядкованою множиною. У цьому разі він називається **методом (принципом) трансфінітної (повної) індукції** і формулюється наступним чином.

Нехай $\langle A, \preceq \rangle$ — повністю впорядкована множина, P — деяке твердження, що сформульовано для кожного $a \in A$ і a_0 — найменший елемент множини A. Нехай виконується наступне:

(I) твердження P вірно для елемента a_0, або, іншими словами, твердження $P(a_0)$ має місце, і

(II) з того, що твердження $P(b)$ має місце для всіх $b \preceq a$, слідує, що і твердження $P(a)$ має місце.

Тоді $P(a)$ *істинно для всіх* $a \in A$.

Частину (I) називається *базою індукції*, а (II) — *індукційним кроком*, в якому припущення про те, що $P(b)$ має місце для всіх $b \prec a$, називається *індукційною гіпотезою*.

Твердження 3.5. Трансфінітна індукція є коректним методом.

Доведення. Припустимо протилежне. Це значить, що в A існують елементи c, для яких $P(c)$ не має місця. Але тоді, в силу повної впорядкованості A, серед цих елементів існує і найменший, скажімо, c^*, для якого $P(c^*)$ невірно. Елемент c^* відмінний від a_0 в силу (I), але для всіх $b \prec c^*$ твердження $P(b)$ має місце і, отже, в силу (II), твердження P повинно виконуватись і для c^*. Протиріччя. Отримуємо, що принцип трансфінітної індукції є коректним методом. *Кінець доведення.*

Наведене доведення є *обгрунтуванням коректності і методу математичної індукції*, оскільки він є частковим випадком методу трансфінітної індукції, коли A є натуральним рядом із природним порядком.

Твердження 3.6, дане нижче, є прикладом застосування принципу трансфінітної індукції для обгрунтування певної властивості так званого лексикографічного порядку.

Нехай задано частково впорядковану множину $\langle A, \preceq \rangle$. *Лексикографічний порядок* $<<$, індукований на $A \times A$ відношенням $\preceq$, визначається наступним чином:

для будь-яких x, y, x', $y' \in A$ пари $\langle x, y \rangle$ і $\langle x', y' \rangle$ перебувають у відношенні $<<$ ($\langle x, y \rangle << \langle x', y' \rangle$) тоді і тільки тоді, коли або $x = x'$ і $y = y'$, або $x \preceq x'$, або $x = x'$ і $y \preceq y'$.

Ми залишаємо читачеві перевірку того, що $<<$ насправді є не тільки частковим, але і лінійним порядком на $A \times A$.

Часто буває корисним таке твердження.

Твердження 3.6. Якщо $\langle A, \leq \rangle$ є повністю впорядкована множина, то повністю впорядкованим є і лексикографічний порядок $<<$, індукований на $A \times A$ відношенням $\leq$.

Доведення. Від противного.

Припустімо, що існує нескінченно спадна послідовність $(\langle x_i, y_i \rangle)_{i \in \mathbf{N}}$. Тоді:

(1) або існує нескінченна кількість дійсно різних x_i,

(2) або є тільки скінченна кількість дійсно різних x_i.

У випадку (1) підпослідовність, що складається з цих дійсно різних елементів, стає нескінченно спадної в A, що суперечить тому, що відношення $\leq$ є повністю впорядкованим.

У випадку (2) можна вказати таке k, що $x_i = x_{i+1}$ для всіх $i \geqslant k$. За визначенням відношення $<<$ послідовність $(y_i)_{i \geqslant k}$ є нескінченно спадною в A, що знову суперечить повній впорядкованості $\leq$.

Отже, $<<$ є повністю впорядкованим відношенням на $A \times A$. *Кінець доведення.*

Використовуючи це твердження, розглянемо приклад, в якому доводиться, що так звана функція Аккермана є загальнорекурсивною (тобто те, що вона є частково рекурсивною і всюди визначеною).

Приклад (Функція Аккермана). Визначимо функцію $A : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$, відому в теорії рекурсивних функцій як функція Аккермана, яка має надзвичайно швидке зростання, таким чином:

$A(x, y) = y + 1$, якщо $x = 0$,

$A(x - 1, 1)$, якщо $y = 0$,

$A(x - 1, A(x, y - 1))$ в інших випадках.

Покажемо, що *ця функція є всюди визначеною.* (У книгах з теорії рекурсивних функцій можна знайти доведення того, що таке рекурсивне визначення задає частково рекурсивну функцію.) Скористаємося для цього повною індукцією за лексикографічним порядком на $\mathbf{N} \times \mathbf{N}$.

Базу індукції являє собою випадок, коли $x = 0$ і $y = 0$, при якому значення $A(0, 0)$ існує і дорівнює 1, оскільки $A(0, y) = y + 1$.

Індукційна гіпотеза стверджує, що для довільної пари $\langle m, n\rangle$ значення $A(m', n')$ існують для будь-яких $\langle m', n'\rangle << \langle m, n\rangle$.

Виконання індукційного кроку забезпечують три випадки.

(1) При $m = 0$ значення $A(0, n)$ визначене і дорівнює $n + 1$, оскільки $A(0, n) = n + 1$.

(2) При $m \neq 0$ і $n = 0$, оскільки $\langle m - 1, 1\rangle << \langle m, 0\rangle$ і $\langle m - 1, 1\rangle \notin \langle m, 0\rangle$, отримуємо, що значення $A(m - 1, 1)$ визначене за індукційною гіпотезою. Тому значення $A(m, 0)$ також визначено, оскільки воно дорівнює $A(m - 1, 1)$.

(3) При $m \neq 0$ і $n \neq 0$, оскільки $\langle m, n - 1\rangle << \langle m, n\rangle$ і $\langle m, n - 1\rangle \notin \langle m, n\rangle$, отримуємо, що значення $A(m, n - 1)$ визначене за індукційною гіпотезою.

Оскільки для будь-яких y і z $\langle m - 1, y\rangle << \langle m, z\rangle$, $\langle m - 1, A(m, n - 1)\rangle << \langle m, n\rangle$ і $\langle m - 1, A(m, n - 1)\rangle \notin \langle m, n\rangle$, то за індукційною гіпотезою значення $A(m - 1, A(m, n - 1))$ визначено. Але це і є $A(m, n)$, тобто значення $A(m, n)$ визначене, що завершує розгляд індукційного кроку.

Отже, функція $A(x, y)$ є всюди визначеною.

3.5 Булеві алгебри і решітки

Є певний зв'язок частково впорядкованих множин з булевими алгебра в їх узагальненому формулюванні, і опис цього зв'язку міститься у даному розділі. Відразу зауважимо, що введені раніше булеві алгебри множин, з одного боку, є їх окремим випадком, а з іншого боку, складових їх множин достатньо, в деякому сенсі, для опису своїх можливих узагальнень.

Абстрактною булевою алгеброю, або просто *булевою алгеброю*, називається множина елементів довільної природи (так званий *носій булевої алгебри*), що містить принаймні два фіксованих елемента — o ("*нуль*" — аналог пустої множини $\varnothing$) і ι ("*одиниця*" — аналог універсуму) і, можливо, інші елементи, яки позначаються a, b, c і т. д., на яких задані бінарні операції $\sqcup$ (аналог звичайного об'єднання $\cup$), $\sqcap$ (аналог звичайного перетину $\cap$) і унарною операції $\tilde{}$(аналог звичайного доповнення $^-$), для яких виконуються наступні аксіоми, які є "копіями" законів булевих алгебр множин, даних вище.

Аксіоми (закони) абстрактної булевої алгебри:
(1) *ідемпотентність "об'єднання" і "перетину"*: $a \sqcup a = a, a \sqcap a = a$;
(2) *комутативність "об'єднання" і "перетину"*: $a \sqcup b = b \sqcup a$, $a \sqcap b = b \sqcap a$;
(3) *асоціативність "об'єднання" і "перетину"*: $a \sqcup (b \sqcup c) = (a \sqcup b) \sqcup c$, $a \sqcap (b \sqcap c) = (a \sqcap b) \sqcap b$;
(4) *аксіоми (закони) поглинання*: $(a \sqcap b) \sqcup a = a$, $(a \sqcup b) \sqcap a = a$;
(5) *дистрибутивність "об'єднання" відносно "перетину"*: $a \sqcup (b \sqcap c) = (a \sqcup b) \sqcap (a \sqcup c)$, *дистрибутивність "перетину" відносно "об'єднання"*: $a \sqcap (b \sqcup c) = (a \sqcap b) \sqcup (a \sqcap c)$;
(6) *закони (правила) де Моргана*: $\widetilde{a \sqcup b} = \tilde{a} \sqcap \tilde{b}$ *(перший закон де Моргана)*, $\widetilde{a \sqcap b} = \tilde{a} \sqcup \tilde{b}$ *(другий закон де Моргана)*;
(7) *властивості нуля*: $a \sqcup o = a$, $a \sqcap o = o$, $\tilde{o} = \iota$;
(8) *властивості единицы*: $a \sqcup \iota = \iota$, $a \sqcap \iota = a$, $\tilde{\iota} = o$;
(9) *інволютивність доповнення*: $\tilde{\tilde{a}} = a$;
(10) *властивості доповнення*: $a \sqcup \tilde{a} = \iota$, $a \sqcap \tilde{a} = o$.

Введені операції є *абстрактними*, оскільки ні вони самі, ні носій, на якому вони визначені, ніяк не конкретизуються, і ніяких інших вимог, крім задоволення вищенаведеним аксіомам, до них не пред'являється. В теорії множин елементи булевої алгебри інтерпретуються як підмножини певного універсуму, які можна перетинати, об'єднувати і брати їх доповнення. Ще зауважимо, що *наведений набір аксіом є надлишковим*, оскільки деякі з них можна отримати з інших за допомогою ланцюжка тотожних перетворень. Наприклад, закони де Моргана є такими і тому в подальшому буде вважатися, що вони завжди виконуються у всіх булевих алгебрах, які розглядаються.

Оскільки наведені аксіоми є "копіями" законів булевих алгебр множин, отримуємо, що *всяка алгебра підмножин будь-якої множини є булева алгебра з "нулем" і "одиницею"*.

Нехай дано дві булеві алгебри з носіями A і A' і взаємнооднозначна відповідність φ між A і A', таке, що рівності (i) $\varphi(a \sqcap b) = \varphi(a) \sqcap \varphi(b)$, (ii) $\varphi(a \sqcup b) = \varphi(a) \sqcup \varphi(b)$, (iii) $\widetilde{\varphi(a)} = \varphi(\tilde{a})$ справедливі для всіх a і b з A. Тоді кажуть, що φ є *булев ізоморфізм* між A і A', а дані алгебри A і A' *булево ізоморфні*.

Очевидно, що з (i)–(iii) слідує, що $\varphi(o) = o$ і $\varphi(\iota) = \iota$. Тобто *булев ізоморфізм — це взаємно-однозначне відображення носіїв*

булевих алгебр, що зберігає операції і особливі елементи o і ι.

Має місце наступна теорема, яка показує, що елементи будь-якої булевої алгебри можна вважати підмножинами деякої множини, а її булеві операції ототожнювати з їх однойменними теоретико-множинними аналогами.

Твердження 3.7 (*теорема Стоуна*). Будь-яка скінченна булева алгебра ізоморфна скінченної булевої алгебри множин, тобто булевої алгебри всіх підмножин деякої скінченної множини.

Як наслідок, отримуємо, що *число елементів в будь-якій скінченної булевої алгебри є степенем двійки.*

Теорема Стоуна допускає узагальнення на випадок нескінченних булевих алгебр: всяка нескінченна булева алгебра ізоморфна подалгебре алгебри всіх підмножин деякої відповідної множини (точніше для знайомих з теорією топологій — подалгебрі алгебри всіх відкрито-замкнутих підмножин деякого компактного цілком незв'язного хаусдорфова топологічного простору).

Серед частково впорядкованих множин винятково важливу роль відіграють так звані решітки.

Решіткою називається множиназ заданими на ней двома бінарними операціями: $\sqcup$ ("об'єднання") і $\sqcap$ ("перетин"), відносно яких виконуються закони (1)–(4), наведені вище.

Ясно, що в решітці існують скінченні об'єднання та перетини будь-яких її елементів. Також ясно, що будь-яка булева алгебра являється решіткою.

Будь-яке лінійно впорядкована множина $\angle A, \leq\rangle$ (наприклад, числова множина $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$ або $\mathbf{R}$ з традиційним відношенням порядку $\leqslant$) є решіткою. Якщо $a, b \in A$, то за $a \sqcup b$ береться більше (щодо порядку $\leqslant$) з чисел a і b, а за $a \sqcap b$ — менше з них.

Множина $\mathbf{N}$ натуральних чисел з відношенням часткового порядку "ділить без залишку" є решіткою, якщо для $a, b \in \mathbf{N}$ визначимо $a \sqcup b = \text{НСК}(a, b)$ і $A \sqcap b = \text{НСД}(a, b)$ (Тут, як і раніше, НСК - найменше спільне кратне, НСД - найбільший спільний дільник). Наприклад, $12 \sqcup 32 = 96$, $12 \sqcap 32 = 4$, $16 \sqcup 5 = 80$, $16 \sqcap 5 = 1$.

Дистрибутивною решіткою називається решітка, в якій для будь-яких $a, b, c \in A$ справедливі закони дистрибутивности з пункту (5) вище.

Частково впорядкована множина, в якої для будь-яких еле-

ментів a і b існують $inf\{a,b\}$ і $sup\{a,b\}$, називається *решітко впорядкованою*.

Ясно, що в решітко впорядкованої множині точні верхні і нижні грані існують для будь-яких скінченних підмножини її елементів.

Існує тісний зв'язок решіток з решітко впорядкованими множинами.

Твердження 3.8 (еквівалентність решітко впорядкованих множин та решіток).

1. Нехай A є решітко впорядкована множина. Якщо припустити, що для будь-яких елементів a і b з A $a \sqcup b$ є $sup\{a,b\}$ і $a \sqcap b$ є $inf\{a,b\}$, то A буде решіткою.

2. Нехай A є решітка. Якщо припустити, що для будь-яких елементів A і b з A $a \preceq b$ тоді і тільки тоді, коли $a \sqcap b = a$ (або $a \sqcup b = b$), то A буде решітко впорядкованою множиною відносно порядку $\preceq$.

Цей результат дозволяє в подальшому *говорити про будь-якому решітко впорядковані множині* $\langle A, \preceq \rangle$ *як про решітці з операціями перетину, об'єднання і доповнення, індукованими на* A *частковим порядком* $\preceq$, що і буде робитися до кінця цього розділу.

Решітко впорядкована множина $\langle A, \preceq \rangle$ називається *повною*, якщо для будь-якої непустий підмножини $B \subseteq A$ в множині A існують найменша верхня і найбільша нижня грані $sup\ B$ і $inf\ B$.

Очевидно, що довільна повна решітка є решіткою, але не будь-яка решітка є повною решіткою.

Якщо $\langle A, \preceq \rangle$ — повна решітка, то найменша верхня грань всієї множини A ($supA$) називається *одиницею повної решітки* A і позначається $\mathbf{1}$, а найбільша нижня грань множини A ($inf\ A$) називається *нулем повної решітки* A і позначається $\mathbf{0}$.

Вибір цих назв і позначень в повній решітці для $supA$ і $inf A$ пояснюється такими *властивостями елементів* $\mathbf{1}$ і $\mathbf{0}$: для довільного елемента $a \in A$ виконуються рівності $a \sqcup \mathbf{1} = \mathbf{1}$, $a \sqcup \mathbf{0} = a$, $a \sqcap \mathbf{1} = a$ і $a \sqcap \mathbf{0} = \mathbf{0}$.

Очевидно, що елементи $\mathbf{0}$ і $\mathbf{1}$ є, відповідно, найменшим і найбільшим елементами повної решітки $\langle A, \preceq \rangle$.

Пояснимо ці поняття на прикладах.

Множина $\mathbf{N}$ натуральних чисел з традиційними відношен-

ням порядку $\leqslant$ не є повною решіткою, оскільки будь-яка його нескінченна підмножина не має найменшої верхньої грані.

Множина всіх дільників натурального числа n, яка частково впорядкована відношенням " один дільник n ділить без залишку інший дільник n", є повною решіткою. Одиницею $\mathbf{1}$ в такий решітці є число n, а нулем $\mathbf{0}$ — натуральне число 1.

Частково впорядкована по відношенню включення множина 2^A всіх підмножин множини A також є повною решіткою, в якій A є одиницею $\mathbf{1}$, а $\varnothing$ — нулем $\mathbf{0}$.

Решітка з доповненням є решітка $\langle A, \leq \rangle$, в якій для будь-якого елемента $a \in A$ існує такий елемент $\hat{a} \in A$, що $a \sqcup \hat{a} = \mathbf{1}$ і $a \sqcap \hat{a} = \mathbf{0}$.

В результаті отримуємо, що якщо ми проведемо переобозначення нуля $\mathbf{0}$ і одиниці $\mathbf{1}$ решітки в нуль o і ι булевої алгебри, а решіткову операцію $\hat{}$ в булеву операцію $\tilde{}$, то для повної дистрибутивної решітки з доповненням виконуються аксіоми (1)–(10) булевої алгебри. Значить, *повна дистрибутивная решітка з доповненням може вважатися булевою алгеброю* з індукованими операціями перетину, об'єднання і доповнення.

З огляду на теорему Стоуна, отримуємо, що повна дистрибутивная решітка з доповненням може бути подана у вигляді булевої алгебри всіх підмножин деякої відповідної множини.

На цьому ми закінчуємо опис співвідношень булевих алгебр, булевих алгебр множин і частково впорядкованих множин.

3.6 Дерева, піддерева та заміщення піддерев

У програмуванні та деяких математичних побудовах часто використовується така структура даних, як дерева, яка, зазвичай, вводиться у вигляді графів спеціального виду. Ми ж визначаємо її нижче через рядки, що складаються з десяткових цифр і задовольняють певним властивостям, даючи тим самим інше визначення поняття слова в скінченному або нескінченному алфавіті.

3.6.1 Рядки

Нехай є деяка (можливо, нескінченна) множина A, яка буде називатися *алфавітом*. *Рядком* на A є функція $u : [n] \mapsto A$, де n —

натуральне число з $\mathbf{N}_+$. За визначенням вважаємо, що при $n = 0$ ми маємо єдину функцію, що відображає пусту множину $[0]$ в так званий *пустой (нульовий) рядок* та позначається e_A, або e у випадку, коли множина A відома.

Для заданого рядка $u : [n] \mapsto A$ натуральне число n називається *довжиною* u і позначається $|u|$.

Для заданої (можливо, нескінченної) множини A множина всіх рядків над A позначається A^*. Якщо має місце $u : [n] \mapsto A$, де $n > 0$, то для кожного $i \in [n]$ $u(i)$ є елемент з A, який позначається u_i; сам же рядок позначається $u_1 u_2 \dots u_n$.

Над рядками можна виконувати операцію *конкатенації*, яка визначається таким чином: Для заданих двох рядків $u : [n] \mapsto A$ і $v : [m] \mapsto A$ $(m, n \geqslant 0)$ їхньою *конкатенацією*, позначеною $u \cdot v$ або uv, є рядок $w : [n + m] \mapsto A$, такий, що $w(i) = u(i)$, якщо $1 \leqslant i \leqslant n$, і $w(i) = v(i - m)$, якщо $m + 1 \leqslant i \leqslant n + m$.

Безпосередньо перевіряється, що для кожного рядка u, $u \cdot e = e \cdot u = u$. Іншими словами, розглядаючи конкатенацію як алгебраїчну операцію над множиною A^* всіх рядків, отримуємо, що e є одиничним елементом. Також очевидно, що, в загальному випадку, конкатенація асоціативна, але не комутативна.

Говорячи алгебраїчною мовою, A^* разом з операцією конкатенації утворює *вільну* (*некомутативну*) *полугруппу з одиницею* (*некомутативний моноїд*).

Для заданого рядка u рядок v є *підрядком* u, якщо існують рядки x і y, такі, що $u = xvy$.

Далі, для заданого рядка u рядок v є *префіксом (головою)* рядка u, якщо існує рядок w, такий, що $u = vw$. Для заданого рядка u, рядок v є *суфіксом (хвостом)* рядка u, якщо існує рядок w, такий, що $u = wv$. Префікс (суфікс, підрядок) v називається *власним*, якщо підрядок v відмінний від u.

3.6.2 Домени дерев та дерева

Нехай $C_{\mathbf{N}}$ позначає множину десяткових цифр $0, 1, \dots, 9$. Тоді $C^*_{\mathbf{N}} = \{e\} \cup \mathbf{N}^*_+$, впорядкованих природним чином.

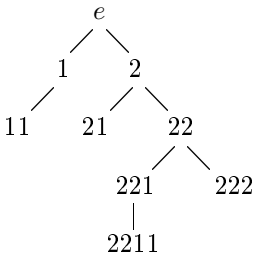
Доменом D дерева є непуста підмножина рядків з $C^*_{\mathbf{N}}$, яка задовольняє умовам:

(1) для кожного рядка $u \in D$ будь-який його префікс, включаючи e, знаходиться в D;

(2) для кожних $u \in D$ та $i \in C_{\mathbf{N}}^{*}$ з того, що $ui \in D$, випливає, що для будь-якого j $(1 \leqslant j \leqslant i)$ рядок uj знаходиться в D.

Приклад 3.1. Домен $D^{\#} = \{e,\ 1,\ 2,\ 11,\ 21,\ 22,\ 221,\ 222,\ 2211\}$ графічно може бути подано у такому вигляді (відповідно порядку $\preceq$ з розділу нижче про степені):

Графічне подання домену $D^{\#}$:

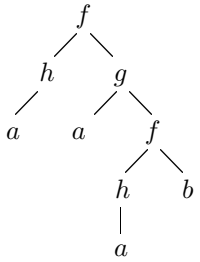


Нехай є домен D дерева і задано множину Σ елементів (званих мітками). Тоді Σ-*деревом* (або просто *деревом*, коли не виникає двозначностей) називається будь-яка функція $t : D \to \Sigma$.

Домен дерева t позначається $dom(t)$. Кожен рядок u в $dom(t)$ називається *вузлом* (або *вершиною*) дерева.

Приклад 3.2. Нехай $\Sigma = \{f, g, h, a, b\}$. Для домену $D^{\#}$ з прикладу 3.1 дерево $t : D^{\#} \to \Sigma$, що має графік $\{(e, f), (1, h), (2, g), (11, a),\ (21, a),\ (22, f),\ (221, h),\ (222, b),\ (2211, a)\}$, графічно може бути подано в такому вигляді:

Дерево t:



3.6.3 Степені вершин і шляхи

Вихідним степенем $d(u)$ вершини u є потужність множини $\{i \mid ui \in dom(t)\}$.

Зазначимо, що вихідний степінь вершини може бути нескінченним.

Дерево називається *звичайно розгалуженим* тоді і тільки тоді, коли степінь кожної вершини є натуральним (скінченним) числом.

Вершина e (e — пустий рядок) називається *коренем* дерева. (З наведених визначень випливає, що будь-яке дерево має вершину e і вона є тільки коренем.)

Дерево є *скінченним*, якщо множина $dom(t)$ є скінченною.

Якщо u є вершиною в $dom(t)$, то кожна вершина виду $ui \in dom(t)$ з $i \in \mathbf{N}_+$ називається *безпосереднім спадкоємцем* (або *сином*) u.

Кажуть, що всі вершини дерева (тотально) *лексиграфічно впорядковані* порядком $\preceq$, якщо виконується таке: $u \preceq v$ в тому і тільки тому випадку, якщо або u є префіксом v, або існують рядки $x, y, z \in C_{\mathbf{N}}^*$ і цифри $i, j \in C_{\mathbf{N}}$, такі, що $i < j$ як числа, $u = xiy$ і $v = xjz$.

У першому випадку ми говоримо, що u є *попередником* v, а в другому — що u *знаходиться ліворуч* від v. Якщо $y = e$ і $z = e$, то йдеться про те, що xi є *лівий брат* xj ($i < j$).

Дві вершини називаються *незалежними*, якщо u не є префіксом v, і навпаки.

Скінченним шляхом з джерелом u і ціллю v називається скінченна послідовність вершин $u_0, u_1, \ldots, u_n$, така, що $u_0 = u, u_n = v$ і для всякого j ($1 \leqslant j \leqslant n$) має місце $u_j = u_{j-1}i_j$ при деякому $i_j \in C_{\mathbf{N}}$. При цьому n називається довжиною шляху та позначається $length(u_0, u_1, \ldots, u_n)$. Якщо $n = 0$, то ми маємо шлях *довжиною* 0 (або *нульовий шлях*) з u в u.

Гілкою, або *ланцюжком (ланцюгом)*, називається шлях від кореня до листу.

Нескінченний шлях із джерела u є нескінченною послідовністю $u_0, u_1, \ldots, u_n, \ldots$, такою, що $u_0 = u$ і для всіх $j \geqslant$ має місце $u_j = u_{j-1}i_j$ для деякого $i_j \in C_{\mathbf{N}}$.

Якщо дано скінченне дерево t, то *вага вершини* u в $dom(t)$ дорівнює $max(\{length(p) \mid p$ є шлях з u в лист$\})$.

Висотою (або *глибиною*) скінченного дерева називається вага його кореня (довжина найдовшого шляху від кореня до листу).

3.6.4 Піддерева та заміщення піддерев

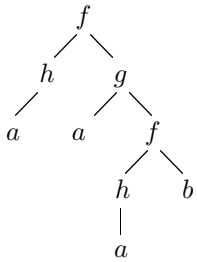
Якщо дано дерево t і його вершина u, то *піддеревом з коренем* u є дерево, яке позначається t/u і доменом якого є множина $\{v \mid uv \in dom(t)\}$, що задовольняє умові $t/u(v) = t(uv)$ для всіх v в $dom(t/u)$.

Важливою операцією над деревами є операція заміщення дерев.

Якщо є два дерева t_1 і t_2, і в дереві t_1 виділена вершина u, то результатом *заміщення піддерева* у вершиніu дерева t_1 на t_2 є функція, яка позначається $t_1[u \leftarrow t_2]$ і графіком якої є множина $\{(v, t_1(v)) \mid u \text{ не є префіксом } v\} \cup \{(uv, t_2(v)\}$.

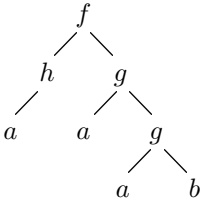
Приклад 3.3. Нехай t і t' є дерева, які мають такі графічні подання (t — дерево з прикладу 3.2):

Дерево t:



Дерево t':

Тоді дерево $t[22 \leftarrow t']$ має такий вигляд:



3.6.5 Ранжовані алфавіти і Σ-дерева

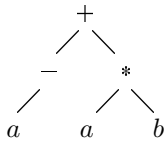
У багатьох ситуаціях є необхідність мати набір символів для іменування операцій з певною (зафіксованою) кількістю аргументів, що приводить до поняття ранжованого алфавіту.

Ранжованим алфавітом називається множина символів Σ разом з *функцією* $r : \Sigma \to \mathbf{N}$ (що ранжує). Тобто, кожному символу $f \in \Sigma$ приписується *ранг* (або, як найчастіше говорять, *арність*) $r(f)$, який визначає ту (фіксовану) кількість аргументів, яка закріплена для f. Кожен символ рангу 0 називається *константою*.

Для кожного $n \geqslant 0$, множина Σ_n позначає підмножину (ранжованої) множини Σ, що складається з усіх символів рангу n, які входять в Σ.

Якщо множина символів (міток) Σ є ранжованим алфавітом, то, як і вище, Σ-деревом називається функція $t : dom(t) \to \Sigma$, для якої додатково виконується умова: для кожної вершини u з $dom(t)$ має місце $d(u) = r(t(u))$. Іншими словами, що вихідний степінь кожної вершини дорівнює рангу її мітки.

Приклад 3.4. Нехай $\Sigma = \{a, b, -, +, *\}$, де a і b мають ранг 0, $-$ має ранг 1, а $+$ і $*$ мають ранг 2. Тоді Σ-дерево має такий вигляд:



4 Про булеві функції

У шкільному курсі математики вивчаються функції двох типів: так звані дійсні функції дійсного змінного та послідовності, що являють собою, як правило, дійсні функції натурального аргументу. У той же час, введене раніше поняття функції, не накладає ніяких обмежень на область визначення і область значення функції. Тому, як би продовжуючи шкільний курс математики в напрямку її сучасного розвитку і використання, ми в цьому розділі зупиняємося на важливому класі функцій — так званих булевих функціях.

Свою назву булеві функції отримали від імені англійського математика Дж. Буля (1815-1864) (який, як це було відмічено раніше, також вніс певний внесок в початковий розвиток теорії множин). З моменту своєї появи ці функції відіграють важливу роль у питаннях основ математики і математичної логіки. З середини 20-го століття булеві функції широко використовуються в різних теоретичних і прикладних задачах дискретної математики та інформатики, а також служать фундаментом для побудови різних обчислювальних пристроїв та/або їх складових частин,наприклад, процесорів сучасних комп'ютерів.

4.1 Поняття булевої функції

Змінна x називається *булевою*, якщо вона здатна приймати тільки два значення 0 ("нуль") і 1 ("одиниця"). В якості прикладу інтерпретації такого роду змінних може виступати звичайний настінний вимикач світла на два положення, коли 1 відповідає положенню вимикача 'включено а 0 — положення 'вимкнено".

Функція називається *булевою*, якщо всі її аргументи є булевими, а сама функція може приймати тільки два значення: 0 і 1.

Більш строго. Нехай $E = \{0, 1\}$, X — деяка зліченна множина булевих змінних, E^n — n-ая декартова ступінь множини E, тобто множина всіх наборів $\langle \alpha_1, \ldots, \alpha_n \rangle$, що складаються з нулів та одиниць, $n \geqslant 1$. Нехай $f^{(n)}$ — відображення множини E^n в E, $n \geqslant 1$, і нехай функція $f^{(n)}(x_1, \ldots, x_n)$ від булевих змінних $x_1, \ldots, x_n$ множини X задає це відображення, де E^n — *область визначення*, E — *область значень*, $x_1, \ldots, x_n$ — булеві змінні, від яких воно зале-

жить. Тоді $f^{(n)}$ називається *булевою* (або *логічною*) функцією, або *функцією алгебри логіки*, а f — *n-місцевим функціональним символом*, відповідним цієї функції. (Верхні індекси у функціональних символів, як правило, опускаються, коли відомо кількість змінних, від яких залежить розглядаєма функція.)

Множину всіх бульових функцій буде позначатися P_2. Так як число (*двійкових*) наборів з 0 і 1 довжини n і звичайно дорівнює 2^n, а кожна функція $f^{(n)}(x_1, \ldots, x_n)$ з P_2 на кожному з 2^n наборів може приймати будь-яке із значень 0 і 1, то *число всіх різних функцій алгебри логіки від змінних* $x_1, \ldots, x_n$ *дорівнює* 2^{2^n}. Таким чином, з одного боку, число функцій від фіксованої (скінченної) множини змінних скінченне, а з іншого – це число дуже швидко зростає з ростом числа змінних.

З теоретико-множинної точки зору функція алгебри логіки $f(x_1, \ldots, x_n)$ — це не просто відображення множини всіх наборів довжини n з нулів та одиниць у множину $\{0, 1\}$, а об'єкт, що складається з такого відображення і впорядкованного набору $x_1, \ldots, x_n$ його бінарних змінних. У сенсі запису функції $f(x_1, x_2, x_3)$ і $f(x_2, x_1, x_3)$, взагалі кажучи, різні, хоча і визначають одне і те ж відображення $\{0, 1\}^3 \mapsto \{0, 1\}$. У відповідності з цим виникає таке поняття рівності булевих функцій, яки мають різні записи: *функції рівні, якщо вони залежать від однієї і тієї ж множини змінних та задають одне і те ж відображення.* А саме, *булеві функції* $f(x_1, \ldots, x_n)$ і $g(x_1, \ldots, x_n)$ від однієї і тиєї ж множини $x_1, \ldots, x_n$ *називаються рівними* (позначення $f = g$), якщо $f(\alpha_1, \ldots, \alpha_n) = g(\alpha_1, \ldots, \alpha_n)$ для будь-якого набору $\alpha_1, \ldots, \alpha_n$ з нулів та одиниць.

4.2 Унарні та бінарні булеві функції

Скінченність області визначення булевої функції має важливу властивість: такі *функції можна задавати у вигляді таблиць значень*, перечисляючи значення функції для різних значень аргументів, розташованих у відповідних стовпцях. Використовуючи саме цей спосіб, задамо унарні і бінарні булеві функції, які у певному сенсі є "аналогами елементарних функцій" в арифметиці і аналізі. (Серед інших способів завдання булевих функцій пізніше ми більш

докладно зупинимося на завданні бульових функцій у вигляді виразів (тобто формул), які являють собою записи, що складаються з констант, бульових змінних та знаків вже введених функцій.)

При $n = 1$ буде всього 4 унарних функції $f(x_1)$, що приведенні в першому рядку таблиці нижче, де 0 — це *функція-константа* 0, яка рівна 0 при будь-якому значенні аргументу, 1 — *функція-константа* 1, яка рівна 1 при будь-якому значенні аргументу, x_1 — *тотожна функція*, $\overline{x_1}$ — *логічне заперечення* (*інверсія*) x_1.

$x_1 \parallel 0$	1	x_1	$\overline{x_1}$
0 ‖ 0	1	0	1
1 ‖ 0	1	1	0

При $n = 2$ буде вже 16 функцій, *які подані у інфіксної формі запису* при наявності двох аргументів, кожен з яких впливає на значення визначається функції.

$x_1\ x_2 \parallel x_1$	$\overline{x_1}$	x_2	$\overline{x_2}$	$x_1 \wedge x_2$	$x_1 \vee x_2$	$x_1 \to x_2$	$x_1 \equiv x_2$	$x_1 \oplus x_2$
0 0 ‖ 0	1	0	1	0	0	1	1	0
0 1 ‖ 0	1	1	0	0	1	1	0	1
1 0 ‖ 1	0	0	1	0	1	0	0	1
1 1 ‖ 1	0	1	0	1	1	1	1	0

$x_1\ x_2 \parallel 0$	1	$x_1 \downarrow x_2$	$x_1 \mid x_2$	$x_1 \leftarrow x_2$	$\overline{x_1 \to x_2}$	$\overline{x_1 \leftarrow x_2}$
0 0 ‖ 0	1	1	1	1	0	0
0 1 ‖ 0	1	0	1	0	0	1
1 0 ‖ 0	1	0	1	1	1	0
1 1 ‖ 0	1	0	0	1	0	0

Кожна із щойно введених функцій має свою індивідуальне ім'я: 0 — *функція-константа 0* (*тотожний нуль*); 1 — *функція-константа 1* (*тотожна одиниця*); x — *тотожна функція* (тобто функція, що переводить x у x); $\overline{x}$ — *логічне заперечення* (*інверсія*) x; $\wedge$ — *кон'юнкція*; $\vee$ — *диз'юнкція*; $\to$ — *пряма* (*матеріальна*) *імплікація*; $\equiv$ — *логічна еквівалентність* (іноді позначається $\leftrightarrow$); $\oplus$ — *додавання за модулем два* (*виключне "або", сума Жегалкина*); $\downarrow$ — *стрілка Пірса* (*антидиз'юнкція*); $\mid$ — *штрих Шеффера* (*антикон'юнкція*); $\leftarrow$ — *зворотна імплікація*; $\overrightarrow{=}$ — *інверсія прямої імплікації*; $\overleftarrow{=}$ — *інверсія зворотної імплікації*.

Тим же самим способом, що був використаний для випадку $n = 2$, можна визначити тетрарні булеві функції (коли $n = 3$) і т.

д. Ми на цьому зупинятися не будемо, а просто зауважимо, що, як це буде показано нижче, *бінарних функцій* (навіть тільки частини їх) *достатньо для того, щоб* за допомогою операції суперпозиції *побудувати будь-яку бінарну функцію* довільної скінченної арності.

4.3 Формули, реалізація булевих функцій формулами. Операції суперпозиції та введення фіктивних змінних

Одним із зручних способів завдання булевих функцій є формули.

Нехай дана деяка (скінченна або зліченна) множина функцій $A = \{f_1(x_1, \ldots, x_{n_1}), f_2(x_1, \ldots, x_{n_2}), \ldots\}$, і B — множина функціональних символів, відповідних функцій з A (тобто $B = \{f_1, f_2, \ldots\}$). Поняття формули над множиною A визначається індуктивно.

1. Вираз x, де x — змінна, є (*тривіальною*) *формулою* над A.

2. Якщо $F_1, \ldots, F_n$ — формули над A, а f — функціональний символ з B, то *вираз F вигляду* $f(F_1, \ldots, F_n)$ (тобто функціональний символ, ліва дужка, формули $F_1, \ldots, F_n$ у цьому порядку, права квадратна дужка), *є формулою над* A; формули $F_1, \ldots, F_n$ називаються *подформулами* формули F. *Подформулами формули* F є також сама формула F і всі підформули формул $F_1, \ldots, F_n$.

3. *Жодних інших формул* над A, крім зазначених у пунктах (1) і (2), *не існує*.

Кожній формулі ставиться у відповідність певна булева функція.

Нехай дана формула $F(x_1, \ldots, x_n)$ над множиною функцій A, де $\{x_1, ..., x_n\}$ — множина всіх змінних цієї формули), і $R = (\langle\alpha_1, \ldots, \alpha_n\rangle$ є деякий набір значень цих змінних. *Значення формули* F (а також значення кожної її підформули) *на наборі змінних* R (позначення — $F|R$) визначається індуктивно.

1. Якщо F — тривіальна формула виду x_i, то $F|R$ *є рівним* α_i.

2. Нехай формула F над A має вигляд $f(F_1, \ldots, F_n)$, де функція $f(F_1, \ldots, F_n)$ належить множині A, $F_1, \ldots, F_n$ — формули над A, для яких значення $F_1|R, \ldots, F_n|R$ вже визначені і рівні

$\beta_1, \ldots, \beta_n$ відповідно. *Тоді* $F|R = f(\beta_1, \ldots, \beta_n)$.

Так як значення формули $F(x_1, \ldots, x_n)$ можна визначити на будь-якому наборі значень змінних $x_1, \ldots, x_n$, то тим самим цій формулі ставиться у відповідність деяка функція $f(x_1, \ldots, x_n)$ з P_2. Про *цю функцію* $f(x_1, \ldots, x_n)$ (задану зазначеним вище способом) кажуть, що вона *реалізується або виражається* формулою $f(F_1, \ldots, F_n)$.

Таким чином, кожна формула виражає якусь функцію алгебри логіки. У цьому випадку говорять, що нові функції породжені із уже наявних у A за допомогою *операції суперпозиції*. Іншими словами, функція f *отримана операцією суперпозиції з функцій системи* A, якщо f реалізована деякою (нетривіальною) формулою над A (або, як ще кажуть, f *записана у сигнатурі* A).

Частковими випадками суперпозиції є наступні операції над булевими функціями: перестановка змінних, перейменування змінних, ототожнення змінних, композиція функцій (тобто підстановка функцій в інші функції на місця їх змінних).

Окремо зупинимося на так званій *операції введення фіктивних змінних* (яка, взагалі кажучи, не є частковим випадком операції суперпозиції).

Змінна x_i функції $f(x_1, \ldots, x_n)$ називається *суттєвою*, якщо існують такі два набору з нулів і одиниць, що розрізняються тільки в i-ої компоненті, що функція f на цих наборах приймає різні значення. У цьому випадку говорять, що функція $f(x_1, \ldots, x_n)$ *суттєво залежить від змінної* x_i.

Змінна x_i, що не є суттєвою, називається *несуттєвою або фіктивною змінною* функції $f(x_1, \ldots, x_n)$; у цьому випадку говорять, що функція $f(x_1, \ldots, x_n)$ *не залежить суттєво від змінної* x_i.

Наприклад, функція $f(x_1, x_2) = x_1 \wedge x_2$ суттєво залежить від змінної x_1, так як $f(0,1) \neq f(1,1)$. Вона також суттєво залежить від змінної x_2, так як $f(1,0) \neq f(1,1)$. Аналогічно показується, що всі інші бінарні функції, що наведені в таблиці вище і мають інфіксну форму запису, суттєво залежать від обох змінних. Очевидно, що функції-константи 0 і 1 не мають суттєвих змінних.

Значення функції на кожному наборі *повністю визначається набором значень її суттєвих змінних*. У зв'язку з цим часто для

зручності використання (і дотримуючись традиції) поняття рівності булевих функцій *поширюється також на функції с різними наборами змінних*, які відрізняються лише несуттєвими змінними, і розуміється наступним чином. *Дві довільні булеві функції називаються рівними*, тоді і тільки тоді, коли у них *множини суттєвих змінних збігаються і на кожному наборі значень цих змінних розглядаємі функції приймають однакові значення.*

Таким чином, можна вважати, що *всяка множина записів (у вигляді формул) булевих функцій разом із записом кожної функції f містить також і всі записи функцій, у яких додатково до змінних із запису f зустрічаються тільки фіктивні змінні.*

Сказане дозволяє наступним чином визначити *операцію введення фіктивних змінних* на розглядуваній множині функцій: якщо запис функції g відрізняється від запису функції f тільки наявністю запису в g фіктивних змінних щодо f і функції f та g рівні, то говорять, що *g отримана з f операцією введення у f фіктивних змінних.*

Наприклад, значення функції $x_1 \vee (x_3 \wedge \overline{x_3})$ збігаються зі значеннями тотожної функції x_1. Тому x_3 є фіктивною змінною для вихідної функції x_1 і, отже, можна вважати, що функція $x_1 \vee (x_3 \wedge \overline{x_3})$ отримана з x_1 введенням в x_1 фіктивної змінної x_3.

Операція введення фіктивних змінних *дозволяє вважати*, з одного боку, коли це потрібно, що при розгляді деякої скінченної сукупності булевих функцій, арности всіх функцій із сукупності збігаються. А з іншого ж боку, вважати, що в записах функцій використовувати тільки їх суттєві змінні. Надалі, *ці угоди часто будуть використовуватися без спеціальних застережень.*

4.4 Логічна еквівалентність формул

Формули, що реалізують однакові функції, називаються *логічно еквівалентними.* Якщо F и F' логічно еквівалентні формули, то ми пишемо $F \asymp F'$ і запис такого сорту називаємо *логічною тотожністю.*

Легко перевіряється рефлексивність, симетричність і транзитивність логічної еквівалентності, тобто вона являється (звичайним) відношенням еквівалентності.

Маючи дві формули F_1 і F_2, ми можемо встановити, чи є вони логічно еквівалентними, чи ні, обчислюючи і порівнюючи їх значення на одних і тих же наборах нулів і одиниць.

Інший спосіб полягає в тому, щоб, маючи вже встановлені тотожності $F_{1,1} \asymp F_{1,2}, \ldots, F_{n,1} \asymp F_{n,2}$, спочатку застосувати одне з них до вихідного виразу F, потім інше до отриманого результату і так далі до тих пір, поки не буде отримано необхідний вираз, скажімо, G (звичайно, якщо є ланцюжок перетворень, що веде від F до G). Виходячи з визначення логічної еквівалентності, отримуємо, що при досяжності G виконується $F \asymp G$; в цьому випадку G називатиметься *формулою, виведеної з F за допомогою тотожностей* $F_{1,1} \asymp F_{1,2}, \ldots, F_{n,1} \asymp F_{n,2}$ за допомогою логічно еквівалентних перетворень.

Надалі в наших формулах будуть зустрічатися тільки функціональні знаки з *сигнатури, що містить позначення унарних і бінарних булевих функцій*, наведені в таблицях вище. При цьому бінарні булеві функції завжди будуть мати вигляд *інфіксного запису*, тобто в формулах знак бінарної функції завжди буде знаходитися між її аргументами. Наприклад, замість $\vee(\oplus(x_1, x_2), \overline{x_3})$ буде писатися $(x_1 \oplus x_2) \vee \overline{x_3}$.

Перерахуємо ряд базових тотожностей, які відіграють важливу роль в теорії булевих функцій і кожне з яких легко доводиться перевіркою того, що їх ліва і права частини реалізують одну й ту ж булеву функцію, що встановлюється за допомогою обчислень, що задаються цими частинами з урахуванням визначення функцій в наведених вище таблицях істинності. Відразу відзначимо "повторення" законами (1)–(10) аксіом (1)–(10) булевих алгебр і, отже, властивостей (1–(10) теоретико-множинних операцій. Такий збіг не випадковий і вдумливий читач легко знайде йому пояснення.

(1) *Ідемпотентність кон'юнкції та диз'юнкції*: $x_1 \vee x_1 \asymp x_1$, $x_1 \wedge x_1 \asymp x_1$.

(2) *Комутативність операцій* $\vee$, $\wedge$, $\oplus$: $x_1 \vee x_2 \asymp x_2 \vee x_1$, $x_1 \wedge x_2 \asymp x_2 \wedge x_1$, $x_1 \oplus x_2 \asymp x_2 \oplus x_1$.

(3) *Асоціативність операцій* $\vee$, $\wedge$, $\oplus$: $x_1 \vee (x_2 \vee x_3) \asymp (x_1 \vee x_2) \vee x_3$, $x_1 \wedge (x_2 \wedge x_3) \asymp (x_1 \wedge x_2) \vee x_3$, $x_1 \oplus (x_2 \oplus x_3) \asymp (x_1 \oplus x_2) \oplus x_3$.

(4) *Закони поглинання*: $x_1 \wedge (x_1 \vee x_2) \asymp x_1$, $x_1 \vee (x_1 \wedge x_2) \asymp x_1$.

(5) *Дистрибутивність*: $(x_1 \vee x_2) \wedge x_3 \asymp (x_1 \wedge x_3) \vee (x_2 \wedge x_3)$, $(x_1 \wedge x_2) \vee x_3 \asymp (x_1 \vee x_3) \wedge (x_2 \vee x_3)$, $(x_1 \oplus x_2) \wedge x_3 \asymp (x_1 \wedge x_3) \oplus (x_2 \wedge x_3)$.

(6) *Правила де Моргана*: $\overline{(x_1 \wedge x_2)} \asymp \overline{x_1} \vee \overline{x_2}$, $\overline{(x_1 \vee x_2)} \asymp \overline{x_1} \wedge \overline{x_2}$.

(7) *Властивості нуля*: $x_1 \vee 0 \asymp x_1$, $x_1 \wedge 0 \asymp= 0$, $\overline{0} \asymp 1$, $x_1 \oplus 0 \asymp x_1$.

(8) *Властивості одиниці*: $x_1 \vee 1 \asymp 1$, $x_1 \wedge 1 \asymp x_1$, $\overline{1} \asymp 0$, $x_1 \oplus 1 \asymp \overline{x_1}$.

(9) *Закон зняття подвійного заперечення (інволютивність заперечення)*: $\overline{\overline{x_1}} = x_1$.

(10) *Властивості заперечення*: $x_1 \vee \overline{x_1} = 1$, $x_1 \wedge \overline{x_1} = 0$, $x_1 \oplus \overline{x_1} = 1$, $x_1 \oplus x_1 = 0$.

(11) *Деякі корисні тотожності*: $x_1 \to x_2 = \overline{x_1} \vee x_2$, $x_1 \equiv x_2 = (x_1 \to x_2) \wedge (x_2 \to x_1) = (\overline{x_1} \vee x_2) \wedge (\overline{x_2} \vee x_1) = (x_1 \wedge x_2) \vee (\overline{x_1} \wedge \overline{x_2})$, $x_1 \oplus x_2 = (x_1 \wedge \overline{x_2}) \vee (\overline{x_1} \wedge x_2) = (x_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{x_2})$.

Як приклад табличного способу доведення наведених логічних тотожностей встановимо справедливість першого закону де Моргана, який стверджує, що $\overline{(x_1 \vee x_2)} \asymp \overline{x_1} \wedge \overline{x_2}$. Для цього побудуємо нвступну таблицю істинності для формул $\overline{(x_1 \vee x_2)}$ і $\overline{x_1} \wedge \overline{x_2}$, що реалізують функції, значення яких розташовані в третьому і шостому стовпчиках і обчислення яких проводиться через попереднє послідовне обчислення значень функцій, реалізують підформули формул $\overline{(x_1 \vee x_2)}$ и $\overline{x_1} \wedge \overline{x_2}$.

x_1	x_2	$x_1 \vee x_2$	$\overline{x_1 \vee x_2}$	$\overline{x_1}$	$\overline{x_2}$	$\overline{x_1} \wedge \overline{x_2}$
0	0	0	1	1	1	1
0	1	1	0	1	0	0
1	0	1	0	0	1	0
1	1	1	0	0	0	0

Порівнюючи значення в третьому і шостому стовпчиках цієї таблиці, отримуємо, що $\overline{(x_1 \vee x_2)}$ і $\overline{x_1} \wedge \overline{x_2}$ реалізують одну й ту ж функцію. Значить, $\overline{(x_1 \vee x_2)} \asymp \overline{x_1} \wedge \overline{x_2}$. Більш того, з таблиць істинності вихідних булевих функцій отримуємо, що цю ж функцію також реалізує вираз $x_1 \downarrow x_2$. Тому для стрілки Пірса маємо $x_1 \downarrow x_2 \asymp \overline{(x_1 \vee x_2)} \asymp \overline{x_1} \wedge \overline{x_2}$.

Також на конкретному прикладі продемонструємо, як проводиться доведення тотожностей за допомогою побудови ланцюж-

ка перетворень (виведення) вихідної тотожності з використанням для досягнення бажаного результату (як правило, отримання найкоротшої формули) вже наявних тотожностей (в нашому прикладі в якості останніх виступатимуть деякі тотожності з (1)–(10)).

$\overline{((a \vee \overline{b}) \wedge b) \to a} \asymp \langle$на підставі (11)$\rangle$ $\overline{((a \vee \overline{b}) \wedge b) \vee a} \asymp \langle$на підставі (6)$\rangle$ $\overline{((a \vee \overline{b}) \wedge b)} \wedge \overline{a} \asymp \langle$на підставі (6)$\rangle$ $\overline{((a \vee \overline{b}) \vee \overline{b})} \wedge \overline{a} \asymp \langle$на підставі (6)$\rangle$ $\overline{((\overline{a} \wedge \overline{\overline{b}}) \vee \overline{b})} \wedge \overline{a} \asymp \langle$на підставі (9)$\rangle$ $((\overline{a} \wedge b) \vee \overline{b}) \wedge \overline{a} \asymp \langle$на підставі (2)$\rangle$ $(\overline{b} \vee (\overline{a} \wedge b)) \wedge \overline{a} \asymp \langle$на підставі (5)$\rangle$ $((\overline{b} \vee \overline{a}) \wedge (\overline{b} \vee b)) \wedge \overline{a} \asymp$ $\langle$на підставі (10)$\rangle$ $((\overline{b} \vee \overline{a}) \wedge 1) \wedge \overline{a} \asymp \langle$на підставі (8)$\rangle$ $(\overline{b} \vee \overline{a}) \wedge \overline{a} \asymp \langle$на підставі (4)$\rangle$ $\overline{a}$. (Очевидно, що формула $\overline{a}$ являється далі неспрощуємой, тобто є найкоротшою.) Остаточно маємо $\overline{((a \vee \overline{b}) \wedge b) \to a} \asymp \overline{a}$.

Використовуючи базові тотожності, можна отримати правила, що полегшують читання складних виразів. Наприклад, на підставі асоціативності диз'юнкції в диз'юнкції з декількох членів можна не звертати увагу на порядок розстановки дужок між диз'юнктивними членами; аналогічно можна чинити і для операцій кон'юнкції і додавання за модулем два, що веде до того, що у нас допускаються записи $x_1 \wedge x_2 \wedge \ldots \wedge x_n$, $x_1 \vee x_2 \vee \ldots \vee x_n$ і $x_1 \oplus x_2 \oplus \ldots \oplus x_n$. (При $n = 1$ кожне з виразів такого сорту являє собою його єдиний член (в нашому випадку, змінну x_1). На підставі законів коммутативности в кон'юнкціях, диз'юнкція та сумах за модулем два можна міняти місцями їх члени, і ці перетворення будуть приводити до формул, логічно тотожних вихідної. Закони дистрибутивности дозволяють вносити і виносити знак кон'юнкції з-під знака диз'юнкції і додавання за модулем два, і такий список досить очевидних перетворень, що зберігають логічну тотожність, може бути легко продовжений. Подробиці можна знайти у наявній літературі з булевих функцій, зокрема, у рекомендованої літератури.

4.5 Стандартні подання булевих функцій

У цьому розділі ми показуємо, що будь-яка булева функція довільної арности може бути подана у вигляді суперпозиції деяких з введених вище функцій.

Визначимо функцію зведення в степінь x^δ наступним чином (x — змінна). Покладемо $x^\delta = x$, якщо $\delta = 1$, $x^\delta = \overline{x}$, якщо $\delta = 0$.

Твердження 4.1 (про розклад булевої функції у диз'юнкцію). Будь-яку булеву функцію $f(x_1, \ldots, x_n)$ $(n \geqslant 1)$, відмінну від 0, можна подати у вигляді $g(x_1, \ldots, x_n) = \bigvee_{\langle \delta_1, \ldots, \delta_m \rangle} (x_1^{\delta_1} \wedge \ldots \wedge x_m^{\delta_m} \wedge f(\delta_1, \ldots, \delta_m, x_{m+1}, \ldots, x_n))$, де $1 \leqslant m \leqslant n$ і диз'юнкція береться по усім можливим наборам $\langle \delta_1, \ldots, \delta_m \rangle$, що складаються з нулів та одиниць. При цьому, $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$ і розклад $f(x_1, \ldots, x_n)$ в диз'юнкцію є єдиним з точністю до порядку диз'юнктивних членів у $g(x_1, \ldots, x_n)$ і кон'юнктивних членів у диз'юнкціях.

Доведення. Перш за все зауважимо, що якщо $\langle \alpha_1, \ldots, \alpha_m \rangle$ — набір з нулів і одиниць, то $\alpha_1^{\delta_1} \wedge \ldots \wedge \alpha_m^{\delta_m} = 1$ тоді і тільки тоді, коли $\alpha_i = \delta_i$ $(i = 1, \ldots, m)$.

Візьмемо довільний набір $\langle \alpha_1, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_n \rangle$ з нулів і одиниць і припустимо, що $f(\alpha_1, \ldots, \alpha_n) = 1$. Оскільки диз'юнкція $g(x_1, \ldots, x_n)$ береться по усім можливим наборам $\langle \delta_1, \ldots, \delta_m \rangle$, то серед них знаходиться і набір $\langle \alpha_1, \ldots, \alpha_m \rangle$. Тому $\alpha_1^{\alpha_1} \wedge \ldots \wedge \alpha_m^{\alpha_m} \wedge f(\alpha_1, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_n) = 1$. Остання кон'юнкція є диз'юнктивним членом диз'юнкції $g(\alpha_1, \ldots, \alpha_n)$. Значить, $g(\alpha_1, \ldots, \alpha_n) = 1$.

Тепер припустимо, що $f(\alpha_1, \ldots, \alpha_n) = 0$. Тоді диз'юнктивний член $\alpha_1^{\alpha_1} \wedge \ldots \wedge \alpha_m^{\alpha_m} \wedge f(\alpha_1, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_n)$ диз'юнкції $g(\alpha_1, \ldots, \alpha_n)$ дорівнює 0. Решта її диз'юнктивних членів також дорівнюють 0, так як у кожному наборі $\langle \delta_1, \ldots, \delta_m \rangle$, що задають такий диз'юнктивний член, є $\delta_i \neq \alpha_i$ і, отже, $\alpha_i^{\delta_i} = 0$, що тягне $\alpha_1^{\delta_1} \wedge \ldots \wedge \alpha_m^{\delta_m} \wedge f(\alpha_1, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_n) = 0$. Значить, $g(\alpha_1, \ldots, \alpha_n) = 0$.

Спосіб визначення $g(x_1, \ldots, x_n)$ тягне єдиність розкладу $f(x_1, \ldots, x_n)$ у диз'юнкцію з вказаною точністю. *Кінець доведення.*

Звертаємо увагу на окремий випадок цього твердження, коли $f(x_1, \ldots, x_n)$ є функція-константа, яка рівна або 1, або 0.

У першому випадку, ми, виходячи з твердження 4.1, отримуємо, що функція-константа 1 може бути подана у вигляді $\bigvee_{\langle \delta_1, \ldots, \delta_m \rangle} (x_1^{\delta_1} \wedge \ldots \wedge x_m^{\delta_m})$, де кон'юнкція береться по всіляким наборам $\langle \delta_1, \ldots, \delta_m \rangle$, що складаються з нулів і одиниць. У другому ж випадку у нас виявляється, що для функція-константа 0 її представлення $g(x_1, \ldots, x_n)$ має бути диз'юнкцією з нулевим числом своїх членів. Тому вважається, що *за визначенням* 0 *представляє*

необхідне розкладання 0.

Як наслідок твердження 4.1 отримуємо результат про можливості подання будь-якої булевої функції $f(x_1, \ldots, x_n)$, відмінної від функції-константи 0, у вигляді *досконалої диз'юнктивної нормальної форми* (ДДНФ), що позначається ДДНФ(f), під якою розуміється вираз вигляду $\bigvee_{\langle\delta_1,\ldots,\delta_n\rangle}(x_1^{\delta_1} \wedge \ldots \wedge x_n^{\delta_n})$, де диз'юнкція береться по усім можливим наборам $\langle\delta_1, \ldots, \delta_n\rangle$ з нулів і одиниць, таким, що виконується рівність $f(\delta_1, \ldots, \delta_n) = 1$. Що ж торкається *функції-константи* 0, то з огляду на вищесказане символ 0 є її ДДНФ.

Наслідок 4.1. Будь-яку булеву функцію можна подати у досконалій диз'юнктивній нормальній формі. При цьому, таке подання є єдиним з точністю до порядку дизъюнктивных членів у ДДНФ і кон'юнктивних членів у диз'юнкціях.

Доведення. Для доведення цього наслідку у разі розгляду функції $f(x_1, \ldots, x_n)$, відмінної від 0, у твердженні 4.1 достатньо взяти $m = n$ і скористатися визначенням диз'юнкції, що дозволяє з $g(x_1, \ldots, x_n)$ видалити диз'юнктивні члени, що задаються наборами, на яких $f(x_1, \ldots, x_n)$ приймає значення 0.

У випадку, коли $f(x_1, \ldots, x_n)$ є функція-константа 0, пуста диз'юнкція, що була позначена 0, дає потрібне. *Кінець доведення.*

При переході від твердження 4.1 до його "двоїстого" формулювання для кон'юнкції отримуємо такий результат.

Твердження 4.2 (про розклад булевої функції у кон'юнкцію). Будь-яку булеву функцію $f(x_1, \ldots, x_n)$ $(n \geqslant 1)$, відмінну від 0 і 1, можна подати у вигляді $g(x_1, \ldots, x_n) = \bigwedge_{\langle\delta_1,\ldots,\delta_m\rangle}(\overline{x_1}^{\delta_1} \vee \ldots \vee \overline{x_m}^{\delta_m} \vee f(\delta_1, \ldots, \delta_m, x_{m+1}, \ldots, x_n))$, де $1 \leqslant m \leqslant n$ і кон'юнкція береться по усім можливим наборам $\langle\delta_1, \ldots, \delta_m\rangle$, що складаються з нулів та одиниць. При цьому, $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$ і розклад $f(x_1, \ldots, x_n)$ у кон'юнкцію є єдиним з точністю до порядку кон'юнктивних членів у $g(x_1, \ldots, x_n)$ і диз'нктивних членів у кон'юнкціях.

Доведення. Перш за все зауважимо, що якщо $\langle\alpha_1, \ldots, \alpha_m\rangle$ — набір з нулів і одиниць, то $\overline{\alpha_1}^{\delta_1} \vee \ldots \vee \overline{\alpha_m}^{\delta_m} = 0$ і тоді тільки тоді, коли $\alpha_i = \delta_i$ $(i = 1, \ldots, m)$.

Візьмемо довільний набір $\langle\alpha_1, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_n\rangle$ з нулів і одиниць і припустимо, що $f(\alpha_1, \ldots, \alpha_n) = 0$. Оскільки

кон'юнкція $g(x_1, \ldots, x_n)$ береться по усім можливим наборам $\langle \delta_1, \ldots, \delta_m \rangle$, то серед них знаходиться і набір $\langle \alpha_1, \ldots, \alpha_m \rangle$. Тому $\overline{\alpha_1}^{\alpha_1} \vee \ldots \vee \overline{\alpha_m}^{\alpha_m} \vee \ f(\alpha_1, \ldots, \alpha_m, \ \alpha_{m+1}, \ldots, \alpha_n) = 0$. Остання диз'юнкція є кон'юнктивним членом кон'юнкції $g(\alpha_1, \ldots, \alpha_n)$. Значить, $g(\alpha_1, \ldots, \alpha_n) = 0$.

Тепер припустимо, що $f(\alpha_1, \ldots, \alpha_n) = 1$. Тоді кон'юнктивний член $\overline{\alpha_1}^{\alpha_1} \vee \ldots \vee \overline{\alpha_m}^{\alpha_m} \vee f(\alpha_1, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_n)$ кон'юнкції $g(\alpha_1, \ldots, \alpha_n)$ дорівнює 1. Решта її кон'юктивні члени також дорівнюють 1, так як в кожному наборі $\langle \delta_1, \ldots, \delta_m \rangle$, задають кон'юнктивний член, є $\delta_i \neq \alpha_i$ і, отже, $\overline{\alpha_i}^{\delta_i} = 1$, що тягне $\overline{\alpha_1}^{\delta_1} \vee \ldots \vee \overline{\alpha_m}^{\delta_m} \vee f(\alpha_1, \ \ldots, \ \alpha_m, \ \alpha_{m+1}, \ \ldots, \ \alpha_n) = 1$. Значить, $g(\alpha_1, \ldots, \alpha_n) = 1$.

Спосіб визначення $g(x_1, \ldots, x_n)$ тягне єдиність розкладання $f(x_1, \ldots, x_n)$ в кон'юнкцію з вказаною точністю. *Кінець доведення.*

Звертаємо увагу на окремий випадок цього твердження, коли $f(x_1, \ldots, x_n)$ є функція-константа, яка рівна або 1, або 0.

У першому випадку, ми, виходячи з твердження 4.2, отримуємо, що функція-константа 0 може бути подана у вигляді $\bigwedge_{\langle \delta_1, \ldots, \delta_m \rangle} (\overline{x_1}^{\delta_1} \vee \ldots \vee \overline{x_m}^{\delta_m})$, де кон'юнкція береться по всіляким наборам $\langle \delta_1, \ldots, \delta_m \rangle$, що складаються з нулів і одиниць. У другому ж випадку у нас виявляється, що для функції-константи 1 її представлення $g(x_1, \ldots, x_n)$ має бути кон'юнкцією з нулевим числом своїх членів. Тому вважається, що *за визначенням* 1 *представляє необхідне розкладання* 1.

Як наслідок твердження 4.2 отримуємо результат про можливості подання будь-якої булевої функції $f(x_1, \ldots, x_n)$, відмінної від функції-константи 1, у вигляді *досконалої кон'юнктивної нормальної форми* (ДКНФ), що позначається ДКНФ(f), під якою розуміється вираз вигляду $\bigwedge_{\langle \delta_1, \ldots, \delta_n \rangle} (\overline{x_1}^{\delta_1} \vee \ldots \vee \overline{x_n}^{\delta_n})$, де диз'юнкція береться по усім можливим наборам $\langle \delta_1, \ldots, \delta_n \rangle$ з нулів і одиниць, таким, що виконується рівність $f(\delta_1, \ldots, \delta_n) = 1$. Що ж торкається *функції-константи* 1, то з огляду на вищесказане символ 1 є її ДКНФ.

Наслідок 4.2. Будь-яку булеву функцію можна подати у вигляді досконалої конъюнктивной нормальній формі. При цьому, такє предстаелення є єдиним з точністю до порядку кон'юнктивних членів у ДКНФ і диз'юнктивних членів у кон'юнкціях.

Доведення. Для доведення цього наслідку у разі розгляду функції $f(x_1, \ldots, x_n)$, відмінної від 1, у твердженні 4.1 достатньо взяти $m = n$ і скористатися визначенням кон'юнкції, що дозволяє з $g(x_1, \ldots, x_n)$ видалити кон'юнктивні члени, що задаються наборами, на яких $f(x_1, \ldots, x_n)$ приймає значення 1.

У випадку, коли $f(x_1, \ldots, x_n)$ є функція-константа 1, пуста кон'юнкція, що була позначена 1, дає потрібне. *Кінець доведення.*

Вищесказане показує, що будь-яка булева функція може бути подана у вигляді суперпозиції кон'юнкції, диз'юнкції і заперечення, тобто, іншими словами, вона *може бути виражена (подана) у сигнатурі* $\{\wedge, \vee, -\}$ ($-$ позначає заперечення).

Звертаємо увагу на те, що якщо ми вважаємо, що диз'юнкція і кон'юнкція з нульовими числами своїх членів також вимагають такого представлення, то 0 і 1 повинні бути додані в сигнатуру $\{\wedge, \vee, -\}$.

Поняття досконалих диз'юнктивної і конъюнктивной нормальних форм дають простий спосіб подання будь-якої булевої функції у вигляді виразу (формули) у сигнатурі $\{\wedge, \vee, -\}$, якщо у нас є таблиця значень функції.

Щоб отримати досконалу дизъюнктивную нормальну форму, треба взяти все набори, на яких значення функції дорівнює 1 і записати для кожного з них кон'юнкцію змінних та їх заперечень. Якщо в наборі значення змінної є 0, то змінну треба взяти з запереченням, якщо 1, то без заперечення. З одержаних конъюнкций змінних та заперечень змінних треба побудувати диз'юнкцію.

Щоб отримати досконалу конъюнктивную нормальну форму, треба взяти все набори, на яких значення функції дорівнює 0 і записати для кожного з них диз'юнкцію змінних і їх заперечень. Якщо в наборі значення змінної є 0, то змінну треба взяти без заперечення, якщо 1, то з запереченням. З одержаних дизъюнкций змінних та заперечень змінних треба побудувати кон'юнкцію.

В якості прикладу побудуємо ДДНФ і ДКНФ функції $f(x, y, z)$, таблично заданої наступним чином: вона приймає значення 1 на наборах (0,1,1), (1,0,1), (1,1,0) і (1,1,1) і значення 0 в інших випадках:

$$\text{ДДНФ}(f(x, y, z)) = (\overline{x} \wedge y \wedge z) \vee (x \wedge \overline{y} \wedge z) \vee (x \wedge y \wedge \overline{z}) \vee (x \wedge y \wedge z),$$
$$\text{ДКНФ}(f(x, y, z)) = (x \vee y \vee z) \wedge (x \vee y \vee \overline{z}) \wedge (x \vee \overline{y} \vee z) \wedge (\overline{x} \vee y \vee z).$$

4.6 Мінімізація булевих функцій

Якщо звернутися до щойно розглянутих прикладів ДДНФ ($f^*(x,y,z)$) і ДКНФ($f^*(x,y,z)$), то можна побачити, що булеві вирази $(\overline{x} \wedge \overline{y}) \vee (x \wedge \overline{y} \wedge z) \vee (x \wedge y \wedge \overline{z}) \vee (x \wedge y \wedge z)$ і $(x \vee \overline{y}) \wedge (\overline{x} \vee y \vee z)$ реалізують ту ж функцію $f^*(x,y,z)$, але містять менше число символів в своїх записах, ніж ДДНФ ($f^*(x,y,z)$) і ДКНФ($f^*(x,y,z)$). Це призводить до так званої *задачі мінімізації булевих функцій*, яка полягає, в контексті даного розгляду, у вивченні підходів до побудови "найкоротших " представлень заданої булевої функції у вигляді булевих виразів, що складаються з змінних і знаків булевих операцій диз'юнкції, кон'юнкції і заперечення. Її ми тут докладно вивчати не будемо, а зупинимося на її основних положеннях і переліку деяких способів її вирішення, зауваживши, що вона виникла в електричної та комп'ютерної інженерії, де мінімізація активно використовується для зменшення електронних компонентів в перемикальних схемах і комп'ютерних пристроях.

Введемо деяку термінологію.

Якщо x — змінна, то як сама змінна x, так і її логічне заперечення $\overline{x}$ називаються *літерами*.

Вираз виду $u_1 \wedge \ldots \wedge u_n$ $(u_1 \vee \ldots \vee u_n)$, де $u_1, \ldots, u_n$ — літери, називається *кон'юнктом*, або *кон'юнкцією* (*диз'юнктом*, або *диз'юнкцією*).

Кон'юнкт $u_1 \wedge \ldots \wedge u_n$ (диз'юнкт $u_1 \vee \ldots \vee u_n$), побудований з використанням всіх змінних $x_1, \ldots, x_m$ або деяких з них, називається *кон'юнктивною імплікантою* (*диз'юнктивною імплікантою*) булевої функції $f(x_1, \ldots, x_m)$ тоді і тільки тоді, коли з того, що на деякому наборі булевих значень змінних $x_1, \ldots, x_m$ кон'юнкт $u_1 \wedge \ldots \wedge u_n$ (диз'юнкт $u_1 \vee \ldots \vee u_n$) приймає значення, рівне 1 (рівне 0), випливає, що і функція $f(x_1, \ldots, x_m)$ на цьому ж наборі змінних $x_1, \ldots, x_m$ приймає значення, рівне 1 (значення, рівне 0).

Очевидно, що диз'юнкція (кон'юнкція) будь-якого числа кон'юнктивних (диз'юнктивних) імплікант булевої функції поводиться як кон'юнктивна (диз'юнктивна) імпліканта цієї функції.

Нехай $u_{1,1}, \ldots, u_{1,n_1}, \ldots u_{m,1}, \ldots, u_{m,n_m}$ — літери. Тоді вираз $(u_{1,1} \wedge \ldots \wedge u_{1,n_1}) \vee \ldots \vee (u_{m,1} \wedge \ldots \wedge u_{m,n_m})$ $((u_{1,1} \vee \ldots \vee u_{1,n_1}) \wedge \ldots \wedge (u_{m,1} \vee \ldots \vee u_{m,n_m}))$ називається *диз'юнктивній нормаль-*

ною формою, ДНФ (*кон'юнктивной нормальною формою, КНФ*).

З цього визначення випливає, що ДДНФ і ДКНФ відносяться до класу ДНФ і КНФ.

Кон'юнктивна (диз'юнктивна) імпліканта булевої функції називається *простий*, якщо ніяка її власна частина не є кон'юнктивной (диз'юнктивной) імплікантой цієї функції.

ДНФ (КНФ) булевої функції називається *скороченою* ДНФ (*скороченою* КНФ), якщо і тільки якщо ця ДНФ (КНФ) складається з усіх простих кон'юнктивних (диз'юнктивних) імплікант розглядаємої функції і тільки їх.

Якщо кон'юнктивна (диз'юнктивна) імпліканта булевої функції є кон'юнкт з її ДДНФ (диз'юнкт з її ДКНФ), то цей кон'юнкт (диз'юнкт) називається *кон'юнктивною конституєнтою* 1 (*диз'юнктивнію конституєнтою* 0) розглядаємої функції.

Значить, *ДДНФ (ДКНФ) булевої функції являє собою диз'юнкцію (кон'юнкцію) всіх її кон'юнктивних конституєнт* 1 *(диз'юнктивних конституєнт* 0). Тому, викреслюючи в кон'юнктивних (диз'юнктивних) конституєнтах ДДНФ (ДКНФ) розглядаємої функції літери до тих пір, поки ці конституєнти не перетворяться в її прості кон'юнктивні імпліканти 1 (прості диз'юнктивні імпліканти 0), і видаляючи потім в отриманому результаті повторювані прості імпліканти, якщо такі є, ми на підставі наслідків 4.1 і 4.2 отримуємо наступний результат.

Твердження 4.3. Будь-яка булева функція може бути подана в вигляді скороченої ДНФ (скороченої КНФ).

Як правило, скорочена ДНФ (скорочена КНФ) булевої функції є коротшою, ніж її ДДНФ (ДКНФ). Наприклад, ДНФ і КНФ, наведені на початку цього розділу для функції $f^*(x, y, z)$, викреслюванням в них літер можуть бути перетворені в вирази $(y \wedge z) \vee (x \wedge z) \vee (x \wedge y)$ і $(x \vee y) \wedge (x \vee z) \wedge (y \vee z)$, що являють собою *скорочені* ДНФ і КНФ для $f^*(x, y, z)$ і являються більш короткими, ніж її ДДНФ і ДКНФ. Тому хотілося б мати певний метод побудови скорочених ДНФ і КНФ з наявних ДДНФ і ДКНФ, діючий більш оптимально, ніж повний перебір всіляких конституєнт з викреслюванням в них "зайвих" літер з подальшою перевіркою отриманих кон'юнктів (диз'юнктів) на предмет виконання для них умови "бути простими кон'юнктивними (диз'юнктивними) імплікантами".

Такі методи були розвинені низкою дослідників і серед них найбільш відомими є метод Куайна, метод Куайна–Мак-Класкі, метод Блейка–Порецкого, метод діаграм Вейча, метод Петрика. В якості ілюстрації їх застосування розглянемо метод Куайна для випадку ДДНФ (уважний читач легко перенесе його на "двоїстий" випадок ДКНФ.)

Метод Куайна містить два правила перетворення ДНФ, а саме: перетворення за *правилом склеювання* і перетворення за *правилом поглинання*. (Зауважимо, що вирази, які беруть участь у формулюванні правил, розглядаються з точністю до перестановки їх кон'юнктивних і диз'юнктивних членів.)

Правило склеювання: У ДНФ вигляду $D \vee (u \wedge C) \vee D' \vee (\widetilde{u} \wedge C \wedge C') \vee D''$ *слід диз'юнктивно додати кон'юнкт* $C \wedge C'$. Тобто результатом застосування правила склейки до вихідної ДНФ є (нова) ДНФ $(C \wedge C') \vee D \vee (u \wedge C) \vee D' \vee (\widetilde{u} \wedge C \wedge C') \vee D''$. (Тут C і C' — (можливо, пусті) кон'юнкти, D, D' і D'' — (можливо, пусті) ДНФ, а u і $\widetilde{u}$ — такі літери, що якщо u — змінна x, то $\widetilde{u} \in \overline{x}$, і навпаки, якщо $u \in \overline{x}$, то $\widetilde{u}$ є змінна x.)

Правило поглинання: З ДНФ $D \vee C \vee D' \vee (C \wedge C') \vee D''$ *слід викреслити кон'юнкт* $C \wedge C'$ (C *поглинає* $C \wedge C'$). Тобто результатом застосування правила поглинання є ДНФ $D \vee C \vee D' \vee D''$.

Метод Куайна складається в застосуванні правил склейки і поглинання, починаючи з їх застосування до вихідної ДДНФ і потім до послідовно одержуємих результатів до тих пір, поки вони можуть бути застосовані з породження нових ДНФ. При цьому *ДНФ, породжена останній, є шуканою скороченою ДНФ для вихідної булевої функції, поданої у вигляді ДДНФ*. Доведення цього результату тут опущено, але його легко знайти в літературі по методам мінімізації булевих функцій.

В принципі, в методі Куайна можна не накладати ніяких обмежень на порядок застосування правил склейки і поглинання — результат буде одним і тим же при будь-якому порядку їх застосувань. Але на практиці зазвичай реалізується так звана *процедура насичення рівнів*:

1. *ДДНФ*, що побудована для заданої булевої функції, *оголошується ДНФ, що розглядається.*

2. Якщо до даної ДНФ не застосовується правило склеюван-

ня, то ця *ДНФ оголошується шуканою скороченою ДНФ.* В іншому випадку виконується пункт 3 (насичення наступного рівня).

3. Правило склеювання спочатку застосовується до даної ДНФ, а потім — до послідовно породжуємих результатів (висновок правила) *з таким обмеженням на його застосування*: кон'юнкти, що додаються в ДНФ, не мають права брати участь в подальших застосуваннях правила склейки на цьому рівні; також робиться заборона на застосування правила склеювання, обидва кон'юнкти якого ($u \wedge C$ і $\widetilde{u} \wedge C \wedge C'$) вже брали участь в застосуваннях на більш ранніх рівнях. Після виконання всіляких дозволених застосувань правила склейки на поточному рівні виконуються всілякі застосування правила скорочення, *остаточно отримана ДНФ оголошується розглядаємою* і робиться перехід на 2.

Якщо ми застосуємо метод Куайна для мінімізації ДДНФ($f^*(x, y, z)$), то отримаємо таку скорочену ДНФ: $(\overline{x} \wedge \overline{y}) \vee (\overline{y} \wedge z) \vee (x \wedge y) \vee (x \wedge z)$. Здається, що ми досягли мети — для $f^*(x, y, z)$ побудували ДНФ з мінімальних числом літер. Але виявляється, що це не так. Якщо з цієї скороченою ДНФ видалити другу просту (кон'юнктивну) імпліканту, то ДНФ $(\overline{x} \wedge \overline{y}) \vee (x \wedge y) \vee (x \wedge z)$ буде приймати ті ж самі значення, що і функція $f^*(x, y, z)$, а ніяка (диз'юнктивна) частина цієї ДНФ цією властивістю вже володіти не буде. Тобто ми отримуємо, що для остаточного вирішення даної завдання мінімізації ДДНФ нам в побудованій для неї скороченої ДНФ необхідно перебрати всілякі способи диз'юнктивного комбінування її простих імплікант і вибрати таку комбінацію, яка дає ДНФ мінімальної довжини.

Кажуть, що ДНФ, що реалізує булеву функцію $f(x_1, \ldots, x_n)$, є *мінімальною ДНФ* для $f(x_1, \ldots, x_n)$ тоді і тільки тоді, коли вона складається з простих кон'юнктивних імплікант функції $f(x_1, \ldots, x_n)$, і викидання будь-який простий кон'юнктивної імпліканти з цієї ДНФ призводить до ДНФ, вже не здатної реалізувати $f(x_1, \ldots, x_n)$.

Вище ми вже побудували мінімальну ДНФ для $f^*(x, y, z)$, але легко перевірити, що $(\overline{x} \wedge \overline{y}) \vee (x \wedge y) \vee (\overline{x} \wedge z)$ також є мінімальною ДНФ для $f^*(x, y, z)$. Тобто мінімальних ДНФ для розглядаємої функції може бути декілька.

Виникає питання: чи можна для побудови мінімальних ДНФ

замінити повний перебір простих імплікант який-небудь розумною процедурою, що дозволяє у якомусь сенсі оптимально породжувати всі мінімальні ДНФ за наявною скороченою ДНФ? Відповідь позитивна. Наприклад, У. Куайн для цієї мети поряд із щойно описаним методом побудови скороченою ДНФ розробив і так званий *табличний метод Куайна* переходу від скороченої ДНФ до мінімальної ДНФ.

Резюмуючи сказане вище, ми отримуємо, що *будь-яка булева функція може бути подана в вигляді мінімальної ДНФ, причому, таких представлень може бути декілька; існують методи досить оптимального побудови мінімальних ДНФ.*

Все що було вище сказано про способи побудови скороченої ДНФ і мінімальної ДНФ за наявною ДДНФ для даної функції *"двоїстим чином"* переноситься на способи побудови за наявною ДКНФ *скороченої КНФ* і *мінімальної КНФ* (після введення "двоїстого" визначення мінімальної КНФ). Так, для $f^*(x,y,z)$ і її ДКНФ$(f^*(x,y,z)) = (x \vee \overline{y} \vee z) \wedge (x \vee \overline{y} \vee \overline{z}) \wedge (\overline{x} \vee y \vee z)$ отримуємо, що існує єдина для $f^*(x,y,z)$ скорочена КНФ, яка рівна $(x \vee \overline{y}) \wedge (\overline{x} \vee y \vee z)$. Аналіз цієї КНФ, проведений за допомогою табличного методу Куайна в його двоїстому формулюванні, призводить до того, що мінімальна КНФ для $f^*(x,y,z)$ збігається з її скороченою КНФ і ця мінімальна КНФ єдина.

У практичних застосуваннях теорії мінімізації булевих функцій часто *потрібно подати розглядаєму булеву функцію в найкоротшій (без урахування дужок) формі серед усіх її можливих записів, що складаються з булевих змінних і знаків булевих операцій* $-$, $\vee$ і $\wedge$, *навіть відмовляючись від обов'язкового подання цієї функції у вигляді ДНФ або КНФ.* Така найкоротша запис називається *тупиковою* (тобто далі не "спрощуємою") *формою* розглядаємої булевої функції, що призводить до *задачі побудови тупикової форми* заданої булевої функції.

Очевидно, що тупикова форма будь-булевої функції не може містити більше символів, ніж їх містять її мінімальні ДНФ і КНФ. Тому при першому погляді здається, що саме якась із мінімальних ДНФ і КНФ і буде необхідної тупикової формою. Наприклад, можна показати, що побудована вище мінімальна КНФ$(f^*(x,y,z))$ є тупикової формою для $f^*(x,y,z)$, довжина запису якої дорівнює

11 (в той час, як довжина побудованої мінімально ДНФ($f^*(x,y,z)$) дорівнює 18), і ця тупикова форма єдина з точністю до перестановки її кон'юнктивних і диз'юнктивних членів.

Але якщо розглянути булеву функцію $f^{**}(x,y,z)$, яка приймає значення 1 на наборах $(0,0,0)$, $(0,0,1)$, $(0,1,1)$ і $(1,0,1)$ і значення 0 в інших випадках, то вона має такі ДНФ і КНФ: $(\overline{x} \wedge \overline{y}) \vee (\overline{x} \wedge z) \vee (\overline{y} \wedge z)$ (скорочена ДНФ) и $(\overline{y} \vee z) \wedge (\overline{x} \vee z) \wedge (\overline{x} \vee \overline{y})$ (скорочена КНФ).

Легко перевіряється, що *ці скорочені ДНФ і КНФ одночасної є і мінімальними ДНФ і КНФ* для $f^{**}(x,y,z)$ і що їх довжини збігаються і дорівнюють 15 символам. Але вони *не можуть бути тупиковими*, оскільки еквівалентними логічними перетвореннями мінімальна ДНФ легко перетворюється в формулу $(\overline{x \vee y}) \vee ((\overline{x \wedge y}) \wedge z)$, яка містить 11 символів і яка, як можна показати, *є тупиковою*.

Ця тупикова форма *не єдина*. Інший є формула $(\overline{x \wedge y}) \wedge ((\overline{x \vee y}) \vee z)$, яку можна отримати еквівалентними логічними перетвореннями з мінімальної КНФ.

На жаль, поки відсутні хороші рекомендації, як можна оптимально будувати тупикові формули (наприклад, в стилі методу Куайна), і доводиться покладатися або на породження всіляких булевих виразів, довжина яких становить менше мінімуму довжин мінімальних ДНФ і КНФ, з подальшою їх перевіркою на властивість "бути тупиковою формою", або на використання техніки проведення еквівалентних логічних перетворень, спрямованої на "згортання" мінімальних ДНФ і КНФ до тупикових форм.

4.7 Поліноми Жегалкина

Будь-яку булеву функцію можна представити також у вигляді так званого *полінома Жегалкина*.

Розглянемо кон'юнкції вигляду $x_{i,1} \wedge \ldots \wedge x_{i,k_i}$, де для кожного i всі змінні $x_{i,1}, \ldots, x_{i,k_i}$ попарно різні, $k_i \geqslant 0$.

При $k_i = 1$ ми маємо кон'юнкції довжини 1, тобто просто змінні. Як це говорилося вище, функція-константа 1 може розглядатися як пуста кон'юнкція (тобто як кон'юнкція з нульовим числом кон'юнктивних членів). Тому нижче вважається, що 1 є полі-

номом Жегалкина, що складається з єдиної пустої кон'юнкції.

Поліномом Жегалкіна називається булев вираз в сигнатурі $\{1, \wedge, \oplus\}$, що складається з довільного числа кон'юнкцій зазначеного вище виду (включаючи випадок 1), з'єднаних знаком операції додавання за модулем два, і який не містить повторюваних кон'юнкцій (так званих *доданків*), розглядаємих з точністю до порядку запису змінних в них.

Тобто *поліном Жегалкина* є вираз вигляду $(x_{1,1} \wedge \ldots \wedge x_{1,k_1}) \oplus \ldots \oplus (x_{n,1} \wedge \ldots \wedge x_{n,k_n})$ ($n \geqslant 0$ и $k_i \geqslant 0$) з зазначеними вище обмеженнями на його складові частини. Зауважимо, що допускаються поліноми, які складаються тільки з одного кон'юнкта, і що вважається, що за визначенням *порожній поліном* (тобто поліном, який не містить кон'юнкцій і який виникає при $n = 0$) завжди реалізує функцію-константу 0. Також у нас є поліноми, в записі яких зустрічається 1. Наприклад, при $k_1 = 0$ вищевказаний поліном перетворюється в $1 \oplus (x_{2,1} \wedge \ldots \wedge x_{2,k_2}) \oplus \ldots \oplus (x_{n,1} \wedge \ldots \wedge x_{n,k_n})$.

Має місце наступний результат.

Твердження 4.4. Будь-яка булева функція може бути подана у вигляді полінома Жегалкина, причому це подання єдино з точністю до порядку доданків за модулем два і порядку кон'юнктивних членів у доданках.

Доведення. Нагадаємо, що кількість різних булевих функцій від n змінних дорівнює 2^{2^n}. У той же час число всіляких кон'юнкція, які побудовані з n змінних (включаючи кон'юнкцію, що не містить жодної змінної) і серед яких немає жодної пари, що складається з одних і тих же змінних, дорівнює 2^n. Значить, число всіляких поліномів Жегалкина дорівнює 2^{2^n} і, отже, воно збігається з числом всіх булевих функцій від n змінних. Тому твердження буде істинно, якщо показати, що різні поліноми реалізують різні функції.

Припустимо противне, тобто що існують два різних полінома Жегалкина f і g, такі, що f і g реалізують одну й ту ж булеву функцію. Це тягне, що і вирази $f \oplus g$ і $g \oplus g$, що позначаються нижче як h і h' відповідно, реалізують одну й ту ж функцію. Але з визначення операції $\oplus$ випливає, що h' реалізує функцію-константу 0. Значить, і поліном h реалізує функцію-константу 0.

Позначимо h'' поліном, який будується з h викреслюванням в h всіх повторюваних доданків, розглянутих з точністю до порядку кон'юнктивні членів в них. В силу припущення отримуємо, що h'' відмінний від порожнього полінома (тобто полінома, що не містить жодного доданка), і що він реалізує функцію-константу 0. Виділимо в h'' доданок, що містить найменше число змінних. (Він єдиний.) Підставами в h'' замість цих змінних 1, а замість інших змінних з h'' — 0. В результаті отримаємо, що на так вибраних наборах значень змінних поліном h'' приймає значення, рівне 1. Протиріччя з тим, що h'' реалізує функцію-константу 0. *Кінець доведення.*

Виникає природне запитання: чи можна якимось чином *у загальних термінах* описати ті (мінімальні) сукупності функцій, через які виражаються всі булеві функції з використанням операції суперпозиції? Виявляється, як це показав Е. Пост, можна. Цьому присвячені наступні розділи.

4.8 Повні системи булевих функцій. Замикання множин булевих функцій. Замкнуті класи

Сукупність функцій F називається *функціонально повною системою* (або просто повною), якщо будь-яка булева функція може бути отримана з функцій системи F за допомогою операції суперпозиції (і, в разі необхідності, операції введення фіктивних змінних), або, іншими словами, якщо будь-яка булева функція може бути виражена формулою в сигнатурі F (тобто формулою, що містить тільки функціональні символи, що зустрічаються в сигнатурі F).

З наведеного вище подання булевих функцій у вигляді ДДНФ випливає, що *система функцій* $\{\wedge, \vee, \text{-}\}$ *є повною системою*. Приклади інших повних систем можуть бути знайдені за використанням такого простого твердження.

Твердження 4.5 (достатня умова повноти). Якщо F і G — системи булевих функцій, такі, що F є повною і будь-яка функція з F виражається деякою формулою у сигнатурі G, то G – повна система.

Скористаємося ним в доведенні наступного твердження.

Наслідок 4.3. Системи булевих функцій $\{\wedge, \text{-}\}$ і $\{\vee, \text{-}\}$ є повними (- позначає логічне заперечення). Такими ж є системи

$\{1, \vee, \oplus\}$, $\{1, \wedge, \oplus\}$, $\{0, \to\}$ і $\{|\}$.

Доведення. В абзаці, що попереджує твердженню 4.5, було сказано, що система $\wedge$, $\vee$, - утворює повну систему. Згідно за правилами де Моргана і законом зняття подвійного заперечення маємо: $x_1 \vee x_2 = \overline{\overline{x_1} \wedge \overline{x_2}}$ і $x_1 \wedge x_2 = \overline{\overline{x_1} \vee \overline{x_2}}$. Значить, $\{\wedge, -\}$ і $\{\vee, -\}$ утворюють повну систему на підставі достатньої умови повноти.

Далі, $\overline{x_1} = 1 \oplus x_1$. Тому повнота $\{\vee, -\}$ і $\{\wedge, -\}$, а також достатня умова повноти тягнуть повноту $\{1, \vee, \oplus\}$ і $\{1, \wedge, \oplus\}$.

Для $\{0, \to\}$ маємо: $\overline{x_1} = x_1 \to 0$ і $x_1 \vee x_2 = (x_1 \to 0) \to x_2$. Використовуючи повноту $\{\vee, -\}$ і достатню умову повноти, отримуємо повноту системи $\{0, \to\}$.

Нарешті, для штриха Шеффера маємо: $\overline{x_1} = x_1|x_1$, $x_1 \vee x_2 = (x_1|x_1)|(x_2|x_2)$ і $x_1 \wedge x_2 = (x_1|x_2)|(x_1|x_2)$. Тому на підставі наслідку 4.1 і достатньої умови повноти отримуємо повноту системи $\{|\}$. *Кінець доведення.*

Замиканням множини F відносно операції суперпозиції називається множина всіх функцій, які можуть бути отримані з функцій системи F зі застосуванням операції суперпозиції (іншими словами, можуть бути реалізовані нетривіальними формулами над F). Замикання множини F позначається через $[A]$.

З наведеного вище визначення поняття рівності функцій випливає, що множини $[F]$ належать також і всі функції, які відрізняються від функцій, що реалізуються нетривіальними формулами над F, лише фіктивними змінними. Таким чином, *фактично замикання систем функцій* розглядається *щодо двох операцій: суперпозиції і введення фіктивних змінних.*

Множина булевих функцій F називається *замкнутою* (щодо операції суперпозиції), якщо $F = [F]$. Замкнуті множини функцій називаються також *замкнутими класами.* (Зауважимо, що за замовчуванням вважається, що для будь-якої змінної x_i *тотожна функція* $f(x_i) = x_i$ *завжди входить у будь-який клас.*)

Операція замикання володіє наступними властивостями.

Нехай F і G — довільні системи булевих функцій. Тоді виконуються таки співвідношення:

(1) $F \subseteq [F]$;

(2) якщо $F \subseteq G$, то $[F] \subseteq [G]$;

(3) $[[F]] = [F]$;

(4) $[F] \cap [G]$ є замкнутою множиною;

(5) F є повною системою тоді і тільки тоді, коли $[F] = P_2$.

4.9 Критерій повноти. Теорема Поста. Предповні класи

Визначимо п'ять *основних* замкнутих класів булевих функцій, що грають важливу роль в теорії булевих функцій: T_0, T_1, M, S і L.

Булева функція $f(x_1, \ldots, x_n)$ *зберігає константу 0*, тоді і тільки тоді, коли виконується рівність $f(0, \ldots, 0) = 0$.

Булева функція $f(x_1, \ldots, x_n)$ *зберігає константу 1* тоді і тільки тоді, коли виконується рівність $f(1, \ldots, 1) = 1$.

Функція $f(x_1, \ldots, x_n)$ називається *монотонною* тоді і тільки тоді, коли для будь-яких двох наборів $\langle \alpha_1, \ldots, \alpha_n \rangle$ і $\langle \beta_1, \ldots, \beta_n \rangle$ з E^n, таких, що $\alpha_1 \leqslant \beta_1, \ldots, \alpha_n \leqslant \beta_n$, виконується нерівність $f(\alpha_1, \ldots, \alpha_n) \leqslant f(\beta_1, \ldots, \beta_n)$.

Функція $f(x_1, \ldots, x_n)$ називається *самодвоїстою* тоді і тільки тоді, коли для будь-якого набору $\langle \alpha_1, \ldots, \alpha_n \rangle$ з E^n виконується рівність $\overline{f(\overline{\alpha_1}, \ldots, \overline{\alpha_1})} = f(\alpha_1, \ldots, \alpha_n)$.

Функція $f(x_1, \ldots, x_n)$ називається *лінійною* тоді і тільки тоді, коли вона має вигляд $f(x_1, \ldots, x_n) = c_0 \oplus (c_1 \wedge x_1) \oplus \ldots \oplus (c_n \wedge x_n)$, де $c_0, c_1, \ldots, c_n$ належать множині $E = \{0, 1\}$ (тобто, коли в поданні цієї функції у вигляді полінома Жегалкина містяться тільки так звані *лінійні члени*, тобто члени вигляду $c_i \wedge x_i$ або c_0).

Наступні множини булевих функцій носять назву *основних замкнутих класів*:

T_0 — *множина всіх функцій, що зберігають константу 0*,

T_1 — *множина всіх функцій, що зберігають константу 1*,

M — *множина всіх монотонних функцій*,

S — *множина всіх несамодвоїстих функцій*,

L — *множина всіх лінійних функцій*.

Усі вони замкнуті, що перевіряється, використовуючи визначення замкнутої множини. Ще відзначимо, що всі вони відмінні від P_2, і ні один з цих класів не міститься в іншому, що підтверджується наступними комбінаціями функцій:

(1) функції-константи 0 і 1 для T_0 і T_1;

(2) x_1 і функції-константи 1 для T_0 і M;

(3) функції-константи 0 і $\overline{x_1}$ для T_0 і S;
(4) $x_1 \wedge x_2$ і $1 \oplus x_1 \oplus x_2$ для T_0 і L;
(5) $\overline{x_1}$ і x для T_1 і M;
(6) функції-константи 1 і x_1 для T_1 і S;
(7) $x_1 \wedge x_2$ і $x_1 \oplus x_2$ для T_1 і L;
(8) $x_1 \wedge x_2$ і $\overline{x_1}$ для M і S;
(9) $x_1 \wedge x_2$ і $1 \oplus x_1 \oplus x_2$ для M і L;
(10) $(x_1 \wedge x_2) \vee (\overline{x_1} \wedge \overline{x_2})$ і $1 \oplus x_1 \oplus x_2$ для S і L.

Наведені в (1)–(10) конкретні функції показують, що основні класи булевих функцій *непусті*. Також звертаємо увагу на те, що *поняття класу булевих функцій не збігається з поняттям класу за деяким відношенням еквівалентності*. Основні класи булевих попарно перетинаються. Наприклад, тотожна функція $f(x_1) = x_1$ лежить в T_0, T_1, M, S і L. Слідуючи традиції, ми тут використовуємо поняття класу у тому вигляді, в якому воно зазвичай використовується в теорії булевих функцій.

Має місце наступний критерій функціональної повноти систем булевих функцій, встановлений американським математиком Е. Постом.

Твердження 4.6 (теорема Поста про функціональну повноту). Система F функцій алгебри логіки функціонально повна тоді і тільки тоді, коли перетин класу $[F]$ з кожним з основних класів є непустою множиною. (або, іншими словами, коли F містить функцію, що не зберігає 0, функцію, що не зберігає 1, немонотонну функцію, самодвоїсту функцію і нелінійну функцію).

Доведення. Необхідність. Припустимо, що $[F] = P_2$. Тоді F не може повністю включатися хоча б в один з класів T_0, T_1, M, S і L, оскільки в іншому випадку, якби, наприклад, $F \subseteq M$, то і $[F] \subseteq M$ у силу замкнутості класу монотонних функцій. Але $\overline{x_1}$ не є монотонною функцією, і, значить, $[F] \neq P_2$. Протиріччя. Значить, F містить немонотонную функцію.

Аналогічно міркуючи для T_0, T_1, S і L, отримуємо, що *необхідність має місце.*

Достатність. Припустимо, що в $[F]$ існують нелінійна функція f_L, немонотонна функція f_M і несамодвоїста функція f_S, а також функції f_0 і f_1, такі, що $f_0(0, \ldots, 0) = 1$ і $f_1(1, \ldots, 1) = 0$.

Якщо $f_0(1, \ldots, 1) = 1$ і $f_1(0, \ldots, 0) = 0$, то можна вважати,

що f_0 і f_1 є функції-константи 1 та 0 відповідно. Значить, $0, 1 \in [F]$.

Якщо ж $f_0(1, \ldots, 1) = 0$ або $f_1(0, \ldots, 0) = 1$, то, оскільки $f_0(0, \ldots, 0) = 1$ і $f_1(1, \ldots, 1) = 0$, $f_0(x_1, \ldots, x_1)$ являє собою функцію логічного заперечення. Позначивши її $\overline{x_1}$, отримуємо, що $\overline{x_1} \in [F]$.

Отже, при наявності f_0 і f_1 ми отримуємо, що, як мінімум, $0, 1 \in [F]$ або $\overline{x_1} \in [F]$. Розглянемо ці два випадки.

1. Нехай $0, 1 \in [F]$.

Так як f_M є немонотонна функція, то знайдеться два (сусідніх) набору $\langle \alpha_1, \ldots, \alpha_i, 0, \alpha_{i+1}, \ldots, \alpha_n \rangle$ і $\langle \alpha_1, \ldots, \alpha_i, 1, \alpha_{i+1}, \ldots, \alpha_n \rangle$, таких, що $f_M(\alpha_1, \ldots, \alpha_i, 0, \alpha_{i+1}, \ldots, \alpha_n) > f_M(\alpha_1, \ldots, \alpha_i, 1, \alpha_{i+1}, \ldots, \alpha_n)$. Тобто функція $h(x_1) = f_M(\alpha_1, \ldots, \alpha_i, x_1, \alpha_{i+1}, \ldots, \alpha_n)$ являє собою логічне заперечення $\overline{x_1}$ і, значить, $\overline{x_1} \in [F]$. Маємо: $0, 1, \overline{x_1} \in [F]$.

2. Нехай $\overline{x_1} \in [F]$.

Оскільки $f_S \in [F]$, то для деякого набору $\langle \alpha_1, \ldots, \alpha_n \rangle$ маємо, що $f_S(\overline{\alpha_1}, \ldots, \overline{\alpha_n}) = f_S(\alpha_1, \ldots, \alpha_n)$.

Визначимо $h_i(x_1)$ наступним чином: $h_i(x_1) = x_1$, якщо $\alpha_i = 0$ і $h_i(x_1) = \overline{x_1}$, якщо $\alpha_i = 1$. Тоді для функції унарної $g(x_1) = f_S(h_1(x_1), \ldots, h_n(x_1))$ маємо $g(0) = g(1)$, тобто $g(x_1)$ являє собою функцію-константи 0 або 1, що належить $[F]$. Але оскільки $\overline{x_1} \in [F]$, то незалежно від того, що є $g(x_1)$, 0 або 1, отримуємо, що $0, 1, \overline{x_1} \in [F]$.

Остаточно маємо: $[F]$ обов'язково містить $0, 1, \overline{x_1}$.

Тепер з допомогою нелінійної функції f_L покажемо, що кон'юнкція $x_1 \wedge x_2$ також належить до $[F]$.

В силу повноти набору $\{1, \wedge, \oplus\}$ (наслідок 4.3) можна вважати, що функція f_L має вигляд $((x_1 \wedge x_2) \wedge f(x_3, \ldots, x_n)) \oplus (x_1 \wedge g(x_3, \ldots, x_n)) \oplus (x_2 \wedge h(x_3, \ldots, x_n)) \oplus e(x_3, \ldots, x_n)$, де $f(x_3, \ldots, x_n)$ не є функція-константа 0, тобто для деякого набору $\langle \alpha_3, \ldots, \alpha_n \rangle$ з 0 і 1 $f(\alpha_3, \ldots, \alpha_n) = 1$.

Так як функції-константи 0 і 1 належать $[F]$, використовуючи операцію суперпозиції по змінним $x_3, \ldots, x_n$ відносно $((x_1 \wedge x_2) \wedge f(x_3, \ldots, x_n)) \oplus (x_1 \wedge g(x_3, \ldots, x_n)) \oplus (x_2 \wedge h(x_3, \ldots, x_n)) \oplus e(x_3, \ldots, x_n)$ і функцій-констант 0 і 1, отримуємо, що у $[F]$ є функція $f'_L(x_1, x_2) = ((x_1 \wedge x_2) \wedge f(\alpha_3, \ldots, \alpha_n)) \oplus (x_1 \wedge g(\alpha_3, \ldots, \alpha_n)) \oplus (x_2 \wedge h(\alpha_3, \ldots, \alpha_n)) \oplus e(\alpha_3, \ldots, \alpha_n)$, або, в іншому записі, $f'_L(x_1, x_2) = (x_1 \wedge x_2) \oplus (\beta \wedge x_1) \oplus (\gamma \wedge x_2) \oplus \delta$, де β, γ, δ

є 0 або 1 (у нас $f(\alpha_3, \ldots, \alpha_n) = 1$).

Покажемо, що кон'юнкція $x_1 \wedge x_2$ може бути виражена у вигляді різних видів суперпозиції 0, 1, логічного заперечення і функції $f'_L(x_1, x_2)$ для різних значеннях β, γ і δ.

У нас є вісім можливих комбінацій для значень β, γ і δ, починаючи з $0, 0, 0$ і закінчуючи $1, 1, 1$. Проаналізуємо кожен окремо, надавши бажаючим самостійно перевірити наведені тотожності.

При $\beta = 0$, $\gamma = 0$ і $\delta = 0$ отримуємо, що $f'_L(x_1, x_2)$ має вигляд $x_1 \wedge x_2$, тобто $x_1 \wedge x_2 = f'_L(x_1, x_2)$.

При $\beta = 0$, $\gamma = 0$ і $\delta = 1$ отримуємо, що $f'_L(x_1, x_2) = (x_1 \wedge x_2) \oplus 1$. За допомогою таблиць істинності можна довести тотожність $(x_1 \wedge x_2) \oplus 1 = \overline{x_1 \wedge x_2}$. Значить, $x_1 \wedge x_2 = \overline{(x_1 \wedge x_2) \oplus 1} = \overline{f'_L(x_1, x_2)}$, що і було потрібно.

При $\beta = 0$, $\gamma = 1$ і $\delta = 0$ отримуємо, що $f'_L(x_1, x_2) = (x_1 \wedge x_2) \oplus x_2$. За допомогою таблиць істинності можна довести тотожність $(x_1 \wedge x_2) \oplus x_2 = \overline{x_1} \wedge x_2$. Значить, $x_1 \wedge x_2 = (\overline{x_1} \wedge x_2) \oplus x_2 = f'_L(\overline{x_1}, x_2)$.

При $\beta = 0$, $\gamma = 1$ і $\delta = 1$ отримуємо, що $f'_L(x_1, x_2) = (x_1 \wedge x_2) \oplus x_2 \oplus 1$. За допомогою таблиць істинності можна довести тотожність $(x_1 \wedge x_2) \oplus x_2 \oplus 1 = \overline{x_1 \wedge x_2}$. Значить, $x_1 \wedge x_2 = \overline{(\overline{x_1} \wedge x_2) \oplus x_2 \oplus 1} = \overline{f'_L(\overline{x_1}, x_2)}$.

При $\beta = 1$, $\gamma = 0$ і $\delta = 0$ отримуємо, що $f'_L(x_1, x_2) = (x_1 \wedge x_2) \oplus x_2$. За допомогою таблиць істинності можна довести тотожність $(x_1 \wedge x_2) \oplus x_2 = x_1 \wedge \overline{x_2}$. Значить, $x_1 \wedge x_2 = (x_1 \wedge \overline{x_2}) \oplus \overline{x_2} = f'_L(x_1, \overline{x_2})$.

При $\beta = 1$, $\gamma = 0$ і $\delta = 1$ отримуємо, що $f'_L(x_1, x_2) = (x_1 \wedge x_2) \oplus x_1 \oplus 1$. За допомогою таблиць істинності можна довести тотожність $(x_1 \wedge x_2) \oplus x_1 \oplus 1 = \overline{x_1 \wedge \overline{x_2}}$. Значить, $x_1 \wedge x_2 = \overline{(x_1 \wedge \overline{x_2}) \oplus x_1 \oplus 1} = \overline{f'_L(x_1, \overline{x_2})}$.

При $\beta = 1$, $\gamma = 1$ і $\delta = 0$ отримуємо, що $f'_L(x_1, x_2) = (x_1 \wedge x_2) \oplus x_1 \oplus x_2$. За допомогою таблиць істинності можна довести тотожність $(x_1 \wedge x_2) \oplus x_1 \oplus x_2 = \overline{\overline{x_1} \wedge \overline{x_2}}$. Значить, $x_1 \wedge x_2 = \overline{(\overline{x_1} \wedge \overline{x_2}) \oplus \overline{x_1} \oplus \overline{x_2}} = \overline{f'_L(\overline{x_1}, \overline{x_2})}$.

При $\beta = 1$, $\gamma = 1$ і $\delta = 1$ отримуємо, що $f'_L(x_1, x_2) = (x_1 \wedge x_2) \oplus x_1 \oplus x_2 \oplus 1$. За допомогою таблиць істинності можна довести тотожність $(x_1 \wedge x_2) \oplus x_1 \oplus x_2 \oplus 1 = \overline{x_1} \wedge \overline{x_2}$. Значить, $x_1 \wedge x_2 = (\overline{x_1} \wedge \overline{x_2}) \oplus \overline{x_1} \oplus \overline{x_2} \oplus 1 = f'_L(\overline{x_1}, \overline{x_2})$.

Проведені вище міркування показують, що $[F]$ обов'язково містить 0, 1, логічне заперечення і кон'юнкцію. В силу повноти цього набору функцій (наслідок 4.3) отримуємо $[F] = P_2$. *Кінець доведення.*

Теорема Поста показує, що у будь повної системи *можна виділити повну підсистему*, складається не більше ніж з п'яти функцій.

Якщо ми повернемося до раніше розглянутих систем $\{0, \to\}$ і $\{|\}$, то легко перевіряється, що кожна з них задовольняє критерію Посту і, отже, вже на підставі тільки нього, тобто без використання достатньої умови повноти, вони є повними. Звертаємо вашу увагу на те, що існують повні системи, які містять тільки по одній булевої функції (штрих Шеффера або, наприклад, стрілка Пірса).

Тобто здається, що проектування та реалізацію реальних обчислювальних пристроїв краще проводити на базі штриха Шеффера. Але на сучасному етапі розвитку обчислювальної техніки такий підхід виявляється невигідним, як економічно так і технічно, оскільки (мінімальні) формульні представлення булевих функцій (потрібних в практичних застосуваннях) у сигнатурі, яка містить штрих Шеффера, часто мають більш громіздку запис, ніж, наприклад, їх аналоги у стандартній (що є надлишковою) сигнатурі $\{\wedge, \vee, \text{-}\}$. Та й сам елемент, що реалізує штрих Шеффера, як правило, є технічно більш складно влаштованим, ніж елементи, що реалізують $\wedge$, $\vee$, і -.

Тут ми припиняємо обговорення цієї теми — вона потребує окремого вивчення і виходить за межі цього посібника. Зацікавленого ж читача відсилаємо до сучасних підручниках і монографій з теорії і практиці проектування обчислювальних пристроїв і комп'ютерів та застосування булевих функцій у практичних застосуваннях.

Критерій Поста може бути переформульований наступним чином.

Наслідок 4.4. Система F функцій алгебри логіки є функціонально повною тоді і тільки тоді, коли жоден з основних замкнутих класів T_0, T_1, M, S і L не містить усі функції F.

Доведення. Необхідність. Якщо F — повний клас, тобто $[F] = P_2$, то, оскільки кожен з основних замкнутих класів різниться

від P_2, $[F]$ не може включатися ні в один з T_0, T_1, M, S і L.

Достатність. Нехай f_0, f_1, f_M, f_S і f_L — булеві функції F, які не належать T_0, T_1, M, S і L, відповідно. Але це означає, що f_0, f_1, f_M, f_S і f_L задовольняють умовам теореми Поста і, отже, утворюють повну систему функцій, тобто $[F] = P_2$. *Кінець доведення.*

На закінчення наведемо ще деякі результати з булевими функціями.

Наслідок 4.5. Кожен замкнутий клас $[F]$ булевих функцій, такий, що $[F] \neq P_2$, включається хоча б в один з п'яти класів T_0, T_1, M, S і L.

Доведення. Якщо $[F]$ не включається ні в один з класів T_0, T_1, M, S і L, $[F]$ можна виділити функції, задовольняють критерію Посту, що тягне $[F] = P_2$, а це суперечить умові. *Кінець доведення.*

Нехай $[F]$ і $[G]$ — замкнені класи булевих функцій, такі, що $[F]$ міститься в $[G]$. Клас $[F]$ називається *предповним в* $[G]$ тоді і тільки тоді, коли $[F] \neq [G]$ і для будь-якої функції f з множини $[G] \dot{-} [F]$ система $[F] \cup \{f\}$ є повною в $[G]$. (У деякій літературі предполные класи називаються *максимальними.*)

Твердження 4.7. В P_2 існує *тільки п'ять* предполных класів, а саме: T_0, T_1, M, S і L.

Доведення. Нехай $[F]$ — предповний клас в P_2. $[F]$ є замкнутим класом і $[F] \neq P_2$. Значить, за наслідком 4.5 клас $[F]$ включається хоча б в один з п'яти класів T_0, T_1, M, S і L. *Кінець доведення.*

Замкнені класи булевих функцій були описані Е. Постом в 1920 році. Він вивчив ряд важливих властивостей. До основних результатів Посту з них, крім наведених вище, відносяться також такі.

Нехай $[F]$ — довільний замкнутий клас булевих функцій, а G — деяка система функцій з $[F]$. Кажуть, що система G *породжує замкнутий клас* $[F]$, якщо $[G] = [F]$. У цьому випадку кажуть також, що *система* G *є повною в* $[F]$.

Базисом класу $[F]$ називається така породжуюча $[F]$ система, будь-яка власна підсистема якої не породжує $[F]$.

Твердження 4.8. Кожен замкнутий клас булевих функцій має скінченний базис.

Твердження 4.9. Множина всіх замкнутих класів функцій алгебри логіки має зліченну потужність.

Е. Пост описав *повну діаграму включень* одного замкненого класу в інший у множині всіх замкнених класів булевих функцій.

Рекомендована література

1. Карнаух Т.О., Ставровський А.Б. Вступ до дискретної математики: Навчальний посібник. – К.: Видав.-полі- граф. центр "Київський університет", 2006. – 113 с.

2. Капітонова Ю.В., Кривий С.Л., Летичевський О.А., Луцький Г.М., Печурін М.К. Основи дискретної математики (підручник). – К.: Наукова думка, 2002. – 579 с.

3. Новиков Ф.А. Дискретная математика для программистов. – СПб: Питер, 2000. – 304 с.

4. Ерусалимский Я.М. Дискретная математика: теория, задачи, приложения. М.: Вузовская книга, 2004. – 268 с.

5. Френкель А.А., Бар-Хиллел И. Основания теории множеств. – М: Мир, 1966. – 555 с.

6. Яблонский С.В. Введение в дискретную математику. М.: Наука, 1986. – 384 с.

7. Яблонский С.В., Гаврилов Г.П., Кудрявцев В.Г. Функции алгебрі логики и классы Поста. М.: Наука, 1966. – 119 с.

Матеріали лекцій
з дисципліни "Дискретна математика"

Лялецький Олександр Вадимович

Окремі розділи дискретної математики

Матеріали лекцій являють собою короткі нотатки з тих розділів дискретної математики, без знання яких стає вельми проблематичною можливість вивчення та розуміння теоретичних основ ряду предметів, що викладаються у вищих навчальних закладах та вимагають знання базових математичних понять і результатів. Він може служити хорошим довідковим матеріалом як для студентів, які починають вивчення математичних дисциплін на перших курсах вузів, так і для викладачів, які бажають використовувати досвід, накопичений автором в процесі його викладацької діяльності та відображений в матеріалах.

Подано до друку 07.12.2018. Формат 60x84/16.
Папір мелований. Гарнитура Times. Друк комп'ютерний.
Умов. др. арк. 9,57

———————————

К.: Арталекс-Принт, 2018