Бінарні відношення. Відношення порядку.

Курінний Г.Ч. Невмержицька О.М. Шугайло О.О.

Травень — 2015

Зміст

1 Бінарні відношення

1.1 Запис. Використання. Приклади

Нижче розглядаємо бінарні відношення $R \subseteq A^2$ на певній множині A. Те, що два елементи $a, b \in A$ знаходяться у відношенні R, крім стандартного запису $(a, b) \in R$, який в історичному масштабі з'явився лише сьогодні вранці, використовувалися і використовуються і інші:

- $R(a, b)$ — префіксний кембріджський запис;
- Rab — префіксний польський запис;
- abR — зворотний постфіксний польський запис;
- aRb — інфіксний запис;
- $(a, b)R$ — постфіксний запис з дужками.

Вибір того чи іншого запису для бінарного відношення диктується традицією, мовним оточенням і вподобаннями того, хто цей запис використовує. Так, для відношення $<$ традиція вимагає писати $a < b$ а не $(a, b) \in <$. А мова програмування ЛІСП вимагає те ж саме записувати у вигляді $< (ab)$. Вибір тієї чи іншої форми запису для бінарного відношення може надавати ті чи інші переваги транслятору програми чи аналізатору програми в програмуванні. Вибір форми запису в тексті висловить повагу чи байдужість автора до читача.

Звернемо увагу, що бінарні відношення вельми часто зустрічаються в обчислювальних системах, зокрема в реляційних[1] базах даних.

Відмітимо три бінарні відношення на множині A

[1] Англійською мовою relation — відношення

1. порожнє відношення $\emptyset$, воно визначається умовою

$$\forall x, y \in A(\neg((x, y) \in \emptyset));$$

2. відношення рівності $=$ або діагональ Δ, це відношення визначається умовою

$$\forall x, y \in A((x, y) \in \Delta \Leftrightarrow x = y);$$

3. універсальне відношення A^2, воно визначається умовою

$$\forall x, y \in A((x, y) \in A^2).$$

1.2 Операції над бінарними відношеннями

Над бінарними відношеннями можна виконувати звичайні теоретико-множинні операції — перетин, об'єднання, різниця, симетрична різниця, доповнення — універсальною множиною вважається A^2.

Крім того, на множині бінарних відношень (на заданій множині A) визначено операцію множення (чи композиції, чи суперпозиції). Якщо $R_1, R_2 \subseteq A^2$ два бінарні відношення, то добутком $R_3 = R_1 \cdot R_2 = R_1 R_2$ називають відношення

$$(a, b) \in R_3 \Leftrightarrow \exists c((a, c) \in R_1 \wedge (c, b) \in R_2).$$

Для прикладу, нехай $A = \mathbb{R}$ і

$$(a, b) \in R_1 \Leftrightarrow a^2 + b^2 = 1, \tag{1}$$

тобто R_1 це коло радіуса 1, а

$$(a, b) \in R_2 \Leftrightarrow (a > 0 \wedge b > 0, \tag{2}$$

тобто R_2 є першим квадрантом.

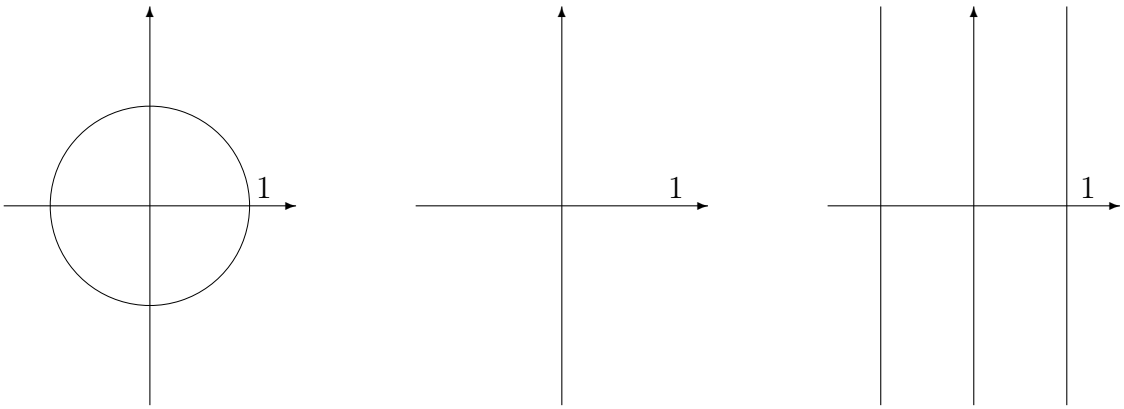


Рис. 1: Добутком кола на кквадрант є смуга

Тоді

$$(a, b) \in R_1R_2 \Leftrightarrow \exists c(a^2 + c^2 = 1 \wedge c > 0 \wedge b > 0.$$

Таким чином (див. рис. 1.2),

$$R_1R_2 = \{(a, b)| - 1 < a < 1, b > 0\}. \tag{3}$$

Подібним чином $R_2R_1 = \{(a, b)|0 < a, -1 < b < 1\}$.

> Множина разом із бінарною операцією в цій множині називається магмою або групоїдом.

Оскільки бінарні відношення на заданій множині можна множити, то сукупність бінарних відношень на цій множині є магмою або групоїдом.

Теорема 1.1 *Множення відношень асоціативне, тобто для будь-яких трьох бінарних відношень α, β, γ на заданій множині A виконується рівність $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.*

Доведення. Нехай A — деяка множина і $\alpha, \beta, \gamma \subseteq A^2$ — три бінарні відношення на цій множині. Потрібно довести, що для будь-яких $a, b \in A$

$$(a, b) \in (\alpha \cdot \beta) \cdot \gamma \Leftrightarrow (a, b) \in \alpha \cdot (\beta \cdot \gamma). \tag{4}$$

За визначенням множення відношень $(a, b) \in (\alpha \cdot \beta) \cdot \gamma$ тоді і тільки тоді, коли для деякого $y \in A$

$$(a, y) \in (\alpha \cdot \beta) \text{ і } (y, b) \in \gamma,$$

а $(a, y) \in (\alpha \cdot \beta)$ тоді і тільки тоді, коли для деякого $x \in A$

$$(a, x) \in \alpha \text{ і } (x, y) \in \beta.$$

Отже $(a, b) \in (\alpha \cdot \beta) \cdot \gamma$ тоді і тільки тоді, коли для деяких $x, y \in A$

$$(a, x) \in \alpha, \quad (x, y) \in \beta \text{ і } (y, b) \in \gamma. \tag{5}$$

Подібним чином $(a, b) \in \alpha \cdot (\beta \cdot \gamma)$ тоді і тільки тоді, коли для деякого $x \in A$

$$(a, x) \in \alpha \text{ і } (x, b) \in \beta \cdot \gamma,$$

а $(x, b) \in \beta \cdot \gamma$ тоді і тільки тоді, коли для деякого $y \in A$

$$(x, y) \in \beta \text{ і } (y, b) \in \gamma.$$

Отже $(a, b) \in \alpha \cdot (\beta \cdot \gamma)$ тоді і тільки тоді, коли для деяких $x, y \in A$

$$(a, x) \in \alpha, \quad (x, y) \in \beta \text{ і } (y, b) \in \gamma. \tag{6}$$

Із (5) і (6) випливає (4)

■

Множину разом із асоціативною бінарною операцією називають напівгрупою.

Використовуючи введене означення, теорему 1.1 можна переформулювати наступним чином.

Теорема 1.2 *Сукупність бінарних відношень на заданій множині разом із операцією множення утворює напівгрупу.*

Прикладом напівгрупи є множина натуральних чисел разом із операцією множення. Натуральні числа разом із операцією додавання також утворює напівгрупу.

Число 0 та число 1 у множині дійсних чисел виділяються властивостями

$$\forall x \in \mathbb{R}(1x = x1 = x), \qquad \forall x \in \mathbb{R}(0x = x0 = 0).$$

У напівгрупі бінарних відношень також є елементи, що мають подібні властивості — їх називають нулем та одиницею напівгрупи.

Для відмічених бінарних відношень $\emptyset$, Δ і для довільного бінарного відношення $\alpha \subseteq A^2$ можна записати

$$\emptyset \cdot \alpha = \alpha \cdot \emptyset = \emptyset; \tag{7}$$

і

$$\Delta \cdot \alpha = \alpha \cdot \Delta = \alpha. \tag{8}$$

З кожним бінарним відношенням R пов'язують відношення R^{-1}:

$$(a, b) \in R^{-1} \Leftrightarrow (b, a) \in R.$$

Відношення R^{-1} називають оберненим до R.

Нехай, для прикладу, маємо множину $\mathbb{R}$ дійсних чисел. Уявляємо її як дійсну пряму. Тоді R^2 уявляємо як площину із прямокутною системою координат. Відношенням буде будь-яка підмножина площини. Два відношення будуть взаємно оберненими, коли множини на площині симетричні відносно бісектриси

1-3 координатних кутів. На множині дійсних чисел відношення R_1, R_2, що задані властивостями (1),(2), самі до себе обернені, тобто симетричні, а відношення $R_1 \cdot R_2$, що задане властивостями (3), само до себе не обернене, не симетричне.

1.3 Властивості бінарних відношень

Відношення R на множині A називають

- рефлексивним, коли $\Delta \subseteq R$, тобто коли $\forall x (x, x) \in R$. На множині студентів відношення "студент x вчиться із студентом y в одній групі" є рефлексивним, тому що кожен студент сам з собою вчиться в одній групі.

- транзитивним, коли $R^2 \subseteq R$, тобто коли

$$\forall x, y, z \in A((x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R).$$

  Відношення "вчитись в одній групі" є транзитивним, а "бути сусідом" не обов'язково транзитивне відношення.

- симетричним, коли $R^{-1} = R$, тобто коли

$$\forall x, y \in A((x, y) \in R \Leftrightarrow (y, x) \in R).$$

  Відношення "бути сусідом" симетричне. А відношення "x подобається y" не обов'язково симетричне.

- антисиметричним, коли $R \cap R^{-1} = \emptyset$, тобто коли $(x, y) \in R \Rightarrow (y, x) \notin R$. Відношення "сидіти справа" антисиметричне. Антисиметричним буде також відношення "x є власною підмножиною множини y".

- антирефлексивним, коли $R \cap \Delta = \emptyset$, тобто коли $\forall x (x, x) \notin R$. Відношення "не дорівнюати самому собі" є антирефлексивним.

2 Відношення порядку

2.1 Відношення часткового та лінійного порядку

2.1.1 Означення та приклади

Відношення R називають

> відношенням строгого часткового порядку, якщо воно транзитивне, антисиметричне і антирефлексивне;
>
> відношенням строгого лінійного порядку, коли воно тринзитивне, антисиметричне, антирефлексивне, і для будь-яких $x, y \in A$ або $(x, y) \in R$ або $(y, x) \in R$.
>
> відношенням нестрогого часткового порядку, якщо воно одержується із часткового строгого порядку об'єднанням з діагоналлю;
>
> відношенням нестрогого лінійного порядку, якщо воно одержується із лінійного строгого порядку об'єднанням з діагоналлю.

Відношення "бути власною підмножиною" — це відношення строгого часткового порядоку. А відношення "бути підмножиною" — це відношення нестрогого часткового порядку. Відношення $<$ та $\leq$ є відношеннями строгого та нестрогого лінійного порядку на множині цілих чисел.

Можна перевірити, що оберненим до часткового строгого порядку є відношення часткового строгого порядку; оберненим до часткового нестрогого порядку є відношення частково строгого порядку; оберненим до лінійного строгого порядку є відношення лінійного строгого порядку; оберненим до лінійного нестрогого порядку є відношення лінійного нестрогого порядку.

Відношення часткового нестрого порядку частіше всього позначають $\leq$ і називають його "менше або дорівнює". З використанням цього позначення визначення часткого нестрогого порядку запишеться так

- $x \leq x$ для будь-якого елемента $x \in A$;
- якщо $x \leq y$ і $y \leq x$, то $x = y$;
- якщо $x \leq y$ і $y \leq z$, то $x \leq z$.

Обернене відношення до "менше або дорівнює" називається "більше або дорівнює". Це відношення позначається $\geq$.

Відповідно, для строгого часткового і лінійного порядку використовується позначення $<$, яке називається "строго менше". Обернене до відношення "строго менше" називається "строго більше" і позначається $>$.

Множина A разом із відношенням часткового порядку $\leq$ називається частково впорядкованою множиною і позначається $\langle A; \leq \rangle$. Те, що в різних частково впорядкованих множинах різні відношення порядку позначаються однаково, звичайно не приводить до непорозумінь. Якщо ж така уніфікація створює незручності, то потрібно для різних відношень порядку вживати різні познаення — наприклад, можна використовувати знаки $\leq_1, \leq_2, \leq_3, \ldots$. Для прикладу, на триелементній множині $\square, \star, \triangle$ в один і той же час можна використовувати порядок

$$\triangle \leq_1 \square \leq_1 \star,$$

і порядок

$$\star \leq_2 \triangle \leq_2 \square.$$

Існує традиція довгу словосполуку "частково впорядкована множина" заміняти абревіатурою чвм. Так чинять не тільки

в українській мові. В англійській замість partially ordered set пишуть poset, а в російській замість “частично упорядоченое множество“ пишуть чум.

Крім того, існує традиція без особливої потреби не підкреслювати порядок частковий чи лінійний, строгий чи нестрогий — уточнення виловлюються із мовного оточення.

Якщо для двох елементів $a, b \in A$ частково впорядкованої множини $\langle A, R\rangle$ виконується одна із умов

$$(a, b) \in R \text{ або } (b, a) \in R, \tag{9}$$

то кажуть, що елементи $a, b \in A$ порівнювані. Якщо ж умова (9) не виконується, то елементи $a, b \in A$ непорівнювані. Порожнє відношення є відношенням строгого часткового порядку — ніякі два елементи не порівнювані. Діагональ є відношення нестрогого порядку — кожен елемент порівнюваний лише сам з собою.

Відношення “бути дільником“ є відношенням порядку на множині натуральних чисел.

2.1.2 Найбільший, найменший, максмальний та мінімальний елементи

Найбільшим елементом множини називається такий елемент, який більше кожного іншого. Природно, що коли найбільший елемент існує, то він єдиний. Елемент, для якого не існує більшого, називають максимальним. Елементи b, c в чвм на рис. 2 максимальні, а найбільшого елемента ця множина не має. Таке розрізнення максимальних і найбльших елементів в математиці дещо відрізняється від побутового вжитку, де ці слова звичайно означають одне і те ж.

Елемент чвм, який менше (або дорівнює) кожного елемента

множини, називають найменшим. Якщо для заданого елемента строго меншого від нього немає,то такий елемент називають мінімальним.

Множина дійсних чисел не має ні найменшого ні мінімального елемента.

2.1.3 Алфавітниий порядок та порядок на прямому добутку двох чвм

На алфавіті — множині, з елементів якої будуються послідовності — слова, звичайно вводять лінійний порядок. Цей порядок дозволяє на множині слів, що будуються із елементів алфавіту (букв), також ввести порядок (як у словнику). Його називають і алфавітним і лексикографічним. Наприклад, коли алфавіт складається із букв а, б, в, г, і на множині букв введений порядок — а йде раніше від б, б йде раніше від в, а в йде раніше від г, то слово “баба“ йде раніше від слова “гав“,

Лексикографічний порядок використовують для того, що записати підряд (в лінійному порядку) доданки многочлена від багатьох змінних. В такому випадку змінні лінійно впорядковують — припустимо $x < y < z$. Далі добутки змінних записують у вигляді степенів змінних — спочатку йде степінь першої змінної, потім іде степінь другої змінної і так далі. Наприклад,

$$zxxyzyyxxxzyyyyzxxx = x^8y^7z^4, \quad zzzzzzzxyzyyxxyyyyyyyxzyyyyz = x^4y^{14}z$$

Потім по черзі порівнюють степені змінних — в якому доданку степінь змінної виявився більшим, той доданок і пишеться першим. В нашому випадку $8 > 7$ і доданок $x^8y^7z^4$ потрібно записувати перед доданком $x^7y^{14}z^{10}$.

Нехай за того ж порядку на змінних x, y, z потрібно записати доданки суми (многочлена)

$$f = x + 8 - 159y^2 + x^3z^{12}y - 2x^3 + 11y^{14}z + xz \qquad (10)$$

в лексикографічному порядку. Спочатку переписуємо суму з використанням нульового степеня:

$$f = xy^0z^0 + 8x^0y^0z^0 - 159x^0y^2z^0 + x^3z^{12}y^1 - 2x^3y^0z^0 + 11x^0y^{14}z^1 + x^1y^0z^1.$$

Далі виписуємо уже в лексикогрфічному порядку — спочатку доданки, що містять x^3, потім доданки, що містять x^2,потім доданки, що містять x^1, і нарештиі доданки, що містять x^0:

$$f = x^3y^1z^{12} - 2x^3y^0z^0 + x^1y^0z^1 + x^1y^0z^0 + 11x^0y^{14}z^1 - 159x^0y^2z^0 + 8x^0y^0z^0 = .$$

$$= x^3yz^{12} - 2x^3 + xz + x + 11y^{14}z - 159y^2 + 8.$$

Виписувати доданки многочлена можна не тільки в спадному порядку, коли спочатку виписуються більші доданки, а потім менші, а і в зростаючому порядку — коли спочатку виписуються менші доданки а потім більші. В зростаючому порядку многочлен (10) матиме наступний запис

$$f = 8 - 159y^2 + 11y^{14}z + x + xz - 2x^3 + x^3yx^{12}.$$

Вибір того чи іншого порядку запису доданків залежить від того, на що збираємося звернути увагу, якщо нам у многочлені $f(x) = 7x - 3 + 5x^2$ важливі доданки малого степеня, то ми пишемо $f(x) = -3 + 7x + 5x^2$, якщо ж важливі доданки більшого степеня, то ми пишемо $f(x) = 5x^2 + 7x - 3$.

В многочленах від кількох змінних важливою є сума степенів змінних у доданках. Тоді лексикографічний порядок використовують лише щоб впорядкувати ті доданки, які мають

один і той же степінь. Так многочлен з дійсними коефіцієнтами від двох змінних, в якому сума степенів змінних у доданках не перевищує 2, має настпний стандартний запис

$$a_{11}x^2+a_{12}xy+a_{22}y^2+a_1x+a_2y+a_0, \quad a_{11}, a_{12}, a_{22}, a_1, a_2, a_0 \in \mathbb{R}).$$

Якщо задані дві чвм A, B і $C = A \times B$, то на прямому добутку C вводиться наступний частковий порядок: для $a_1, a_2 \in A, \quad b_1, b_2 \in B, \quad c_1 = (a_1, a_2), c_2 = (a_2, b_2) \in C$

$$(c_1 < c_2) \Leftrightarrow ((a_1 < a_2) \wedge (b_1 < b_2)).$$

2.1.4 Використання лінійного порядку в інформатиці

В машинній обробці даних часто приходиться шукати потрібний елемент в множині. Один із способів — лінійно впорядкувати множину і по черзі перебирати елементи до тих пір, поки не знайдеться порібний. Але часто на множині уже існує певний частковий порядок. Для таких випадків розроблені спеціальні прийоми.

Крім того, буває недоцільно зберігати всі дані для обробки — наприклад, всі доданки певної суми. Може бути, що більш доцільно всі ці дані послідовно породжувати (створювати) — а для цього знову ж потрібно встановити на даних певний порядок і потім їх по черзі породжувати.

Для прикладу візьмемо завдання — надрукувати (вивести на друк, породити) всі підмножини множини $\{1, 2, \ldots, n\}$. Для цього можна запропонувати наступний алгоритм. Спочатку виводимо символ порожньої, множини. Потім виконуємо n кроків — на першому кроці до вивиденої множини (порожньої) додаємо 1 — вивели одноелементну множину $\{1\}$. Далі на другому кроці до виведених множин додаємо 2 — виводимо $\{2\}$ і

$\{1, 2\}$. На третьому кроці до виведених на попередніх кроках підмножин додаємо 3 — виводимо $\{3\}$, $\{2, 3\}$, $\{1, 2, 3\}$. І так далі — на останньому $n-$у кроці до раніше виведених множин додаємо число n і результат виводимо на друк.

Таким чином ми всі підмножини розташували у послідовність, тобто лінійно впорядкували. Але цей порядок суттєво відрізняється від порядку, який визначається відношенням включення, відношення "бути підмножиною".

2.1.5 Нетранзитивні відношення "краще" та "сильніше"

Найвідомішою множиною із нетранзитивним відношенням "сильніше" є

камінь, ножиці,папір.

Папір сильніший за камінь, тому що може його обгорнути. Камінь сильніший за ножиці, тому що камінь може ножиці затупити. А ножиці сильніші за папір, тому що вони можуть папір розрізати. Використовується значна кількість різновидів цієї множини, — і в дитячих іграх, і у випадковому виборі одного із кількох, і в дорослих змаганнях.

Другий приклад, не настільки простий як попередній, і досить неочевидний, дає нам гра, яку в 1969 році придумав Уолтер Пені. В цій грі Аліса та Біл задумують послідовність довжини 3, яка складається із 0 та 1. Далі вони підкидають монету і пишуть 1, якщо монета впала гербом вверх, і пишуть 0, коли монета впала гербом вниз. Таким чином вони одержують послідовність 0 та 1. Виграє в цій грі той, чия послідовність з'виться першою. Для прикладу, нехай Аліса задумала 000, а Біл задумав 101. При підкиданні монети записувалась послі-

довність

011110011000

Оскільки три нулі підряд появилися, а послідовність 101 не появилася, то виграла Аліса.

В деяких випадках послідовність Аліси може бути “кращою“, ніж послідовність Біла в тому розумінні, що Аліса частіше буде вигравати, коли задумані ними послідовності не змінюватимуться. Так, припустимо, що Аліса задумала 100, а Біл задумав 000. Тоді у випадку, коли першою вони записали 1, шансів виграти Білові у Аліси немає, а коли випав 0 то шанси виграти є у обох, — в цьому випадку послідовність 100 “краща“, ніж послідовність 000. Можна довести, що для кожної послідовності Біла Аліса може придумати “кращу“ послідовність, отже найкращої послідовності немає, і транзитивність у відношення “краще“ відсутня.

Наведені приклади повинні показати, що із того, що якесь бінарне відношення назване “більше“, “краще“, “вище“, не випливає його транзитивність, не впливає, що це відношення є відношенням порядку.

2.2 Діаграми

2.2.1 Діаграми скінченних чвм

Кажуть, що елемент x чвм A покриває елемент y цієї множини і пишуть $x \succ y$, коли $x > y$ і не існує елемента z такого, що $x > z > y$.

Введене відношення використовується для побудови так званих діаграм чвм. На діаграмах елементи чвм зображаються точками, і якщо $x \succ y$, то x зображається дещо вище від y і з’єднується з y відрізком. Можна також будувати діаграми

чвм так, що коли $x \succ y$, то x зображається дещо правіше від y і з'єднується з y відрізком. Як саме зображати — більший елемент зображати вище від меншого чи правіше від меншого, залежить від ситуації, від традиції, від типографських вимог та подібного. На рис. 7 більший елемент зображений правіше, а на рис. 6 більший елемент зображений вище. При великому бажанні можна також більший елемнт зображати нижче від меншого

Зобразимо кілька відношень порядку на триелементній множині $\{a, b, c\}$ (див. рис. 2,3,4 5). Всього на триелементній множині можна ввести 19 відношень часткового порядку.

Всі три елементи чвм на рис. 3 є і мінімальними і максимальними, але ні найменшого ні найбільшого серед них немає. На рис. 2 елемент a є найменшим і, відповідно, мінімальним, а обидва елементи b, c є максимальними, але жоден з них не є найбільшим. На рис. 5 елемент a є і мінімальним і найменшим, а елемент c є максимальним і найбільшим.

2.2.2 Лінійний та деревоподібний порядок на скінченних множинах

Часто зустрічаються два типи часткового порядку — при наявності першого порядку будь-які два елементи порівнювані, це так званий лінійний порядок, а множина називається в такому разі лінійно впорядкованою, а при наявності другого у множині є наменший елемент, а будь-які непорівнювані елементи не мають спільного більшого від них елемента. Діаграми таких чвм називають деревами, а сам порядок називають деревоподібним. Дійсні числа лінійно впорядковані, а структура сайту часто деревоподібна. З лінійним порядком легше працювати, а деревоподібний порядок постачає практика.

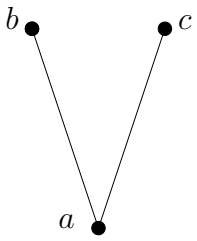


Рис. 2: $b > a, c > a$ і b, c непорівнювані

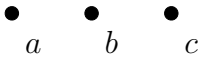


Рис. 3: Всі елементи непорівнювані

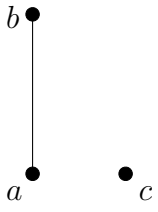


Рис. 4: $b > a$. Елементи a, c та елементи b, c непорівнювані

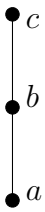


Рис. 5: $a < b < c$. Будь-яка пара елементів порівнювана.

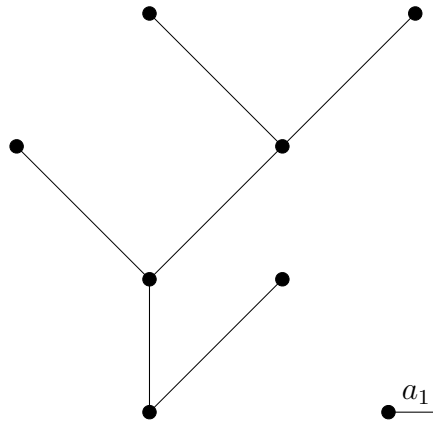


Рис. 6: Дерево

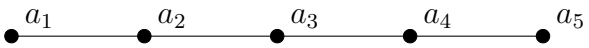


Рис. 7: Лінійний порядок

Взаємозалежність підрозділів великої організації часто зображають у вигляді дерев.

2.2.3 Ключі в інформатиці, в базах даних

Часто стан речей змушує впорядковувати великі за обсягом множини (масиви) даних — світлини, дані про студентів, проплати в фінансових закладах та подібне. В реляційний базах даних дані організовуються у вигляді прямокутних таблиць. Елементи цих таблиць називають полями, рядки називають записами. Поля одного запису можуть бути досить різнорідними — мони можуть містити шляхи доступу до файлів, імена, номери, дійсні числа та подібне. В одному стовпичку поля обов'язково однотипні — якщо одне поле числове, то і всі поля стовпчика числові, якщо одне поле містить текст, то і всі поля цього містять виключно тексти. Поля можуть бути незаповненими — в будь-якому стовпчику. Стовпчики називають

23
456
550
201
17
12445
943

Табл. 1: Список із 7 чисел

1	23
2	456
3	550
4	201
5	17
6	12445
7	943

Табл. 2: Перенумерований список із 7 чисел

5	17
1	23
4	201
2	456
3	550
7	943
6	12445

Табл. 3: Активний другий ключ

ключами. Поля одного стовпчика (ключа) можна лінійно впорядкувати. Якщо командою зробити ключ активним, то всі записи впорядкуються (рядки переставляться) так, щоб поля активного ключа йшли в порядку зростання або у порядку спадання.

Наведемо приклад. Нехай є дані, що складаються із 7 записів, 7 чисел

$$23, 456, 550, 201, 17, 12445, 943.$$

Оскільки записи це рядки, то їх потрібно розташувати у стовпчик (див. табл. 1).

Досить зручно перенумерувати ці числа

$$(1, 23), (2, 456), (3, 550), (4, 201), (5, 17), (6, 12445), (7, 943).$$

(див. табл. 2). Тепер записи складаються із двох полів. Так запис (4,201) має поле 4 і має поле 201. Перший стовпчик табл. 2) є першим ключем і записи впорядковані в порядку зростання першого ключа. Другий стовпчик — це другий ключ. Його можна зробити активним, і тоді таблиця прийме вигляд (табл. 3).

Отже ключем світлини може бути її назва, а також рік одержання, тематична спрямованість, кого стосується та подібне.

Назву світлини можна назвати ключем, а місце, де записується назва, можна назвати полем.

У кожного запису звичайно багато ключів, які дозволяють з належною швидкістю відшукувати потрібний запис серед багатьох подібних. Одна з головних властивостей набору ключів — кожен запис супроводжується унікальним набором ключів, тобто два різні записи мають різні ключі — в таблиці немає однакових рядків. Одна з важливих задач, яка розв'язується за допомогою часткового порядку на наборах ключів — задача пошуку, пошуку певного елемента, певного запису, чи пошуку всіх записів, що маєть задані властивість.

У файловій системі комп'ютера файл супроводжується ключами — шляхом доступу (на якому диску, в якій послідовності папок), назвою, розширенням (якою програмою створений), коли файл створений чи видозмінений, обсяг файла, права доступу до нього. Будова файлової системи деревоподібна. Бази даних (БД) що побудовані подібно до файлової системи комп'ютера з використанням деревоподібного часткового порядку, називають ієрархічними БД.

2.2.4 Ключі в інформатиці, в криптографії

В організаціях службовці на різних щаблях управлінської структури мають доступ до різної інформації. Інформація звичайно записується у такому вигляді, який не дозволяє знайомитися з нею тим, кому це не дозволене — шифрується. При шифруванні та дешифруванні використовуються певні параметри — числа, послідовності чисел, послідовності букв та подібне. Ці параметри називають ключами. Отже ключі тут дозволяють знайомитися із зашифрованою інформацією.

Існує проблема створення такої системи шифрування і, від-

повідно, підбору ключів, щоб службовці з більш високим правом до ступу до інформації могли читати те, що призначене слюжбовцю з низьким правом доступу, а службовці з низьким правом доступу не могли читати інформацію, яка призначена для тих хто має високе право доступу. Службовці одного щобля, однакового права доступу утворюють так званий клас безпеки. Оці класи безпеки і, відповідно, їх ключі, утворюють ієрархію, деревоподібну частково впорядковану множину.

2.3 Ізоморфізм частково впорядкованих множин

2.3.1 Означення та приклади

Нехай $\langle A; \leq \rangle$, і $\langle B; \leq \rangle$ дві частково впорядковані множини. Бієктивне відображення (бієкція) $f : A \to B$, яке задовольняє умову

$$\forall x, y \in A(x \leq y \Leftrightarrow f(x) \leq f(y), \tag{11}$$

низивають ізоморфізмом (або подібністю) частково впорядкованих множин. В загальному випадку, коли відображення f не обов'язково є бієкцією, але задовольняє умову (12), f називають (не строго) монотонним відображенням. Якщо ж умову (12) замінити на

$$\forall x, y \in A(x < y \Leftrightarrow f(x) < f(y), \tag{12}$$

то функцію, яка задовольняє цю умову називають строго монотонною. Таким чином, ізоморфізм (український термін — подібність) — це строго монотонна бієкція.

Дві частко впорядковані множини, між якими можна встановити ізоморфізм (побудувати ізоморфізм із однієї чвм в другу чвм) називають ізоморфними або подібними. Часто міркування проводять "з точністю до ізоморфізму", тобто ізоморфні

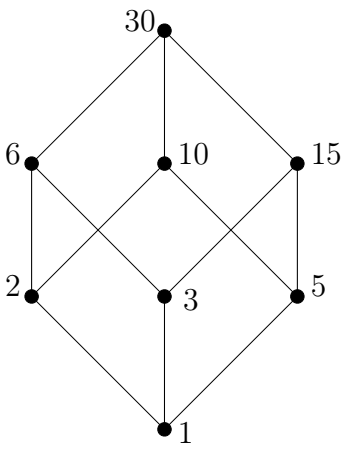


Рис. 8: Дільники числа 30

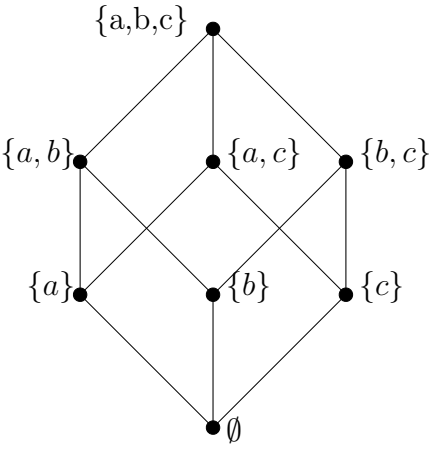


Рис. 9: Підмножини множини $\{a, b, c\}$

частко впорядковані множини не розрізняються, вважається, що це одна і та ж частко впорядкована множина.

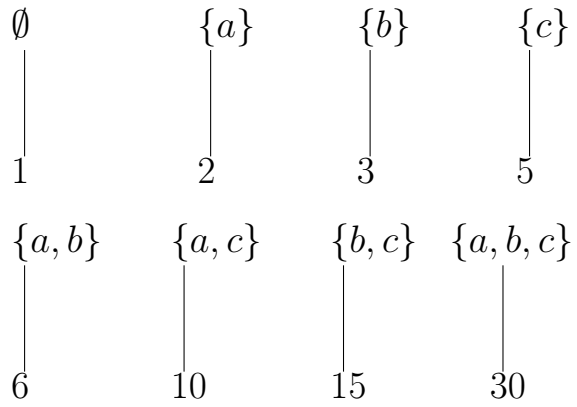
Бієктивне відображення (бієкція) $f : A \to B$, яке задовольняє умову

$$\forall x, y \in A(x \leq y \Leftrightarrow f(x) \geq f(y),$$

низвають антиізоморфізмом із чвм A в чвм B.

Ізоморфізм скінченних чвм легко розгледіти, зобразиши ці частково впорядковані множини діаграмами. Для прикладу, розглянемо чвм A усіх підмножин множини $\{a, b, c\}$ і чвм B усіх дільників числа 30, що впорядковані за подільністю — елемент x менше y коли x є дільником y (див. рис. 8, 9)

Ізоморфізм між множиною дільників і множиною підмножин встановлюється правилом



2.3.2 Сортування. Сім фундаметальних алгоритмів сортування.

> Встановлення ізоморфізму із скінченної лінійно впорядкованої множини в початковий відрізок натурального ряду називають сортуванням.

Для прикладу, результатом сортування частково впорядкованої множини $A = \{a, b, c\}$, де

$$c < a < b,$$

буде або перезапис цієї множини у порядку зростання (елементу множини відповідає номер цього елемента в результуючій по слідовності), тобто

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

або біля кожного елемента із A виписуєть той елемент початкового відрізка натурального ряду, який відповідає цьому елементу, в нашому випадку

a	b	c
2	3	1

Елементи множини, яку потрібно відсортувати, записуються у послідовність, тому замість слова множина в даному мовному оточенні використовується слово список. В послідовності кожен елемент одержує свій номер. Цей номер називаємо адресою елемента у списку.

Найважливішими алгоритмами сортуваня, тобто алгоритмами встановлення потрібного ізоморфізму, є

- лінійний вибір;
- лінійний вибір з обміном;
- лінійний вибір з підрахунком;
- стандартний обмін;
- парний обмін;
- просіювання;
- лінійна вставка.

Дію алгоритмів будемо пояснювати на прикладі, в якому потрібно сортувати множину

$$A = \{23, 456, 550, 201, 17, 12445, 943\}. \tag{13}$$

Переписуємо множину із вказівкою адреси елементів

$$\begin{array}{ccccccccc} 23 & 456 & 550 & 201 & 17 & 12445 & 943 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \tag{14}$$

Лінійний вибір

Для роботи алгоритму виділяється робоча комірка r і місце результуючого списку, списку виведення. На початку роботи

вони порожні, цей факт будемо позначати символом □. Отже перед початком роботи алгоритму маємо $r = \square$ і

23	456	550	201	17	12445	943
1	2	3	4	5	6	7
□	□	□	□	□	□	□

(15)

Робота алгоритму розбивається на стільки переглядів всього списку, скільки елементів в цьому списку. Отже в нашому прикладі всього буде 7 переглядів всього списку.

Прослідкуємо за першим переглядом. Кандидатом на перший елемент результуючого списку обирається перший елемент джерела — заданого списку. В нашому випадку цим елементом є 23. В робочу комірку заноситься адреса цього елемента — в нашому випадку адреса 1, отже $r = 1$. Кандидат в перші елементи по черзі порівнюється з наступними до тих пір, поки не знайдеться менший, або не закінчиться перегляд. Порівнюючи перший елемент з 5-м, бачимо, що 5-й елемент 17 менший від 23. Цей новий елемент (в нашому випадку 17) стає новим кандидатом на перший елемент результуючого списку, його адреса заноситься в робочу комірку, і порівняння продобжується знову до тих пір, поки не зустрінеться менший елемент, або поки не закінчиться список. В нашому випадку список закінчиться раніше, ніж знайдеться менший. Коли список закінчився, перегляд закінчується, кандидат в найменші елементи стає справді найменшим елементом (першим елементом) результуючого списку, а його місце в джерелі заповнюється фіктивним елементом, з яким елементи не порівнюються.

Робота першого перегляду в нашому прикладі приведе до результату (фіктивний елемент позначено x)

23	456	550	201	x	12445	943
1	2	3	4	5	6	7
17	□	□	□	□	□	□

Наступає черга другого перегляду, результатом якого є другий елемент результуючого списку.

Шукається перший нефіктивний елемент в джерелі. Він стає кандидатом у другі елементи, а його адреса заноситься у робочу комірку. По черзі кандидат порівнюється із наступними елементами джерела. Якщо знайшовся менший, то він заміняє кандидата, і робоча комірка одержує нову адресу, адресу нового елемента. Якщо ж перегляд завершився, то кандидат займає місце другого елемента результуючого списку, робоча комірка стає порожньою. На місце переміщеного кандидата ставиться фіктивний символ.

Результатом роботи другого перегляду в нашому прикладі є

x	456	550	201	x	12445	943
1	2	3	4	5	6	7
17	23	□	□	□	□	□

Подібним чином здійснюються решта переглядів — в нашому прикладі 3, 4,5,6 та 7. Сортування закінчене. Результуючий список створено. В нашому прикладі після сьомого перегляду одержуємо

x	x	x	x	x	x	x
1	2	3	4	5	6	7
17	23	201	456	550	943	12445

і результуючий список має вигляд

$$B = \{17, 23, 201, 456, 550, 943, 12445\}.$$

Лінійний вибір з обміном. Лінійний вибір з обміном також має перегляди, але на один менше, ніж кількість елементів у списку до сортування — джерелі.

В цьому алгоритмі не виділяється місце для результуючого списку, результуючий список формується на місці джерела.

Кожен з переглядів визначає наступний елемент результуючого спску. В нашому прикладі маємо джерело

23	456	550	201	17	12445	943
1	2	3	4	5	6	7

Перший перегляд починається з того, що кандидатом на найменший елемент обирається перший елемент джерела. Далі він порівнюється із наступними елементами до тих пір, поки не закінчиться список, або не зустрінеться менший елемент. Якщо список закінчився, то перегляд закінчився, а якщо зустрівся менший елемент, то він міняється місцем із першим, і перегляд продовжується. Результатом першого перегляду в нашому прикладі буде

17	456	550	201	23	12445	943
1	2	3	4	5	6	7

Другий перегляд починається з того, що кандидатом на другий елемент обирається другий елемент видозміненого перешим переглядом джерела. Далі він порівнюється із наступними елементами до тих пір, поки не закінчиться список, або не зустрінеться менший елемент. Якщо список закінчився, то перегляд закінчився, а якщо зустрівся менший елемент, то він міняється місцем із другим, і перегляд продовжується. Результатом другого перегляду в нашому прикладі буде

17	23	550	445	201	12445	943
1	2	3	4	5	6	7

Подібним чином здійснюються решта переглядів — k-й перегляд працює з тією частиною видозміненого джерела, яка починається із k-ого місця.

Результатом роботи алгоритму в нашому прикладі буде

17	23	201	456	550	943	12445
1	2	3	4	5	6	7

Лінійний вибір з підрахунком

Знову маємо заданий список — у прикладі ним є (14). Створюємо лічильники — в (14) додаємо порожній рядок, в якому в результаті роботи алгоритму одержимо адреси (порядкові номери) елементів джерела в результуючому списку. Одержуємо (15). Комірку нижнього рядка називаємо лічильником того елемента списку, що стоїть у першому рядку.

Всі комірки першого рядка — всі лічильники, заповнюємо одиничками.

Алгоритм розбивається на стільки переглядів всього списку, скільки елементів у заданому списку.

При першому перегляді перший елемент джерела порівнюється із кожним (крім себе) елементом джерела. Якщо порівнюваний елемент менше першого, то до лічильника цього першого елемента додається 1. А якщо порівнюваний елемент більший першого, то не робиться нічого, просто переходимо до наступного порівняння.

В результаті роботи першого перегляду в нижньому рядку перший елемент одержить в лічильнику кількість елементів, що менше нього, плюс 1. В нашому прикладі перший перегляд дасть

23	456	550	201	17	12445	943
1	2	3	4	5	6	7
2	1	1	1	1	1	1

При другому перегляді другий елемент джерела порівнюється із кожним (крім себе) елементом джерела. Якщо порівнюваний елемент менше другого, то до лічильника цього другого елемента додається 1. А якщо порівнюваний елемент більший другого, то не робиться нічого, просто переходимо до наступного порівняння.

І так далі.

При $k-$ому перегляді $k-$й елемент джерела порівнюється із кожним (крім себе) елементом джерела. Якщо порівнюваний елемент менше другого, то до лічильника цього $k-$го елемента додається 1. А якщо порівнюваний елемент більший $k-$го, то не робиться нічого, просто переходимо до наступного порівняння.

В результаті роботи алгоритму під кожним елементом джерела в його лічильнику одержиться число, яке на одиничку більше ніж кількість елементів джерела, що менші за нього, тобто лічильник позазуватиме місце елемента джерела в результуючому списку.

В нашому прикладі матимемо

23	456	550	201	17	12445	943
1	2	3	4	5	6	7
2	4	5	3	1	7	6

Стандартний обмін Стандартний обмін називають також методом бульки, тому що кожен елемент списку пересуваєься на своє місце подібно бульці, що спливає вверх у воді.

В стандартному обміні додаткова пам'ять не використовується. Отже в нашому прикладі маємо джерело

$$A = \{23, 456, 550, 201, 17, 12445, 943\}.$$

При кожному перегляді ведеться підрахунок кількості обмінів. Якщо обмінів при перегляді не було, то робота алгоритма завершується. При кожному наступному перегляді кількість учасників перегляду зменшується. Якщо ця кількість дорівнює 0, то алгоритм закінчує роботу.

При першому перегляді розглядаються пари (перший-другий), (другий-третій), (третій-четвертий) і т.д. Якщо наступний елемент пари менше попереднього, то вони міняються місцями (відбувається обмін, який враховується лічильником). Якщо ж другий елемент більше першого, то переходимо до наступної пари. В результаті першого перегляду найбільший елемент списка стане на останнє місце і виключається із розглядання.

В нашому прикладі перший перегляд дасть

$$A_1 = \{23, 456, 201, 17, 550, 943, 12445\}.$$

Другий перегляд здійснюється так як і перший, за винятком того, що останній елемент не розглядається. В нашому прикладі другий перегляд дасть

$$A_1 = \{23, 201, 17, 456, 550, 943, 12445\}.$$

Другий перегляд гарантує, що два останні елементи саме ті, які повинні стояти у результуючому списку.

Решта переглядів відбувається подібним чином. В нашому прикладі другий перегляд дасть

$$A_2 = \{23, 17, 201, 456, 550, 943, 12445\},$$

третій перегляд дасть

$$A_2 = \{17, 23, 201, 456, 550, 943, 12445\}, \tag{16}$$

четвертий перегляд покаже, що обмінів не було і алгоритм закінчив роботу.

Парний обмін В цьому алгоритмі не використовується додаткова пам'ять, але сам алгоритм організовується досить складно. Як і попередні алгоритми, парний обмін розбивається на перегляди. При кожному перегляді розглядаються пара елементів списку-джерела.

На переглядах з непарними номерами розглядаються пари позицій (адрес) (1,2) (3,4), (5,6) і т. д. , тобто пари вигляду $(2k-1, 2k)$. Порівнюються елементи з адресами, які утворюють пару. Якщо елемент з меншою адресою більший елемента з меншою адресою, то вони обмінюються місцями. В протилежному випадку вони залишаються на місці

На переглядах з парними номерами розглядаються пари позицій (адрес) (2,3) (4,5), (6,7) і т. д. , тобто пари вигляду $(2k, 2k+1)$. Порівнюються елементи з адресами, які утворюють пару. Якщо елемент з меншою адресою більший елемента з меншою адресою, то вони обмінюються місцями. В протилежному випадку вони залишаються на місці.

Якщо останній елемент списку не має пари, то він у перегляді не бере участі.

На кожному перегляді ведеться облік кількості обмінів позиціями. Якщо кількість обмінів при двох послідовних переглядах дорівнює нулю, то алгоритм закінчує роботу.

Прослідкуємо за роботою цього алгоритму на нашому прикладі.

На першому кроці розглядаються пари

$$(23, 456), (550, 201), (17, 12445).$$

І після першого перегляду одержуємо список

$$\{23, 456, 201, 550, 17, 12445, 943\}.$$

На другому перегляді розглядаються пари

$$(456, 201), (550, 17), (12445, 943).$$

Результатом роботи перегляду буде

$$\{23, 201, 456, 17, 550, 943, 12445\}.$$

Третій, четвертий та п'ятий перегляди дадуть списки

$$\{23, 201, 17, 456, 550, 943, 12445\}, \quad \{23, 17, 201, 456, 550, 943, 12445\},$$

$$\{17, 23, 201, 456, 550, 943, 12445\}.$$

Шостий та сьомий перегляди переконують нас в тому, що сортування завершене, і відповіддю є список $\{17, 23, 201, 456, 550, 943, 12445\}$.

Просіювання В просіюванні немає окремих переглядів всього списку, але перегляд природно розбивається на частини. На одних частинах рух відбувається в сторону зростання адреси, а на інших рух відбувається в сторону зменшення адреси.

В цьому алгоритмі порівнюються, як і в методі стандартного обміну, пари сусідніх елементів списку. Якщо більший елемнт має меншу адресу, то він міняється місцем із сусідом, з яким порівнюється.

Починається алгоритм із порівняння елементів списку з адресам 1 та 2. Після порівняння переходимо до пари з адресами 2 та 3. Такий перехід назвемо прямим переходом, або переходом у сторону зростання. Якщо в парі відбувся обмін місцями елементів списку, то

1. запам'ятовується місце, та пара, де відбувся обмін;
2. починається рух в зворотному напрямку — адреси пари зменшуються на 1.

Якщо при русі в зворотному напрямку відбувся обмін, то рух в зворотному напрямку продовжується (якщо це можливо, коли пара не перша). Якщо ж обмін не відбувся, або пара перша, то починається рух у прямому напрямку починаючи із запам'ятованого місця. Алгоритм закінчує роботу, коли розглянута остання пара в списку і відбувся, якщо це необхідно, рух у зворотному напрямку.

Покажемо, як працює цей метод на нашому прикладі

$$A = \{23, 456, 550, 201, 17, 12445, 943\}.$$

Спочатку розглядаються пара (23,456). Обміну немає. Рухаємося у прямому напрямку. Переходимо до пари (456,550), обміну немає. Рухаємося у прямому напрямку, переходимо до пари (550,210). Є обмін. Запам'ятовуємо, що ми розглядали пару з адресами (3,4).

Рухаємося у зворотному напрямку. Розглядаэмо пару (456,210). Робимо обмін і рухаємося у зворотному напрямку. Розглядаємо пару (23,210). Обміну немає, зворотний рух припинено. Одержали список

$$A = \{23, 210, 456, 550, 17, 12445, 943\}.$$

Починаємо рух у прямому напрямку з пари, що має адреси (4,5), тобто (550, 17). Є обмін. Запам'ятовуємо місце для початку наступного прямого руху.

Починаємо рух назад, у зворотному напрямку. Пара (456,17) дає обмін, рухаємося назад. Пара (210,17) дає обмін, рухаємося назад. Пара (23, 17) дає обмін, але рух назад припиняємо, тому що це перша пара. Одержали список

$$\{17, 23, 210, 456, 550, 12445, 943\}.$$

Починаємо рух у прямому напрямку з пари, що має адреси (5,6) — обміну немає, рухаємося далі. Наступна пара (12445,943), обмін є. Оскільки пара була останньою, то запам'ятовувати місце не потрібно — алгоритм закінчиться, коли закінчиться зворотний рух.

Зворотний рух починається із пари (550,943) — обміну нема, зворотний рух припинився, алгоритм закінчено, одержано кінцевий список

$$\{17, 23, 210, 456, 550, 943, 12445\}.$$

Лінійна вставка.

При застосуванні цього методу спочатку утворюється порожній результуючий список, який в кінці роботи алгоритму перетворюється на справжній впорядкований підсумковий список.

Кожен крок алгоритму полягає у вставлянні чергового елемента списка-джерела $A = \{a_1, a_2, \ldots, a_n\}$ у підсумковий список $B = b_1, b_2, \ldots, b_n$.

Перед початком роботи підсумковий список порожній — символьно цей факт записуємо як $b_i = \square, \quad i = 1, 2, \ldots, n$.

На першому кроці береться перший елемент списка-джерела і ставиться на перше місце підсумкового списку, отже $b_1 = a_1$.

На другому кроці береться другий елемент a_2 списка-джерела A, порівнюється із першим елементом b_1 підсумкового списку і, якщо $a_2 > b_1$, то пишемо наступний елемент списка B — $b_2 = a_2$. Якщо ж $a_2 < b_1$, то пишемо $b_1 = a_2, b_2 = a_1$.

На кожному наступному (скажемо $k-$му, $k = 3, 4, \ldots, n$ кроці маємо визначені елемент $b_1, b_2, \ldots, b_{k-1}$, і при цьому

$$\{a_1, a_2, \ldots, a_{k-1}\} = \{b_1, b_2, \ldots, b_{k-1}\}.$$

Вибираємо елемент $a_k \in A$ і по черзі порівнюємо його з елементами $b_1, b_2, \ldots, b_{k-1}$. Якщо $a_k < b_1$, то на перше місце підсумкового списку ставимо a_k, а решту списку зсуваємо на одну позицію вправо.

Якщо $a_k > b_{k-1}$, то на $k-$е місце підсумкового списку ставимо a_k.

Якщо $a_k < b_{k-1}$, і $a_k > b_1$, то знаходимо місце i, $1 < i < k-1$ таке, що

$$b_i < a_k < b_{i+1},$$

розділяємо підсумковий список на дві частини — до $i-$го місця і після $i-$го місця. Праву частину зсуваємо на одну позицію вправо. На вивільнену $i-$у поозицію вставляємо елемент a_k. Черговий крок завершено.

Покажемо, як працює метод лінійної вставки на нашому прикладі списку (13). Перед початком роботи маємо

$$A = \{23, 456, 550, 201, 17, 12445, 943\}.$$
$$B_0 = \{\square, \square, \square, \square, \square, \square, \square\}.$$

Випишемо 7 послідовних виглядів $B_1, B_2, B_3, B_4, B_5, B_6, B_7 = B$ підсумкового списку (рисочку ставимо зверху над тим елементом, який щойно вставлений)

$$
\begin{aligned}
B_1 &= \{\overline{23}, \square, \square, \square, \square, \square, \square\},\\
B_2 &= \{23, \overline{456}, \square, \square, \square, \square, \square\},\\
B_3 &= \{23, 456, \overline{550}, \square, \square, \square, \square\},\\
B_4 &= \{23, \overline{201}, 456, 550, \square, \square, \square\},\\
B_5 &= \{\overline{17}, 23, 201, 456, 550, 12445, \square\},\\
B_6 &= \{17, 23, 201, 456, 550, \overline{12445}, \square\},\\
B_7 &= \{17, 23, 201, 456, 550, \overline{943}, 12445\}.
\end{aligned}
$$

2.4 Верхні та нижні межі

2.4.1 Означення та позначення

Верхньою межею підмножини $B \subseteq A$ частково впорядкованої множини $\langle A; \leq \rangle$ називають елемент $a \in A$, для якого

$$\forall x \in B (x \leq a).$$

Одна і та ж підмножина може мати багато верхніх меж.

Верхня межа, яка менша (або дорівнює) всіх інших верхніх меж, називається точною верхньою межею. Точна верхня межа підножини $B \subseteq A$ позначається $\sup B$. Точну верхню межу називають також “супремум“ і найменшою верхньою межею.

Якщо підмножина чвм має верхню межу, то ця підмножина називається обмеженою зверху Найбільший елемент є точною верхньою межею всєї чвм.

В частково впорядкованій множині $\{a, b, c, d\}$ з порядком

$$a < b, \quad c < d$$

підмножина $\{a, c\}$ не має жодної верхньої грані. А в частково впорядкованій множині $\{a, b, c, d\}$ з порядком

$$a < b, \quad c < d, \quad c < b, \quad a < d$$

підмножина $\{a, c\}$ має дві верхні грані b та d, але не має жодної точної верхньої грані.

Нижньою межею підмножини $B \subseteq A$ частково впорядкованої множини $\langle A; \leq \rangle$ називають елемент $a \in A$, для якого

$$\forall x \in B(a \leq x).$$

Одна і та ж підмножина може мати багато нижніх меж.

Якщо підмножина чвм має нижню межу, то вона називається обмеженою знизу.

Нижня межа, яка більше (або дорівнює) всіх інших нижніх меж, називається точною нижньою межею. Точна нижня межа підножини $B \subseteq A$ позначається $\inf B$. Точну нижню межу називають також "інфімум" і "найбільша нижня межа".

На рис. 10 зображена діаграма чвм, в якій елементи a, c (підмножина $\{a, c\}$) не має жодної верньої грані і, відповідно, не має точної верхньої грані.

На рис. 11 зображена діаграма чвм, в якій елементи a, c (підмножина $\{a, c\}$) має дві верхні грані — елементи b, d, але не має точної верхньої грані.

Функція, яка обчислює точну верхню (відповідно, нижню) межу підмножини в заданій чвм, позначається sup (відповідно, inf). В чвм $\{a, b, c\}$, що зображена на рис. 2 , буде $\inf(b, c) = a$, а $\sup(b, c)$ не існує.

Функція, яка обчислює найменший (відповідно, найбільший) елемент в заданій чвм, позначається min (відповідно, max).

У частково впорядкованій множині всіх підмножин заданої множини точною верхньою гранню двох елементів є їх об'єднання, а точною нижньою гранню є перетин цих двох елементів. Тому і у загальному випадку точну верхню (відповідно, нижню) межу для двох елементів в чвм також називають об'єднанням (відповідно, перетином) цих елементів.

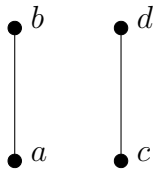


Рис. 10: Підмножина $\{a, c\}$ не має жодної верхньої і жодної нижньої грані

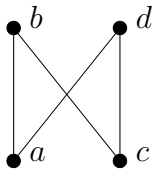


Рис. 11: Підмножина $\{a, c\}$ має дві верхні грані і не має точної верхньої грані

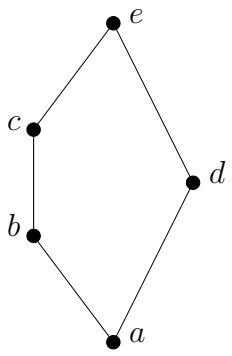


Рис. 12: Будь-яка пара елементів має точну верхню і точну нижню межу. Дистрибутивний закон для операції sup та inf не виконується

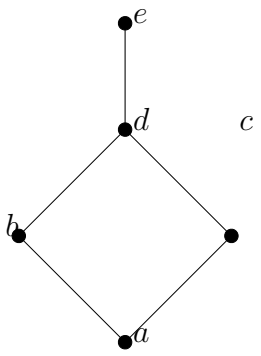


Рис. 13: Будь-яка пара елементів має точну верхню і точну нижню межу. Дистрибутивний закон для операції sup та inf виконується

Звернемося до чвм, чия діаграма зображена на рис. 12. Використовуючи знак $\cup$ для позначення об'єднання, можна записати

$$b \cup d = e.$$

Подібним чином, для позначення операції знаходження точної нижньої грані використовують знак $\cap$. Отже для елементів чвм, чия діаграма зображена на рис. 12, можна написати

$$b \cap d = a.$$

Якщо в одному мовному оточенні використовуються і теоретико-множинні операції перетину та об'днання і операції знаходження точної верхньої та точної нижньої межі, тоді для позначення точної верхньої межі можна використовувати знак $\vee$,а для позначення точної нижньої межі можна використовувати знак $\wedge$, а можна для для позначення точної верхньої межі можна використовувати знак $+$,а для позначення точної нижньої межі можна використовувати знак $\cdot$

2.4.2 Властивості операцій знаходження точної верхньої та точної нижньої межі.

Розглянемо наступну задачу. В кожній із кількох груп студентів вибрали найменшого за зростом студента, а потім із вибраних вибрали найвищого. Позначимо зріст цього найвищого студента через a. Іншим разом в кожній із цих груп вибрали найвищого за зростом студента, а потім із вибраних вибрали найнижчого. Позначимо зріст цього найнижчого студента через b. Чи можна наперед сказати, яке число більше a чи b? Відповідь — ні, тобто можливий випадок, коли $a < b$ і можливий випадок, коли $b < a$.

Пояснимо відповідь прикладами. Припустимо що груп дві. В першому прикладі група A складалася із студентів зростом 1.70, 1.71, 1.72 та 1.73. Група B складалася із студентів зростом 1.71, 1.72, 1.73 та 1.74. В цьому прикладі

$$\sup A = 1.73, \quad \sup B = 1.74, \quad a = \inf\{\sup A, \sup B\} = \inf\{1.73, 1.74\} = 1.73$$

$$\inf A = 1.70, \quad \inf B = 1.71, \quad b = \sup\{\inf A, \inf B\} = \sup\{1.70, 1.71\} = 1.71$$

і $b < a$.

В другому прикладі група A складалася із студентів зростом 1.70 та 1.71. Група B складалася із студентів зростом 1.72 та 1.73. В цьому прикладі

$$\sup A = 1.71, \quad \sup B = 1.73, \quad a = \inf\{\sup A, \sup B\} = \inf\{1.71, 1.73\} = 1.71$$

$$\inf A = 1.70, \quad \inf B = 1.72, \quad b = \sup\{\inf A, \inf B\} = \sup\{1.70, 1.72\} = 1.72$$

і $b > a$.

Якщо розглядати $\sup, \inf$ як бінарні всюди визначені операції на певній чвм M, то ці операції

- ідемпотентні, тобто $\sup\{a, a\} = a$, $\inf\{a, a\} = a$ для будь-якого $a \in M$;
- асоціативні, тобто $\sup\{a, \sup\{b, c\}\} = \sup\{\sup\{a, b\}, c\}$, $\inf\{a, \inf\{b, c\}\} = \inf\{\inf\{a, b\}, c\}$ для будь-яких $a, b, c \in M$;
- комутативні, тобто $\sup\{a, b\} = \sup\{b, a\}$, $\inf\{a, b\} = \inf\{b, a\}$ для будь-яких $a, b \in M$.

Між собою операцію знаходження точної верхньої та точної нижньої межі двох елементів зв'язна законами поглинання

- $\inf\{a, \sup\{a, b\} = a$;
- $\sup\{a, \inf\{a, b\} = a$.

Наявність виписаних властивостей обгрунтовується тим, що для будь-яких $a, b \in M$

$$\sup\{a, b\} \geq a, \qquad \inf\{a, b\} \leq a.$$

2.4.3 Напівгратки та гратки.

Напівграткою називають множину разом із ідемпотентною, комутативною, асоціативною операцією.

Із означення випливає, що чвм, в якій для будь-яких двох елементів існує точна верхня межа, є напівгракою — бінарною операцією можна взяти операцію знаходження точної верхньої межі. Також чвм, в якій для будь-яких двох елементів існує точна нижня межа, є напівгракою — бінарною операцією можна взяти операцію знаходження точної нижньої межі.

Зворотне твердження оформим у вигляді теореми

Теорема 2.1 *В будь-якій напівгратці можна ввести відношення часткового порядку так, що існуюча на ній бінарна операція буде операцією знаходження точної верхньої (або точної нижньої) межі.*

Доведення.

Нехай множина M разом із операцією додавання $+$ утворює напівгратку, тобто для будь-яких елементів $a, b, c \in M$

$$a + a = a, \quad a + b = b + a, \quad a + (b + c) = (a + b) + c.$$

Введемо на M бінарне дношення $\alpha \subseteq M^2$ правилом: для $a, b \in M$

$$(a, b) \in \alpha \Leftrightarrow \exists c \in M(a = b + c).$$

Доведемо, що так введене відношення є відношенням частового порядку.

Рефлексивність відношення α випливає із ідемпотентності додавання

$$\forall a \in M(a + a = a \Rightarrow ((a, a) \in \alpha)).$$

Транзитивність випливає із асоціативного закону. Дійсно, припустимо, що для деяких $a, b, c \in M$ $(a, b), (b, c) \in \alpha$. Тоді за визначенням відношення α для деяких $x, y \in M$, можна записати

$$a = b + x, \quad b = c + y$$

Звідси

$$a = (c + y) + x = c + (y + x),$$

і $(a, c) \in \alpha$.

Доведемо антисиметричність, тобто коли $(a, b), (b, a) \in \alpha$, то $a = b$. В такому разі за визначенням бінарного відношення α для деяких $x, y \in M$ будуть виконуватися рівності

$$a = b + x, \quad b = a + y.$$

Виписані рівності дозволяють записати

$$b + y = (a + y) + y = a + (y + y) = a + y = b,$$

і

$$a = (b + y) + x = (b + x) + y = a + y = b,$$

і антисиметричніть перевірена.

Якщо бінарне відношення α назвати "більше або дорівнює", то операція додавання буде збігатися із операцією $\sup$. Якщо ж бінарне відношення α назвати "менше або дорівнює", то операція додавання буде збігатися із операцією $\inf$.

Теорема доведена.

■

Граткою називають множину M разом із двома ідемпотентними, комутативними, асоціативними операціями операціями (назвемо ці операції додаванням та множенням), що пов'язані між собою двома законами поглинання: для будь-яких $x, y \in M$

$$x(x+y) = x, \qquad x + xy = x.$$

Кожна із двох операцій гратки визначає на множині M, на якій вони задані два відношення порядку. А закони поглинання забезпечують збіг цих відношень. Наведені міркування дозволяють користуватися в певному розумінні більш наочним означенням напівгратки та гратки:

Верхньою напівграткою називають частково впорядковану множину, в якій для будь-яких двох елементів існує точна точна верхня межа.

Нижньою напівграткою називають частково впорядковану множину, в якій для будь-яких двох елементів існує точна точна нижня межа.

Граткою називають частково впорядковану множину, в якій для будь-яких двох елементів існує точна точна верхня межа і точна нижня межа.

На рис. 2 і на рис. 6 зображені нижні напівгратки, які не є верхніми напівгратками і, відповідно, не є гратками. На рис. 8,9, 12 зображені гратки.

Важливим є випадок, коли в частково впорядкованій множині будь-яка підмножина має точну верхню межу (тоді ця чвм називаються повною верхньою напівграткою), точку нижню межу (тоді ця чвм називається повною нижньою граткою) або будь-яка підмножина має у множині і точну верхню і точну нижню межу.

Чвм підполів даного поля, чвм підгруп даної групи, чвм підкілець даного кільця і т. п. утворюють повні напівгратки.

В кожній гратці можна розглядати підгратки — частково впорядковані підмножини (частковий порядок на підмножині збігається із частковим порядком на всій множині), в яких для будь-яких двох елементів існує точна верхня і точна нижня межа.

3 Гратка підалгебр універсальної алгебри

Нагадаємо, що універсальню алгеброю $\mathcal{A} = \langle A; \Sigma \rangle$ називають множину A (її називають носієм універсальної агебри $\mathcal{A}$) разом із операціями, на цій множині. Множину Σ операцій універсальної алгебри називають сигнатурою цієї універсальної алгебри. У практичній роботі звичайно універсальну алгебру позначають так же як і її носія. Звичайно це не призводить до непорозумінь. Так ми можемо говорити про множину дійсних чисел $\mathbb{R}$ і про $\mathbb{R}$ як множину дійсних чисел разом із операціями додавання та множення. Універсальна алгебра $\mathcal{B} = \langle B, \Xi \rangle$ буде підалгеброю алгебри $\mathcal{A}$, коли

$$B \subseteq A, \qquad \Sigma = \Xi.$$

Рівність $\Sigma = \Xi$ розуміється як

- збіг назв операцій на A та на B
- результат застосування операції з певною назвою до елементів із B буде один і той же незалежно від того, взяли ми операцію з цією назвою із Σ чи із Ξ

Для прикладу, якщо Σ складається тільки з додавання, то Ξ повинна складатися також виключно із додавання, причому сума елементів із B не залежить від того, взяли ми додавання із Σ чи із Ξ. Якщо в Σ є нульмісна операція (виділений елемент, наприклад, 0), то в Ξ також повинен бути відділений той же самий елемент (в нашому прикладі 0). Якщо в Σ є одномісна операція $x \mapsto f(x)$, то в Ξ також повинна бути одномісна операція з цим же іменем, яка є звуженням операції $f \in \Sigma$ на B.

Приклади підалгебр розглянема в наступних розділах — і визначення стане зрозумілішим.

Якщо в сигнатурі алгебри є нульмісна операція (виділений елемент), то носій підалгебри не може бути порожнім — в ньому обов'язково повинен бути цей виділений елемент. Якщо ж нульмісних операцій немає, то носій може бути порожнім. Так порожня множина буде підалгеброю алгебри з однією одномісною операцією (унара).

Замість словосплуки "універсальна алгебра" будемо користуватися абревіатурою у.а.

Є дещо видозмінений підхід до означення підалгебри універсальної алгебри.

Нехай на множині A задана $n-$місна операція $f : A^n \to A$, і підмножина $B \subseteq A$ має властивість

$$\forall x_1, x_2, \ldots, x_n \in B(f(x_1, x_1, \ldots, x_n) \in B).$$

Тоді кажуть, що підмножина B замкнена відносно операції f. Якщо підмножина B замкнена відносно операції f, то операцію $\overline{f} : B^n \to B$, що задана правилом

$$\forall x_1, x_2, \ldots, x_n \in B \left(\overline{f}(x_1, x_1, \ldots, x_n) = f(x_1, x_2, \ldots, x_n)\right),$$

називають звуженням операції f на B.

Точно кажучи, операції f і $\overline{f}$ це різні операції, коли $A \neq B$, — вони мають різні області визначення. Проте в практичній діяльності і операція і її звуження позначаються однаково і не розрізняються. Щоб одержати при цьому непорозуміння, потрібні хист та бажання.

Так, множина натуральних чисел замкнена відносно додавання та відносно множення, які визначені на множині цілих чисел, але не замкнена відносно операції віднімання. Множина цілих чисел замкнена відносно операції віднімання, яка задана на множині дійсних чисел, але не замкнена відносно часткової операції ділення (ділення на ненульове число), яка визначена на множині дійсних чисел. Суму двох натуральних чисел n, m позначаємо $n + m$ незалежно від того, додаємо ми їх як натуральні числа чи як цілі.

Нехай задана у.а. $\mathcal{A} = \langle A, \Sigma \rangle$ і підмножина $B \subseteq A$ замкнена відносно всіх операцій із Σ. Тоді у.а. $\mathcal{B} = \langle B, \Sigma \rangle$ називається пдіалгеброю у.а. $\mathcal{A} = \langle A, \Sigma \rangle$.

Підалгебри заданої у.а. $\mathcal{A}$ частково впорядковані: якщо $\mathcal{B}_1 = \langle B_1, \Sigma \rangle$, $\mathcal{B}_2 = \langle B_2, \Sigma \rangle$ дві підалгебри у.а. $\mathcal{A} = \langle A, \Sigma \rangle$, то

$$\mathcal{B}_1 \leq \mathcal{B}_2 \Leftrightarrow B_1 \subseteq B_2.$$

Теорема 3.1 *Для будь-якої сім'ї* $\mathcal{B}_i = \langle B_i, \Sigma\rangle$ $i \in I \neq \emptyset$ *підалгебр алгебри* $\mathcal{A} = \langle A, \Sigma\rangle$ *існує підалгебра*

$$\mathcal{B} = \inf\{\mathcal{B}_i | i \in I\},$$

яка визначена умовою

$$\mathcal{B} = \langle B, \Sigma\rangle =< \bigcap_{i\in I} B_i, \Sigma > .$$

Доведення. Доведення. Спочатку переконаємося, що $\mathcal{B}$ є підалгеброю алгебри $\mathcal{A}$, тобто переконаємося, що множина

$$B = \bigcap_{i\in I} B_i$$

замкнена відносно всіх операцій із Σ. Для цього вибираємо довільну $n-$місну операцію $f \in \Sigma$ і елементи $x_1, x_2, \ldots, x_n \in B$. отрібно довести, що $f(x_1, x_2, \ldots, x_n) \in B$.

Дійсно,

$$x_1, x_2, \ldots, x_n \in B \overset{(1)}{\Rightarrow} \forall i \in I(x_1, x_2, \ldots, x_n \in B_i) \overset{(2)}{\Rightarrow}$$

$$\overset{2}{\Rightarrow} \forall i \in I(f(x_1, x_2, \ldots, x_n) \in B_i) \overset{(3)}{\Rightarrow} f(x_1, x_2, \ldots, x_n) \in B.$$

Імплікації (1) та (3) правильні за означенням перетину множин, а імпликація (3) правильна тому, що $\mathcal{B}_i = \langle B_i, \Sigma\rangle$ $i \in I$ є підалгебрами алгебри $\mathcal{A} = \langle A, \Sigma\rangle$.

■

Серед усіх підалгебр алгебри $\mathcal{A}$ є найменша — точна нижня межа всіх підалгебр, і є найбільша — вся алгебра.

Теорема 3.2 *Для будь-якої сім'ї* $\mathcal{B}_i = \langle B_i, \Sigma\rangle$ $i \in I \neq \emptyset$ *підалгебр алгебри* $\mathcal{A} = \langle A, \Sigma\rangle$ *існує підалгебра*

$$\mathcal{B} = \sup\{\mathcal{B}_i | i \in I\}.$$

Доведення. Задана сім'я підалгебр має верхні межі, однією з них буде вся алгебра. А точна нижня межа всіх верхніх меж (вона існує згідно теореми 3.2) буде точною верхньою межею — за визначенням точної верхньої межі.

■

Зауважимо, що носій точної верхньої межі сукупності підалгебр не обов'язково є об'єднанням носіїв підалгебр. Для прикладу можна взяти два підполя

$$\mathbb{Q}(\sqrt(2)) = \left\{a + b\sqrt{2} | a, b \in \mathbb{Q}\right\}$$

і

$$\mathbb{Q}(\sqrt(3)) = \left\{a + b\sqrt{3} | a, b \in \mathbb{Q}\right\}$$

поля дійсних чисел. Точна верхня межа цих двох підполів містить у собі число $\sqrt{6}$, але цього числа немає ні в полі $\mathbb{Q}(\sqrt(2))$ ні в полі $\mathbb{Q}(\sqrt(3))$.

Перевіримо, що числа $\sqrt{6}$ немає в полі $\mathbb{Q}(\sqrt(2))$. Дійсно, нехай для деяких раціональних чисел a, b

$$\sqrt{6} = a + b\sqrt{2} \tag{17}$$

Тоді $a \neq 0$, в протилежному випадку ми можгли б розілілити рівність (17) на $\sqrt{2}$ і одержати, що $\sqrt{3}$ є раціональним числом.

Число b також не нуль, в протилежному випадку було б раціональним число $\sqrt{6}$.

Піднісши рівність 17 до квадрату, одержимо

$$6 = a^2 + 2ab\sqrt{2} + 2b^2, \qquad \sqrt{2} = \frac{6 - a^2 - 2b^2}{2ab},$$

тобто ми одержали, що число $\sqrt{2}$ є раціональним. Одержане хибне твердження доводить, що рівність 17 неможлива, і $sqrt6$

не належить полю $\mathbb{Q}(2)$. Точно так же перевіряємо, що $sqrt6$ не належить полю $\mathbb{Q}(3)$.

Таким чином, $\sqrt{6}$ не належить об'єднанню полів $\mathbb{Q}(2)$, $\mathbb{Q}(3)$ і точна верхня межа цих підполів не збігається із їх об'єднанням.

Оскільки кожна підалгебра універсальної алгебри більша від кожної підалгебри порожньої сукупності підалгебр, і кожна підалгебра менша від кожної підалгебри порожньої сукупності підалгебр, то найменша підалгебра буде точною верхньою межею всіх підалгебр із порожньої сукупності підалгебр, а вся алгебра буде точною нижньою межею всіх підалгебр із порожньої сукупності підалгебр.

3.1 Найменше підкільце на найменше підполе

Нагадаємо, що кільце — це універсальна алгебра з двома бінарними пераціями (вони називаються додаванням та множенням, однією нульмусною (виділений елемент, він називається нулем), та однією одномісною операцією (вона називається "знаходження протилежного елемента". Додавання та множення асоціативні, додавання комутативне, між собою додавання та множення зв'язані двома (лівим та правим) розподільними (дистрибутивними) законами. Виділений елемент 0 та операція знаходження протилежного елемента зв'язані тотожностями: для будь-якого елемента a кільця

$$a + (-a) = -a + a = 0, \qquad a + 0 = 0 + a = a. \tag{18}$$

Оскільки кільце має в своїй сигнатурі нульмісну операцію (нуль), то порожнім кільце і, відповідно, підкільце бути не може. А складатися виключно із нуля може. Отже найменше

підкільце в будь-якому кільці складається лише із нуля.

Якщо кільце містить в собі елемент x, то це кільце обов'язково містить

$$\underbrace{x \cdot x \cdot x \cdot \ldots \cdot x}_{n} = x^n, \qquad \underbrace{x + x + x + \ldots + x}_{n} = nx$$

Тому найменше підкільце, яке містить заданий елемент x всього кільця, складається із нуля і тих елементів усього кільця, які можна записати у вигляді

$$n_1 x + n_2 x^2 + \cdots + n_k x^k$$

для деякого натурального k, і для $n_1, n_2, \ldots, n_k \in \mathbb{N} \cup \{0\}$.

Поле має в своїй сигнатурі додавання, множення (бінарні операції, нуль та один (два різні виділені елементи), одну одномісну операцію знаходження протилежного елемента, та одну часткову одномісну операцію — знаходження для будь-якого ненульового елемента оберненого. Як і в кільці, операції додавання та множення асоціативні, між собою зв'язані дистибутивними законами, нуль та операція знаходження протилежного елемента зв'язані співвідношеннями (18), множення в полі комутативне (некомутативні поля називають тілами).

Часткова операція знаходження оберненого елемента (вона визначена на ненульових елементах поля) підкоряється умовам: для будь-якого елемента $a \neq 0$ із поля

$$a \cdot a^{-1} = a^{-1} \cdot a = 1, \qquad a \cdot 1 = 1 \cdot a = a. \tag{19}$$

Оскільки поле містить в собі два різні вділені елементи, то ні порожнім, ні одноелементним підполе бути не може. Двоелементним поле може бути — таким є поле лишків за модулем

2. Воно складається із нуля та одиниці і сума двох одиниць дорівнює нулю.

Оскільки поле замкнене відносно додавання, то в полі обов'язково для любого натурального n є

$$\underbrace{1+1+1+\ldots+1}_{n}$$

Цей елемент позначається також n. Але варто пам'ятати, що в полі сума одиниць може дорівнювати нулю. Але якщо сума одиниць не нуль, то для цієї суми є обернений елемент в полі.

Із сказаного випливає, що коли в полі сума будь-якої кількості одиниць не дрівнює нулю, то це поле містить в собі підполе, що ізоморфне полю раціональних чисел.

> Поля, в яких сума натуральної кількості одиниць не дорівнює нулю, називають полями характеристики нуль.

Отже поле характеристики нуль містить найменше підполе, яке ізоморфне полю раціональних чисел. Найменшим підполем поля дійсних чисел є поле раціональних чисел. Найменшим підполем поля комплексних чисел є також поле раціональних чисел. Все це поля харктеристики 0.

> Якщо сума кількох одиниць поля дорівнює нулю, то найменша кількість одиниць, які в сумі дають нуль, називається характеристикою цього поля.

Теорема 3.3 *Ненульова характеристика поля є простим числом*

Доведення. Доводиться теорема методом від протилежного. Припустимо, що $p \geq 2$ є характиристикою поля F і p є складеним числом, тобто $p = m \cdot n$ для деяких натуральних чисел $m, n \geq 2$.

Оскільки

$$(\underbrace{1+1+1+\ldots+1}_{m})\cdot(\underbrace{1+1+1+\ldots+1}_{n}) = (\underbrace{1+1+1+\ldots+1}_{mn=p} = 0,$$

то $m \cdot n = 0$ в полі F і при цьому $m.n \neq 0$ (нагадаємо, що найменшою кількістбю одиниць, які в сумі дають нуль, є p.) Рівність $mn = 0$ для $m.n \neq 0$ в полі неможлива, оскільки в протилежному випадку було б

$$1 = n^{-1}m^{-1}mn = n^{-1}m^{-1} \cdot 0 = 0.$$

■

Теорема 3.4 *В полі ненульової характеристики найменшим полем буде поле, яке ізоморфне полю класів лишків за деяким простим модулем.*

Доведення. Нехай p — ненульова характеристика деякого поля F і $F_1 \subseteq F$,

$$F_1 = \{0, 1, 2, \ldots, p-1\}.$$

Елементи поля $\mathbb{Z}_p$ позначимо $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-2}, \overline{p-1}$. Перевіримо, що відображення $f : F_1 \to \mathbb{Z}_p$, що задане правилом

$$x \mapsto \overline{x}, \quad x \in F,$$

є ізоморфізмом.

Виберемо два натуральні числа $0 < m, n < p$ і нехай для деяких $q_1, r_1, q_2, r_2 \in \mathbb{N} \cup \{0\}$ в кільці цілих чисел можна записати

$$m+n = q_1 p + r_1, \quad 0 \le r_1 < p, \qquad m \cdot n = q_2 p + r_2, \quad 0 \le r_2 < p.$$

тоді в полі Z_p

$$\overline{m} \oplus \overline{n} = \overline{r}_1, , \qquad \overline{m} \star \overline{n} = r_2$$

— знаками $\oplus, \star$ позначені операції додавання та множення в полі $\mathbb{Z}_p$.

В полі F_1

$$(\underbrace{1+1+1+\ldots+1}_{m}) + (\underbrace{1+1+1+\ldots+1}_{n}) = (\underbrace{1+1+1+\ldots+1}_{m+n} =$$

$$(\underbrace{1+1+1+\ldots+1}_{pq_1}) + (\underbrace{1+1+1+\ldots+1}_{r_1}) = (\underbrace{1+1+1+\ldots+1}_{r_1}$$

$$(\underbrace{1+1+1+\ldots+1}_{m}) \cdot (\underbrace{1+1+1+\ldots+1}_{n}) = (\underbrace{1+1+1+\ldots+1}_{mn} =$$

$$(\underbrace{1+1+1+\ldots+1}_{pq_2}) + (\underbrace{1+1+1+\ldots+1}_{r_2}) = (\underbrace{1+1+1+\ldots+1}_{r_2}.$$

Наведені рівності переконують в узгодженості відображення f з операціями додавання та множення в F_1 та в $\mathbb{Z}_p$.

Також відображення f узгоджене з нульмісними операціями — виділені елемнети 0 та 1 переходять у виділені елементи $\overline{0}$ та $\overline{1}$.

Видно, що відображення f бієктивне. В такому разі перевіряти узгодежність відображення f з одномісною операцією знаходження оберненого не потрібно — це випливає із решти узгодженостей.

Те, що відображення f є ізоморфізмом, доведене. Отже і вся теорема доведена.

■

Найменшим підполем поля $\mathbb{Z}_2(i) = \{0, 1, i, 1+i\}$, в якому додавання та множення задані таблицями 3.1, є поле $\mathbb{Z}_2$.

x	0	0	0	0	1	1	1	1	i	i	i	i	$1+i$	$1+i$	$1+i$	$1+i$
y	0	1	i	$1+i$	0	1	i	$1+i$	0	1	i	$1+i$	0	1	i	$1+i$
$x+y$	0	1	i	$1+i$	1	0	$1+i$	i	i	$1+i$	0	1	$1+i$	i	1	0
xy	0	0	0	0	0	1	i	$1+i$	0	i	$i+1$	1	0	$1+i$	$1+i$	i

Табл. 4: Таблиця додавання та множення в полі $\mathbb{Z}_2(i) = \{0, 1, i, 1+i\}$

Множення в полі $\mathbb{Z}_2(i) = \{0, 1, i, 1+i\}$ визначається рівністю $i^2 = i + 1$, а додавання визначається тотожністю $x + x = 0$, — це поле характеристики 2.

Також полем характеристики 2 буде поле $\mathbb{Z}_2(j) = \{0, 1, j, 1+j, j^2, 1+j^2, j+j^2, 1+j+j^2.\}$ В цьому полі $j^3 = j+1$ і $x+x = 0$ для будь-якого $x \in \mathbb{Z}_2(j)$. Найменшим підполем поля $\mathbb{Z}_2(j)$ є поле $\mathbb{Z}_2$.

3.2 Найменша піднапівгрупа

Сигнатура напівгрупи не містить виділених елементів, тому є порожня напівгрупа. Звідси випливає, що найменшою піднапівгрупою в будь-якій напівгрупі є порожня.

3.3 Найменша група

Група містить виділений елемент — одиницю, якщо операцію названо множенням, тобто в мультиплікативній групі, і нуль,

коли операцію названо додаванням (в адитивній групі). В загальному випадку виділений елемент називають нейтральним відносно бінарної операції групи. Множина, яка складається лише із виділеного елемента, замкнена відносно бінарної операції. Тому найменшою підгрупою в будь–якй групі є одноелементна підгрупа — вона складається лише із виділеного елемента.

3.4 Найменше підполе, що містить заданий елемент

Нехай F — певне поле, F_1 — його найменше підполе, і $\alpha \in F \setminus F_1$. Найменше підполе $F_2, F_1 \subseteq F_2 \subseteq F$, що містить в собі α, називають розширенням поля F_1 за допомогою елемента α.

розрізняють два випадки — коли α є коренем якогось ненульового многочлена з коефіцієнтами із F_1, і коли α не корінь някого ненульового многочлена з коефіцієнтами із F_1. В першому випадку кажуть про алгебраїчне розширення поля, а в другому — про трансценентне розширення поля.

В першому випадку поле F_2 складається лише із многочленів від α з коефіцієнтами із найменшого підполя, а в другому F_2 складається із дробів вигляду

$$\frac{a_0 + a_1\alpha + \ldots + a_n\alpha^n}{b_0 + b_1\alpha + \ldots + b_m\alpha^m}, \quad a_i, b_j \in F_1 (0 \leq i \leq n, 0 \leq j \leq m), \quad b_0 + b_1\alpha + \ldots + b_m\alpha^m$$

При доведенні сказаного використовують знання про найбільший спільний дільник двох многочленів. Проводити ретельне доведення не будемо.

3.5 Найменша піднапівгрупа, що містить заданий елемент

Якщо мультиплікативна напівгрупа містить елемент α, то будь-яка піднапівгрупа обов'язково містить всі натуральні степені цього елемента. А з другого боку, всі натуральні стпені заданого елемента замкнені відносно множення. Тому найменша піднапівгрупа, що містить заданий елемент, складається із усіх натуральних степенів цього елемента. Так елементи

$$2, 2^2, 2^3 \ldots, 2^n, \ldots$$

утворюють найменшу піднапівгрупу, що містить в собі 2.

Якщо операція в напівгрупі називається додаванням, то кожна піднапівгрупа разом з елементом α містить в собі всі кратні цьому елементу, тобто $2\alpha, 3\alpha, \ldots, n\alpha, \ldots$.

Так в адитивній напівгрупі цілих чисел найменшою піднапівгрупою, що містить число 2, буде $2, 4, 6, \ldots, 2k, \ldots$.

3.6 Найменша група, що містить заданий елемент

Нехай операція групи G названа множенням і $\alpha \in G$. Тоді з одного боку в будь-якій підгрупі повинні міститися всі цілі (як додатні так і від'мні) степені елемента α, а з другої сторони, всі цілі степені одного елемента утворюють підгрупу. Отже найменша підгрупа, що містить заданий елемент α, складається із усіх цілих степенів цього елемента. Ця підгрупа називається циклічною.

3.7 Найменший підунар, що містить заданий елемент

Нехай M — множина, $f : M \to M$ — відображення, $\langle M, f\rangle$ — унар і $\alpha \in M$. Вводимо позначення

$$f^n(\alpha) = \overbrace{f(f(f(\ldots f}^{n}(\alpha))\ldots), \quad n \in \mathbb{N}, f^0(\alpha) = \alpha.$$

Використовуючи введене позначення ми можемо сказати, що будь-який підунар який містить в собі α, містить в собі всі $f^n(\alpha), \quad n \in \mathbb{N}$, а з другого боку всі елементи,, які можна записати у вигляді $f^n(\alpha), \quad n \in \mathbb{N} \cup \{0\}$, замкнені відносно відображення f і, таким чином, утворюють підунар.

Звідси випливає, що найменшим підунаром, який містить заданий елемент α складається із $f^n(\alpha), \quad n \in \mathbb{N} \cup \{0\}$.

3.8 Алгоритм знаходження всіх підалгебр заданої універсальної алгебри

Щоб знайти всі підалгебри універсальної алгебри, потрібно для кожного її елемента знайти найменшу підалгебру, що містить цей елемент. Такі підалгебри в загальному випадку називають однопородженими. Однопороджені групи називають циклічними.

На наступному кроці шукають точну верхню межу підмножини таких однопороджених підалгебр. Цими точними верхніми межами вичерпуються всі підалгебри.

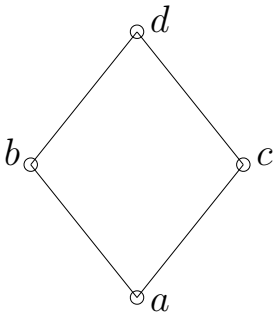
Наведемо приклади універсальних алгебр та гратки всіх її підалгебр.

Приклад 1 гратки L та гратки $S(L)$ всіх її піжграток

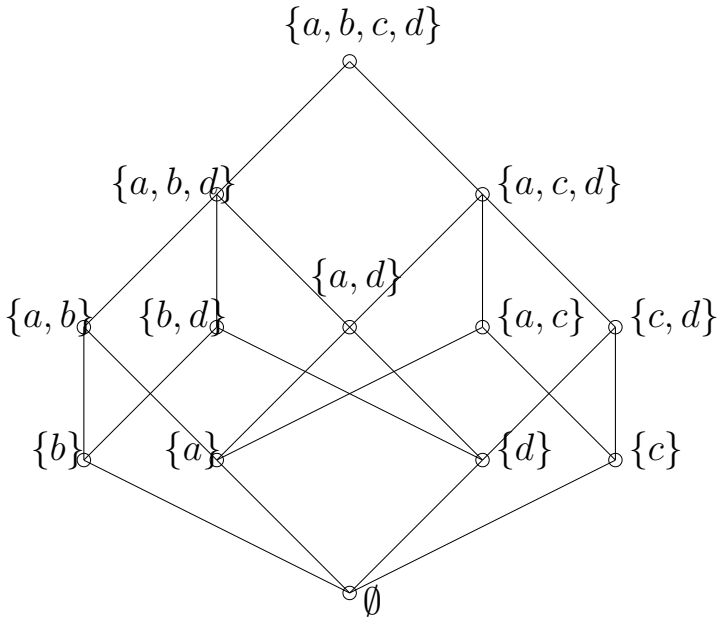
Гратка $L = \{a, b, c, d\}$ задана за допомогою часткового порядку

$$a < b, \quad a < c, \quad b < d, \quad c < d.$$

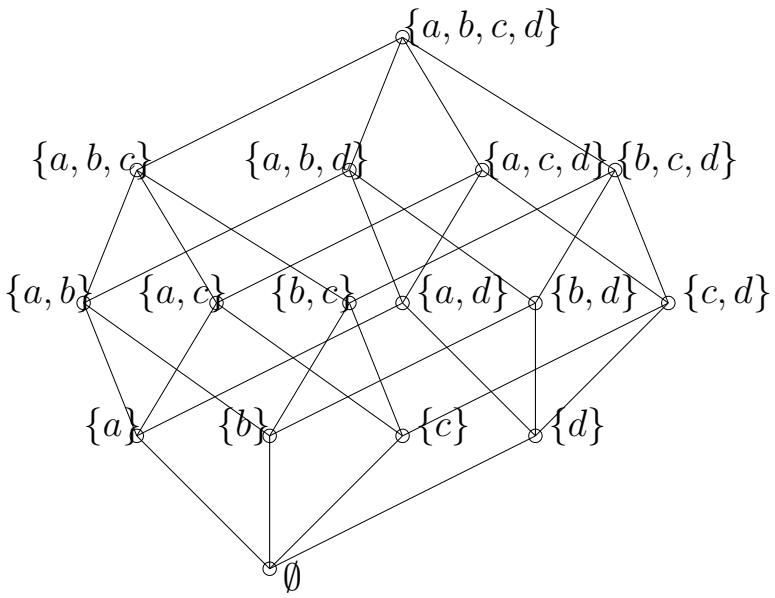
Ця гратка має діаграму



Гратка $S(L)$ має діаграму

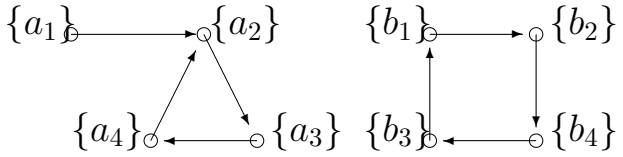


Приклад 2 гратки $\mathfrak{B}(M)$ всіх підмножин чотириелементної множини $M = \{a, b, c, d\}$

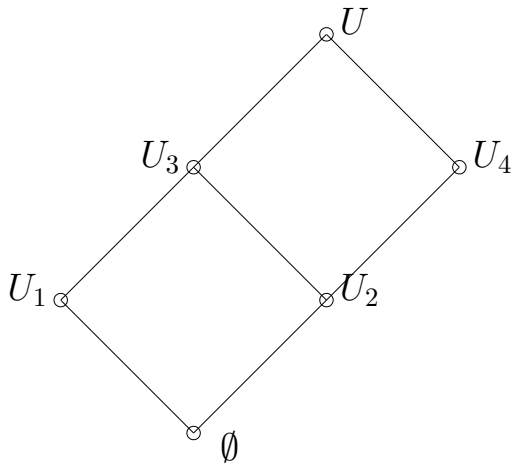


Гратку всіх підмножин чотириелементної множини можна назвати чотиривимірним кубом.

Приклад 3 гратки $L(U)$ всіх підунарів унара $U = \langle U, f\rangle$, де $U = \{a_1, a_2, a_3,\ a_4, b_1, b_2, b_3, b_4\}$, а відображення $f : U \to U$ задане графічно наступним чином.



Гратка $L(U)$ всіх підунарів має вигляд



де

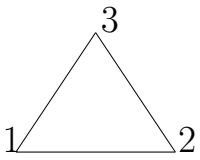
$$U_1 = \{b_1, b_2, b_3, b_4\}, \quad U_2 = \{a_2, a_3, a_4\}, \quad U_3 = U_1 \cup U_2 = \{a_2, a_3, a_4, b_1, b_2, b_3, b_4\},$$

$$U_4 = \{a_1, a_2, a_3, a_4\}.$$

Приклад 4. Розглядаємо группу G, яка складається із усіх обертань площини, що переводять правильний $n-$кутник в себе. Ця група називається циклічною. Вона складається із усіх обертань правильнийа $n-$кутника на кути $\frac{2\pi \cdot k}{n}, k = 0, 1, 2, \ldots n-1$. Гратка підгруп цієї групи ізоморфна гратці всіх дільників числа n — дільнику d числа n ввідповідає підгрупа обертань на кути $\frac{2\pi \cdot d \cdot k}{n}, k = 0, 1, 2, \ldots \frac{n}{d} - 1$. Коли $n = 30 = 2 \cdot 3 \cdot 5$, то гратка всіх підгруп зображена на рис. 8, А коли $n = 175 = 7 \cdot 5^2$, то гратка всіх підгруп ізоморфна гратці підунарів попереднього прикладу.

Приклад 5 всіх підгруп групи S_3 симетрій правильного трикутника.

Нехай правильний трикутник має вершини 1,2,3



Симетрії переводять вершини у вершини і ми можемо ці симетрії задати саме як відображення із множини вершин у множину вершин. Таким чином ми можемо записати, що $S_3 = \{e, a, b, c, x, y\}$, де

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad e = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

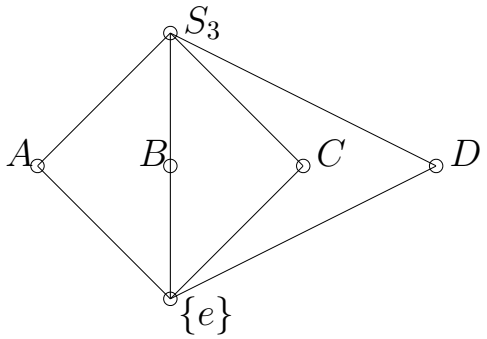
Група S_3 має 4 підгрупи. Дві з них — одинична $\{e\}$ та вся група S_3, є тривіальними. І ще є три двоелементні підгрупи:

$$A = \{e, a\}, \quad B = \{e, b\}, \quad C = \{e, c\},$$

і одна триелементна

$$D = \{e, x, y\}.$$

Діаграма чвм підгруп групи S_3 має вигляд



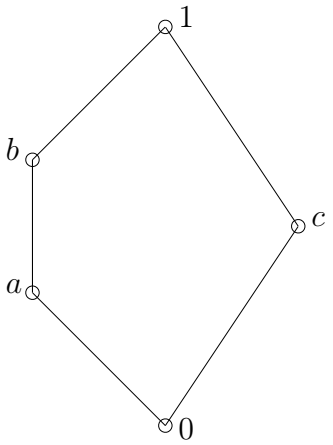


Рис. 14: Гратка N_5

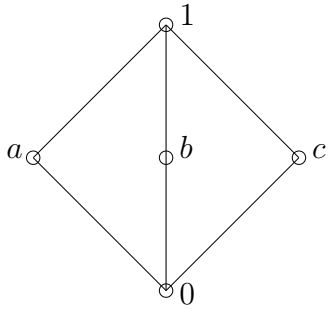


Рис. 15: Гратка M_3

3.9 Заборонені гратки

Розгладаючи ту чи іншу гратку звертають увагу на те, чи є в ній підгратки, що ізоморфні N_5, або M_3 (див рис. 14, 15)

Справа в тому, що в роботі зручно користуватися розподільним (дистрибутивним) законом, що з'єднує додавання та множення чисел

$$x(y+z) = xy + xz. \tag{20}$$

Якщо назвати операцію знаходження точної верхньої межі додаванням, а операцію знаходження точної нижньої межі множенням, то зручними в роботі виявляються ті гратки, в яких виконується розподільний закон (20). В гратках N_5 та M_3 розподыльний закон не виконується. Так в гратці N_5

$$a{+}c = b{+}c = 1, \quad b(a{+}c) = b{\cdot}1 = b, \quad ba = a, \quad bc = 0, \quad ba{+}bc = a{+}0 = a \neq b$$

В гратці N_5 також

$$a{+}c = b{+}c = 1, \quad b(a{+}c) = b{\cdot}1 = b, \quad ba = 0, bc = 0, \quad ba{+}bc = 0{+}0 = 0 \neq b.$$

Звідси робимо висновок, що коли гратка має в собі підгратку, що ізоморфна одній із граток N_5 чи M_3, то операції знаходження точний верхньої та нижньої межі не зв'язані між собою розподільним законом.

Можна довести, що і зворотне твердження правильне, якщо операції знаходження точний верхньої та нижньої межі не зв'язані між собою розподільним законом, то гратка має в собі підгратку, що ізоморфна одній із граток N_5 чи M_3.

4 Ординальні числа.

4.0.1 Цілком впорядковані множини

Коли мова йшла про математичну індукцію, ми згадували принцип найменшого числа, згідно якого в будь-якій непорожній підмножині множини натуральних чисел існує найменше число — число, що менше будь-якого іншого числа в цій підмножині. Цей принцип найменшого числа для натуральних чисел може бути узагальнений на інші множини.

> Лінійно впорядковані множини, в яких кожна непорожня підмножина має найменший елемент, називають цілком впорядкованими множинами.

Цілком впорядковані множини є — наприклад, множина натуральних чисел. Відмітимо кілька властивостей цілком впорядкованих множин.

Теорема 4.1 *Якщо P — цілком впорядкована множина і $f : P \to P$ є строго монотонним відображенням, то для будь-якого $x \in P$ буде $f(x) \geq x$.*

Доведення. Доведення методом від протилежного. Нехай $A \subseteq P$ є підмножиною тих елементів із P, для яких $f(x) < x$. Якщо ця підмножина не порожня, то в ній є найменший елемент — позначимо його a. Тоді $f(a) < a$ і $f(a) = b \notin A$, $f(b) \geq b$. А це суперечить тому, що функція f монотонна і

$$b < a \Rightarrow f(b) < f(a) = b.$$

■

Відтинком чвм A називають підмножину $B \subseteq A$, яку для деякого $x \in A$ можна представити у вигляді

$$B = A_x = \{y \in A | y < x\}.$$

Теорема 4.2 *Нехай P — цілком впорядкована множина і $Q = P_x$ її відтинок для деякого $x \in P$. Стверджується, що не існує строго монотонної функції $f : P \to Q$.*

Доведення. Правильність сказаного в теоремі 4.2 випливає з теореми 4.1 — для монотонної функції f за теоремою 4.1 буде $f(x) \geq x$ і $f(x) \notin Q$.

■

Теорема 4.3 *. Для будь-яких двох цілком впорядкованих множин P, Q виконується одна і тільки одна із наступних трьох умов*

1. *Чвм P подібна (ізоморфна) чвм Q.*
2. *Чвм P подібна (ізоморфна) деякому відтинку Q_y чвм Q.*
3. *Чвм Q подібна (ізоморфна) деякому відтинку P_x чвм P.*

Доведення. Нехай маємо дві цілком впорядковані чвм — P та Q. Будуємо відповідність f між елементами P та Q — $(x, y) \in f$ в тому і тільки тому випадку, коли відтинки P_x та Q_y подібні (ізоморфні).

Перевіримо, що f є функціональною відповідністю, точніше, перевіримо, що

$$(x, y_1), (x, y_2) \in f \Rightarrow y_1 = y_2; (x_1, y), (x_2, y) \in f \Rightarrow x_1 = x_2. \tag{21}$$

Дійсно, якщо $(x, y_1), (x, y_2) \in f$ і $y_1 < y_2$, то чвм Q_{y_1} подібна Q_{y_2} і Q_{y_1} є відтинком Q_{y_2}. А таке неможливе згідно теореми 2. Отже $y_1 = y_2$. Подібним чином перевіряється, що коли $(x_1, y), (x_2, y) \in f$ то $x_1 = x_2$.

Перейдемо до більш звичного зі школи запису відображень. Функціональне відношення f задає два взаємно обренені відображення $u : P \to Q$ і $v : Q \to P$:

$$(x, u(x)) \in f, \qquad (v(y), y) \in f.$$

Відображення u, v часткові.

Відображення u і v монотонні. Для перевірки візьмемо $a, b \in P$, для яких $a > b$ і визначені елементи $u(a) = c, u(b) = d$. Існування елементів $c, d \in Q$ означає існування двох подібностей

$$\alpha : P_a \to Q_c, \qquad \beta : P_b \to Q_d.$$

Оскільки $a > b$, то $P_b \subset P_b$ і визначена подібність

$$\delta : Q_d \to Q_c, \qquad h(x) = \alpha \cdot \beta^{-1}(x).$$

За теоремою 4.2 подібність h може існувати лише у випадку, коли $d < c$. Монотонність доведена.

Далі перевіримо, що виконуєтсья одна із умов — або

$$\forall x \in P \exists y \in Q((x, y) \in f), \tag{22}$$

або

$$\forall y \in Q \exists x \in P((x,y) \in f), \tag{23}$$

Перевіряємо методом від протилежного. Припустимо, що обидві умови порушуються. Отже, припускаємо, що для деякого $p \in P$ не існує $y \in Q$ такого, що $(p,y) \in f$ і для деякого $q \in Q$ не існує $x \in P$ такого, що $(x,q) \in f$. В множині таких p виберемо найменший, і в множині таких q виберемо найменший — знову позначаємо їх p та q. Отже p це найменший елемент у множині

$$\{x \in P | \forall y \in Q((x,y) \notin f)\}$$

а елемент q найменший у множині

$$\{y \in Q | \forall x \in P((x,y) \notin f)\}.$$

Подібність між відтинками P_p та Q_q (якої за припущенням не існує) встановлюється відношенням f. Перевіркою цього і займемося.

Спочатку перевіряємо, що коли $x \in P_p$ і $(x,y) \in f$, то $y \in Q_q$. Справді (метод від протилежного), якщо $y \notin Q_q$, то $y \geq q$. Подібність $w : Q_y \to P_x$ встановлює подібність між Q_q і $w(Q_q)$ — а такої подібності, за припущенням$<$ не існує. Одержана суперечність доводить, що $y < q, y \in Q_q$.

Ми уже перевірили, що відображення $u : P_p \to Q_q$ є повним (не частковим), монотонним, ін'ктивним та сюр'ктивним (див. (21)). Таким чином ми перевірили, що відображення $u : P_p \to Q_q$ є подібністю (ізоморфізмом). А це суперечить припущенню, що відтинок P_p е подібний ніякому відтинку Q_y. Ми одержали суперечність, яа доводить, що одна із умов (22)(23) виконується.

Тепер маємо три випадки

1. виконуєтсья умова (22) але не виконується умова (23)

2. виконується умова (23) але не вионується умова (22)

3. виконуються обидві умови (22), (23).

В першому випадку відобаження u встановлює подібність між P та відтинком Q_q; в другому випадку відображення v втановлює подібність між Q та відтинком P_p; і в третьому випадку обидва відображення u, v встановлюють подібність між цілком впорядкованими множинами P а Q.

Теорема 4.3 доведена повністю.

■

4.0.2 Мотивація вивчення ординалів

В цьому місці варто зупинитися і звернути увагу на те, що ми працюємо з речами, які важко уявити у світі матеріальних речей. Тобто ми працюємо в світі абстрактного. Щоб тут працювати, потрібен певний досвід, певні навички. На цю роботу можна мати досить негативну точку зору і, відповідно, називати її схоластикою, на відміну від роботи з графіками, фізичними процесами, поверхнями та подібним. На сьогодні навички роботи з цілком впорядкованими нескінченними множинами є важливими в практичній роботі по перевірці дієздатності програм для ЕВМ — в так званій верифікації програм. Звичайно, для програми підбирається параметр, який знаходиться в цілком впорядкованій множині, на кожному кроці роботи цей параметр зменшується. А спадна послідовність елементів ціком впорядкованої множини завжди скінченна (кажуть, що цілком впорядкована мноижна задовольняє умову обриву спадних послідовностей - умова осп, або уосп). Тому програма з таким параметром за скінченну кількість кроків буде виконана. До

теперішніх часів робота з цілком впорядкованими множинами відносилась до вузькоспеціальних розділів математики.

4.0.3 Ординали, ординальні числа.

Багато книг з математики в передмові попереджають: для розуміння матеріалу спеціальні знання не потрібні, вимагається лише певна культура — читай, досвід. Будемо вважати, що читач уже придбав певну культуру. Отже можна ввести наступне поняття — ординальне число, або ординал.

Нехай A ціком впорядкована множина. Розглянемо нову множину

$$B = \{A_x | x \in A\}$$

Вона природно подібна множині A, подібність встановлюється канонічним відображенням $x \mapsto A_x$. Далі відтинки A_x таким же чином замінюємо на ізоморфну цілком впорядковану множину відтинкв вітинка. Оскільки цілком впорядкована множина задовольняє умов осп, то послідовність конкретних замін завжди закінчується порожньою множиною. Таки чином одержується канонічна цілком впорядкована множина, яку називають ординалом.

Тепер дамо визначення ординалу.

Ординал A визначається умовами

- ординал є множиною, елементами якої є множини;
- Ординал є цілком впорядкованою множиною, причому порядок $x \leq y$ збігається з відношенням $x \subseteq y$ на множинах;
- Ординал є транзитивною множиною в тому розумінні, що коли $x \in A$ і $y \in x$, то $y \in A$.

Множина ординалів позначається $\mathbb{O}n$. Вона цілком впорядкована відношенням включення це випливає із теореми 3.

Кожен ординал має найменший елемент множину $\emptyset$. Цей ординал позначається 0. цей ординал найменший. Наступний ординал має один елемент $\{\emptyset\}$. Він позначається 1. Якщо ординали $0, 1, 2, \ldots, n-1$ уже є, то ординал $\{0, 1, 2, \ldots, n-1\}$ позначається через n. Є ординал, який складається із усіх ординалів, що п означені натуральними числами та 0 — це так званий ординал ω. За ним іде ординал $\omega + 1$

$$\omega + 1 = \{0, 1, 2, \ldots, n, \ldots, \omega\}.$$

Над ординалами можна виконувати операції додавання, множення, піднесення до степеня. Але цього вже торкатися не будемо.

Про ординали можна прочитати в інтернет-файлі

`t2_set.pdf`

М.М.Попова "Аксіоматична теорія множин" Цей файл використаний при підготовці тексту.

Покажчик