МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

КАФЕДРА СИСТЕМНОЇ ІНЖЕНЕРІЇ

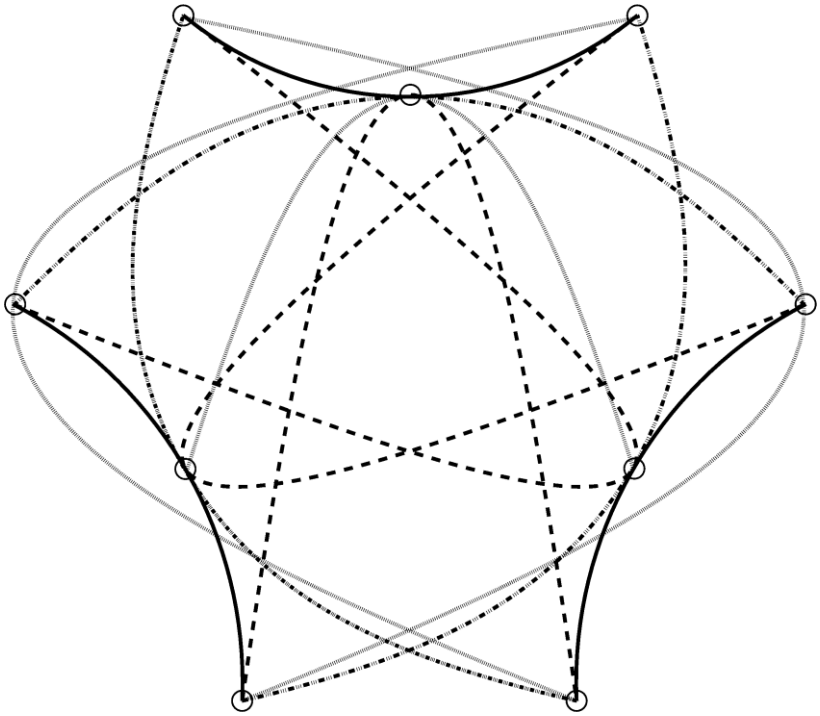
ОПОРНИЙ КОНСПЕКТ ЛЕКЦІЙ

з дисципліни

«СПЕЦРОЗДІЛИ МАТЕМАТИКИ»

для студентів напряму підготовки “Системна інженерія”

освітньо-кваліфікаційного рівня “бакалавр”



ТЕРНОПІЛЬ

Укладач: Якименко І.З., к.т.н.

УДК 519.6 (07)
ББК 22.193 (я7)

Опорний конспект лекцій з дисципліни “Спецрозділи математики” для студентів напряму підготовки “Системна інженерія” освітньо-кваліфікаційного рівня “бакалавр”/ Тернопільський національний економічний університет; Уклад. І.З. Якименко –Тернопіль,ФО-П Шпак В., 2016. – 80 с.

Рецензенти: Березький О.М.., д. т.н., професор;

Чорний В.З., к.ф.-м.н., доцент кафедри математичного аналізу Тернопільського національного педагогічного університету ім. В. Гнатюка.

Відповідальний за випуск: Николайчук Я.М., д.т.н., професор

Опорний конспект лекцій з дисципліни “Спецрозділи математики” для студентів напряму підготовки “Системна інженерія” освітньо-кваліфікаційного рівня “бакалавр” містить теоретичні відомості та приклади розвязання задач та дозволяє студентам засвоїти теоретичні знання набути практичних навичок з математичних основ, які спеціалізуються в галузях прикладної математики та інформатики, математичної кібернетики і в подальшому вивчатимуть такі розділи сучасної інформатики, як теорія алгоритмів і математична логіка, системне програмування, системи автоматизованого керування, системи аналізу і проектування обчислювальної техніки та інших пристроїв дискретної дії, системи обробки і передачі інформації, аналіз даних, оптимізація обчислень, системи штучного інтелекту, комп’ютерної графіки, розпізнавання образів тощо.

РОЗДІЛ 1. МНОЖИНИ І ВІДНОШЕННЯ

Тема 1.1. ОСНОВНІ ПОНЯТТЯ ТЕОРІЇ МНОЖИН

Коротка історична довідка

Основи теорії множин були закладені відомим німецьким математиком Георгом Кантором у другій половині минулого століття (1871-1873 рр.). У 1904-1908 рр. Е.Цермело сформулював першу систему аксіом теорії множин. Ця теорія давала можливість створення метамови математики, тобто формальної єдиної системи понять і принципів, за допомогою якої можна викласти різні розділи математики.

Однак пізніше було виявлено суперечності теорії множин Кантора: так звані *парадокси* або *антиномії*. Виникла потреба в пошуках обґрунтованіших та точніших принципів і концепцій для несуперечливості теорії множин.

Значний внесок у становлення аксіоматичної теорії множин зробили такі видатні математики і мислителі нашого століття, як Б.Рассел, Д.Гільберт, К.Гедель та ін.

Сьогодні теорія множин – це одна з основних математичних теорій, на якій ґрунтується більшість розділів сучасної математики, як неперервної, так і дискретної.

Детальніше ознайомитися з історією виникнення та розвитку теорії множин можна, прочитавши монографію А.Френкеля і І.Бар-Хіллела "Основи теорії множин" або книгу М.Клайна "Математика. Втрата певності".

1.1.1. Поняття множини

Часто теорію множин, в якій закони скінчених множин поширюються на нескінченні, називають *“інтуїтивною”* або *“наївною”*. Це не означає, що поняття чи результати цієї теорії є інтуїтивними чи наївними. Такими є лише методи введення понять і обґрунтування тверджень. Самі ж поняття чи результати входять до аксіоматичної теорії, причому їх дістають уже формально та строго доводять.

В інтуїтивній теорії множин поняття "***множина***" належить до первинних не означуваних понять (як “число”, “нескінченність” в алгебрі, “точка”, “пряма” в геометрії тощо). Це поняття не може бути означено через інші простіші терміни або об’єкти, воно є настільки широким та загальним, що не входить до як частина в жодне інше, ще загальніше поняття. Його пояснюють на прикладах, апелюючи до нашої уяви та інтуіції.

Певний час користувалися канторівським означенням: "Множина – це об’єднання в єдине спільне визначених об’єктів, які чітко розрізняються нашою інтуїцією або думкою". Проте його не можна вважати строгим математичним означенням через нематематичні терміни “об’єднання”, “інтуїція”, “думка”, це є швидше поясненням поняття множини. Істотним тут є лише те, що множину означено як єдине ціле, причому на природу об’єктів, що складають множину, ніяких обмежень не накладається.

В оточуючому світі існують як окремі об’єкти, так і їх сукупності (множини). Наприклад, будинки на вулиці, студенти групи тощо. Іншими синонімами основного слова “множина” є “сукупність”, “набір”, “колекція”, “об’єднання”, “клас”, “масив” тощо.

1.1.2. Елементи множини

Означення 1.1.1. Об’єкти, які утворюють дану множину, називають її ***елементами***.

Елементами множини можуть бути найрізноманітніші об’єкти: парні числа, літери, люди, автомобілі на стоянці, картини в музеї тощо.

Множини, як правило, позначують великими латинськими літерами: *A, B, C, ..., M, ...,* а елементи множин – малими: *a, b, c, ..., m, ...* . Записують:

$A\{a, b, c, \ldots, x, y, \ldots\}$ (перелічивши всі елементи у фігурних дужках, якщо множина складається з невеликої кількості елементів), або

$A\{a_1, a_2, \ldots, a_i, \ldots\}$ (використовуючи змінні з індексами).

При цьому слід розрізняти загальний елемент множини x, довільний – a_i чи конкретний – $a, b, c, \ldots$.

Для деяких найважливіших множин у математиці вживаються загальноприйняті позначення:

- $\mathbb{N}$ – множина натуральних чисел;
- $\mathbb{Z}$ – множина цілих чисел;
- $\mathbb{Q}$ – множина раціональних чисел;
- $\mathbb{R}$ – множина дійсних чисел;
- C – множина комплексних чисел;
- $[a; b]$ – числовий проміжок (відрізок);
- $(a; b)$ – числовий інтервал тощо.

Якщо A – деяка числова множина, то через A_+ позначують множину її додатних елементів, а через A_- – від'ємних.

Те, що об'єкт a є елементом множини M записуються так: $a \in M$ (читають: "a належить множині M", "a є елементом множини M", "Множина M містить елемент a", "a входить до множини M"). ***Знак належності*** елемента множині $\in$ є стилізацією першої літери грецького слова εστι (бути). Для того, щоб підкреслити, що деякий елемент a не належить множині M, вживають позначення $a \notin M$, $a \in M$ або $\overline{a \in M}$.

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

Множину називають ***скінченною***, якщо кількість її елементів скінчена, тобто існує натуральне число k, що є кількістю елементів цієї множини. У протилежному разі множина є ***нескінченною***.

Елементами множини можуть бути ще й інші множини. Наприклад, нехай множина $S\{s_1, s_2, \ldots, s_n\}$ – множина студентів деякої групи, які складали іспит. Цю множину можна означити й по-іншому: $S\{S_2, S_3, S_4, S_5\}$, де S_2 – множина студентів, які склали іспит на оцінку "2", відповідно S_3, S_4, S_5 – на "3", "4" і "5". У цьому випадку множини S_2, S_3, S_4, S_5 називають ***підмножинами*** множини S.

Необхідно розрізняти такі два різні об'єкти, як елемент a і множина $\{a\}$, яка складається з єдиного елемента a.

Множину вважають ***заданою***, якщо про кожен її об'єкт можна сказати є він елементом даної множини чи ні. Це дає змогу сформулювати ***інтуїтивний принцип абстракції (аксіома згортання)***: елементами множини є лише ті і тільки ті об'єкти, які мають певну характеристичну властивість.

Іноді може не існувати об'єктів, які мають характеристичну властивість для складання множини. Тоді кажуть, що ця властивість визначає ***порожню множину***. Її позначують символом "$\varnothing$". Записують: $A = \varnothing$, $x \in \varnothing$.

Елементи множин можуть бути ***різними*** і ***рівними***. Рівні (однакові) елементи мають такі властивості:

- $x = x$ – *рефлексивність*;
- якщо $x = y$, то $y = x$ – *симетричність*;
- якщо $x = y$ і $y = z$, то $x = z$ – *транзитивність*.

1.1.3. Рівність множин

Іноді означення рівності множин називають ***інтуїтивним принципом об'ємності (аксіомою екстенсіональності)***.

Означення 1.1.2. Множини A і B називають ***рівними***, якщо вони складаються з одних і тих самих елементів, тобто кожний елемент множини A є елементом множини B і навпаки.

Записують: $A = B$.

Наприклад, $\mathbb{Z}_+=\mathbb{N}$, $\mathbb{N}_+=\mathbb{N}$, $[-2; 5]_- = [-2; 0)$.

Властивості рівності множин:

- $A = A$ – *рефлексивність*;
- якщо $A = B$, то $B = A$ – *симетричність*;
- якщо $A = B$ і $B = C$, то $A = C$ – *транзитивність*.

Запис $A \neq B$ означає, що принаймні одна з розглядуваних множин містить елемент, який не належить іншій.

Наприклад, $\mathbb{Z}_+\neq\mathbb{Z}$, $[-2; 5)_+ \neq [-2; 5)$, $\{\{a,b\}\}\neq\{a,b\}$, $\{(a,b)\}\neq\{a,b\}$.

1.1.4. Задання та запис множин

Для ***задання множини***, утвореної з будь-яких елементів, будемо використовувати такі способи. В основі всіх способів лежить позначення множини за допомогою фігурних дужок.

СПОСІБ 1. Якщо $a_1, a_2, ..., a_n$ – деякі об'єкти, то множину цих об'єктів можна позначити через $\{a_1, a_2, ..., a_n\}$, де у фігурних дужках перелічують всі елементи відповідної множини. Таким способом переважно задають скінченні множини, які мають невелику кількість елементів. Порядок запису елементів множини при цьому позначенні є неістотним. Якщо множина містить однакові елементи, то у фігурних дужках їх прийнято записувати лише один раз.

Наприклад, множину десяткових цифр записуєть {0,1,2,3,4,5,6,7,8,9}, множину основних арифметичних операцій – {+,-,*,/} або {*,/,+,-}, множину розв'язків нерівності $x^2 +1\leq 1$ – {1}.

СПОСІБ 2. Цей спосіб задання множин ґрунтується на описі загальної характеристичної властивості (умови) для всіх об'єктів, що утворюють множину.

У загальному випадку задання множини M має вигляд:

$$M = \{a \mid P(a)\}.$$

Цей вираз читається так: "множина M – це множина всіх таких елементів a, для яких виконується властивість P", де через $P(a)$ позначено властивість, яку мають елементи множини M і тільки вони. Іноді замість вертикальної риски записують двокрапку.

Наприклад,

$S = \{ n \mid n$ - непарне число $\}$

$X = \{ x \mid x = \pi k, k\in\mathbb{Z} \}$,

$F = \{ f_i \mid f_{i+2} = f_{i+1} + f_i, i\in N, f_1 = f_2 = 1 \}$.

Порожню множину можна визначити за допомогою будь-якої суперечливої властивості, наприклад: $\varnothing=\{x \mid x\neq x\}$ тощо. Твердження "множина M – не порожня" можна замінювати рівносильним йому твердженням "існують елементи, які належать множині M".

СПОСІБ 3. Елементи множини можна задати за допомогою елементів вже відомих множин із застосуванням для них деякого правила чи операцій над вже відомими множинами. При цьому задання множини повинно обов'язково містити опис допоміжних (вже відомих) множин.

Наприклад,

$\mathbb{N}_0=\{0, \mathbb{N}\}$, $\mathbb{N}=\{1, 2, 3, 4, 5, \ldots\}$;

$\mathbb{N}_{2n}= \{ 2n \mid n=1, 2, 3, \ldots\}$ – множина всіх парних натуральних чисел;

$X = \{ x \mid x = \pi k, k\in\mathbb{Z} \}$,

Останнім способом задано множину всіх можливих пар, перша компонента яких належить множині $\{a_1, a_2, \ldots a_n\}$, а друга – $\{b_1, b_2, \ldots b_n\}$.

Отже, після вертикальної риски слід записати опис допоміжних множин.

1.1.5. Підмножини. Універсальна множина.

Означення 1.1.3. Множину A називають ***підмножиною*** множини B тоді і тільки тоді, коли кожний елемент множини A належить і множині B.

Позначують $A \subseteq B$ або $B \supseteq A$. Читають: "множина A міститься у множині B", "множина B містить множину A". Знаки $\subseteq$ і $\supseteq$ називаються ***знаками включення*** або ***нестрогої нерівності***.

Якщо $A \subseteq B$, однак $A \neq B$, то пишуть $A \subset B$ і називають множину A ***власною*** (*строгою* або *істинною*) ***підмножиною*** множини B. Знак $\subset$ (або $\supset$), на відміну від знака $\subseteq$ (або $\supseteq$), називається ***знаком строгого включення***.

Очевидно, що для будь-якої множини A виконується $A \subseteq A$. Крім того, прийнято вважати, що порожня множина є підмножиною будь-якої множини A, тобто $\varnothing \subseteq A$ (зокрема, $\varnothing \subseteq \varnothing$). Множини A і $\varnothing$ називають ***невласними підмножинами*** множини A, всі інші – ***власні***.

Слід чітко розуміти різницю між знаками $\in$ і $\subseteq$ та не плутати ситуації їхнього вживання. Для будь-якого об'єкта x виконується $x \notin \varnothing$.

Наприклад,

$\{a,b\} \subseteq \{\{a,b\},\{b,c\}\}$, $a \in \{a,b\}$, $\{c\} \notin \{a,c\}$, $\{a\} \subseteq \{a,b\}$.

Властивості підмножин:

- $A \subset A$ – *рефлексивність*;
- якщо $A \subset B$ і $B \subset A$, то $A = B$ – *антисиметричність*;
- якщо $A \subset B$ і $B \subset C$, то $A \subset C$ – *транзитивність*.

Разом з множиною A іноді доводиться мати справу з множиною всіх її підмножин, яку на честь Джорджа Буля назвали ***буліаном*** множини A і позначають $ß(A)$. Отже, за означенням:

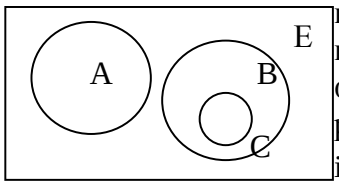
$$ß(A) = \{B \mid B \subseteq A\}.$$

Наприклад, якщо $A = \{a,b,c\}$, то $ß(A) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$.

Зауважимо, що якщо множина A має n елементів, то буліан $\beta(A)$ міститиме 2^n елементів, через що його називають ***множиною-степенем*** множини A.

У конкретній математичній теорії буває зручно вважати, що всі розглядувані множини є підмножинами деякої фіксованої множини, яку називають ***універсальною множиною*** або ***універсумом*** і позначають через E (або U). Наприклад, в елементарній алгебрі такою універсальною множиною можна вважати множину дійсних чисел R, у вищій алгебрі – множину комплексних чисел C, в арифметиці – множину цілих чисел Z, в традиційній планіметрії – множину всіх точок площини або множину всіх геометричних об'єктів, тобто множину множин точок на площині тощо.

У процесі вивчення множин зручно застосовувати так звані діаграми Ейлера-Венна. На них універсальну множину схематично зображують у вигляді прямокутника, а різні її підмножини – у виглядів кругів чи інших фігур всередині цього прямокутника. Наприклад, на даному рисунку зображено універсальну множину E та її підмножини A, B і C, причому $C \subset B$.



1.1.6. Операції над множинами та їхні властивості

Для множин можна ввести ряд операцій (теоретико-множинних операцій), результатом виконання яких будуть також множини. За допомогою цих операцій можна конструювати із заданих множин нові множини.

Нехай A і B – деякі множини.

1.1.6.1. Означення 1.1.4. ***Об'єднанням*** множин A і B (позначають $A \cup B$) називають множину тих елементів, які належать хоча б одній з множин A чи B. Символічно операція об'єднання множин записується так

$$A \cup B = \{x \mid x \in A \text{ або } x \in B\} \text{ або } x \in A \cup B \Leftrightarrow \begin{bmatrix} x \in A, \\ x \in B \end{bmatrix}.$$

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

Властивості об′єднання множин:

1) комутативність: $A \cup B = B \cup A$;
2) асоціативність: $(A \cup B) \cup C = A \cup (B \cup C)$;
3) ідемпотентність $A \cup A = A$;
4) $A \cup \varnothing = A$;
5) $A \cup E = E$.

1.1.6.2. Означення 1.1.5. ***Перетином (перерізом)*** множин A і B (позначають $A \cap B$) називають множину, що складається з тих і тільки тих елементів, які належать множинам A і B одночасно. Тобто

$$A \cap B = \{x \mid x \in A \text{ і } x \in B\} \text{ або } x \in A \cap B \Leftrightarrow \begin{cases} x \in A, \\ x \in B \end{cases}.$$

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

Кажуть, що множини A і B ***не перетинаються***, якщо $A \cap B = \varnothing$.

Операції об'єднання та перетину множин можуть бути поширені на випадок довільної сукупності множин $\{A_i \mid i \in \mathbb{N}\}$. Так об'єднання множин A_i (записується $\bigcup_{i \in I} A_i$) складається з тих елементів, які належать хоча б одній з множин A_i даної сукупності. А перетин множин A (записується $\bigcap_{i \in I} A_i$) містить тільки ті елементи, які одночасно належать кожній з множин A_i.

Властивості перерізу множин:

1) комутативність: $A \cap B = B \cap A$;
2) асоціативність: $(A \cap B) \cap C = A \cap (B \cap C)$;
3) дистрибутивність операції $\cap$ відносно операції $\cup$: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
4) дистрибутивність операції $\cup$ відносно операції $\cap$: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
5) ідемподентність: $A \cap A = A$;
6) $A \cap \varnothing = \varnothing$;
7) $A \cap E = A$;
8) $A \cap (A \cup B) = A$;
9) $A \cup (A \cap B) = A$.

} закони поглинання

1.1.6.3. Означення 1.1.6. ***Різницею*** множин A і B (записується $A \setminus B$) називають множину тих елементів, які належать множині A і не належать множині B. Отже,

$$A \setminus B = \{x \mid x \in A \text{ і } x \notin B\} \text{ або } x \in A \setminus B \Leftrightarrow \begin{cases} x \in A, \\ x \notin B \end{cases}.$$

Наприклад, $\{a,b,c\} \setminus \{a,d,c\} = \{b\}$,
$\mathbb{Z} \setminus \mathbb{Z}_+ = \mathbb{Z}_-$,
$\{a,b\} \setminus \{a,b,c,d\} = \varnothing$.

Властивості різниці множин:

1) $A \setminus A = \varnothing$;
2) $A \setminus \varnothing = A$;
3) $A \setminus E = \square$;
4) $A \setminus B \neq B \setminus A$ – різниця не комутативна;

5) $(A \setminus B) \setminus C \neq A \setminus (B \setminus C)$ – різниця не асоціативна;
6) $(B \cup C) \setminus A = (B \setminus A) \cup (C \setminus A)$ – правий закон дистрибутивності операції \ відносно операції □ ;
7) $(B \cap C) \setminus A = (B \setminus A) \cap (C \setminus A)$ – правий закон дистрибутивності операції \ відносно операції ∩.

1.1.6.4. Означення 1.1.7. ***Симетричною різницею*** множин A і B (записують $A\Delta B$, $A\oplus B$ або $A\div B$) називають множину, що складається з усіх елементів множини A, які не містяться в B, а також усіх елементів множини B, які не містяться в A. Тобто

$$A\oplus B = \{\, x \mid (\, x\in A \text{ і } x\notin B\,) \text{ або } (\, x\in B \text{ і } x\notin A\,)\} \text{ або } x\in A\oplus B \;\Leftrightarrow\; \left[\begin{array}{l} \begin{cases} x \in A, \\ x \notin B \end{cases} \\ \begin{cases} x \notin A, \\ x \in B \end{cases} \end{array}\right. .$$

Наприклад, $\{a,b,c\}\oplus\{a,c,d,e\} = \{b,d,e\}$,
$\{a,b\}\oplus \{a,b\} = \varnothing$.

Властивості симетричної різниці:
1) комутативність: $A\oplus B = B\oplus A$;
2) асоціативність: $(A\oplus B)\oplus C = A\oplus(B\oplus C)$;
3) дистрибутивність операції ∩ відносно операції ⊕: $A\cap(B\oplus C)=(A\cap B)\oplus(A\cap C)$;
4) $A\oplus A = \varnothing$;
5) $A\oplus\varnothing = A$;
6) $A\oplus B = (A \setminus B) \cup (B \setminus A)$.

Введені теоретико-множинні операції можна проілюструвати діаграмою (рис.1.1).

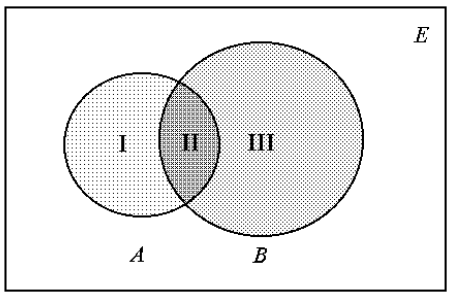


Рис. 1.1.

Тут множини A і B – це множини точок двох кругів.
Тоді $A\cup B$ – складається з точок областей I, II, III,
$A\cap B$ – це область II,
$A \setminus B$ – область I,
$B \setminus A$ – область III,
$A\oplus B$ – області I і III.

1.1.6.5. Означення 1.1.8. Якщо зафіксована універсальна множина E, то ***доповненням*** множини A (яке є підмножиною універсальної множини E) називають множину всіх елементів універсальної множини, які не належать множині A. Записують $\overline{A}$.

Тобто

$$\overline{A} = \{\, x \mid x\in E \text{ і } x\notin A\,\} \text{ або } x\in \overline{A} \;\Leftrightarrow\; x\notin A.$$

Неважко помітити, що $\overline{A} = E \setminus A$.

Наприклад, якщо за універсальну множину прийняти множину N всіх натуральних чисел, то доповненням $\overline{P}$ множини P всіх парних натуральних чисел буде множина всіх непарних натуральних чисел.

Властивості доповнення:

1) $A \cup \overline{A} = E$;
2) $A \cap \overline{A} = \varnothing$;
3) $\overline{E} = \varnothing$;
4) $\overline{\varnothing} = E$;
5) інволютивність: $\overline{\overline{A}} = A$;
6) $\overline{A} \setminus B = A \cap B$;
7) якщо $A=B$, то $\overline{A} = \overline{B}$;
8) якщо $A \subset B$, то $\overline{B} \subset \overline{A}$;
9) правила (закони) де Моргана $\overline{A \cup B} = \overline{A} \cap \overline{B}$; $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Зазначимо, що правила де Моргана припускають узагальнення для сукупності множин:

$$\overline{\bigcup_{i \in \mathbf{N}} A_i} = \bigcap_{i \in \mathbf{N}} \overline{A_i}; \qquad \overline{\bigcap_{i \in \mathbf{N}} A_i} = \bigcup_{i \in \mathbf{N}} \overline{A_i}.$$

Приклад. Покажемо істинність однієї з наведених тотожностей – правила де Моргана.

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

Доведемо спочатку, що $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$.

Нехай елемент $x \in \overline{A \cup B}$, тоді $x \in E \setminus (A \cup B)$, тобто $x \notin A$ і $x \notin B$, звідси $x \in \overline{A}$ і $x \in \overline{B}$, отже, $x \in \overline{A} \cap \overline{B}$. Отже, за означенням підмножин: $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$.

Доведемо обернене включення: $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$.

Припустимо $x \in \overline{A} \cap \overline{B}$, це означає, що $x \in \overline{A}$ і $x \in \overline{B}$, тобто $x \notin A$ і $x \notin B$, тому $x \notin A \cup B$, отже $x \in \overline{A \cup B}$. Зі справедливості обох включень $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$ і $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$ за законом антисиметричності для підмножин випливає істинність рівності $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Твердження доведено. <

Аналогічно можуть бути доведені всі інші наведені теоретико-множинні тотожності. Ці тотожності дають змогу спрощувати різні складні вирази над множинами.

Приклад. $(A \cap B \cap C \cap \overline{D}) \cup (\overline{A} \cap C) \cup (\overline{B} \cap C) \cup (C \cap D) = (A \cap B \cap C \cap \overline{D}) \cup ((\overline{A} \cup \overline{B} \cup D) \cap C) =$
$= ((A \cap B \cap \overline{D}) \cup (\overline{A \cap B \cap \overline{D}})) \cap C = E \cap C = C.$ <

1.1.7. Потужність множин

Усі введені вище теоретико-множинні операції та їхні властивості мають місце як для скінченних, так і для нескінченних множин. Суттєва різниця між скінченними та нескінченними множинами виявляється, коли мова заходить про “кількість елементів” та при спробі порівняти такі множини за “кількістю елементів”. Тут слова “кількість елементів” беруться в лапки тому, що зрозуміла умовність та невизначеність цього поняття для нескінченних множин.

Одними з 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 ґрунтується на такому спостереженні: для того щоб порівняти за кількістю елементів дві скінченні множини, зовсім необов’язково перелічувати елементи кожної з них. Можна діяти таким чином. Наприклад, необхідно порівняти за кількістю дві множини – множину S студентів та множину M всіх місць в аудиторіях. Запропонуємо кожному студенту 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. У протилежному 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 виявляється взаємно однозначною, тоді коли у другому і третьому випадках умови взаємної однозначності не виконуються: або порушується умова ***повної визначеності***

(принаймні один студент не дістав місця), або порушується умова ***сюр'єктивності*** (хоча б одне місце залишилося вільним).

Кількість елементів множини A прийнято позначати через $|A|$.

Отже, неважко переконатися, що між двома скінченними множинами A і B існує взаємно однозначна відповідність тоді і тільки тоді, коли $|A|=|B|$.

Сформульоване твердження дозволяє розв'язувати задачу обчислення кількості елементів множини A шляхом встановлення взаємно однозначної відповідності між множиною A і деякою множиною B, кількість елементів якої відома або легко може бути визначена.

Означення 1.1.9. Елементи двох множин A і B перебувають у ***взаємно однозначній*** відповідності, якщо кожному елементу $a \in A$ відповідає єдиний елемент $b \in B$ і, навпаки, кожен елемент $b \in B$ є зіставленим єдиному елементу $a \in A$.

Множини A і B назвемо ***еквівалентними*** або ***рівнопотужними***, якщо існує взаємно однозначна відповідність між множинами A і B.

Якщо еквівалентність множин A і B позначити через $A\sim B$, то безпосередньо з означення випливають такі властивості еквівалентності:

- $A\sim A$ (рефлексивність);
- Якщо $A\sim B$, то $B\sim A$ (симетричність);
- Якщо $A\sim B$ і $B\sim C$, то $A\sim C$ (транзитивність).

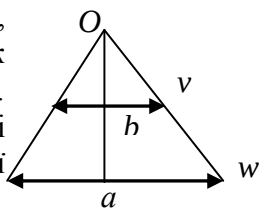
Наведемо декілька *прикладів* еквівалентних нескінченних множин.

1) Множина натуральних чисел $\mathbb{N}$ еквівалентна множині квадратів натуральних чисел $\mathbb{N}^2=\{1,4,9,16,...\}$. Взаємно однозначна відповідність встановлюється за законом: кожне натуральне число має єдиний квадрат, і навпаки, кожен елемент множини $\mathbb{N}^2$ має єдиний корінь у множині $\mathbb{N}$, тобто (n,n^2), $n\in\mathbb{N}$, $n^2\in\mathbb{N}^2$.

2) Множина $\mathbb{Z}$ всіх цілих чисел еквівалентна множині $\mathbb{P}$ всіх парних чисел. Тут взаємно однозначна відповідність встановлюється так: $(n,2n)$, $n\in\mathbb{Z}$, $2n\in\mathbb{P}$.

3) Множина точок інтервалу $(-\pi/2, \pi/2)$ еквівалентна множині точок дійсної прямої. Шукана взаємно однозначна відповідність встановлюється за допомогою тригонометричної функції tg: $(x,\operatorname{tg} x)$, $x\in(-\pi/2, \pi/2)$, $\operatorname{tg} x\in(-\infty,\infty)$.

4) Множини точок двох довільних відрізків a і b еквівалентні. Правило, за яким встановлюється взаємно однозначна відповідність між точками відрізків a і b різної довжини, зображено на рисунку. Кожний промінь з точки O, який перетинає відрізки a і b в точках v і w, утворює одну пару (v,w) необхідної взаємно однозначної відповідності.



Множина A еквівалентна множині $\mathbb{N}$ натуральних чисел називається ***зліченною*** множиною.

Іншими словами, зліченна множина A – це така множина, всі елементи якої можна занумерувати числами 1,2,3,..., тобто можна вказати спосіб, за яким першому елементу множини A ставиться у відповідність число 1, другому – число 2, третьому – число 3 і т.д. Отже, будь-яку зліченну множину A можна подати у вигляді

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

Неважко переконатись, що множини квадратів натуральних чисел, усіх парних чисел, усіх непарних чисел, чисел кратних деякому числу k, чисел, які закінчуються парою цифр 00 тощо є зліченними множинами.

Теорема Кантора. Множина всіх дійсних чисел з інтервалу (0,1) незліченна.

Будь-яка множину, еквівалентну множині всіх дійсних чисел з інтервалу (0,1), називають ***континуальною***, або множиною ***потужності континуум***.

Тема 1.2. ВІДНОШЕННЯ У МНОЖИНАХ

1.2.1. Поняття впорядкованої пари

Нехай $A=\{1, 2\}$ і $B=\{2, 1\}$ – множини. Оскільки вони містять однакові елементи, то $A = B$. При цьому порядок розміщення їх елементів до уваги не береться.

Проте, коли ми говоримо про точки $A(1; 2)$ і $B(2; 1)$, то порядок запису їхніх координат має принципове значення. Точки *A* і *B* не рівні.

Коли порядок розміщення елементів у множині відіграє важливу роль, то говорять про впорядковану сукупність елементів.

Означення 1.2.1. ***Впорядкована n-ка*** – це сукупність *n* не обов'язково різних об'єктів із заданим порядком їх розташування.

Якщо $n = 2$, то говорять про впорядковану пару, при $n = 3$.

Впорядковану пару елементів позначують $\langle a,b\rangle$ або (a,b).

За допомогою поняття множини впорядковану пару означують так:

$$\langle a,b\rangle = \{\{a\},\{a,b\}\}.$$

Може статися, що впорядкована пара має однакові елементи:

$$\langle a,a\rangle = \{\{a\},\{a,a\}\} = \{\{a\}\}.$$

Теорема 1.2.1. Рівність $\langle a,b\rangle = \langle c,d\rangle$ справджується тоді і тільки тоді, коли $a = c$ і $b = d$.

Оскільки елементи *a* і *b* впорядкованої пари $\gamma = \langle a,b\rangle$ – нерівноправні, то елемент a називають ***першою (лівою) координатою (проекцією, компонентою)***, а b – ***другою (правою) координатою (проекцією, компонентою)*** цієї пари.

Використовуючи поняття впорядкованої пари можна означити впорядковану трійку:

$$\langle a,b,c\rangle := \langle\langle a,b\rangle,c\rangle.$$

У літературі впорядковані *n*-ки, зокрема пари, трійки, іноді називають ***n-вимірними*** (відповідно, двовимірними, тривимірними) ***векторами*** або ***кортежами***.

1.2.2. Декартовий (прямий) добуток множин

Окремо розглянемо ще одну дуже важливу операцію над множинами.

Означення 1.2.2. ***Декартовим*** (***прямим***) ***добутком*** множин *A* і *B* (записується $A\times B$) називають множину всіх пар $\langle a,b\rangle$, в яких перша компонента належить множині *A* ($a\in A$), а друга – множині *B* ($b\in B$).

Тобто

$$A\times B = \{\langle a,b\rangle \mid a\in A \text{ і } b\in B\} \text{ або } \langle a,b\rangle \in A\times B \Leftrightarrow \begin{cases} a\in A, \\ b\in B. \end{cases}$$

Декартовий добуток природно узагальнюється на випадок довільної сукупності множин. Якщо $A_1, A_2,..., A_n$ – множини, то їхнім декартовим добутком називають множину

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

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

Як зазначалося, набір $\langle a_1,a_2,...,a_n\rangle$, щоб відрізнити його від множини, яка складається з елементів $a_1,a_2,...,a_n$, записують не у фігурних, а в круглих дужках і називають ***кортежем***, ***вектором*** або ***впорядкованим набором***. ***Довжиною*** кортежу називають кількість його координат. Два кортежі $\langle a_1,a_2,...,a_n\rangle$ і $\langle b_1,b_2,...,b_n\rangle$ однакової довжини вважаються ***рівними*** тоді і тільки тоді, коли рівні їхні відповідні координати, тобто $a_i=b_i$, i=1,2,...,*n*.

Декартовий добуток множини *A* на себе *n* разів, тобто множину $A\times A\times...\times A$ називають ***n-м декартовим*** (або ***прямим***) ***степенем*** множини *A* і позначають A^n.

Прийнято вважати, що $A^0 = \varnothing$ (n=0) і $A^1 = A$ (n=1).

Наприклад, якщо $A = \{a,b\}$ і $B = \{b,c,d\}$, то
$A\times B = \{(a,b),(a,c),(a,d),(b,b),(b,c),(b,d)\}$,
$A^2 = \{(a,a),(a,b),(b,a),(b,b)\}$.

Якщо R – множина дійсних чисел або множина точок координатної прямої, то R^2 – це множина пар (a,b), де $a,b\in R$, або множина точок координатної площини.

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

Операція декартового добутку неасоціативна і не комутативна, тобто множини $(A\times B)\times C$ і $A\times(B\times C)$, а також множини $A\times B$ і $B\times A$, у загальному випадку, не рівні між собою.

Зв'язок декартового добутку з іншими теоретико-множинними операціями встановлюється такими тотожностями:

1. $(A \cup B) \times C = (A\times C) \cup (B\times C)$,
2. $(A\cap B) \times C = (A\times C)\cap(B\times C)$,
3. $A \times (B \cup C) =(A\times B) \cup (A\times C)$,
4. $A \times (B\cap C) =(A\times B)\cap(A\times C)$.

1.2.3. Бінарні відношення

Означення 1.2.3. Підмножина R декартового степеня M^n деякої множини M називається ***n-місним*** або ***n-арним відношенням*** на множині M. Кажуть, що елементи $a_1,a_2,...,a_n\in M$ знаходяться у відношенні R, якщо $\langle a_1,a_2,...,a_n\rangle\in R$.

При $n=1$ відношення $R\subseteq M$ називають ***одномісним*** або ***унарним***. Таке відношення часто називають також *ознакою* або *характеристичною властивістю* елементів множини M. Кажуть, що елемент $a\in M$ має ознаку R, якщо $a\in R$ і $R\subseteq M$. Наприклад, ознаки "парність" і "кратність 3" виділяють із множини N натуральних чисел унарні відношення $R' = \{2k \mid k\in N\}$ і $R'' = \{3k \mid k\in N\}$, відповідно.

Найбільш популярними в математиці є ***двомісні*** або ***бінарні*** відношення ($n=2$), на вивченні властивостей яких ми зупинимось детальніше. Далі скрізь під словом "відношення" розумітимемо бінарне відношення. Якщо елементи $a,b\in M$ знаходяться у відношенні R (тобто $\langle a,b\rangle\in R$), то це часто записують у вигляді aRb. Зауважимо, що бінарні відношення іноді розглядають, як окремий випадок відповідностей, а саме – відповідності між однаковими множинами.

Наприклад, на різних множинах можна задати такі бінарні відношення.

1. Відношення на множині N натуральних чисел:
   R_1 - відношення "менше або дорівнює", тоді $7R_19$, $2R_12$, $1R_1m$ для будь-якого $m\in\mathbb{N}$;
   R_2 - відношення "ділиться на", тоді $12R_23$, $49R_27$, mR_21 для будь-якого $m\in N$;
   R_3 - відношення "складаються з однакових цифр", тоді $107R_3701$, $123R_33213311$.
2. Відношення на множині точок координатної площини R^2:
   R_4 - відношення "знаходяться на однаковій відстані від початку координат", тоді $(3,2)\ R_4\ (\sqrt{5},-\sqrt{8})$, $(0,0)R_4(0,0)$;
   R_5 - відношення "симетричні відносно осі ординат", тоді $(1,7)R_5(-1,7)$, а в загальному випадку $(a,b)R_5(-a,b)$ для будь-яких $a,b\in R$;
   R_6 - відношення "менше або дорівнює". Вважаємо, що $(a,b)R_6(c,d)$, якщо $a \le c$ і $b \le d$. Зокрема, $(1,7)R_6(20,14)$, $(-12,4)R_6(0,17)$.
3. Відношення на множині людей:
   R_7 - відношення "є другом",
   R_8 - відношення "є молодшим за віком від".

Слід звернути увагу на такі основні моменти:

- розглядуване відношення має місце не для всіх пар елементів заданих множин, а лише для деяких з них;
- не завжди якщо елемент x перебуває у відношенні з елементом y, то елемент y перебуває у тому самому відношенні з елементом x;

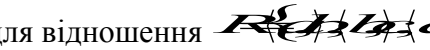
– кожне відношення між елементами даної множини можна розглядати як сукупність деяких впорядкованих пар декартового добутку двох однакових або різних множин.

Позначимо символом R_- сукупність лівих координат впорядкованих пар бінарного відношення R, тобто:

Множину R_- називають ***лівою областю*** або ***областю визначення*** відношення R.

Аналогічно множину

називають ***правою областю*** або ***множиною значень*** відношення R.

Наприклад, для відношення  , $R_- = \{a,b,c\}$, а $R_+ = \{a,b,c,d\}$.

Множину $F(R) = R_- \cup R_+$ називають ***полем*** відношення R. Для розглянутого прикладу $F(R) = \{a,b,c,d\}$.

Якщо будь-який елемент заданої множини перебуває у відношенні з будь-яким елементом цієї множини, то таке відношення називають ***універсальним***. Якщо ж жоден елемент заданої множини не перебуває у відношенні з жодним елементом цієї множини, то таке відношення називають ***порожнім***.

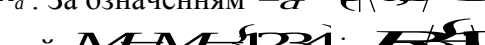
Відношення $\Delta = \{\langle a,a\rangle \mid a \in M\}$ називають ***діагональним*** або ***одиничним***.

1.2.4. Переріз відношення. Фактор-множина

Нехай R – деяке відношення у множині $M_1 \times M_2$ ($R \subset M_1 \times M_2$) і $a \in M_1$.

Означення 1.2.4. Сукупність всіх таких елементів $b \in M_2$, для яких $\langle a,b\rangle \in R$, називають ***перерізом*** відношення R за елементом a.

Позначують R_a. За означенням $R_a = \{b \mid \langle a,b\rangle \in R\}$.

Наприклад, нехай $M_1 = M_2 = \{1,2,3,4\}$ і  . Тоді:

$$R_1 = \{2,3\},\ R_2 = \{1,2,3,4\},\ R_3 = \{4\},\ R_4 = \varnothing.$$

Означення 1.2.5. Сукупність всіх перерізів відношення R за елементами множини M_1 називають ***фактором*** або ***фактор-множиною*** множини M_2 і позначають M_2 / R.

Отже, $M_2 / R = \{R_a \mid a \in M_1\}$.

Для розглянутого прикладу  .

Оскільки за означенням елементами буліана $\beta(M_2)$ є підмножини множини M_2, то довільна фактор-множина M_2 / R є підмножиною цього булана: $M_2 / R \subset \beta(M_2)$.

Нехай R – деяке відношення у множині $M_1 \times M_2$ ($R \subset M_1 \times M_2$) і $M_1' \subset M_1$.

Означення 1.2.6. ***Перерізом*** відношення R за множиною M_1' називають об'єднання всіх перерізів відношення R за елементами множини M_1', тобто

$$R_{M_1'} = \bigcup_{a \in M_1'} R_a.$$

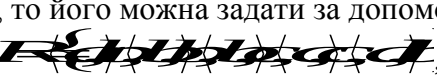
Якщо у розглянутому прикладі покласти $M_1' = \{2,3\}$, то

 .

Якщо $M_1' = R_-$, то $R_{M_1'} = R_+$.

1.2.5. Способи задання відношень

1. Множинний спосіб. Оскільки відношення є множиною, елементами якої є впорядковані пари, то його можна задати за допомогою способів задання множин.

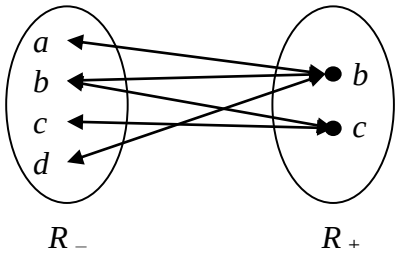
Наприклад,  ,

 .

2. Стрілочний спосіб. Елементи області визначення і множини значень відношення зображують точками площини напроти одна від одної, а впорядковані пари зображують стрілками, спрямованими від відповідних точок області визначення до точок множини значень.

Наприклад, задамо стрілочним способом відношення R, задане вище множинним способом. Спочатку знайдемо його область визначення і множину значень:

$$R_- = \{a,b,c,d\},\ R_+ = \{b,c\}.$$



3. Табличний спосіб. Таблиця відношення складається з двох рядків і стількох стовпців, скільки елементів в області визначення. Під кожним елементом області визначення записують переріз відношення за цим елементом.

Наприклад, задамо стрілочним способом згадане відношення R.

a	b	c	d
$\{b\}$	$\{b,c\}$	$\{c\}$	$\{b\}$

4. Матричний спосіб. Матриця відношення має стільки рядків, скільки елементів у області визначення, і стільки стовпців, скільки елементів у множині значень. Елементами матриці відношення є:

$$q_{ij} = \begin{cases} 1, \text{ якщо } \langle i,j \rangle \in R, \\ 0, \text{ якщо } \langle i,j \rangle \notin R. \end{cases}$$

Наприклад, задамо матричним способом побудоване раніше відношення R.

$$R = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{cc} b & c \end{array} \\ \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix} \end{array}$$

Для діагонального, універсального та порожнього відношень у множині $M = \{a_1, a_2, a_3\}$ матриці матимуть вигляд:

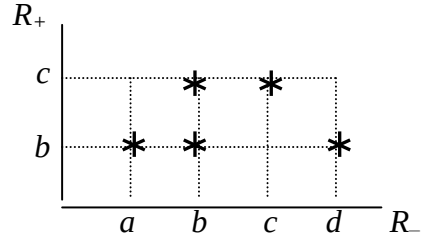
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

5. Графічний спосіб. Цей спосіб передбачає побудову ***графіка*** та ***графа*** відношення.

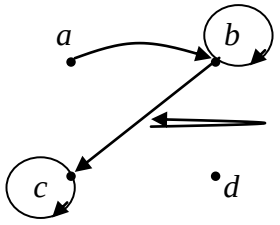
Для побудови графіка у першому координатному куті на горизонтальній осі відкладають точками елементи області визначення, а на вертикальній – точки множини значень. Кожну впорядковану пару зображують точкою або зірочкою у цьому координатному куті (отримані точки не сполучають!).

Для побудови графа відношення елементи поля цього відношення зображують точками довільно на площині. Кожну впорядковану пару зображують дугою, спрямованою від точки області визначення до точки множини значень.

Наприклад, зобразимо графічно розглядуване відношення R, знайшовши його поле: $\mathrm{Dom}R=\{a;b;c\}$.



Графік



Граф

Тема 1.3. ВЛАСТИВОСТІ ВІДНОШЕНЬ

1.3.1. Теоретико-множинні операції над відношеннями

Оскільки відношення є множинами, елементами яких є впорядковані пари, то над ними можна виконувати всі відомі операції над множинами.

Наприклад, якщо $P=\{\langle a;b\rangle;\langle a;c\rangle\}$, а $Q=\{\langle b;a\rangle;\langle c;a\rangle\}$, то

$R=\{\langle a;b\rangle;\langle b;a\rangle;\langle b;c\rangle;\langle c;a\rangle\}$;

$PQ=\{\langle b;c\rangle\}$;

$PQ=\{\langle a;c\rangle;\langle b;a\rangle\}$;

$P\setminus Q=\{\langle a;b\rangle;\langle a;c\rangle\}$.

Якщо відношення “менше”, “більше”, “дорівнює” тощо записати значками для їх позначення у дужках, то операції над цими відношеннями матимуть вигляд:

$$(<)\cup(=)=(\le),\quad (<)\cap(=)=\varnothing,\quad (\le)\setminus(<)=(=).$$

Якщо для двох відношень R і S виконується умова $R\subset S$, то S називають ***розширенням*** відношення R, а R – ***звуженням*** відношення S.

Наприклад, $(\le)$ – розширення відношень $(<)$ і $(=)$, бо $(<)\subset(\le)$ і $(=)\subset(\le)$.

1.3.2. Композиція відношень

Крім теоретико-множинних операцій над відношеннями можна виконувати й інші операції. Однією з них є композиція.

Означення 1.3.1. ***Композицією*** відношень R і S називають множину всіх таких впорядкованих пар $\langle a,b\rangle$, для кожної з яких існує деякий елемент c такий, що $\langle a,c\rangle\in R$, $\langle c,b\rangle\in S$.

Позначають композицію $R\circ S$. Отже, за означенням:

$$R\circ S=\{\langle x;y\rangle\mid\ldots\}.$$

Наприклад, якщо $P=\{\langle a;b\rangle;\langle a;c\rangle\}$, а $Q=\{\langle b;a\rangle;\langle c;a\rangle\}$, то

$$P\circ Q=\{\langle a;a\rangle;\langle a;a\rangle\},$$

$$Q\circ P=\{\langle b;b\rangle;\langle b;c\rangle;\langle c;b\rangle;\langle c;c\rangle\}.$$

Приклад свідчить, що композиція відношень, у загальному випадку, – операція не комутативна, тобто $R\circ S\neq S\circ R$. Однак, композиція має такі властивості:

1) асоціативність: $(R\circ S)\circ T=R\circ(S\circ T)$;
2) дистрибутивність $\circ$ відносно $\cup$: $(R\cup S)\circ T=(R\circ T)\cup(S\circ T)$.

1.3.3. Обернені відношення

Означення 1.3.2. Відношення R^{-1}, задане на множині $M_2 \times M_1$, називають ***оберненим (інверсним)*** до відношення R, заданого на $M_1 \times M_2$, якщо

$$R^{-1} = \{\langle b,a\rangle \mid \langle a,b\rangle \in R\}.$$

Означення 1.3.3. ***Інверсією*** називають операцію, яка довільному відношенню R ставить у відповідність відношення R^{-1}.

З означення видно, що область визначення R_- відношення R є множиною значень $R^{-1}{}_+$ для відношення R^{-1}, і навпаки.

Геометричне зображення інверсії R^{-1} графіка R легко утворити за допомогою перетворення симетрії координатної площини відносно бісектриси першого координатного кута. При цьому вісь абсцис і вісь ординат міняються місцями, а точка $\langle x, y\rangle$ переходить у точку $\langle y, x\rangle$.

Зрозуміло, що у випадку універсального, діагонального та порожнього відношень:

$$E^{-1} = E; \quad \Delta^{-1} = \Delta; \quad \varnothing^{-1} = \varnothing.$$

Властивості обернених відношень:

1) $\left(R^{-1}\right)^{-1} = R$;
2) якщо $R \subset S$, то $R^{-1} \subset S^{-1}$;
3) $\overline{R}^{-1} = \overline{R^{-1}}$;
4) $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$;
5) $(R \cup S)^{-1} = S^{-1} \cup R^{-1}$.

1.3.4. Рефлексивні, симетричні і транзитивні відношення

Означення 1.3.4. Бінарне відношення *R* називають ***рефлексивним*** у множині $A = F(R)$, якщо будь-який елемент $a \in F(R)$ перебуває у відношенні сам з собою ($\langle a,a\rangle \in R$).

Означення 1.3.5. Бінарне відношення *R* називають ***рефлексивним***, якщо з того, що $\langle a,b\rangle \in R$ слідує, що $\langle a,a\rangle \in R$ і $\langle b,b\rangle \in R$.

Наприклад, відношення $R = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 2,3\rangle\}$ рефлексивне у множині $A = \{1,2,3\}$, проте не рефлексивне у множині $A = \{1,2,3,4\}$.

Рефлексивними є відношення рівності, подільності, паралельності, конгруентності, подібності фігур, універсальне та діагональне відношення.

Означення 1.3.6. Бінарне відношення *R* називають ***антирефлексивним (іррефлексивним)*** у множині $A = F(R)$, якщо жоден елемент $a \in F(R)$ не перебуває у відношенні сам з собою ($\langle a,a\rangle \notin R$).

Наприклад, відношення $S = \{\langle 1,2\rangle, \langle 1,3\rangle, \langle 2,3\rangle\}$ антирефлексивне у множині $A = \{1,2,3\}$. Анти рефлексивними є відношення “не дорівнює”, “менше”, “більше”, перпендикулярності тощо.

Порожнє відношення прийнято вважати як рефлексивним, так і антирефлексивним.

Якщо відношення є ні рефлексивним, ні анти рефлексивним, то його називають ***не рефлексивним***.

Наприклад, відношення $P = \{\langle 1,1\rangle, \langle 1,3\rangle, \langle 2,1\rangle, \langle 3,3\rangle\}$ не рефлексивне, оскільки елемент *2*, на відміну від всіх інших, не перебуває у відношенні сам з собою $(\langle 2,2\rangle \notin P)$.

При зображенні рефлексивного відношення з допомогою графіка видно, що всі точки діагоналі $A \times A$ належать графіку відношення.

Означення 1.3.7. Бінарне відношення R називають ***симетричним***, якщо з того, що $\langle a,b\rangle \in R$ слідує, що $\langle b,a\rangle \in R$.

Наприклад, відношення $R=\{\langle 1,1\rangle,\langle 2,3\rangle,\langle 3,2\rangle\}$ симетричне. Симетричними є відношення паралельності, перпендикулярності, подібності, конгруентності, універсальне відношення тощо.

Для симетричного відношення його графік симетричний відносно діагоналі – бісектриси координатного кута.

Означення 1.3.8. Бінарне відношення R називають ***антисиметричним***, якщо з того, що $\langle a,b\rangle \in R$ слідує, що $\langle b,a\rangle \notin R$.

Наприклад, відношення $S=\{\langle 1,2\rangle,\langle 2,3\rangle,\langle 3,4\rangle\}$ антисиметричне. Антисиметричними є відношення включення, "менше", "більше", "менше дорівнює" тощо.

Відношення рівності, діагональне та порожнє вважають як симетричними, так і антисиметричними.

Означення 1.3.9. Бінарне відношення R називають ***транзитивним***, якщо з того, що $\langle a,b\rangle \in R$ і $\langle b,c\rangle \in R$ слідує, що $\langle a,c\rangle \in R$.

Наприклад, відношення $R=\{\langle 1,2\rangle,\langle 1,3\rangle,\langle 2,3\rangle,\langle 2,4\rangle\}$ транзитивне. Транзитивними також є відношення "менше", "більше дорівнює", подільності, паралельності, подібності, включення, діагональне, порожнє та універсальне відношення тощо.

Не транзитивними є відношення "не дорівнює", перпендикулярності, належності тощо.

Графік транзитивного відношення має властивість $R\circ R\subseteq R$ і навпаки.

Операція обернення зберігає 5 властивостей відношень: рефлективність, антирефлексивність, симетричність, антисиметричність і транзитивність.

Означення 1.3.10. Відношення R^* називають ***транзитивним замиканням*** відношення R на множині A, якщо $\langle a,b\rangle \in R^*$ тоді і тільки тоді, коли у множині A існує послідовність елементів $a_1,a_2,\ldots a_n$ така, що $a_1=a$, $a_n=b$ і $\langle a_1,a_2\rangle \in R$, $\langle a_2,a_3\rangle \in R$, ..., $\langle a_{n-1},a_n\rangle \in R$.

1.3.5. Відношення еквівалентності

Означення 1.3.11. Бінарне відношення R називають ***відношенням еквівалентності***, коли воно рефлексивне, симетричне і транзитивне.

Отже, R є відношенням еквівалентності, якщо:

1) $\langle a,a\rangle \in R$;
2) $\langle a,b\rangle \in R \Rightarrow \langle b,a\rangle \in R$;
3) $\langle a,b\rangle \in R \wedge \langle b,c\rangle \in R \Rightarrow \langle a,c\rangle \in R$.

Якщо при цьому $A=F(R)$, то говорять, що R – відношення еквівалентності на множині A.

Наприклад, відношення $R=\{\langle 1,1\rangle,\langle 2,2\rangle\}$ є відношенням еквівалентності.

Відношеннями еквівалентності є також відношення рівності, рівно потужності множин, конгруентності, подібності, діагональне, порожнє та універсальне відношення.

Важливу роль відіграє в математиці відношення "мають однакову остачу при діленні на k" або "конгруентні за модулем k", яке є відношенням еквівалентності на множині $\mathbb{N}$ натуральних чисел для будь-якого фіксованого $k\in\mathbb{N}$. *Відношення конгруентності* за модулем k часто позначають $a \equiv b \pmod k$. Цьому відношенню належать, наприклад, пари натуральних чисел (17,22), (1221,6), (42,57) для k=5, тобто $17 \equiv 22 \pmod 5$, $1221 \equiv 6 \pmod 5$, $42 \equiv 57 \pmod 5$.

Нехай $R(R\subseteq A\times A)$ – відношення еквівалентності і $a \in A$.

Означення 1.3.12. Переріз R_a відношення R за елементом a називають класом еквівалентності за відношенням R і позначають $[a]$ або $[a]_R$.

Отже, за означенням $[a]_R=\{x\in A \mid \langle x,a\rangle\in R\}$. Тобто клас еквівалентності $[a]$ містить всі такі елементи множини A, які перебувають у відношенні R з елементом a.

Наприклад, якщо R – відношення паралельності у площині α, а l – деяка фіксована пряма у цій площині, то клас еквівалентності $[l]$ містить усі прямі площини α, паралельні прямій l.

Теорема 1.3.1. Будь-які два класи еквівалентності за відношенням R або не мають спільних елементів, або збігаються.

Теорема 1.3.2. Будь-яку множину A, в якій задано відношення еквівалентності R, можна подати у вигляді об'єднання різних класів еквівалентності за відношенням R, тобто $A=\bigcup_{a\in A}[a]$.

Означення 1.3.13. Множину всіх класів еквівалентності за відношенням R називають ***фактор-множиною*** множини A за відношенням R: $A/R=\{[a] \mid a\in A\}$ або $A/R=\{[a] \mid a\in M\}$, де M – сукупність таких елементів множини A, яким відповідають різні класи еквівалентності.

Наприклад, якщо A – сукупність всіх студентів певної групи, які отримали за іспит оцінку k, а R – відношення еквівалентності, що визначається умовою $\langle a,b\rangle\in R$ тоді і тільки тоді, коли $a\in A_k$ і $b\in A_k$, то $A/R=\{A_2, A_3, A_4, A_5\}$. Фактор-множина для відношення "конгруентні за модулем 3" на множині $\mathbb{N}$ натуральних чисел складається з трьох класів $\{3k \mid k\in\mathbb{N}\}$, $\{3k\text{-}1 \mid k\in\mathbb{N}\}$ і $\{3k\text{-}2 \mid k\in\mathbb{N}\}$.

Потужність фактор-множини $|A/R|$ називають ***індексом розбиття*** або ***індексом відношення еквівалентності*** R.

Нехай R відношення еквівалентності на множині A. Відображення множини A на фактор-множину A/R, яке кожному елементу $a\in A$ ставить у відповідність клас еквівалентності $[a]_R$, називають ***канонічним*** або ***природним відображенням*** множини A на фактор-множину A/R.

1.3.6. Відношення порядку

Означення 1.3.14. Бінарне відношення R називають ***відношенням строгого порядку***, коли воно антисиметричне і транзитивне. Позначають: $<(>)$ або $<_R$ $(>_R)$.

Отже R – відношення строгого порядку, якщо:

1) $\langle a,b\rangle\in R \Rightarrow \langle b,a\rangle\notin R$;
2) $\langle a,b\rangle\in R \wedge \langle b,c\rangle\in R \Rightarrow \langle a,c\rangle\in R$.

Наприклад, розташування символів у довільному скінченному алфавіті означує відношення ***строгого лексикографічного порядку***, яке лежить в основі впорядкування словників, енциклопедій, індексів, довідників, списків, таблиць тощо.

Означення 1.3.15. Якщо відношення порядку є рефлексивним ($\langle a,a\rangle\in R$), то його називають ***відношенням часткового*** (***нестрогого***) або ***квазіпорядку***. Позначають: $\leq(\geq)$ або $\leq_R$ $(\geq_R)$.

Наприклад, у числових множинах N, Q, R встановлено відношення строгого ($<(>)$) і нестрогого ($\leq(\geq)$) порядку.

Множину M, на якій задано відношення порядку, називають ***впорядкованою***, а елементи $a,b\in M$ – ***порівнюваними*** за відношенням R, якщо виконується $\langle a,b\rangle\in R$ або $\langle b,a\rangle\in R$. Запис $\langle A;\leq\rangle$ означає, що у множині A відношення порядку $\leq$.

Впорядковану множину M, в якій будь-які різні два елементи є порівнюваними між собою, називають ***лінійно впорядкованою*** множиною або ***ланцюгом***. Відповідне відношення

R (як строге, так і нестроге), задане на лінійно впорядкованій множині, називають ***лінійним*** (***досконалим***) ***порядком***.

Очевидно, відношення рівності є відношенням часткового порядку на будь-якій множині M, цей порядок називають ***тривіальним***.

Теорема 1.3.3. Якщо R – відношення строгого (нестрогого) порядку, то обернене відношення R^{-1} – теж відношення строгого (нестрогого) порядку.

Нехай M частково впорядкована множина і A деяка непорожня підмножина множини M.

Означення 1.3.16. ***Верхньою гранню*** підмножини $A \subseteq M$ в множині M називається елемент $b \in M$ такий, що $a \le b$ всіх $a \in A$. Елемент b називається ***найбільшим елементом*** множини M, якщо b – верхня грань множини M. Відповідно, елемент c частково впорядкованої множини M називається ***нижньою гранню*** підмножини $A \subseteq M$, якщо $c \le a$ для будь-якого $a \in A$. Елемент c – ***найменший*** в множині M, якщо c – нижня грань самої множини M.

Означення 1.3.17. Елемент $x \in M$ називається ***максимальним*** в множині M, якщо не існує елемента $a \in M$ такого, що $x < a$. Відповідно, елемент $n \in M$ називається ***мінімальним*** у множині M, якщо не існує елемента $a \in M$ такого, що $a < n$.

1.3.7. Відображення і функції

Означення 1.3.18. Відношення F, задане на множинах $A_1, A_2, \ldots A_n, E$ називають ***функціональним***, якщо для будь-якого елемента $(a_1, a_2, \ldots a_n) \in A_1 \times A_2 \times \ldots \times A_n$ існує не більше одного елемента $b \in B$, такого, що $(a_1, a_2, \ldots a_n, b) \in F$.

Якщо ж деякого $(a_1, a_2, \ldots a_n)$ такий елемент $b \in B$ існує, то його позначають $F(a_1, a_2, \ldots a_n)$ і записують $b = F(a_1, a_2, \ldots a_n)$.

Нехай $F^{-1}(b) = \{(a_1, a_2, \ldots a_n) \mid (a_1, a_2, \ldots a_n, b) \in F\}$. Очевидно, для будь-якого функціонального відношення F, заданого на множині $A_1 \times A_2 \times \ldots \times A_n$ виконується включення $\bigcup_{b \in B} F^{-1}(b) \subseteq A_1 \times A_2 \times \ldots \times A_n$, де $\bigcup_{b \in B} F^{-1}(b)$ – ***область визначення*** відображення. Коли ж $\bigcup_{b \in B} F^{-1}(b) = A_1 \times A_2 \times \ldots \times A_n$, то відношення F називають ***повністю визначеним***, у випадку $\bigcup_{b \in B} F^{-1}(b) \subset A_1 \times A_2 \times \ldots \times A_n$ – ***частково визначеним*** або ***частковим***.

Означення 1.3.19. Відношення F, задане на множинах $A_1, A_2, \ldots A_n, E$ називають ***відображенням*** або ***функцією***, якщо F – функціональне і часткове. Позначують: $F: A_1 \times A_2 \times \ldots \times A_n \to B$.

Число n називають ***арністю*** функції F.

Якщо $F: A_1 \times A_2 \times \ldots \times A_n \to B$ та існує $b \in B$, такий, що $b = F(a_1, a_2, \ldots a_n)$, то елемент b називають ***образом*** елемента $(a_1, a_2, \ldots a_n)$ при відображенні F, а $(a_1, a_2, \ldots a_n)$ – ***прообразом*** елемента b.

Відношення $F: A_1 \times A_2 \times \ldots \times A_n \to B$ називають ***відображенням*** тоді і тільки тоді, коли для довільного $b \in B$: $F^{-1}(b) \neq \varnothing$. Множину всіх таких елементів b називають ***множиною значень*** відображення F.

Відображення F множини $A_1 \times A_2 \times \ldots \times A_n$ на множину B називають ***взаємно однозначним відображенням*** або ***взаємно однозначною відповідністю*** тоді і тільки тоді, коли обернене відношення F^{-1} є відображенням B на $A_1 \times A_2 \times \ldots \times A_n$.

РОЗДІЛ 2. ТЕОРІЯ ГРАФІВ

Тема 2.1. ОСНОВНІ ЕЛЕМЕНТИ ТЕОРІЇ ГРАФІВ

2.1.1. Поняття графа

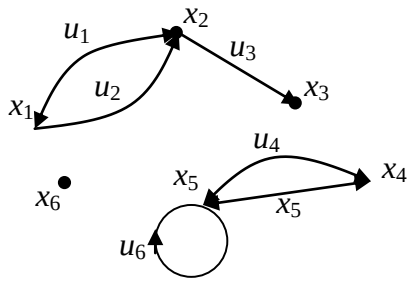
Теорія графів – важливий розділ дискретної математики, який зародився при розв'язанні головоломок та ігор, таких як задача про кенігсбергські мости (1736 р.), задача про три криниці і три будинки, гра Гамільтона, задача про чотири фарби. Зараз ця теорія стала потужним засобом дослідження і розв'язання багатьох задач, які виникають при дослідженні великих і складних систем, зокрема обчислювальних. Одним з основних напрямків її використання в обчислювальній техніці є побудова та опис ефективних алгоритмів і аналіз їх складності.

Теорію графів відносять до ***якісної геометрії*** (яка оперує безрозмірними величинами: одиниці вимірювання ролі не грають, основне – наявність просторових елементів (точок, ліній, поверхонь) і зв'язків між ними).

Основним поняттям є поняття графа.

Означення 2.1.1. ***Графом*** G називають пару об'єктів $G(X,\Gamma)$, де X – скінчена непорожня множина, а Γ – скінчена підмножина прямого добутку $X\times X\times\mathbb{N}$ (можливо і порожня), причому X називають множиною вершин, а Γ – множиною дуг графа G.

Наприклад: $X=\{x_1,x_2,x_3,x_4,x_5,x_6\}$, $\Gamma=\{u_1,u_2,u_3,u_4,u_5,u_6\}$, де $u_1=(x_1,x_2,1)$, $u_2=(x_1,x_2,2)$, $u_3=(x_2,x_3,1)$, $u_4=(x_4,x_5,1)$, $u_5=(x_5,x_4,1)$, $u_6=(x_5,x_5,1)$. У позначенні дуги $u_k=(x_i,x_j,n)$ вершини x_i та x_j, які визначають дугу, називають ***кінцевими*** або ***граничними***, причому перша координата x_i вказує на вихідну вершину дуги u_k, друга координата x_j – на вхідну, а де $n\in\mathbb{N}$ – номер дуги для позначення різних дуг з однаковими вихідними та вхідними вершинами (при цьому не обов'язково використовують номери від 1 до кількості дуг).



Означення 2.1.2. Дві вершини графа називають ***суміжними***, якщо вони є кінцевими для хоча б однієї дуги.

Означення 2.1.3. Дві дуги графа називають ***суміжними***, якщо вони мають принаймні одну спільну вершину.

Зауважимо, що суміжність – відношення між однорідними елементами графа – вершиною і вершиною, дугою і дугою. Для позначення відношення між різнорідними елементами графа вводять поняття "інциденція".

Означення 2.1.4. Дугу $u\in\Gamma$ та вершину $x\in X$ графа $G(X,\Gamma)$ називають ***інцидентними***, якщо ця вершина є початком або кінцем даної дуги (першою або другою проекцією: $x=\mathrm{pr}_1 u$ або $x=\mathrm{pr}_2 u$.

У наведеному прикладі графа вершини x_1 і x_2, x_2 і x_3, x_4 і x_5 – суміжні, а x_1 і x_3, x_3 і x_4, x_5 і x_6 – несуміжні, дуги u_1 і u_2, u_4 і u_6 – суміжні, а u_1 і u_4, u_3 і u_6 – несуміжні, вершина x_1 і дуга u_1 – інцидентні, а вершина x_1 і дуга u_4 – неінцидентні.

Дуги з однаковими кінцевими вершинами називають ***паралельними*** або ***кратними***. У наведеному прикладі ребра u_1 та u_2 – паралельні.

Якщо кінцеві вершини дуги однакові, то її називають ***петлею***. Дуга $u_6=(x_5,x_5,1)$ є петлею.

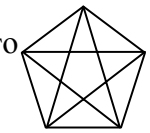
Граф, який не містить петель і паралельних ребер називають ***простим***, у протилежному випадку – ***мультиграфом***.

Граф G є графом порядку n, якщо множина його вершин складається з n елементів: $|X|=n$.

Якщо у графі G вершина x_i не є початком і кінцем жодного ребра, то її називають ***ізольованою***. У прикладі: вершина x_6 – ізольована.

Граф, який складається з ізольованих вершин, тобто не містить жодного ребра, називають ***нуль-графом***, ***порожнім*** або ***виродженим***.

Якщо у графі вершина x_i є початком або кінцем лише одного ребра, то її називають ***висячою*** або ***тупиком***. У прикладі вершина x_3 – висяча.



Якщо граф має n вершин (n>1) і кожна пара вершин з'єднана ребром, то його називають повним.

Граф називають ***плоским***, якщо він має геометричну реалізацію на площині.

Області площини, окреслені ребрами плоского графа, називають його ***гранями***.

Граф $G(X,\Gamma)$ називають ***дводольним***, якщо множину його множин X можна розбити на дві такі підмножини X_1 та X_2, що кожне ребро, яке належить Γ має одну кінцеву вершину у множині X_1, а другу – в X_2.

Рефлективним називають граф, що має петлю у кожній вершині.

Симетричним називають граф, у якому кожній дузі $u=(x_1,x_2)$ відповідає дуга $u'=(x_2,x_1)$.

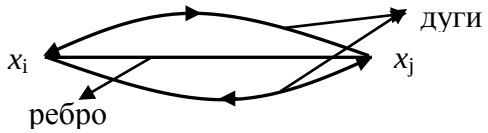
Транзитивним називають граф, у якому існування дуг $u_1=(x_1,x_2)$ і $u_2=(x_2,x_3)$ означає існування дуги $u_3=(x_1,x_3)$.

Граф $G(X,\Gamma)$ називають ***орієнтованим*** або ***орграфом***, якщо розрізняють початкову і кінцеву вершини дуги. Для геометричного зображення використовують стрілки.

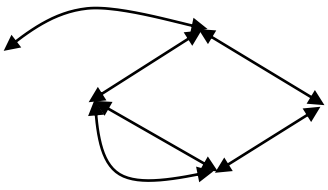
У випадку орієнтованого графа, його ребра називають дугами, заданими впорядкованими парами (трійками):

Тоді, коли зв'язок між вершинами не позначений стрілками, його називають ***ребром*** графа, причому початок x_i і кінець x_j ребра не розрізняють, тобто пара (x_i, x_j) є не впорядкованою.

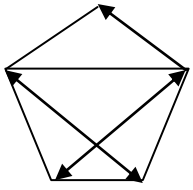
Якщо дуги (x_i,x_j,n) та (x_j,x_i,n) є різними, то ребро – це підмножина виду  , причому номери n – однакові.



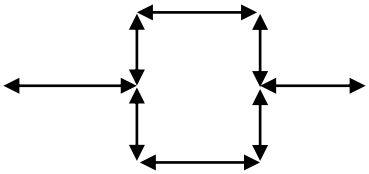
Графи бувають неорієнтованими, орієнтованими та змішаними:



орієнтований



неорієнтований



змішаний

2.1.2. Ізоморфізм графів. Підграф. Суграф. Частковий граф

Нехай $G=(X,\Gamma)$ і $G'=(X',\Gamma')$ – графи і $h:G\to G'$ – взаємно однозначна відповідність.

Означення 2.1.5. Відображення h називають ***ізоморфізмом графів*** G і G', якщо для довільних вершин x_i і x_j графа G їх образи $h(x_i)$ і $h(x_j)$ суміжні у графі G' тоді і тільки тоді, коли x_i і x_j суміжні в G.

Якщо таке відображення існує, то графи G і G' називають ***ізоморфними***. Відношення ізоморфізму графів є відношенням еквівалентності.

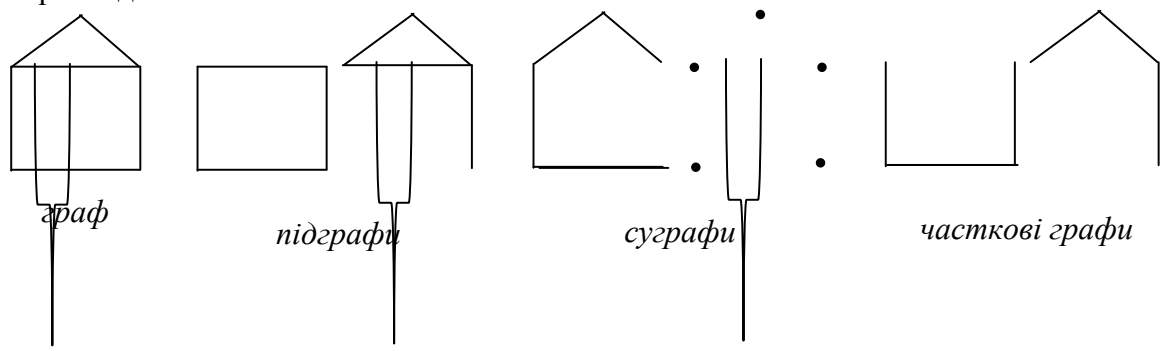
Означення 2.1.6. ***Підграфом*** $G'(X',\Gamma')$ графа $G(X,\Gamma)$ називають граф, у якого $X' \subseteq X$, $\Gamma'=\Gamma \cap (X \times X \cap \mathbb{N})$, тобто ребро (x_i, x_j) міститься в Γ' лише тоді, якщо x_i та x_j містяться в X', граф G називається ***надграфом*** графа G'.

Означення 2.1.7. Якщо всі вершини $X'=X$ графа G присутні у підграфі G', то G' називають ***остовним підграфом*** G або ***суграфом***.

Означення 2.1.8. ***Частковим графом*** $G'(X',\Gamma')$ графа $G(X,\Gamma)$ називають граф, у якого $X' \subseteq X$, $\Gamma' \subseteq \Gamma$.

Іншими словами, суграф отримуємо з графа видаленням деякої кількості дуг із збереженням всіх вершин, підграф – деякої кількості вершин разом з дугами цих вершин, а частковий граф – поєднання двох вищезгаданих операцій.

Наприклад:



Якщо множина вершин X' графа G' є найменшою підмножиною X, що містить всі кінцеві вершини ребер в Γ', то підграф G' називають ***реберно породженим підграфом*** графа G і позначують $\langle \Gamma' \rangle$.

Якщо множина ребер Γ' графа G' є найбільшою *підмножиною* Γ такою, що кінцеві вершини всіх його ребер належать X', то G' називають ***вершинно породженим підграфом*** графа G.

Означення 2.1.9. Граф $\overline{G}=(X,\Gamma')$ називають ***доповненням*** простого графа $G=(X,\Gamma)$ якщо ребро (x_i, x_j) входить в Γ' лише тоді, коли воно не входить в Γ.

2.1.3. Числові характеристики графа

Означення 2.1.10. ***Напівстепенем виходу*** p вершини x називають кількість вихідних з неї дуг.

Означення 2.1.11. ***Напівстепенем входу*** q вершини x називають кількість вхідних до неї дуг.

Означення 2.1.12. ***Степенем (валентністю)*** вершини x називають суму її вхідних та вихідних дуг.

$$s(x)=p+q.$$

Вершину, степінь якої дорівнює 0, називають ***ізольованою***. Вершину, степінь якої дорівнює 1, називають ***висячою***.

Граф, всі вершини якого мають однаковий степінь, називають ***регулярним*** або ***однорідним***.

Лема про рукостискання. Сума степенів всіх вершин графа є парним числом.

Наслідок. У довільному графі кількість вершин непарного степеня – число парне.

Теорема 2.1.1. Максимальна кількість ребер у плоскому графі обчислюється за формулою $|\Gamma|_{\max}=3(|X|-2)$.

Теорема 2.1.2. Кількість ребер у повному графі обчислюється за формулою $|\Gamma| = \frac{|X|(|X|-1)}{2}$.

Теорема 2.1.3. Кількість ребер у регулярному плоскому графі обчислюється за формулою $|\Gamma| = \frac{|X|r}{2}$, де r – показник регулярності графа (степінь всіх вершин).

Теорема 2.1.4. Найбільша кількість ребер у графі, який не має трикутних граней, обчислюється за формулою $|\Gamma| = \frac{|X|^2}{4}$.

Теорема 2.1.5. Максимальна кількість ребер у повному дводольному графі обчислюється за формулою $|\Gamma|_{\max} = mn$, де $m = |X_1|, n = |X_2|$.

Теорема 2.1.6. Стала залежність між кількістю вершин, ребер і граней плоского графа визначається за ***формулою Ейлера***: $S_0 + S_1 - S_2 = 2$, де S_0 – кількість вершин, S_1 – кількість ребер, а S_2 – кількість граней графа.

2.1.4. Маршрути незамкнені (ланцюги, шляхи) і замкнені (цикли, контури). Повнота. Зв'язність. Сильна зв'язність

Коли задають або шукають певну послідовність ребер (дуг), то говорять про маршрути у графах..

Означення 2.1.13. Скінченну послідовність ребер (дуг) графа $u_1, u_2, \dots u_n$ (не обов'язково різних) називають ***маршрутом довжини n***, якщо існує послідовність вершин $x_1, x_2, \dots x_{n+1}$ (не обов'язково різних), таких що $u_i = (x_i, x_{i+1}), i = \overline{1, n}$.

Вершини x_1 і x_{n+1} називають ***кінцевими*** або ***термінальними***.

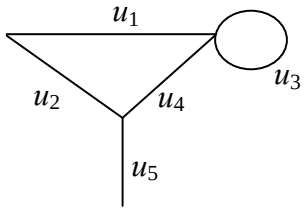
Означення 2.1.4. Маршрут називають ***відкритим*** або ***незамкненим***, якщо $x_1 \neq x_{n+1}$ і ***замкненим*** у протилежному випадку.

Означення 2.1.5. Незамкнений маршрут, у якого немає ребер (дуг), що повторюються, називають ***ланцюгом*** для неорієнтованого і ***шляхом*** для орієнтованого графа.

Означення 2.1.6. Замкнений маршрут, у якого немає ребер (дуг), що повторюються, називають ***циклом*** для неорієнтованого і ***контуром*** для орієнтованого графа.

Кажуть, що граф ***ациклічний*** або ***без контурний***, якщо він не має циклів чи контурів.

Наприклад,



u_1, u_4, u_2, u_1, u_3 – незамкнений маршрут;

u_1, u_4, u_5, u_5, u_2 – замкнений маршрут;

u_1, u_4, u_5 – ланцюг;

u_1, u_4, u_2 – цикл.

Граф називають ***повним***, якщо будь-які його дві вершини суміжні.

Орієнтований граф $G=(X,\Gamma)$ називають ***повним***, якщо з того, що $(x_i, x_j) \in \Gamma$ слідує, що $(x_j, x_i) \in \Gamma$.

Означення 2.1.7. Неорієнтований граф $G=(X,\Gamma)$ називають ***зв'язним***, якщо в ньому існує ланцюг між кожною парою вершин.

Властивості зв'язних графів:

1) граф зв'язний тоді і тільки тоді, коли множину його вершин X не можна розбити на дві непорожні підмножини X_1 та X_2 так, що дві граничні точки кожного ребра були в одній і тій самій множині;
2) у зв'язному графі довільні два шляхи максимальної довжини мають спільну вершину;
3) якщо граф $G=(X,\Gamma)$ – зв'язний, то граф $G'=(X,\Gamma-u)$, отриманий в результаті видалення циклічного ребра u, також зв'язний.

Означення 2.1.8. Орієнтований граф називають ***зв'язним***, якщо зв'язним є неорієнтований граф, що лежить в його основі.

Означення 2.1.9. Орієнтований граф $G=(X,\Gamma)$ називають ***сильно зв'язним***, якщо для кожної пари різних вершин x_i і x_j існує шлях з x_i до x_j і навпаки – з x_j до x_i.

2.1.5. Способи задання графа

Існує три основних способи задання графа:
- геометричний;
- табличний;
- абстрактний
- матричний

Геометричний – найпоширеніший спосіб задання графів, тому що він є зручним, наочним і цим способом можна задати довільний плоский граф.

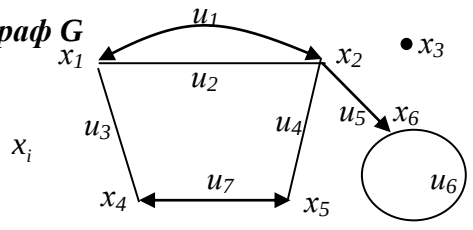
Для початку введемо визначення евклідового простору (ε^n) – це множина послідовностей із n дійсних чисел $x=(x_1,x_2,\dots,x_n)$, у якій відстань між довільними двома точками $x=(x_1,x_2,\dots,x_n)$ та $y=(y_1,y_2,\dots,y_n)$ визначена так: $\rho(x,y)=\left[\sum_{i=1}^{n}(x_i-y_i)^2\right]^{\frac{1}{2}}$.

Простою незамкненою кривою в евклідовому просторі називають неперервну криву, що самонеперетинається і з'єднує дві різні точки в (ε^n) (тобто криву, отриману неперервною деформацією прямолінійного відрізка). Аналогічно простою замкненою кривою називають неперервну криву, яка самонеперетинається і кінцеві точки якої співпадають.

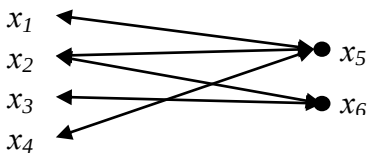
Означення 2.1.10. ***Геометричний граф*** у просторі (ε^n) – це множина $X=\{x\}$ точок простору (ε^n) і множина $\Gamma=\{u_i\}$ простих кривих, які задовольняють такі умови:
1) кожна замкнена крива в Γ містить лише одну точку з множини X;
2) кожна незамкнена крива в Γ містить лише дві точки з множини X, які є її граничними точками;
3) криві в Γ не мають спільних точок, за виключенням точок множини X.

Отже, геометричний граф – це проста конфігурація чи структура в просторі $\mathbb{R}^n$, яка складається з множини точок взаємопов'язаних множиною кривих, які є неперервними і самонеперетинаються. Нагадаємо, що для геометричного зображення орієнтованого графа використовують стрілки.

Граф G



- геометричні вершини;
u_j - геометричні ребра.



Дводольний граф задають аналогічно стрілочному способу задання відношень:

Хоча багато графів, які представляють реальні об'єкти (після їх ідеалізації) є геометричними графами, з точки зору теорії графів їх єдиною структурною особливістю є те, що з кожним ребром пов'язані дві геометричні вершини (які можуть в співпадати). Теорія графів побудована із вираховуванням цієї особливості і не враховує реальної природи ребер та вершин.

Ребра	Відповідні вершини
u_1	x_1, x_2
u_2	x_1, x_2
u_3	x_1, x_4
u_4	x_2, x_5
u_5	x_2, x_6
u_6	x_6, x_6
	x_3

Отже для опису геометричного графа можна подати ***таблицю***, у якій в першому стовпці записують ребра (дуги), а у другому – інцидентні їм вершини. Нумерація ребер та вершин, задання їх даною таблицею містить всю інформацію про даний геометричний граф.

Наприклад, для графа, побудованого геометричним способом вище, таблиця матиме такий вигляд.

Введемо поняття невпорядкованого добутку множини на себе.

Нагадаємо, що впорядкованим (декартовим прямим) добутком множини S на себе $S \times S$ називають множину впорядкованих пар (S_1, S_2) $S_1, S_2 \in$. Тут (S_1, S_2) і (S_2, S_1) – різні елементи, якщо $S_1 \neq S_2$. Символом & позначимо невпорядковану пару елементів – $(S_1 \& S_2) = (S_2 \& S_1)$, а невпорядкований добуток позначимо $S\&S$.

Якщо $S \times S$ складається з k^2 впорядкованих пар, то $S\&S$ – з $k(k+1)/2$ різних невпорядкованих пар.

Означення 2.1.11. ***Абстрактний граф*** – це сукупність непорожньої множини X, ізольованої від неї множини Γ (можливо і порожньої) і відображення Φ множини Γ на $X\&X$. Елементи множини X називають вершинами графа, а Г – ребрами. Φ називають ***відображенням інцидентності*** графа: $\Phi(u) = x_1 \& x_2$ – ребро u інцидентне кожній з вершин x_1 і x_2 і навпаки. Часом відображення Φ не задають у явному вигляді, а записують $u \sim (x_1 \& x_2)$ і читають: "ребро u з'єднує вершини x_1 і x_2".

Якщо X і Γ – скінченні множини (порожня множина теж скінчена), то граф $G(X,\Gamma)$ – скінчений. У протилежному випадку кажуть, що граф нескінчений.

Введення абстрактного графа дає змогу зберегти найсуттєвіші комбінаторні характеристики графа, на відміну від геометричного.

Наприклад, граф G, наведений вище можна зобразити абстрактним способом так:

Матричне зображення графів передбачає побудову різних видів матриць – інциденцій, суміжності вершин, суміжності ребер, циклів, розрізів, шляхів, доступності, ваг тощо. Розглянемо деякі з них.

Нехай G – граф, який має n вершин і m ребер. Графу G можна зіставити ***матрицю інциденцій*** розміром $n \times m$, рядки і стовпці якої відповідають вершинам та ребрам графа відповідно. Розглянемо випадок неорієнтованого графа:

Елемент матриці a_{ij} набуває значення 1 або 0 залежно від того, інцидентне j-е ребро i-й вершині чи ні. Для петлі всі елементи стовпця дорівнюють нулеві.

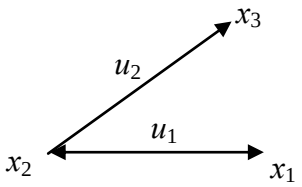
Наприклад, вище згаданий граф G має таку матрицю інциденцій:

		u_1	u_2	u_3	u_4	u_5
	x_1	1	1	1	0	0
	x_2	1	1	0	1	1
$G=$	x_3	0	0	0	0	0
	x_4	0	0	1	0	0
	x_5	0	0	0	1	0
	x_6	0	0	0	0	1

Матриця інциденцій не вказує на існування петлі, тому при току му способі задання графів слід виключати графи з петлями.

При описі орієнтованих графів елементів 0 і 1 недостатньо, оскільки дуга може бути інцидентною даній вершині і спрямована до неї, інцидентною даній вершині і

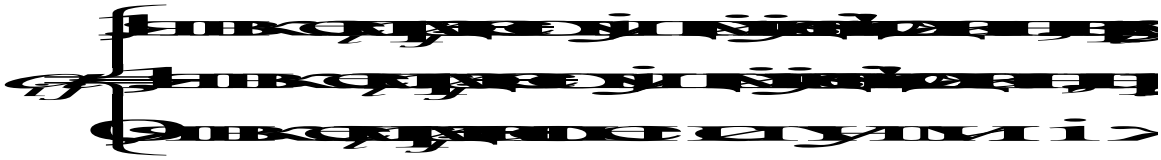
спрямованою від неї, неінцидентною даній вершині. Тому елементи матриць можуть набувати значень: -1, 1 та 0.



$$A = \begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \end{array} \begin{array}{c} \begin{array}{cc} u_1 & u_2 \end{array} \\ \begin{pmatrix} -1 & 0 \\ 1 & 1 \\ 0 & -1 \end{pmatrix} \end{array}$$

Матриця суміжності вершин має розмірність $n \times n$, де n – кількість вершин графа. Елементи матриці неорієнтованого графа визначають так:

Елементами матриці орієнтованого графа можуть бути такі числа:

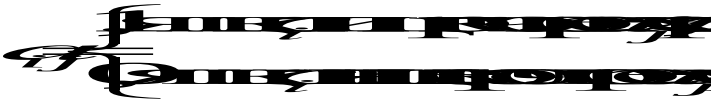


Матриця суміжності ребер має розмірність $m \times m$, де m – кількість ребер графа. Елементи матриці неорієнтованого графа визначають так:

Матриця суміжності вершин має розмірність $n \times n$, де n – кількість вершин графа. Елементи матриці неорієнтованого графа визначають так:

Матриця циклів має стільки рядків, скільки незалежних циклів у графа і стільки стовпців, скільки у ньому ребер (дуг). Елементи матриці циклів визначають так:

а) неорієнтований граф:



б) орієнтований граф:

Матриця розрізів має стільки рядків, скільки простих розрізів у графі і стільки стовпців, скільки у ньому ребер. Елементи матриці розрізів визначають для неорієнтованого графа так:

Тема 2.2. ОПЕРАЦІЇ НАД ГРАФАМИ

2.2.1. Поняття графа

Існують різні перетворення заданих графів, в результаті яких отримують нові графи. Ці перетворення називають операціями над графами.

2.2.1.1. Операція вилучення ребра (дуги). Якщо $G(X,\Gamma)$ – заданий граф і $u \in \Gamma$ – його ребро (дуга), то граф $G_1(X,\Gamma\backslash\{u\})$ називають графом, отриманим з G вилученням ребра (дуги). Кінцеві вершини вилученого ребра (дуги) із множини X не вилучаються.

2.2.1.2. Операція вилучення вершини. Якщо $G(X,\Gamma)$ – заданий граф і $x \in X$ – його вершина, то граф $G_2(X\backslash\{x\},\Gamma)$ називають графом, отриманим з G вилученням вершини, якщо із множини Γ вилучено всі ребра (дуги), інцидентні вилученій вершині.

2.2.1.3. Операція введення ребра (дуги). Якщо $G(X,\Gamma)$ – заданий граф, $x_1, x_2 \in X$ – його вершини, причому $(x_1,x_2) \notin \Gamma$, то граф $G_3(X,\Gamma \cup \{(x_1,x_2)\})$ називають графом, отриманим з G введенням ребра (дуги).

2.2.1.4. Операція введення вершини. Якщо $G(X,\Gamma)$ – заданий граф, $(y,z) \in \Gamma$ – його ребро (дуга) і $x \notin X$, то граф $G_4(X\cup\{x\},\Gamma)$ називають графом, отриманим з G введенням вершини, якщо із множини Γ вилучено ребро (дугу) (y,z) і введено два нових – (y,x) і (x,z).

2.2.1.5. Операція об'єднання графів. Якщо $G(X,\Gamma)$ і $G^*(X^*,\Gamma^*)$ – задані графи, то граф $G_5(X\cup X^*,\Gamma\cup\Gamma^*)$ називають об'єднанням графів G та G^*.

2.2.1.6. Операція перерізу (перетину) графів. Якщо $G(X,\Gamma)$ і $G^*(X^*,\Gamma^*)$ – задані графи, то граф $G_6(X\cap X^*,\Gamma\cap\Gamma^*)$ називають перерізом графів G та G^*.

2.2.1.7. Операція віднімання графів. Якщо $G(X,\Gamma)$ і $G^*(X^*,\Gamma^*)$ – задані графи, то граф $G_7(X,\Gamma\backslash\Gamma^*)$ називають різницею графів G та G^*.

2.2.1.8. Операція строгої диз'юнкції графів. Якщо $G(X,\Gamma)$ і $G^*(X^*,\Gamma^*)$ – задані графи, то реберно породжений граф G_8: $[\Gamma\oplus\Gamma^*]$ називають симетричною різницею графів G та G^*.

2.2.1.9. Операція множення графів. Якщо $G(X,\Gamma)$ і $G^*(X^*,\Gamma^*)$ – задані графи, то граф $G_8(X\times X^*,\Gamma^{**})$ називають добутком графів G та G^*, якщо $((x,x^*),(y,y^*)) \in \Gamma^{**}$ тоді і тільки тоді, коли $(x,y) \in \Gamma$ і $(x^*,y^*) \in \Gamma^*$.

Для операції над матрицями при визначенні об'єднання, перетину, різниці, симетричної різниці використовують правила:

$0\cup0=0$	$0\cap0=0$	$0\backslash0=0$	$0\oplus0=0$
$0\cup1=1$	$0\cap1=0$	$0\backslash1=0$	$0\oplus1=1$
$1\cup0=1$	$1\cap0=0$	$1\backslash0=1$	$1\oplus0=1$
$1\cup1=1$	$1\cap1=1$	$1\backslash1=1$	$1\oplus1=0$

Щоб розглянути матрично добуток графів, впорядковують елементи $X\times X^*$ так:

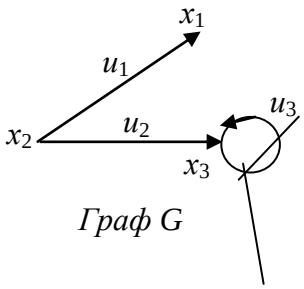
$$\begin{matrix} (x_1^{(1)},x_1^{(2)}) & \dots, & (x_1^{(1)},x_l^{(2)}) \\ (x_2^{(1)},x_1^{(2)}) & \dots, & (x_2^{(1)},x_l^{(2)}) \\ \dots, & \dots, & \dots \\ (x_m^{(1)},x_1^{(2)}) & \dots, & (x_m^{(1)},x_l^{(2)}) \end{matrix},$$

де n і m – кількості вершин графів G та G^*, тобто $|X|=m, |X^*|=l$.

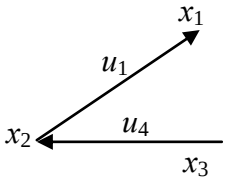
Тоді якщо $A=\|a_{ij}^{(1)}\|$, $A^*=\|a_{ij}^{(2)}\|$ – матриці суміжностей вершин графів G та G^* відповідно, то $A^{**}=\|b_{(I,k),(j,l)}\|= a_{ij}^{(1)}\cdot a_{ij}^{(2)}$ – матриця суміжності вершин графа $G^{**}=G\times G^*$:

$$A^{**}=\begin{Vmatrix} a_{11}A^* & a_{12}A^* & \dots & a_{1n}A^* \\ a_{21}A^* & a_{22}A^* & \dots & a_{2n}A^* \\ \dots & \dots & \dots & \dots \\ a_{n1}A^* & a_{n2}A^* & \dots & a_{nn}A^* \end{Vmatrix}.$$

Наприклад, нехай задано графи G та G^* так:

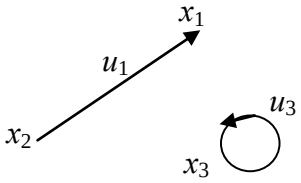


Граф G

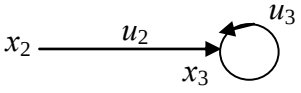


*Граф G**

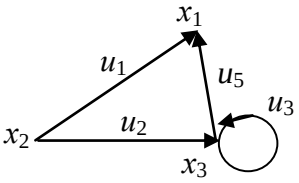
Здійснимо над цими графами всі описані вище операції.



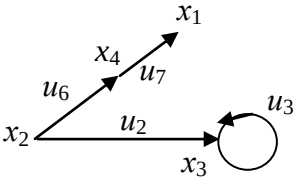
Граф $G_1=G-u_2$



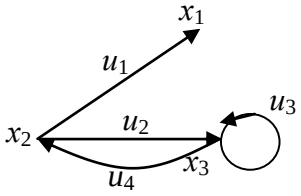
Граф $G_2=G-x_1$



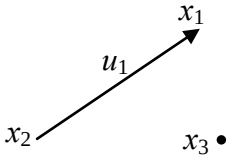
Граф $G_3=G+u_5$



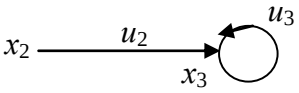
Граф $G_4=G+x_4$



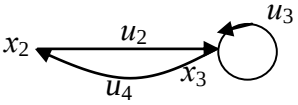
Граф $G_5=G\cup G^*$



Граф $G_6=G\cap G^*$



Граф $G_7=G\setminus G^*$



Граф $G_8=G\oplus G^*$

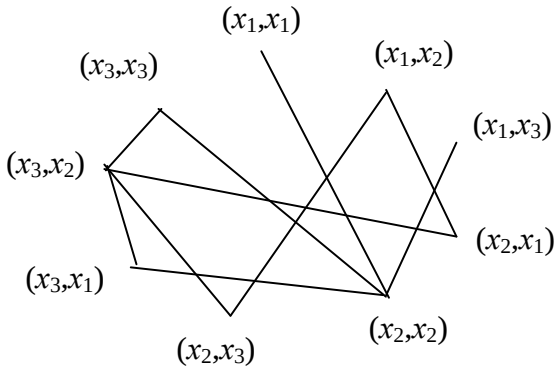
Для геометричного зображення графа добутку, не беручи до уваги орієнтацію графів G та G^*, побудуємо спочатку його матрицю суміжності вершин за матрицями суміжності вершин графів G та G^*.

$$G=\begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \end{array}\begin{array}{c} \begin{array}{ccc} x_1 & x_2 & x_3 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \end{array},\quad G^*=\begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \end{array}\begin{array}{c} \begin{array}{ccc} x_1 & x_2 & x_3 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \end{array}$$

$$G_3=\begin{array}{c} \\ (x_1,x_1) \\ (x_1,x_2) \\ (x_1,x_3) \\ (x_2,x_1) \\ (x_2,x_2) \\ (x_2,x_3) \\ (x_3,x_1) \\ (x_3,x_2) \\ (x_3,x_3) \end{array}\begin{array}{c} \begin{array}{ccc} (x_1,x_1) & (x_1,x_2) & \cdots \end{array} \\ \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \end{array} \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array}\begin{array}{c} \begin{array}{ccc} & & \end{array} \\ \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \end{array} \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array}\begin{array}{c} \begin{array}{ccc} & & \end{array} \\ \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \end{array}$$

$$=\begin{array}{c} \\ (x_1,x_1) \\ (x_1,x_2) \\ (x_1,x_3) \\ (x_2,x_1) \\ (x_2,x_2) \\ (x_2,x_3) \\ (x_3,x_1) \\ (x_3,x_2) \\ (x_3,x_3) \end{array}\begin{array}{c} \begin{array}{ccc} (x_1,x_1) & (x_1,x_2) & \cdots \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array}.$$

Кожну вершину графа зображуємо впорядкованою парою і з’єднуємо відповідні пари за матрицею суміжності вершин.



Граф $G_9=G\times G^*$

Тема 2.3. ДЕРЕВА І ЦИКЛИ У ГРАФАХ

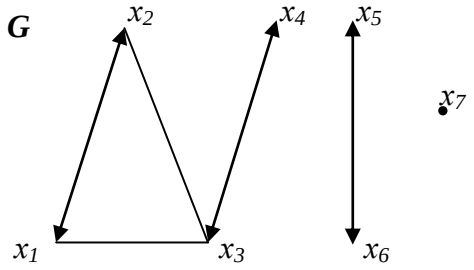
2.3.1. Компоненти зв'язності

Нагадаємо, що граф G називають ***зв'язним***, якщо у ньому існує шлях між кожною парою вершин.

Позначимо X_a множину, що складається з даної вершини a і всіх тих вершин графа, що можуть бути з'єднані з нею ланцюгом.

Означення 2.3.1. ***Компонента зв'язності*** чи просто ***компонента*** – це підграф, породжений множиною типу X_a або вершинно породжений підграф $\langle X_a \rangle$.

Розглянемо незв'язний неорієнтований граф $G(X,\Gamma)$.



Множину його вершин $X=\{x_1,x_2,x_3,x_4,x_5,x_6,x_7\}$ можна розбити на такі підмножини: $X_1=\{x_1,x_2,x_3,x_4\}$; $X_2=\{x_5,x_6\}$; $X_3=\{x_7\}$, так, що вершинно породжені підграфи $\langle X_1 \rangle$, $\langle X_2 \rangle$, $\langle X_3 \rangle$ були зв'язними, і жодна вершина з підмножини X_i не була суміжною з жодною вершиною підмножини X_j, $i \neq j$.

Очевидно, виконуються такі властивості для підмножин X_i, які утворюють розбитття множини X:

1) $X_i \neq \varnothing$;
2) $X_i \cap X_j = \varnothing$;
3) $\cup X_i = X$.

Підграфи $\langle X_1 \rangle$, $\langle X_2 \rangle$, $\langle X_3 \rangle$ – компоненти зв'язності графа G. Кожен з них – максимально зв'язний підграф графа G, тобто $\langle X_i \rangle$ не є власним підграфом будь-якого іншого підграфа $\langle X_j \rangle$.

Отже, наведений на прикладі граф G має три компоненти зв'язності.

Теорема 2.3.1. Граф буде зв'язним лише у тому випадку, якщо він складається з однієї компоненти зв'язності.

2.3.2. Ранг та цикломатичне число графа

Розглянемо граф G на n вершинах і m ребрах, який має p компонент зв'язності.

Означення 2.3.2. ***Рангом графа*** G називають число, яке дорівнює різниці між кількістю його вершин і компонент зв'язності:

$$\rho(G)=n-p.$$

Означення 2.3.3. ***Цикломатичним числом графа*** G називають число, яке дорівнює різниці між кількістю його ребер і вершин плюс кількість компонент компонент зв'язності:

$$\nu(G)=m-n+p.$$

Зауважимо, що існує зв'язок між рангом і цикломатичним числом графа:

$$\rho(G)+\nu(G)=m.$$

Ранг і цикломатичне число – найважливіші характеристики графа.

Теорема 2.3.2. Нехай G' граф, одержаний з графа G додаванням нового ребра між вершинами x_i та x_j. Тоді:

1) якщо $x_i = x_j$ чи вони можуть бути з'єднані ланцюгом в G, то

$$\rho(G')=\rho(G) \text{ та } \nu(G')=\nu(G)+1;$$

2) якщо $x_i \neq x_j$ чи вони не можуть бутиз'єднані ланцюгом в G, то

$$\rho(G')=\rho(G)+1 \text{ та } \nu(G')=\nu(G).$$

Доведення.

Якщо виконується умова 1), то додавання нового ребра кількості компонент зв'язності графа не змінює. Очевидно, що $p'=p$.

Тому

$$\rho(G')=n-p=\rho(G),$$

$$\nu(G')=m+1-n+p=\nu(G)+1.$$

Випадок 1) доведено.

Якщо ж виконується умова 2), то додане ребро – перешийок між компонентами зв'язності графа G, тому воно зменшує їх кількіть на 1.

У цьому випадку $p'=p-1$.

Тоді

$$\rho(G')=n-(p-1)=\rho(G)+1,$$

$$\nu(G')=m+1-n+(p-1)=\nu(G).$$

Випадок 2) доведено. Теорему доведено□.

Наслідок. $\rho(G)\geq 0, \nu(G)\geq 0$.

Доведення.

Якщо граф – вироджений, тобто має лише вершини, а ребра – відсутні, то $\rho(G)=0$ і $\nu(G)=0$. За теоремою 2.3.2 додавання нового ребра збільшує або $\rho(G)$, або $\nu(G)$. Отже, числа $\rho(G)$ та $\nu(G)$ можуть лише зростати.

Наслідок доведено□.

Підсумовуючи вище сказане, бачимо, що цикломатичне число графа вказує на **кількість** у ньому **циклів.**

2.3.3. Дерева і ліси

Серед зв'язних графів найпростішу структуру мають дерева.

Означення 2.3.4. ***Деревом*** називають скінчений зв'язний граф без циклів, який має щонайменше дві вершини.

Граф є деревом тоді і тільки тоді, коли кожна пара різних його вершин з'єднана одним і тільки одним ланцюгом.

Видалення довільного ребра з дерева робить його незв'язним, оскільки це ребро є складовою єдиного ланцюга, що з'єднує будь-які дві точки.

Теорема 2.3.3. Для графа G, який має n ($n>1$) вершин і m ребер, наступні твердження є еквівалентними:

1) G є деревом;
2) є лише один ланцюг між будь-якими двома вершинами в G;
3) G є зв'язним і $m=n-1$;
4) G не має циклів і $m=n-1$;
5) G не має циклів і при з'єднанні ребром довільних двох несуміжних вершин отримуємо граф, який має лише один цикл;
6) G є зв'язним проте втрачає цю властивість, якщо вилучити одне ребро.

Означення 2.3.5. ***Деревом графа*** G називають зв'язний підграф графа G, що не має циклів.

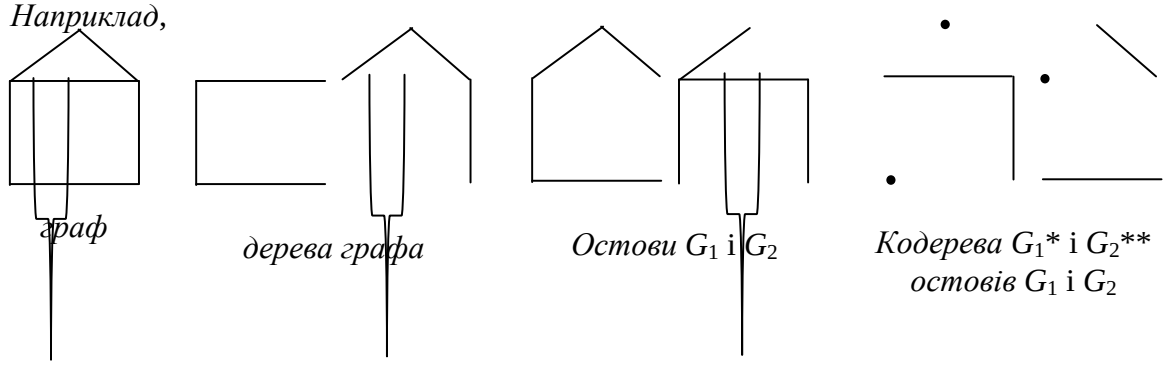
Означення 2.3.6. ***Остовом*** або ***покриттям*** графа G називають дерево графа G, що містить всі вершини графа G.

Означення 2.3.7. ***Кодерево*** T^* остова T графа G – це підграф графа G, що містить всі вершини графа G і лише ті ребра, які не входять в T.

Орієнтований граф G називається ***орієнтованим деревом*** (або ***прадеревом***), що росте з кореня x_0, якщо:

1) він є деревом без врахування орієнтації;
2) з x_0 є орієнтований шлях до всіх інших вершин графа G.

Наприклад,



Ребра остова графа G називають ***гілками*** дерева T, а ребра відповідно кодерева – ***хордами*** або ***зв'язками***.

Додання однієї хорди до остова графа вказує на незалежний цикл.

Теорема 2.3.4. Граф G є зв'язним тоді і тільки тоді, коли він має остов.

Означення 2.3.8. ***Лісом з k дерев*** називають граф, що не має циклів і складається з k компонент.

Теорема 2.3.5. Кожне дерево з n вершинами має $n-1$ ребро.

Теорема 2.3.6. Ліс з дерев, який містить n вершин, має $n-k$ ребер.

Тема 2.4. РОЗФАРБУВАННЯ ГРАФА

2.4.1. Задача про чотири фарби. Правильне розфарбування графа

В основу теорії розфарбування графа лягла задача "Про чотири фарби". Полягала вона в тому, щоб на політико-адміністративній карті розфарбувати країни так, щоб ніякі дві країни, що мають спільний кордон, не були розфарбовані однаковою фарбою, чотирма фарбами. При цьому спільний кордон, який зображений точкою, я не лінією, не враховувався.

Ця задача зводилася до задачі про розфарбування плоского графа: маючи деяку кількість фарб, розфарбувати кожну вершину (грань) так, щоб довільні дві суміжні вершини мали різний колір.

Це одна з перших задач теорії графів. Гіпотезу про чотири фарби вперше було висунуто в 1840р. На лекціях Мьобіуса. Нею займався Де Морган (1850р.). У 1878р. Келей не зміг отримати строгого доведення цієї гіпотези. У 1890р. Хівуд довів суперечність і показав, що необхідно п'ять кольорів.

Надалі вважатимемо, що граф G – плоский, не має кратних ребер і неорієнтований.

Крім розфарбування граней графа існує його реберне і вершинне розфарбування.

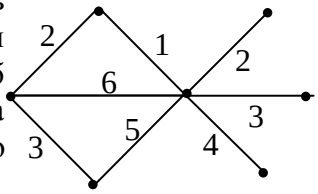
Означення 2.4.1. ***Реберним k-розфарбуванням*** графа називають присвоєння ребрам графа k різних фарб.

Означення 2.5.2. Граф $G(X,\Gamma)$ називають ***правильно реберно розфарбованим*** k фарбами, якщо кожне його ребро розфарбоване однією з k фарб і з того що два ребра u_i і u_j є суміжними слідує, що вони розфарбовані різними фарбами.

Означення 2.5.3. ***Хроматичний індекс*** або ***реберне хроматичне число*** $X'(G)$ графа G – це мінімальне число k, для якого граф має правильне реберне k-розфарбування.

Теорема Візинга. Якщо $G(X,\Gamma)$ – простий граф, то або $X'(G)=\Delta$, або $X'(G)=\Delta+1$, де Δ - максимальний степінь вершини у графі G (для дводольного графа $X'(G)=\Delta$).

Наприклад, у заданого графа максимальний степінь вершини 6, тобто 6 ребер є суміжними і повинні бути розфарбовані різними фарбами, тому менше, ніж 6 фарб неможливо використати для правильного розфарбування. На рисунку наведено один із способів правильного реберного розфарбування заданого графа.



Означення 2.5.4. Граф $G(X,\Gamma)$ називають ***правильно вершинно розфарбованим*** Δ фарбами, якщо кожна його вершина розфарбована однією з Δ фарб і якщо з $(x_i,x_j)\in\Gamma$ слідує, що x_i і x_j розфарбовані різними фарбами.

Означення 2.5.5. Граф $G(X,\Gamma)$ називають ***p-хроматичним***, якщо існує правильне розфарбування вершин графа G p фарбами. Мінімальне з таких p називають ***хроматичним числом графа.***

2.5.2. Визначення хроматичного числа. Хроматичний поліном

Для обчислення хроматичного числа вводять функцію $\pi(G,\lambda)$.

Означення 2.5.6. Для заданого графа G і натурального числа λ через $\pi(G,\lambda)$ (хроматичний поліном) позначається кількість всіх правильних розфарбувань графа G з допомогою λ фарб.

Слід відмітити що наступна формула справедлива для достатньо малих S_0.

Теорема 2.5.2. Справедлива формула:

 , де

S – кількість ребер суграфів графа G;

C – кількість компонент зв'язаності суграфів графа G;

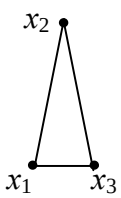
$\rho(S,C)$ - кількість суграфів графа G.

Якщо суграфів немає, то $\rho(S,C)=0$.

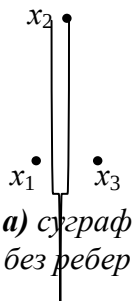
Ця формула дає змогу прослідкувати такі властивості функції $\pi(G,\lambda)$:

1) $\pi(G,\lambda)$ це многочлен степеня S_0 з коефіцієнтом 1 при старшому члені;
2) $\pi(G,\lambda)$ ділиться на λ.

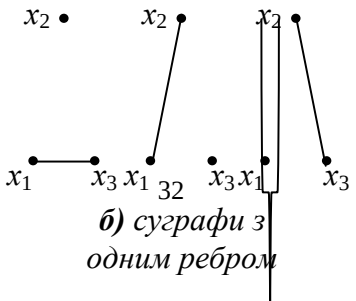
Нариклад, за теоремою 2.5.2 обчислимо $\pi(G,\lambda)$ для трикутного графа G.



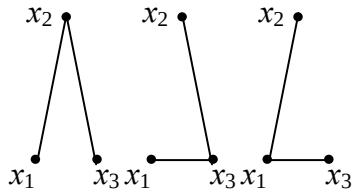
Граф G



а) *суграф без ребер*



б) *суграфи з одним ребром*



в) *суграфи з двома ребрами*

Розпишемо кожен з випадків, нагадавши, що сам граф є своїм суграфом (випадок *г*):

а) S=0, C=3, $\rho(S,C)=1$

б) S=1, C=2, $\rho(S,C)=3$

в) S=2, C=1, $\rho(S,C)=3$

г) S=3, C=1, $\rho(S,C)=1$.

Тоді [illegible].

Простим перебором чисел від 1, знаходимо хроматичне число. Підставивши у цю формулу $\lambda=1$ або $\lambda=2$, отримаємо, що $\pi(G,1)=\pi(G,2)=0$, тобто кількість правильних розфарбувань графа однією чи двома фарбами дорівнює нулеві – однією або двома фарбами граф розфарбовувати не можна. Хроматичне число цього графа є 3, оскільки його підставляння у формулу дало позитивний результат:

$$\pi(G,3)=1\cdot2\cdot3=3!=6$$

Властивості хроматичних поліномів:

1) $\pi(G,\lambda)=\pi(G_1,\lambda)\cdot\pi(G_2,\lambda)$ (якщо $G(\pi,\lambda)$ складається з двох незв'язних частин, то розфарбування можна вибирати незалежно для двох незв'язних графів).

2) $\pi(G,\lambda)=\frac{1}{\lambda}\pi(G_1,\lambda)\cdot\pi(G_2,\lambda)$ (якщо граф G отримано з двох графів склеюванням в одній точці x_0).

3) $\pi(G,\lambda)=\left(1-\frac{1}{\lambda}\right)\pi(G_1,\lambda)\cdot\pi(G_2,\lambda)$ (якщо граф G отримано з двох незв'язних графів склеюванням по ребру, зовнішньому для обох графів).

4) $\pi(G,\lambda)=\pi(G_1,\lambda)-\pi(G',\lambda)$ (якщо граф G отримано з G_1 доданням ребра без зміни вершин, G' – граф, отриманий з G_1 склеюванням вершин, які інцидентні доданому ребру).

Граф G є однохроматичним тоді і тільки тоді, коли він не містить ні одного ребра; двохроматичним – тоді і тільки тоді, коли він не містить циклів непарної довжини.

Для розфарбування граней, утворених перетином прямих ліній на площині достатньо двох кольорів.

Необхідною і достатньою умовою розфарбування двома кольорами є те, що кожна вершина повинна мати парний степінь ≥ 2.

РОЗДІЛ 3. ЗАГАЛЬНА АЛГЕБРА

Тема 3.1. ГРУПИ

3.1.1. Поняття алгебраїчної операції

Ще в середній школі розглядають різноманітні числові множини: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Якщо поставити завдання – проаналізувати, які спільні властивості мають ці множини і чим відрізняються, то прийдемо до висновку, що для цього числові множини слід розглядати не самі по собі, а відносно певних ***математичних дій*** або ***математичних операцій***.

$$\mathbb{N} \xrightarrow{(-)} \mathbb{Z} \xrightarrow{(:)} \mathbb{Q} \xrightarrow{(\sqrt{2})} \mathbb{R} \xrightarrow{(\sqrt{-1})} \mathbb{C}.$$

Отже, зазначені множини чисел відрізняються одна від одної здійсненністю або нездійсненністю в них тих чи інших математичних операцій.

У цьому ж проявляється і спільність властивостей цих числових множин. Справді, є операції, які здійсненні у кожній з них. Це дві основні дії арифметики – ***додавання*** і ***множення***, відносно яких інші арифметичні дії виступають як залежні, а саме – як обернені. Яку б названих множин ми не взяли, дії додавання і множення можна виконувати над довільними двома елементами цієї множини.

Крім того, основні закони цих дій – комутативний, асоціативний, дистрибутивний – справедливі в кожній з цих множин.

З цього випливає, що однією з найважливіших характеристик числових множин є можливість виконувати над її елементами ті чи інші операції (насамперед, + і *), не виходячи за межі цієї множини.

Наведемо властивості дій додавання і множення.

Властивості додавання:

1) для довільних елементів *a* і *b* даної множини існує єдиний елемент *c* цієї ж множини такий, що $c = a + b$ (*c* називають сумою, а *a* і *b* – доданками);
2) асоціативність додавання: $(a+b)+c = a+(b+c)$;
3) для довільного елемента *a* даної множини існує єдиний нульовий елемент θ такий, що $a + \theta = a$ (роль θ відіграє 0);
4) для довільного елемента *a* даної множини існує єдиний протилежний елемент *-a* такий, що $a + (-a) = \theta$.

Властивості множення:

5) для довільних елементів *a* і *b* даної множини існує єдиний елемент *c* цієї ж множини такий, що $c = a \cdot b$ (*c* називають добутком, а *a* і *b* – множниками);
6) асоціативність множення: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
7) для довільного елемента *a* даної множини існує єдиний одиничний елемент *e* такий, що $a \cdot e = a$ (роль *e* відіграє 1);
8) для довільного елемента *a* даної множини існує єдиний обернений елемент a^{-1} такий, що $a \cdot a^{-1} = e$.

Властивості додавання і множення аналогічні, тому їх можна об’єднати, якщо назвати елементи θ і *e* ***нейтральними***, а *–a* і a^{-1} – ***симетричними***. Очевидно, нейтральний елемент симетричний сам собі.

Означення 3.1.1. Нехай *M* – множина елементів довільної природи. Кажуть, що в *M* введено якусь ***алгебраїчну операцію***, якщо довільним двом елементам з даної множини $a, b \in M$ поставлено у відповідність єдиний третій елемент $c \in M$.

Довільну бінарну операцію позначають ∗:

$$a * b = c.$$

Отже, операція * є ***допустимою*** і ***однозначною***.

3.1.2. Означення і приклади груп

Означення 3.1.2. Непорожню множину G елементів довільної природи, в якій введено якусь бінарну алгебраїчну операцію *, називають ***групою***, якщо виконуються такі умови:

1) операція * – асоціативна: $(a*b)*c=a*(b*c)$;
2) існує єдиний нейтральний елемент $\eta \in G$ такий, що для довільного $a \in G$: $a*\eta=a$ і $\eta*a=a$;
3) існує єдиний симетричний елемент $a' \in G$ такий, що для довільного $a \in G$: $a*a'=\eta$ і $a'*a=\eta$.

Властивості 1)-3) називають ***аксіомами групи***.

Очевидно, визначена в групі G бінарна операція * не обов'язково комутативна. Якщо ж вона комутативна, то G називають ***комутативною*** або ***абелевою*** групою (Абель – норвезький математик, який вивчав рівняння, теорія яких тісно пов'язана з теорією комутативних груп).

Групу G називають ***скінченною***, якщо множина її елементів – скінченна, і ***нескінченною*** у протилежному випадку. Кількість елементів скінченої групи називають її ***порядком***.

Якщо в групі G бінарну операцію * називають додаванням і використовують відповідну символіку (+), то G називають ***адитивною*** групою. А якщо в групі G бінарну операцію * називають множенням і використовують відповідну символіку ($\cdot$), то G називають ***мультиплікативною*** групою. Якщо в групі G бінарну операцію * називають додаванням і використовують відповідну символіку (+), то G називають ***адитивною*** групою.

Приклади груп.

1. Множина всіх цілих чисел $\mathbb{Z}$ є абелевою адитивною групою (у $\mathbb{Z}$ визначена операція додавання, яка асоціативна і комутативна. У множина $\mathbb{Z}$ існує єдиний нейтральний елемент 0. Кожне ціле число a має симетричне $(-a) \in \mathbb{Z}$. Отже, всі аксіоми групи виконуються).
2. Множина всіх раціональних чисел $\mathbb{Q}$ і множина всіх дійсних чисел $\mathbb{R}$ є абелевими адитивними групами.
3. Множина всіх парних чисел є абелевою адитивною групою.
4. Множина всіх додатних раціональних чисел $\mathbb{Q}_+$ – абелева адитивна група.
5. Множина всіх відмінних від 0 дійсних чисел $\mathbb{R}\setminus\{0\}$ є абелевою мультиплікативною групою.
6. Множина всіх додатних дійсних чисел $\mathbb{R}_+$ і множина всіх відмінних від 0 дійсних чисел $\mathbb{R}\setminus\{0\}$ – абелеві мультиплікативні групи.
7. Послідовність чисел 1 і –1 є абелевою мультиплікативною групою.
8. Множина, що складається з одного числа 0, є абелева адитивна група.

Очевидно, що множина непарних чисел не є групою відносно додавання, бо в ній не визначена операція +: додавання непарних чисел виходить за межі цієї множини (може бути парним числом).

Може статися, що частина H елементів групи G є у свою чергу групою. Тоді H називають ***підгрупою*** групи G.

Означення 3.1.3. Підмножину H групи G називають ***підгрупою групи G***, якщо H є групою відносно бінарної операції *, визначеної в групі G.

Тема 3.3. ПОЛЯ

3.3.1. Означення поля. Приклади полів

У кожному кільці для операції додавання здійсненна обернена операція – віднімання. Про обернену до операції множення – ділення – в означенні кільця не йдеться.

Слід зауважити, що ділення на нуль неможливе у жодній з числових множин. Ця властивість має місце і в абстрактних кільцях – не можна ділити на нульовий елемент □.

Важливу роль в математиці відіграють комутативні кільця, в яких здійсненна операція ділення (крім ділення на нуль). Їх називають ***полями***.

Означення 3.3.1. Комутативне кільце P називають ***полем***, якщо воно має принаймні один елемент, відмінний від нульового і якщо в ньому в усіх випадках здійсненна операція ділення, крім ділення на нуль, тобто якщо для довільних елементів кільця a і b, a□□ у кільці міститься, і при тому єдиний, такий елемент q, для якого a□ q=b.

Елемент q називають ***часткою*** елементів a і b і записують $q = \frac{a}{b}$.

Аналогічно означують і числові поля. Існують ще й інші означення поля.

Означення 3.3.2. Комутативне кільце P з одиницею, яке воно має принаймні один елемент, відмінний від нульового, називають ***полем***, якщо для його кожного елемента a, a□□ існує єдиний обернений елемент a^{-1}, такий що a□ a^{-1}=e.

Означення 3.3.3. Комутативне кільце P, в якому існує хоча б один елемент, відмінний від нульового, називають ***полем***, якщо сукупність його елементів без □ утворює групу відносно операції множення.

Приклади полів.

1. Множини всіх раціональних, дійсних і комплексних чисел $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ є полями.
2. Множина чисел виду $a+\sqrt{2}b$, де a і b – раціональні числа, є полем.

Доведення

Доведемо, що результати операцій додавання, віднімання, множення і ділення належать також до чисел виду $a+\sqrt{2}b$. Для цього візьмемо два різних числа заданого виду $a_1+\sqrt{2}b_1$ і $a_2+\sqrt{2}b_2$.

1) Операції ***додавання і віднімання***:  .

Тут роль a відіграє вираз $a_1 \pm a_2$, який сумою (різницею) двох раціональних чисел a_1 і a_2, а тому і раціональним числом, а роль b – вираз $b_1 \pm b_2$, що є також раціональним числом з аналогічних міркувань.

2) Операція ***множення***:

 .

Тут у ролі a виступає вираз $a_1a_2+2b_1b_2$, а роль b – вираз $a_1b_2+a_2b_1$, що є раціональними числами, отриманими в результаті додавання множення раціональних чисел a_1, a_2, b_1, b_2.

3) Операція ***ділення*** (для виділення чисел a і b позбудемося ірраціональності в знаменнику):

 .

Очевидно, що вирази $\frac{a_1a_2-2b_1b_2}{a_2^2-2b_2^2}$ та $\frac{a_2b_1-a_1b_2}{a_2^2-2b_2^2}$, що виступають в ролі a і b, є раціональними, але викликає сумнів те, чи вони завжди мають зміст, тобто чи не дорівнює знаменник нулеві. Доведемо це від супротивного.

Припустимо, що $a_2^2 - 2b_2^2 = 0$.

Звідси $a_2^2 = 2b_2^2$, або $\frac{a_2^2}{b_2^2} = 2$, або $\left(\frac{a_2}{b_2}\right)^2 = 2$, або $\frac{a_2}{b_2} = \sqrt{2}$. Останній вираз є суперечністю, оскільки частка двох раціональних чисел не може бути числом ірраціональним. Твердження доведено.

3.3.2. Властивості полів

Через те, що поле є кільцем, всі властивості кілець автоматично переносяться на поля, до них лише слід додати властивості операції ділення. Розглянемо ряд властивостей поля, що випливають безпосередньо з його означення.

1. Жодне поле не має дільників нульового елемента.
2. Для відношень $\frac{b}{a}$ елементів поля P ($a \neq \theta$) справедливі арифметичні властивості звичайних дробів, а саме:
   1) якщо $a_1, a_2 \neq \theta$, то $\frac{b_1}{a_1} = \frac{b_2}{a_2}$ і тільки тоді, коли $b_1 a_2 = a_1 b_2$;
   2) для довільних елементів поля a_1, a_2, b_1, b_2 ($a_1, a_2 \neq \theta$) виконується рівність $\frac{b_1}{a_1} + \frac{b_2}{a_2} = \frac{b_1 a_2 + a_1 b_2}{a_1 a_2}$;
   3) для довільних елементів поля a_1, a_2, b_1, b_2 ($a_1, a_2 \neq \theta$) виконується рівність $\frac{b_1}{a_1} \cdot \frac{b_2}{a_2} = \frac{b_1 b_2}{a_1 a_2}$;
   4) для довільних елементів поля a_1, a_2, b_1, b_2 ($a_1, a_2 \neq \theta$) виконується рівність $\frac{b_1}{a_1} : \frac{b_2}{a_2} = \frac{b_1 a_2}{a_1 b_2}$;
   5) для довільних елементів поля a_1, b_1 ($a_1 \neq \theta$) виконується рівність $\frac{-b_1}{a_1} = -\frac{b_1}{a_1}$.
3. У полі P справедливі звичайні арифметичні правила дій з цілими степенями:

$$a^m \cdot a^n = a^{m+n}, \quad (a^m)^n = a^{mn}.$$

При цьому за означенням $a^0 = e$, $a^{-m} = \frac{1}{a^m}$ при $m > 0$.

РОЗДІЛ 4. КОМБІНАТОРНИЙ АНАЛІЗ

Тема 4.1. ОСНОВНІ ПОНЯТТЯ КОМБІНАТОРНОГО АНАЛІЗУ

Для вирішення багатьох задач різних галузей людської діяльності доводиться знаходити кількість способів можливих розміщень деяких предметів скінченої множини або число всіх можливих способів виконання певної дії із скінченої множини таких дій. Такі задачі ми вже розв'язували (знаходження булана скінченої множини, побудова все можливих відношень на заданій множині, знаходження шляхів у графах, транспортна задача тощо). Такі задачі вивчає ***комбінаторика***, а методи їх розв'язування називають ***методами комбінаторного аналізу***. Оскільки комбінаторика має справу із скінченними множинами, на природу об'єктів яких ніяких обмежень не накладають, то її часто називають ***теорією скінченних множин***.

Комбінаторика виникла у XVI столітті, коли у житті верхніх прошарків суспільства важливе місце займали азартні ігри (карти, кості, пасьянси, лотереї). Це стало рушійною силою у розвитку комбінаторики та теорії ймовірностей. Ряд перших комбінаторних задач розв'язали такі відомі математики як Паскаль, Ферма, Ейлер, Бернуллі, Лейбніц.

В економіці комбінаторні методи дискретної математики використовують при розв'язанні транспортної задачі, складанні все можливих розкладів, планів виробництва і реалізації продукції, призначення на посади тощо.

Встановлено зв'язки між комбінаторикою та теорією алгоритмічних структур, лінійним програмуванням, статистикою, кодуванням і декодуванням шифрів, вирішенням інших проблем теорії інформації.

4.1.1. Основні правила комбінаторики

Отже, комбінаторні задачі бувають різних видів. Проте більшість з них використовує 2 основних правила комбінаторики – ***правило суми*** і ***правило добутку***.

Правило суми. Якщо деякий об'єкт a можна вибрати m способами, а інший об'єкт b можна вибрати n способами, то вибір „a або b" можна здійснити $m+n$ способами.

При використанні правила суми треба слідкувати, щоб жоден із способів вибору об'єкта a не співпадав з будь-яким способом вибору об'єкта b. Якщо ж такі співпадіння існують, правило суми втрачає силу, і ми отримаємо лише $m+n-k$ способів вибору, де k – кількість співпадінь.

Правило добутку. Якщо деякий об'єкт a можна вибрати m способами і при кожному виборі об'єкта а інший об'єкт b можна вибрати n способами, то вибір пари „a і b" можна здійснити $m \cdot n$ способами.

Наочно правило добутку можна продемонструвати за допомогою таблиці чи матриці:

$$\begin{pmatrix} (a_1,b_1) & \dots & (a_1,b_n) \\ (a_2,b_1) & \dots & (a_2,b_n) \\ \dots & \dots & \dots \\ (a_m,b_1) & \dots & (a_m,b_n) \end{pmatrix}.$$

Узагальнене правило добутку. Якщо об'єкт a_1 можна вибрати m_1 способами, об'єкт a_2 – m_2 способами і т.д., об'єкт a_r – m_r способами, то вибір впорядкованої системи об'єктів (кортежу) $(a_1,a_2,..a_r)$ можна здійснити $m_1 \cdot m_2 \cdot m_r$ способами.

Приклад. Нехай з пункту A до пункту B існує m доріг, з пункту A до пункту C – n доріг, з пункту B до пункту D – k доріг, а з пункту C до пункту D – l доріг. Пункти B і C між собою дорогами не сполучені. Скількома способами можна пройти з пункту A до пункту D?

Розв'язання

Згідно з правилом добутку з пункту A до пункту D через пункт B веде mk доріг, а через пункт C – nl доріг. Тому за правилом суми кількість доріг з пункту A до пункту D дорівнює $mk+nl$. □

4.1.2. Розміщення. Розміщення з повтореннями

Нагадаємо означення впорядкованої множини.

Означення 4.1.1. Множину M називають впорядкованою, коли в ній встановлено відношення порядку "менше", що має такі властивості:

1) $\forall a,b\in M$: або $a<b$, або $b<a$;
2) $a<b, b<c \Rightarrow a<c$.

Означення 4.1.2. Нехай $|M|=n$, тобто множина M складається з n елементів, $k\le n$ $(k,n\in N)$. ***Розміщенням без повторень*** з n елементів по k називають довільну впорядковану підмножину M' множини M $(M'\subset M)$, всі елементи якої різні.

Кількість різних розміщень з n елементів по k без повторень позначають:

$$A_n^k.$$

Два розміщення вважають різними не лише тоді, коли вони відрізняються один від одного хоча б одним елементом, але й тоді, коли вони складаються з однакових елементів, але відрізняються порядком їх розміщення.

Теорема 4.1.1. Кількість k-розміщень без повторень з n елементів $(k\le n)$ визначається так:

$$A_n^k=n(n-1)(n-2)\dots(n-k+1).$$

Доведення

Перший елемент впорядкованої пари n-елементної множини можна вибрати n способами, другий – $(n-1)$ способами. Впорядковану пару за правилом добутку вибирають $n(n-1)$ способами, впорядкована трійка – $n(n-1)(n-2)$ способами. Продовжуючи цей процес далі, отримаємо:

$$A_n^k=n(n-1)(n-2)\dots(n-k+1).$$

Теорему доведено. <

Теорема 4.1.2. Кількість різних розміщень без повторень з n елементів по k дорівнює добутку k послідовних чисел, більшим з яких є n:

$$A_n^k=\frac{n!}{(n-k)!}.$$

Приклад. Нехай студенту необхідно скласти чотири екзамени протягом десяти днів. Скількома способами можна це зробити?

Розв'язання

$$A_{10}^4=\frac{10!}{(10-4)!}=\frac{10!}{6!}=7\cdot8\cdot9\cdot10=5040.$$ □

Означення 4.1.3. Нехай $|M|=n$, а $k\in N$. ***Розміщенням з повтореннями*** з n елементів по k називають довідний впорядкований k-елементний набір виду $(a_1,a_2,\dots a_k)$, де $a_1,a_2,\dots a_k$ – елементи множини M, не обов'язково різні.

Кількість різних розміщень з повтореннями позначають $\overline{A_n^k}$.

Теорема 4.1.3. Кількість різних розміщень з повтореннями з n елементів по k, де n і k – довільні натуральні числа дорівнює:

$$\overline{A_n^k} = n^k .$$

Приклад. Скількома способами можна записати шестизначний телефонний номер, якщо не зважати на зміст розміщення цифр (тобто номер 000000 вважати можливим)?

Розв'язання

Оскільки всіх цифр є 10 і у номері вони можуть повторюватися, то

$$\overline{A_{10}^6} = 10^6 = 1000000.$$

4.1.3. Перестановки. Перестановки з повтореннями

Означення 4.1.4. Розміщення з n елементів по n називають ***перестановкою*** з n елементів.

Кількість різних перестановок без повторень позначають P_n.

Теорема 4.1.4. різних перестановок без повторень дорівнює добутку всіх натуральних чисел з 1 до n:

$$P_n = 1 \cdot 2 \cdot \ldots \cdot n = n!.$$

Доведення випливає з того, що $P_n = A_n^n$.

Приклад. Одного разу 10 друзів зайшли до ресторану. Хазяїн запропонував їм приходити до нього щодня і кожного разу сідати за один і той самий стіл по-іншому. Доки всі способи розміщення будуть вичерпані, їх годуватимуть у ресторані безкоштовно. Коли настане цей день?

Розв'язання

$$P_{10} = 10! = 3628800.$$

Означення 4.1.5. Нехай $|M| = n$. ***Перестановкою з повтореннями*** з n елементів називають будь-яке впорядкування n-множини, серед елементів якої є однакові. Якщо серед елементів множини M є n_1 елементів першого типу,

n_2 елементів другого типу,

...

n_k елементів k-го типу $n_1 + n_2 + \ldots + n_k = n$,

то кількість всіх перестановок такої множини з повтореннями позначують $\overline{P_n}(n_1, n_2, \ldots n_k)$.

Теорема 4.1.5. Має місце формула:

$$\overline{P_n}(n_1, n_2, \ldots n_k) = \frac{n!}{n_1! n_2! \ldots n_k!}.$$

Приклад. Скільки перестановок можна зробити з літер слова "Міссісіпі"?

Розв'язання

Оскільки літера "м" входить до слова 1 раз, літера "і" – 4 рази, "с" – 3 рази, "п" – 1 раз, а всіх літер у слові 9, то

$$\overline{P_9}(1,4,3,1) = \frac{9!}{1!4!3!1!} = 2520.$$

4.1.4. Комбінації. Комбінації з повтореннями

У тих випадках, коли нас не цікавить порядок елементів у розміщення, а лише його склад, вводять поняття комбінації..

Означення 4.1.6. Нехай $|M| = n$, тобто множина M складається з n елементів, $k \le n$ $(k, n \in N)$. ***Комбінацією без повторень*** з n елементів по k називають довільну k-підмножину M' множини M $(M' \subset M, |M'| = k)$, всі елементи якої різні.

Кількість різних комбінацій з n елементів по k без повторень позначають:

$$C_n^k.$$

Отже, комбінація не є впорядкованою множиною, на відміну від розміщення, тобто дві різні комбінації відрізняються хоча б одним елементом.

Теорема 4.1.6. Для довільних натуральних чисел n і k $(k \le n)$ має місце формула:

$$C_n^k = \frac{n!}{k!(n-k)!}.$$

Теорема 4.1.7. Для C_n^k виконується рівність:

$$A_n^k = C_n^k \cdot P_k.$$

Доведення

Серед розміщень з n елементів по k можна виділити класи впорядкованих *k*-множин, які відрізняються лише порядком розміщення одних і тих самих елементів. У кожному класі таких множин буде $P_n = k!$, а кількість різних класів – C_n^k. Отже, $A_n^k = C_n^k \cdot P_k$. □

Приклад. Скільки діагоналей у правильному *n*-кутнику?

Розв'язання

Кількість пар вершин в *n*-кутнику, серед яких одні визначають діагональ, а інші – сторону *n*-кутника дорівнює:

$$C_n^2 = \frac{1}{2}n(n-1).$$

Оскільки всіх сторін *n*, кількість діагоналей визначатимемо так:

$$D_n = \frac{1}{2}n(n-1) - n = \frac{1}{2}n(n-3).$$ □

Приклад. Скільки натуральних дільників має число 2310=2□ 3□ 5□ 7□ 11?

Розв'язання

Кожен дільник, який не дорівнює одиниці, має вигляд: $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, де $\{p_1, p_2, \ldots, p_k\} \subset \{2, 3, 5, 7, 11\}$.

Оскільки порядок множників у добутку – неістотний, то кожен дільник задається комбінацією з 5 по *k*, де $1 \le k \le 5$. Всього дільників буде:

$$C_5^1 + C_5^2 + C_5^3 + C_5^4 + C_5^5 = 5 + 10 + 10 + 5 + 1 = 31.$$ □

Означення 4.1.7. ***Комбінацією з повтореннями*** з *n* елементів по *k* називають довідний *k*-елементний набір виду $(a_1, a_2, \ldots a_k)$, де кожен з елементів $a_1, a_2, \ldots a_k$ належить до одного з *n* типів.

Кількість різних комбінацій з повтореннями позначують $\overline{C_n^k}$.

Теорема 4.1.8. Кількість різних комбінацій з повтореннями з n елементів по k, де n і k – довільні натуральні числа дорівнює:

$$\overline{C_n^k} = C_{n+k-1}^k = \frac{(n+k-1)!}{k!(n-1)!}.$$

Приклад. У кондитерський відділ завезли 4 види тістечок. Скількома способами можна купити 7 тістечок?

Розв'язання

$$\overline{C_4^7} = C_{4+7-1}^7 = C_{10}^7 = \frac{10!}{7!3!} = 120.$$ □

4.1.6. Біном Ньютона. Трикутник Паскаля. Властивості біноміальних коефіцієнтів

З елементарної математики відомі формули скороченого множення:

$$(a+b)^2 = a^2 + 2ab + b^2.$$

Ці формули можна записати і так:

Очевидно, існує загальна закономірність.

Теорема 4.1.9. Справедлива рівність:

Цю рівність називають ***біномом Ньютона***.

Біноміальні коефіцієнти можна подати у вигляді трикутної таблиці, яку називають трикутником Паскаля:

					1	1						n=1
				1		2		1				n=2
			1		3		3		1			n=3
		1		4		6		4		1		n=4
	1		5		10		10		5		1	n=5
					...							

У n-му рядку трикутника Паскаля кожен коефіцієнт розкладу, крім двох крайніх, що дорівнюють 1, – це сума відповідних коефіцієнтів із попереднього рядка.

Узагальненням бінома Ньютона є наступна теорема:

Теорема 4.1.10 (поліноміальна теорема). Справедлива рівність:

де 

Числа $C_n(r_1, r_2, \ldots r_k)$ називають ***біноміальними коефіцієнтами***.

Властивості біноміальних коефіцієнтів:

1. $C_n^k = C_n^{n-k}$ (випливає з теореми 4.1.6, якщо замінити у формулі k на $(n-k)$, то $(n-k)$ заміниться на $(n-(n-k))=k$).
2. $C_{m+n}^m = C_{m+n}^n$ (формула симетрії).
3. $C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$ (формула додавання).
4. $C_n^0 + C_n^1 + C_n^2 + \ldots + C_n^{n-1} + C_n^n = 2^n$ (2^n – кількість всіх розміщень з повтореннями з елементів 2-х типів).
5. $C_n^k = \frac{n}{k} C_{n-1}^{k-1}$ (формула винесення за дужки).
6. $C_{n+1}^0 + C_{n+1}^1 + C_{n+1}^2 + \ldots + C_{n+1}^m = C_{n+1}^n$.
7. $C_n^k \cdot C_{n-k}^{m-k} = C_m^k \cdot C_n^m$.

РОЗДІЛ 5 . ЗАГАЛЬНІ ПИТАННЯ ТЕОРІЇ ЧИСЕЛ
ТЕМА 5.1. МНОЖИНИ ТА ОПЕРАЦІЇ.

5.1.1. Бінарні алгебраїчні операції.

Як зазначалось вище, кожна математична теорія вивчає множини, в яких введено певні відношення між їх елементами. Алгебра вивчає множини, для елементів яких визначені відношення, що дістали назву *алгебраїчних операцій*. З прикладами алгебраїчних операцій читачеві доводилося зустрічатися ще в шкільному курсі математики, а також у попередньому викладі (розд. I—III). Додавання і множення чисел, многочленів, алгебраїчних дробів, додавання векторів площини, кон'юнкція та диз'юнкція висловлень, додавання і множення функцій (наприклад, синусів і косинусів), композиція відповідностей —все це приклади алгебраїчних операцій. Ці операції виконуються над парами елементів однієї й тієї самої множини: над парами чисел, многочленів, векторів, функцій. Тому їх називають *бінарними алгебраїчними операціями*, або скорочено просто *бінарними операціями*. Загальне означення бінарної алгебраїчної операції, якому задовольняють, зокрема, перелічені вище операції, формулюють так.

Означення 1. *Нехай M — довільна множини елементів a, b, c, ...*

Під бінарною операцією в множині M розуміють закон, за яким будь-яким двом (різним чи однаковим) елементам a і b цієї множини, взятим у повному порядку, ставиться у відповідність єдиний елемент цієї множини.

В означення бінарної операції, як бачимо, входить вимога однозначності операції і її здійсненності для будь-яких двох елементів множини. В цьому означенні вказано також порядок, в якому беруться елементи множини *M* при виконанні над ними операції. Це означає, що парам елементів *a, b* і *b, a* ставляться у відповідність, взагалі кажучи, різні елементи множини *M*.

З точки зору загального означення бінарної операції, віднімання цілих, раціональних чисел, додавання векторів, розміщених у деякій площині *a,* є бінарні операції. Бінарними операціями є також диз'юнкція й кон'юнкція висловлень, додавання й множення дійсних функцій від змінної *x*, визначених для всіх дійсних значень *x*, композиція (множення) відображень деякої множини *A* в себе. Знаходження найбільшого спільного дільника і найменшого спільного кратного двох натуральних чисел — бінарні операції в множині натуральних чисел.

Зауважимо, що хоч наведене означення бінарної операції і досить широке, проте воно не охоплює всіх відомих читачеві математичних операцій. Так, утворення скалярного добутку двох векторів площини *a* не є бінарною операцією в множині *M* всіх векторів цієї площини, бо скалярний добуток двох векторів є число, а не вектор, і, отже, не є елементом множини *M*. Так само операція знаходження спільного дільника натуральних чисел *m* і *n* не є бінарною операцією в множині натуральних чисел, бо хоч вона здійсненна завжди, але не є однозначною: числа *m* і *n* можуть мати кілька спільних дільників.

Для скорочення запису кожну конкретну операцію позначають спеціальним знаком: додавання позначають знаком «+», множення — знаком «•», операцію перетину двох множин — знаком «∩» і т. д. Проте коли вивчають загальні властивості бінарних операцій, тобто властивості, що притаманні багатьом конкретним бінарним операціям, то говорять не про конкретні, а про довільні операції. Для позначення довільних бінарних операцій користуватимемося символами τ *і X* - Елемент, який бінарна операція *τ*(операція Х) ставить у відповідність парі елементів *a* і *b*, позначатимемо символом a *τ b (a X b)* і називатимемо *композицією* елементів *a* і *b*, елементи *a* і *b* називатимемо *членами* композиції.

Якщо композиція *a τ b(a X b)* дорівнює елементу *c*, то записуватимемо *a τ b =c (a X b=C*) і читатимемо «*a* в композиції з *b* дає *c*», або «композиція *a* і *b* дорівнює *c*». Якщо над елементами множини треба виконати одну чи кілька бінарних операцій декілька разів підряд, то порядок їх виконання, так само як це робиться при виконанні операцій над числами, вказуватимемо за допомогою дужок.

Зауважимо, що будь-яка бінарна операція *τ* в множині *M* є, очевидно, деяке відображення:

$$\varphi : M \times M \to M \qquad (5.1)$$

Бінарні алгебраїчні операції можна також розглядати і як тернарні відношення. Справді, нехай у множині *M* задано бінарну операцію *X*- Де означає, що будь-якій упорядкованій парі (*a, b*) елементів *a Є M, b Є M* поставлено у відповідність єдиний елемент *a X b= c Є M*. Позначимо символом P_* сукупність усіх упорядкованих трійок (*a, b, c*) елементів з *M* таких, що *c = a X b*. Очевидно, що $P_* M^3$ і тому $p_* = (P_*, M)$ є тернарне відношення між елементами множини *M*. При цьому $P_* abc = [a X b = c]$. Отже, бінарна операція *X* рівносильна тернарному відношенню p_*.

5.1.2. Асоціативність, комутативність та дистрибутивність бінарних операцій.

Нехай τ — бінарна операція, визначена в множині *M*.

Означення 1. Бінарна операція Т називається асоціативною, якщо

$\forall$ *[(a τ b) τ c = a τ(b τ c)]*. Вона називається неасоціативною, якщо в множині М є *a,b,c Є M* принаймні одна трійка елементів a, b і c така, що *(p τ b) τ c ≠ a τ (b τ c).*

Операції додавання і множення, наприклад, цілих чисел, як відомо, асоціативні. Асоціативні також операції об'єднання і перетину підмножин даної множиняОперація ж віднімання цілих чисел не асоціативна, бо *(10 - 3) - 1 ≠10 – (3 - 1).*

Означення 2. Бінарна операція Т називається комутативною, якщо $\forall$ *[a τ b = b τ a]*. Вона називається некомутативною, якщо в множині *M* є принаймні *a,c Є M* одна пара елементів a *і b* таких, що *a τ b ≠b τ a.*

Операції об'єднання і перетину підмножин множини А, як відомо, комутативні. Комутативні також операції додавання й множення цілих чисел. Операція ж віднімання цілих чисел некомутативна, бо 10 — 3 ≠ 3 — 10.

Припустимо, що у множині *M* визначені бінарні операції *τ* і *X*.

Означення 3. Бінарна операція Х називається дистрибутивною відносно операції τ, якщо:

$$\forall\ [(a\tau b)X c = (a X c)\tau(b X c)\ c X (a \tau b) = (c X a) \tau (c X b),\ a,b,c \in M^1 \qquad (5.2)$$

Операція *X* недистрибутивна відносно операції *τ*, якою в множині *M* є принаймні одна трійка елементів *a, b і c*, для яких не справджується хоч одна з записаних вище рівностей.

Так, операція множення цілих чисел дистрибутивна відносно операції додавання їх, але операція додавання не дистрибутивна відносно операції множення, бо 5 + 3 • 2≠(5+ 3) •(5+2). З'ясуємо тепер значення асоціативності й комутативності бінарних операцій.

Яку роль відіграє комутативність бінарної операції, читачеві зрозуміло: вона дає можливість переставляти місцями елементи, до яких застосовується бінарна операція, і завдяки цьому спрощувати формули й міркування.

Асоціативність бінарної операції, визначеної в множині *M*, дає можливість означити композицію трьох і взагалі будь-якого скінченного числа елементів, взятих у певному порядку. Справді, нехай у множині *M* визначена асоціативна бінарна операція τ.

Припустимо, що нам дано три елементи *a, b і c* множини *M*. Поки що ми не знаємо, що слід розуміти під композицією цих трьох елементів; адже в означенні бінарної операції говориться про композицію лише двох елементів, узятих в певному порядку. Отже, вирази виду *a τ b τ c* поки що не визначені. Однак ми знаємо, що означають вирази *(a τ b)τ c і a τ (b τ c).* Перший з цих виразів — це композиція елемента *a τ b* і елемента с, другий — композиція елемента *a* і елемента *b τ c*. Із асоціативності операції *τ* обидві ці композиції дорівнюють

---

[1] Якщо операція Х комутативна, то в означенні дистрибутивності операції Х говорять про справедливість лише однієї з рівностей:

(a τ b) X c = (a X c) τ (b X c) і c X (aτ b) = (c X a) τ (c X b) ,

оскільки в цьому випадку кожна з цих рівностей є наслідком іншої.

одному і тому самому елементу множини М. Цей елемент природно прийняти за композицію $a \tau b \tau c$, записану вже без дужок. Таким чином, рівність $a \tau b \tau c = (a \tau b) \tau c = a\tau(b\tau c)$ можна розглядати як означення композиції $a \tau b \tau c$ трьох елементів *a, b, c,* узятих в тому порядку, в якому вони записані.

Припустимо тепер, що дано п елементів множини *M*, записаних у певному порядку: a_1, a_2 ... a_n. Можна кількома способами розставити дужки, які вказуватимуть порядок послідовного виконання бінарної операції τ над цими елементами. Доведемо справедливість такої теореми.

Теорема 1. Результат послідовного виконання асоціативної операції над елементами упорядкованої множини a_1, a_2 … a_n порядку, вказаному за допомогою дужок, не залежить від способу розставляння дужок, тобто при різних розставляннях дужок результати будуть рівні між собою.

Доведення. Доводитимемо цю теорему методом математичної індукції. Для $n = 3$ теорема справедлива. Тому вважатимемо, що $n>3$. Припустимо, що теорема справедлива для будь-якого натурального числа k, меншого ніж n і не меншого ніж 3, тобто що результат послідовного виконання операції над елементами упорядкованої множини $a_{l1}, a_{l2} \ldots a_{lk}$ визначений однозначно. (Називатимемо цей результат композицією елементів $a_{l1}, a_{l2} \ldots a_{lk}$ і позначатимемо його символом $a_{l1} \tau a_{l2} \tau \ldots \tau a_{lk}$). Доведемо, що в такому разі теорема праведлива і для n. Для цього насамперед доведемо, що для кожного натурального числа $k < n - 1$ справджується рівність:

$$(a_1 \tau a_2 \tau \ldots \tau a_k) \tau (a_{k+1} \tau a_{k+2} \tau \ldots \tau a_n) = (a_1 \tau a_2 \tau \ldots \tau a_k \tau a_{k+1}) \tau (a_{k+2} \tau a_{k+3} \tau \ldots \tau a_n) \quad (5.3)$$

Це справді так. Композиції $a_1 \tau a_2 \tau \tau \ldots a_k$ і $a_{k+2} \tau a_{k+3} \tau \ldots \tau a_n$, за припущенням, однозначно визначені. Нехай

$a_1 \tau a_2 \tau \ldots \tau a_k = b$, $a_{k+2} \tau a_{k+3} \tau \ldots \tau a_n = c$.

Тоді

$(a_1 \tau a_2 \tau \ldots \tau a_k) \tau (a_{k+1} \tau a_{k+2} \tau \ldots \tau a_n) = b \tau (a_{k+1} \tau c)$,

$(a_1 \tau a_2 \tau \ldots \tau a_k \tau a_{k+1}) \tau (a_{k+2} \tau a_{k+3} \tau \ldots \tau a_n) = (b \tau a_{k+1}) \tau c$

Із асоціативності операції τ

$b \tau (a_{k+1} \tau c) = (b \tau a_{k+1}) \tau c$

і, отже,

$(a_1 \tau a_2 \tau \ldots \tau a_k) \tau (a_{k+1} \tau a_{k+2} \tau \ldots \tau a_n) = (a_1 \tau a_2 \tau \ldots \tau a_k \tau a_{k+1}) \tau (a_{k+2} \tau a_{k+3} \tau \ldots \tau a_n)$

Із справедливості рівності (5.3) випливає, що для будь-яких натуральних чисел k і l, менших ніж n, справджується рівність:

$$(a_1 \tau a_2 \tau \ldots \tau a_k) \tau (a_{k+1} \tau a_{k+2} \tau \ldots \tau a_n) = (a_1 \tau a_2 \tau \ldots \tau a_l) \tau (a_{l+1} \tau a_{l+2} \tau \ldots \tau a_n) \quad (5.4)$$

Доведемо це. Не втрачаючи загальності міркувань, вважатимемо, що $l>k$. Нехай $l=k+s$. Тоді з рівності (5.3)

$(a_1 \tau a_2 \tau \ldots \tau a_k) \tau (a_{k+1} \tau a_{k+2} \tau \ldots \tau a_n) = (a_1 \tau a_2 \tau \ldots \tau a_k \tau a_{k+1}) \tau (a_{k+2} \tau a_{k+3} \tau \ldots \tau a_n) =$

$= (a_1 \tau a_2 \tau \ldots \tau a_{k+1} \tau a_{k+2}) \tau (a_{k+3} \tau a_{k+4} \tau \ldots \tau a_n) = \ldots = (a_1 \tau a_2 \tau \ldots \tau a_{k+s-1}) \tau (a_{k+s} \tau$

$\tau a_{k+s+1} \tau \ldots \tau a_n) = (a_1 \tau a_2 \tau \ldots \tau a_l) \tau (a_{l+1} \tau a_{l+2} \tau \ldots \tau a_n)$

і, отже,

$(a_1 \tau a_2 \tau \ldots \tau a_k) \tau (a_{k+1} \tau a_{k+2} \tau \ldots \tau a_n) = (a_1 \tau a_2 \tau \ldots \tau a_l) \tau (a_{l+1} \tau a_{l+2} \tau \ldots \tau a_n)$

Припустимо тепер, що в системі елементів $a_1, a_2 \ldots a_n$ двома будь-якими різними способами розставлено дужки, що вказують, в якому саме порядку треба послідовно виконувати операцію τ. Доведемо що в обох випадках результат виконання операції буде той самий.

Справді, якщо ми послідовно виконуватимемо операцію τ в порядку, що вказується розставлянням дужок першим способом, то останнім кроком буде виконання операції τ над композиціями:

$a_1 \tau a_2 \tau \ldots \tau a_k$ і $a_{k+1} \tau a_{k+2} \tau \ldots \tau a_n$ $(1 \le l \le n-1)$.

При виконанні операції τ в порядку, вказаному розставлянням дужок другим способом, останнім кроком буде виконання операції τ над деякими композиціями

$a_1 \tau a_2 \tau \ldots \tau a_l$ і $a_{l+1} \tau a_{l+2} \tau \ldots \tau a_n$ $(1 \le l \le n-1)$.

Але за рівністю (1.4)

$(a_1 \tau a_2 \tau \ldots \tau a_k) \tau (a_{k+1} \tau a_{k+2} \tau \ldots \tau a_n) = (a_1 \tau a_2 \tau \ldots \tau a_l) \tau (a_{l+1} \tau a_{l+2} \tau \ldots \tau a_n)$

Отже, в обох випадках матимемо той самий результат. Тому, за принципом математичної індукції, теорема справедлива для будь-якого натурального $n \ge 3$. Цим теорему доведено.

Результат послідовного виконання операції Т над елементами системи $a_1, a_2 \ldots a_n$, таким чином, визначається однозначно. Його ми називатимемо *композицією* елементів $a_1, a_2 \ldots a_n$ і позначатимемо символом $a_1 \tau a_2 \tau \ldots \tau a_n$. Елементи $a_1, a_2 \ldots a_n$ називатимемо *членами* цієї композиції.

Якщо в композиції $a_1 \tau a_2 \tau \ldots \tau a_n$. всі члени дорівнюють одному й тому самому елементу а, то позначатимемо її символом $\overset{n}{\tau}$ а .Застосовуючи теорему 1 до композиції, що містить однакові члени, дістаємо формули:

$$\overset{m+n}{\tau} a = (\overset{m}{\tau} a) \tau (\overset{n}{\tau} a), \quad \overset{mn}{\tau} a = \overset{m}{\tau} (\overset{n}{\tau} a), \qquad (5.5)$$

де m і n—будь-які натуральні числа.

Припустимо тепер, що бінарна операція τ, яка визначена в множині *M*, не лише асоціативна, а й комутативна. Тоді буде правильним таке твердження:

Теорема 2. *Композиція будь-яких n елементів $a_1, a_2 \ldots a_n$ множини M не залежить від того, в якому порядку йдуть її члени.*

Доведення. Нехай $a_{l1} \tau a_{l2} \tau \ldots \tau a_{ln}$ — композиція елементів $a_1, a_2 \ldots a_n$ розташованих у будь-якому порядку, відмінному від їх розташування в композиції $a_1 \tau a_2 \tau \ldots \tau a_n$. Доведемо, $a_{l1} \tau a_{l2} \tau \ldots \tau a_{ln} = a_1 \tau a_2 \tau \ldots \tau a_n$. При $n=2$ теорема справедлива, бо $a_1 \tau a_2 = a_2 \tau a_1$. Припустимо, що теорема справедлива для будь-якого числа членів, меншого ніж *n* і не меншого ніж 2, і доведемо, що тоді вона справедлива й для *n* членів.

Нехай $i1$ = n. Тоді за теоремою 1

$A_{i1} \tau a_{i2} \tau \ldots \tau a_{in} = a_n \tau (a_{i2} \tau a_{i3} \tau \ldots \tau a_{in})$.

За припущенням, $a_{i2} \tau a_{i3} \tau \ldots \tau a_{in} = a_1 \tau a_2 \tau \ldots \tau a_{n-1}$. Отже,

$a_{i1} \tau a_{i2} \tau \ldots \tau a_{in} = a_n \tau (a_{i2} \tau a_{i3} \tau \ldots \tau a_{in}) = a_n \tau (a_1 \tau a_2 \tau \ldots \tau a_{n-1}) =$

$= (a_1 \tau a_2 \tau \ldots \tau a_{n-1}) \tau a_n = a_1 \tau a_2 \tau \ldots \tau a_{n-1} \tau a_n$

Якщо i_k=n(1<k<n),то за теоремою 1 й індуктивним припущенням,

$a_{i1} \tau a_{i2} \tau \ldots \tau a_{in-1} \tau a_k \tau a_{k+1} \tau \ldots a_{in} = (a_{i1} \tau a_{i2} \tau \ldots \tau a_{in-1}) \tau [a_n \tau (a_{ik+1} \tau a_{ik+2} \tau \ldots \tau a_{in})] =$

$= (a_{i1} \tau a_{i2} \tau \ldots \tau a_{in-1}) \tau [(a_{ik+1} \tau a_{ik+2} \tau \ldots \tau a_{in}) \tau a_n] =$

$= (a_{i1} \tau a_{i2} \tau \ldots \tau a_{in-1}) \tau (a_{ik+1} \tau a_{ik+2} \tau \ldots \tau a_{in}) \tau a_n =$

$= (a_{i1} \tau a_{i2} \tau \ldots \tau a_{in-1} \tau a_{ik+1} \tau a_{ik+2} \tau \ldots \tau a_{in}) \tau a_n = (a_1 \tau a_2 \tau \ldots \tau a_{n-1}) \tau a_n =$

$= a_1 \tau a_2 \tau \ldots \tau a_{n-1} \tau a_n$.

Нарешті, якщо $i_n = n$, то за теоремою 1 й індуктивним припущенням,

$a_1 \tau a_2 \tau \ldots \tau a_{n-1} \tau a_n = (a_{i1} \tau a_{i2} \tau \ldots \tau a_{in-1}) \tau a_n = (a_1 \tau a_2 \tau \ldots \tau a_{n-1}) \tau a_n = a_1 \tau a_2 \tau \ldots \tau a_n$.

Отже, в усіх випадках з припущення, що теорема справедлива для будь-якого числа членів, не меншого ніж 2 і меншого ніж я, випливає правильність її й для *n* членів. Тому, за принципом математичної індукції, вона справедлива для будь-якого числа членів. Цим теорему доведено.

В алгебрі вивчають бінарні операції, які за своїми властивостями більш-менш близькі до операцій додавання і множення чисел, і тому кожну з них також називають або додаванням, або множенням. Якщо бінарну операцію, визначену в множині *M*, називають додаванням, то тоді елемент *c*, який цією операцією ставиться у відповідність упорядкованій парі елементів $\langle a, b \rangle$, називають *сумою* цих елементів, а елементи *a* і *b* – *доданками* і записують: $a + b = c$; якщо ж її називають множенням, то *c* називають *добутком* елементів *a* і *b*, а *a* і *b* – *співмножниками* і записують:

$a \cdot b = c$, або $ab = c$.

Читач самостійно легко сформулює для операцій додавання і множення теореми 1 і 2, а також означення поняття суми і добутку *n* елементів.

Означення 4. Суму *n* доданків, кожен з яких дорівнює елементу *a*, називають *n*-кратним елемента *a* і позначають символом *na*.

Означення 5. Добуток *n* співмножників, кожен з яких дорівнює елементу *a*, називають *n*-м степенем елемента a і позначають символом a^n.

Формули (1.5) в символах операцій додавання і множення запишуться відповідно так:

$$(m + n)a = ma + na,\ (mn)\ a = m\ (na) \qquad (5.5')$$

і

$$a^{m+n} = a^m\ a^n,\ a^{mn} = (a^n)^{\ m}. \qquad (5.5'')$$

5.1.3. Обернені операції.

Нейтральний елемент; симетричні елементи. Нехай у множині *M* визначена бінарна операція τ.

Означення 1. *Говорять, що для визначеної у множині M бінарної операції τ здійсненна обернена бінарна операція , якщо для будь-яких елементів a і b множини M існує одна і тільки одна пара таких елементів x° і y°,* що $a\ \tau\ x^\circ = b$ *і* $y^\circ\ \tau\ a = b$. Зауважимо, що коли операція τ комутативна, то елементи x° і y°, про які йде мова в означенні 1, збігаються.

Якщо τ є комутативна операція додавання (множення), то обернену їй операцію називають відніманням (діленням). Елемент x°, що задовольняє умови a τ x° = x° τ a = b, називають різницею (часткою) елементів b і a і записують x°= b-a (x°= b: a, або x° = $\frac{a}{b}$).

Серед множин, з якими читачеві доводилося мати справу в шкільному курсі алгебри, є такі, в яких операції додавання і множення визначені, але обернені їм операції віднімання і ділення — нездійсненні. Такою, наприклад, є множина натуральних чисел. Є також множини, наприклад, множина цілих чисел, в яких визначена операція додавання і здійсненна обернена їй операція — віднімання, а також такі, як, наприклад, множина відмінних від нуля раціональних чисел, в яких визначена операція множення і здійсненна обернена їй операція — ділення. Обернена операція ⊥, очевидно, не є новою незалежною операцією: вона є похідною від операції τ.

Означення 2. Елемент *η Є M* називається нейтральним елементом відносно операції τ, якщо: $\forall a \in M\ \left[a \perp \eta = a \wedge \eta \tau a = a\right]$

Так, у множині всіх підмножин деякої множини *M* порожня підмножина *Ø* є нейтральним елементом відносно операції об'єднання U, а *M* — відносно операції перетину ∩. Число 0 є нейтральним елементом відносно додавання цілих чисел, а число 1 — відносно їх множення. Нейтральним елементом відносно композиції (множення) відображень множини *M* в *M* є тотожне відображення *M* на *M*.

Нейтральний елемент відносно операції додавання, визначеної в деякій множині *M*, називають нульовим елементом (скорочено нулем) і позначають символом 0, а відносно операції множення - одиничним елементом (одиницею) і позначають символом *e*.

Теорема 3. *Якщо в множині M з бінарною операцією τ в нейтральний елемент η, то тільки один.*

Справді, якщо ŋ і ŋ'— нейтральні елементи, то ŋ = ŋ τ і ŋ'=ŋ'

Означення 3. Нехай у множині *M* з бінарного операцією τ є нейтральний елемент ŋ. Елемент *a′* називають симетричним елементу *a Є M*, якщо $a'\ \tau\ a = a\ \tau\ a' = \eta$.

Нейтральний елемент ŋ, очевидно, симетричний сам собі. Якщо *a* — відмінне від нуля раціональне число, то число — *a* симетричне йому відносно додавання, $\frac{1}{a}$ число відносно множення.

Елемент множини *M*, симетричний елементу *a Є M* відносно операції додавання, називають *протилежним a* і позначають символом—*a*, а симетричний відносно операції множення називають *оберненим a* і позначають символом a^{-1}.

Теорема 4. *Якщо бінарна операція т, визначена в множині М, асоціативна, то для будь-якого елемента а множини М в ній може існувати не більше, ніж один симетричний елемент.*

Справді, якщо *а′* і *а″* — елементи, симетричні елементу *а*, то
а′ = а′ τ ŋ = а′ τ (а τ а″) = (а′ τ а) τ а″=ŋ τ а″= а″, тобто *а′ = а″.*

5.1.4 Алгебраїчні структури.

Бінарна операція виконується над парами елементів певної множини. Однак в алгебрі і в інших розділах математики розглядаються також операції, що виконуються над одним об'єктом, їх називають *унітарними операціями.* Загальне означення унітарної операції таке.

Означення 1. *Нехай М — множина елементів а, b, с, ... довільної природи. Говорять, що в множині М – введено деяку унітарну операцію, якщо кожному елементу а множини М поставлено у відповідність єдиний елемент b цієї ж множини.*

Унітарна операція в множині *М* є, таким чином, однозначним відображенням множини *М* самої в себе. Прикладами унітарної операції є операція піднесення числа до квадрата, взяття доповнення підмножини даної множини, заперечення висловлення, знаходження абсолютної величини дійсного числа і ін.

В алгебрі розглядаються також *n*-арні операції, тобто операції, що виконуються над упорядкованими системами *n* елементів даної множини. Проте ми не будемо торкатися цього питання.

Означені вище унітарні й бінарні операції виконуються над елементами певної множини, і результат виконання операції належить також до тієї ж множини. Тому їх називають *внутрішніми* операціями або *внутрішніми законами композиції.* Поряд з внутрішніми законами композиції в алгебрі розглядаються також зовнішні закони композиції, в яких, крім основної множини *М*, бере участь ще й допоміжна множина *Q,* елементи якої називають *операторами.* Зовнішній закон композиції парі <α, *а*>, утвореної оператором α і елементом *а*, ставить у відповідність деякий цілком визначений елемент b множини *М*. Точне означення зовнішнього закону композиції формулюють так.

Означення 2. *Зовнішнім законом композиції елементів множини Q, що називається множиною операторів (або областю операторів) закону, і елементів множини М називають правило, за яким кожній парі (α, а) (α є Q, а. Є М) ставиться у відповідність єдиний елемент b множини М, тобто відображення* $\psi : Q \times M \to M$. Часто цей зовнішній закон називають *множенням* елементів множини *М* на оператори множини *Q;* композицію елементів α і *а* при цьому позначають символом α• , або α*а*. і називають добутком елемента *а* на оператор α.

Означення 3. *Множина М, для елементів якої задано один або кілька законів композиції (внутрішніх чи зовнішніх), називається алгебраїчною структурою.*

Завдання алгебри є вивчення алгебраїчних структур. Безперечно, алгебра вивчає далеко не всі алгебраїчні структури. Можна побудувати чимало прикладів алгебраїчних структур, але в переважній більшості вони не матимуть ніяких застосувань ні в теорії, ні в практиці, а «теорія» таких структур складатиметься з означень і тривіальних наслідків з них. Такі структури, очевидно, не можуть бути об'єктом вивчення.

У процесі розвитку математики виділилася й стала докладно вивчатися невелика кількість основних типів алгебраїчних структур, алгебраїчні операції в яких за своїми властивостями більш-менш близькі до операцій додавання і множення чисел. Найважливішими серед різних алгебраїчних структур є група, кільце, поле, лінійний простір, лінійна алгебра. Вивчення властивостей саме цих алгебраїчних структур, опис їх будови і зв'язків між ними й іншими основними математичними об'єктами є одним з найважливіших завдань алгебри на сучасному етапі її розвитку.

До викладу елементарних відомостей про групи, кільця й поля ми зараз і перейдемо.

Тема 5.2 Теоретико-числові базиси.

До основних дискретних теоретико-числових базисів належать унітарні функції та коди, функції Хаара та розрядно-позиційні коди, дискретно-фазові функції та коди Лібова-

Крейга, функції Радемахера та двійкові коди, функції Грея та коди Грея, функції Уолша, функції Ґалуа та кодові системи Ґалуа. Вибір кодової системи, базису або системи функцій залежить від задачі, властивостей інформаційного потоку, умов застосування даних та інш.

Зокрема, базисами для виконання дискретних ортогональних перетворень і дискретного подання одновимірного інформаційного потоку зі скінченною енергією, визначеного в просторі $L_2[a,b]$ на часовому інтервалі $T=[a,b]$, є повні ортонормовані системи функцій. Вейвлет-аналіз здійснюється на основі ортогональних або базисів Ріса. Повними ортонормованими системами функцій у просторі $L_2[a,b]$ є тригонометрична система та дискретні експоненціальні функції – як базис перетворення Фур'є, системи Уолша, Хаара, функції пилкоподібного базису, Віленкіна-Крестенсона та інші, проте актуальною залишається задача визначення галузей, способів і методів їх ефективного застосування, формування та дослідження інших базисів. Визначення особливостей та ефективності застосування різних систем функцій для виконання дискретних перетворень і аналізу інформаційних потоків зумовлює необхідність дослідження властивостей цих систем, наведених у наступних викладках.

1. Унітарні функції та коди.

В якості вихідних у засобах перетворення форми інформації широкого застосування набули унітарні коди, розрядність бінарного подання слова яких відповідає повній шкалі квантування діапазону перетворення *N*. Здійснити перехід до ефективніших кодів із меншою розрядністю дозволяє аналітичне подання унітарних кодів і встановлення функціональних залежностей з іншими кодами чи системами кодування.

Для подання унітарних кодів використовуються унітарні функції

$$Uni(m,\theta,i) = sign(\sin(2^m \pi(\theta + i \cdot 2^{-n}))), \qquad (5.7)$$

де $m = 0, 1, \ldots, n+1$ – порядок набору системи функцій; $n = \log_2 N$; N – модуль цілочислових дискретних значень системи; $\theta = t/T$; $(0 \le \theta < 1)$ – нормований параметр часу; $T = 2\pi$; t – потокове значення часу; $0 \le t < 2\pi$; $i = 0,1,\ldots,2^{n-m+1} - 1$ – порядковий номер функції в наборі порядку m.

Набір нульового порядку $Uni(0,\theta,i)$ містить *2N* функцій (рис.5.1).

Властивості унітарних функцій:

1. Система з перших *N* унітарних функцій порядку *m* є лінійно незалежною, оскільки виконується достатня умова лінійної незалежності: ранг матриці *N* функцій дорівнює кількості функцій *N*. Наступні *N* функцій є лінійними комбінаціями *N* перших.

2. Унітарні функції не ортогональні, оскільки $\int_0^1 Uni(m,\theta,i)Uni(k,\theta,j)d\theta \neq 0$.

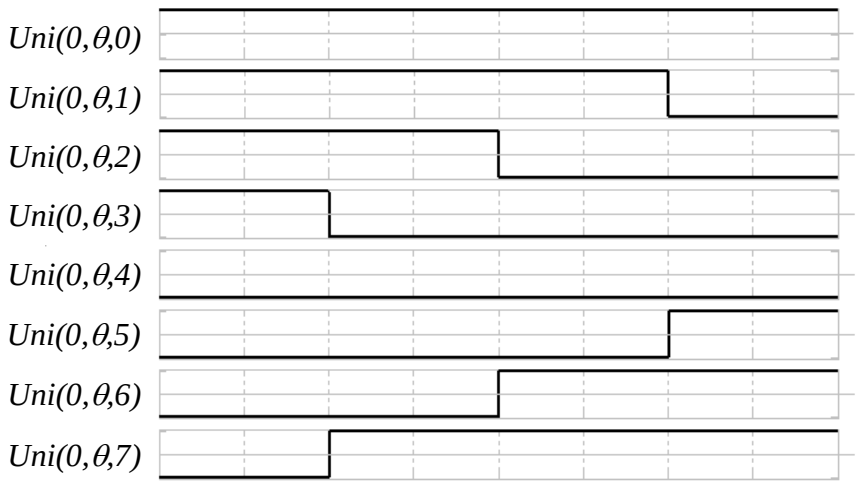


Рис. 5.1. Унітарні функції нульового порядку.

Неортогональність системи унітарних функцій зумовлює некомпактне пакування кодових елементів системи, що приводить до значної надлишковості інформаційних потоків. Внаслідок неортогональності та відсутності досліджень властивостей система не використовується як основа ТЧП.

Породжуючу кодову матрицю унітарного коду розміру $N\times N$ одержують при дискретизації з інтервалом $1/N$ за параметром часу перших $N=2^n$ із системи $2N$ унітарних функцій та здійсненні бінарної заміни значень функцій *1* на *0*, *–1* на *1* в точках $\theta_s = s/2^n$, $s=0,1,\ldots,2^n-1$, яка реалізується за допомогою операції

$$u_i = (1 - Uni(0,\theta_s, 2^n - 1 - i))/2, \quad (5.8)$$

де $u_0, u_1, \ldots, u_i, \ldots, u_{2^n-1}$ – значення розрядів унітарного коду θ_s, $i=0,1,\ldots,2^n-1$.

Для прикладу, при $n=3$ восьми функціям відповідають такі елементи кодової матриці

$$\begin{aligned}
Uni(0,\theta,0) &\rightarrow 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\\
Uni(0,\theta,1) &\rightarrow 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\\
Uni(0,\theta,2) &\rightarrow 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\\
Uni(0,\theta,3) &\rightarrow 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\\
Uni(0,\theta,4) &\rightarrow 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\\
Uni(0,\theta,5) &\rightarrow 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\\
Uni(0,\theta,6) &\rightarrow 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1\\
Uni(0,\theta,7) &\rightarrow 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1
\end{aligned}$$

Наведені властивості системи унітарних функцій дозволяють у наступних викладках визначити процедури перетворення до інших базисів. У ролі первинних при перетворенні форми інформації та при переході від N-розрядних унітарних до кодів із меншою розрядністю також використовуються розрядно-позиційні коди.

2. Функції Хаара та розрядно-позиційні коди.

Основою розрядно-позиційних кодів є система функцій Хаара. Функції Хаара $Har(n,\theta,j)$ (рис.1.2) визначаються за формулою:

$$Har(n,\theta,j) = \begin{cases} 2^{\frac{n-1}{2}}\, sign(\sin 2^n \pi\theta), & \frac{j}{2^{n-1}} \le \theta < \frac{j+1}{2^{n-1}}, \\ 0 \quad \text{їðè}\ \ ^3\text{íøèõ}\ \ \theta \in [0,1), \end{cases} \quad (5.9)$$

де $n = 0,1,\ldots,\log_2 N$; $j = 0,1,\ldots,2^{n-1}-1$; ($j=0$ при $n=0$), $0 \le \theta < 1$.

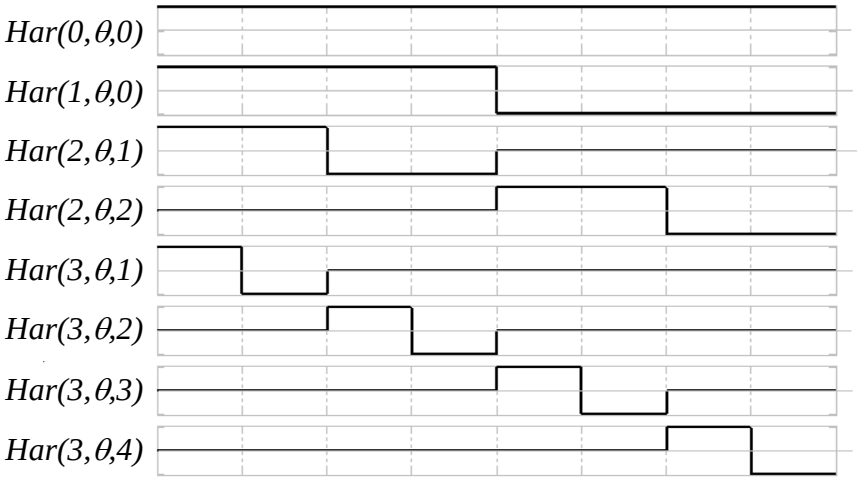


Рис.5.2. Система функцій Хаара.

При реалізації ТЧП використовуються наступні властивості системи Хаара.

1. Функції Хаара $\{Har(n,\theta, j)\}$ утворюють повну ортонормовану систему в просторі інтегровних із квадратом функцій $L_2[0,1)$, що дає можливість використовувати систему в якості базису для виконання ортогонального перетворення, яке є вейвлет-перетворенням.

2. На значній частині інтервалу визначення функції дорівнюють нулю, що дає можливість скоротити кількість арифметичних операцій при обчисленні перетворення. У результаті зменшується час обробки інформації.

Ненормований базис Хаара $\{sign(\sin 2^n \pi\theta)\}$ (без нормуючого множника $2^{\frac{n-1}{2}}$), в якому функції набувають значень ±1, 0, є основою розрядно-позиційних кодів. Розрядно-позиційні коди застосовуються в засобах перетворення форми інформації, в якості проміжних при аналогово-цифровому перетворенні, в давачах переміщень, для ініціювання комірок пам'яті тощо.

Для встановлення аналітичних співвідношень зв'язку систем функцій, які лежать в основі перетворення даних із розрядно-позиційного коду та в розрядно-позиційний код, використовуються розрядно-позиційні функції

$$RP(i,\theta) = \begin{cases} -1, \frac{i}{2^n} \le \theta \le \frac{i+1}{2^n}, \\ 1 \ при\ інших\ \theta \in [0,1], \end{cases} \qquad (5.10)$$

$n = 0,1,2,\ldots,\ i = 0,1,\ldots,2^n - 1$.

Дискретне подання 2^n розрядно-позиційних функцій та бінарна заміна значень функцій *1* на *0*, *–1* на *1*, яка подається за допомогою виразу

$$p_i = (1 - RP(i,\theta_s))/2 = \frac{1}{2^{n/2}} Har(n+1,\theta_s, i-1), \qquad (5.11)$$

де p_i – значення розрядів розрядно-позиційного коду,
породжує кодову матрицю

$$\begin{array}{cccccccc} 0 & 0 & 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & 0 & 0 & \ldots & 1 & 0 \\ \hline 0 & 1 & 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & 0 & 0 & \ldots & 0 & 0 \end{array}$$

За умови простої реалізації перетворення інформації унітарному та розрядно-позиційному кодам властивий недолік необхідності використання повної *N*-розрядної шини кодового подання даних для кодування *N* дискретних повідомлень. Це зумовлює необхідність переходу до ефективніших методів кодування зі зменшеною розрядністю кодів до $n = log_2 N$ в системах Радемахера та Грея.

В якості проміжних при переході до *n*-розрядних кодів використовуються коди Лібова-Крейга, які дозволяють у два рази зменшити розрядність коду та характеризуються властивістю абсолютного позиціонування.

3. Дискретно-фазові функції та коди Лібова-Крейга.

Залежність унітарних кодів з іншими встановлюється за допомогою системи дискретно-фазових функцій, що є основою кодів Лібова-Крейга.

Дискретно-фазові функції порядку m подаються згідно наступного аналітичного виразу

$$Dyf(m,\theta,i) = sign(\sin(2^m \pi(\theta + i \cdot 2^{-n}))), \qquad (5.12)$$

де $i = 0,\ 1,\ldots,\ 2^{n-m+1}\text{-}1$ – порядковий номер функції в наборі порядку m.

Графіки дискретно-фазових функцій першого порядку наведені на рис.5.3.

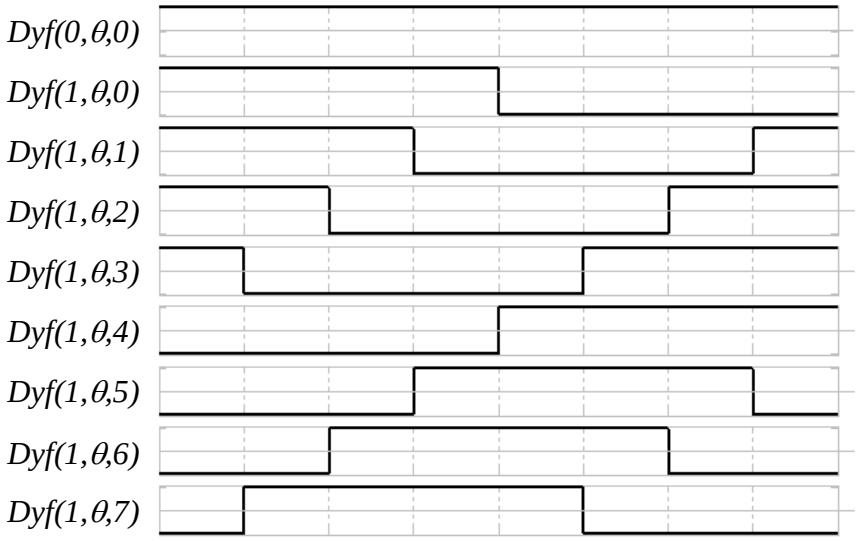


Рис.5.3. Дискретно-фазові функції першого порядку.

Властивості дискретно-фазових функцій:

1. Система з N дискретно-фазових функцій є лінійно залежною, оскільки частина функцій системи є лінійною комбінацією інших функцій системи

$$Dyf\,(m,\theta,\, j+2^{n-m}) = -Dyf\,(m,\theta,\, j)\,,$$

де $j = 0,1,\ldots,2^{n-m}-1$.

Внаслідок лінійної залежності перші N функцій не утворюють повної системи.

2. Система є неортогональною, тому що $\int_0^1 Dyf\,(m,\theta,i)\,Dyf\,(m,\theta,\, j)\,d\theta \neq 0$.

Породжуючу кодову матрицю розміру $\frac{N}{2}\times N$ одержують за допомогою дискретизації перших $N=2^{n-1}$ дискретно-фазових функцій порядку m та здійснення бінарної заміни значень функцій 1 на 0, –1 на 1, яка реалізується за формулою

$$d_j = (1 - Dyf\,(1,\theta_s,2^{n-1}-1-j))/2\,, \qquad (5.13)$$

де $d_0, d_1, \ldots, d_j, \ldots, d_{2^{n-1}-1}$ – значення розрядів коду Лібова-Крейга $\theta_s = \frac{s}{2^n}$, $s=0,1,\ldots,2^n-1$.

Наприклад, при N=8 елементи матриці відповідатимуть таким функціям

$$\begin{array}{lcccccccc}
Dyf\,(1,\theta,0) & \to & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1\\
Dyf\,(1,\theta,1) & \to & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0\\
Dyf\,(1,\theta,2) & \to & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0\\
Dyf\,(1,\theta,3) & \to & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0\\
s & \to & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7.
\end{array}$$

Внаслідок неповноти, система не використовується як основа для ортогональних ТЧП. Дискретно-фазові функції розглядаються як перехідні та як основа творення базисів і систем функцій Радемахера, Грея, кодування даних в яких здійснюється з розрядністю $n = log_2 N$ порівняно з N для унітарних кодів. Із цією метою в складі системи дискретно-фазових функцій виокремлюють дві підсистеми функцій виду $sign(sin(2^n \pi\theta))$ та $sign(cos(2^n \pi\theta))$.

4. Система функцій Радемахера та двійкові коди.

Екстракція *sin*-складових набору дискретно-фазових функцій утворює систему функцій Радемахера (рис. 5.4).

$$Rad(n,\theta) = Dyf(n,\theta,0) = sign(\sin(2^n \pi\theta)). \quad (5.14)$$

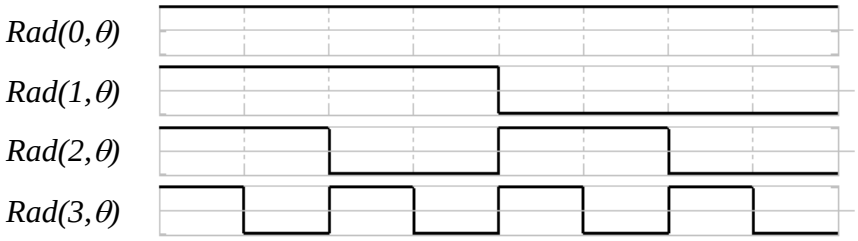


Рис.5.4. Функції Радемахера.

Система Радемахера є основою двійкової системи числення.

Відповідність між значеннями функцій у точках $\theta_s = s/2^n$, $s=0,1,\ldots,2^n-1$ та їх поданням у двійковому коді $\theta_s = r_n r_{n-1} \ldots r_0$ встановлюється співвідношенням

$$r_k = (1 - Rad(n-k,\theta_s))/2, \quad (5.15)$$

де r_k – значення розрядів двійкового коду, $k = 0,1,\ldots,n$.

Наприклад, при $n=3$ чотирьом функціям відповідають такі елементи кодової матриці розміру 4×8

$$\begin{array}{lcccccccc}
Rad(0,\theta) & \to & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
Rad(1,\theta) & \to & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
Rad(2,\theta) & \to & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
Rad(3,\theta) & \to & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
s & \to & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7.
\end{array}$$

Наступні властивості системи Радемахера:

- функції Радемахера ортонормовані на відрізку $[0,1)$, оскільки

$$\int_0^1 Rad(n,\theta)Rad(k,\theta)d\theta = 0 \text{ та } \int_0^1 Rad(n,\theta)Rad(n,\theta)d\theta = 1.$$

- система функцій Радемахера утворює в просторі інтегровних із квадратом функцій $L_2[0,1)$ неповну систему ортонормованих функцій, оскільки для довільного n не виконується означення повноти системи

$$\int_0^1 Rad(n,\theta)Rad(1,\theta)Rad(2,\theta)d\theta = 0,$$

тобто існує функція $Rad(1,\theta)Rad(2,\theta)$, яка тотожно не дорівнює нулю на інтервалі $[0,1)$ та ортогональна до всіх функцій системи.

Неповнота системи Радемахера обмежує її застосування для подання інформаційних потоків на основі ортогональних перетворень. Одночасно із широким застосуванням, створенням за допомогою системи Радемахера двійковим кодам властивий недолік, що полягає в неоднозначності формування відліків суміжних кодів при міжрозрядному позиціонуванні. Уникнути такої вади дозволяє перехід до кодів Грея

5. Система функцій Грея та коди Грея.

Екстракція *cos*-складових згідно кожного з порядків n набору дискретно-фазових функцій утворює систему функцій Грея. Система функцій Грея є підмножиною системи дискретно-фазових функцій

$$Gry(0,\theta) = Dyf(0,\theta + 2^{-1},0);$$

$$Gry(m,\theta) = Dyf(m,\theta,2^{n-m-1}),\ m = 1,2,\ldots,n. \quad (5.16)$$

Графіки функцій Грея наведено на рис.5.5.

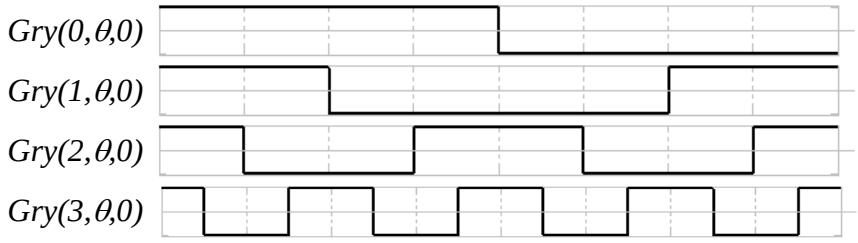


Рис.5.5. Функції Грея.

Система функцій Грея є ортонормованою та неповною, що доводиться наступними викладками.

Відомо, що система Грея є складовою підсистемою функцій Уолша. Оскільки система функцій Уолша є ортонормованою, то і функції Грея, як її підсистема, є ортонормованими, тобто $\int_0^1 Gry(n,\theta)Gry(k,\theta)d\theta = 0$, $\int_0^1 Gry(k,\theta)Gry(k,\theta)d\theta = 1$.

Функції Грея утворюють у $L_2[0,1)$ неповну систему, оскільки існують функції, які тотожно не дорівнюють нулю та ортогональні до всіх функцій системи, зокрема, для довільного n $\int_0^1 Gry(n,\theta)Rad(2,\theta)d\theta = 0$.

Неповнота системи Грея обмежує її застосування для розкладання інформаційних потоків та реалізації ТЧП.

Розширення функціональних можливостей при реалізації системних функцій перетворення форми та обробки інформації забезпечує перехід до базису Уолша. Аналітичні залежності процедури переходу базуються на наступній властивості скінченних добутків функцій системи Грея.

Якщо $(k_1,\ldots, k_m)$ і $(l_1,\ldots, l_r)$ дві різні скінченні послідовності, то

$$\int_0^1 [Gry(k_1,\theta)\ldots Gry(k_m,\theta)][Gry(l_1,\theta)\ldots Gry(l_r,\theta)]d\theta = 0. \qquad (5.17)$$

Для доведення властивості необхідно перепозначити множники в підінтегральному виразі $Gry(j_1, \theta), Gry(j_2, \theta),\ldots, Gry(j_p, \theta)$ $(j_1<j_2<\ldots<j_p)$. Добуток пар функцій $Gry(j_k, \theta)Gry(j_k, \theta)=1$. Добуток інших множників $Gry(j_1, \theta)\ Gry(j_2, \theta)\ldots\ Gry(j_{p-1}, \theta)$ є частково-сталою функцією, кожний з інтервалів сталості якої можна поділити на парне число рівних підінтервалів, на яких $Gry(j_p,\theta)$ набуває почергово значення $+1$ і -1 або -1 і $+1$. Із врахуванням чого

$$\int_0^1 [Gry(j_1,\theta)\ldots Gry(j_p,\theta)]d\theta = const\int_I Gry(j_p,\theta)d\theta = 0,$$

а тому буде рівним нулю значення інтегралу на інтервалі $[0;1)$. Тобто два різні добутки функцій системи є ортогональними, що і треба довести.

Система функцій Грея є основою кодів Грея. Відповідність між значеннями функцій у точках $\theta_s = s/2^n$, $s=0,1,\ldots,2^n-1$ та їх поданням у коді Грея $\theta_s = h_n h_{n-1}\ldots h_0$ встановлюється співвідношенням

$$h_k = (1 - Gry(n-k-1,\theta_s))/2, \qquad (5.18)$$

де $k = 0,1,\ldots,n-1$.

Наприклад, чотирьом функціям відповідають елементи кодової матриці розміру 4×8

$$
\begin{array}{lcccccccc}
Gry(0,\theta) & \to & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
Gry(1,\theta) & \to & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
Gry(2,\theta) & \to & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
Gry(3,\theta) & \to & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
s & \to & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7.
\end{array}
$$

Кодування Грея дозволяє зменшити похибки формування відліків суміжних кодів унаслідок зміни тільки одного розряду порівняно із застосуванням двійкових кодів. Однак, неповнота систем функцій Радемахера та Грея звужує галузі їх ефективного застосування. Розширення функціональних можливостей при реалізації системних функцій перетворення форми та обробки інформації забезпечує базис Уолша.

6. Система функцій Уолша.

Властивості систем Радемахера, Грея та відповідних кодів визначають процедуру переходу в базис Уолша $Wal(i,\theta)$, $i = 0,1,\ldots,2^n - 1$, впорядкований за Уолшем, із системи Радемахера $Rad(n,\theta)$. Функції Уолша $Wal(i,\theta)$ (рис.5.6) визначаються, як добуток функцій Радемахера

$$Wal(i,\theta) = Rad(1,\theta)^{b_0}\, Rad(2,\theta)^{b_1} \ldots Rad(n,\theta)^{b_{n-1}} = \prod_{k=0}^{n-1} (Rad(k+1,\theta))^{b_k}\,, \qquad (5.19)$$

де $i = b_{n-1}b_{n-2}\ldots b_1 b_0$ – подання в коді Грея порядкового номера функції $Wal(i,\theta)$.

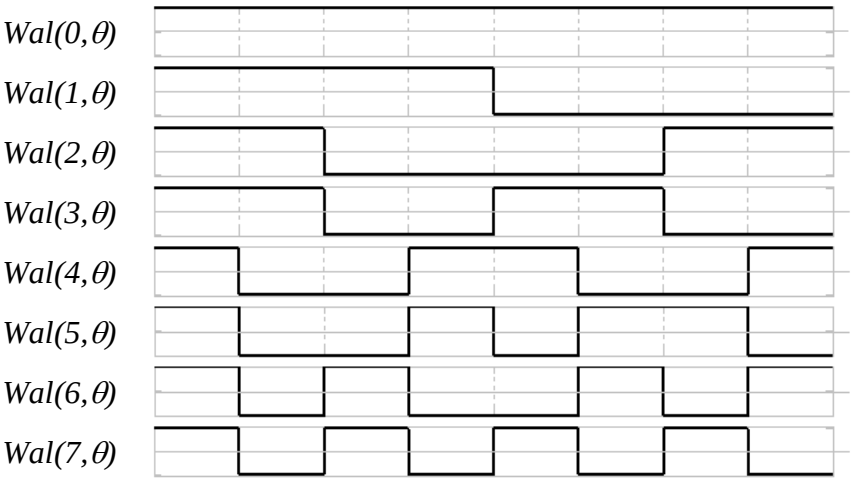


Рис.5.6. Система функцій Уолша.

Система функцій Уолша є ортонормованою, повною та мультиплікативною.

Функції Уолша ортонормовані на інтервалі $0 \le \theta \le 1$

$$\int_0^1 Wal(k,\theta)Wal(i,\theta)d\theta = \begin{cases} 1 \ при\ k = i, \\ 0 \ при\ k \ne i. \end{cases}$$

Функції Уолша утворюють мультиплікативну систему

$$Wal(k,\theta)Wal(i,\theta) = Wal(k \oplus i,\theta)\,.$$

Системи Радемахера та Грея є підсистемами функцій Уолша

$$Wal\,(2^n{-}1,\theta) = Rad(n,\theta),$$

$$Wal\,(2^n,\theta) = Gry(n,\theta).$$

Відомі схеми генераторів функцій Уолша базуються на методі формування функцій Уолша із системи Радемахера, але використання в ньому двійкового коду зумовлює виникнення помилки неоднозначності. З властивості ортогональності добутків функцій Грея розроблено альтернативний метод формування функцій Уолша із системи функцій Грея:

$$Wal(i,\theta) = Gry(0,\theta)^{a_0}\, Gry(1,\theta)^{a_1} \ldots Gry(n\text{-}1,\theta)^{a_{n-1}} = \prod_{k=0}^{n-1} (Gry(k\theta))^{a_k}\,, \tag{5.20}$$

де $i = a_{n-1}a_{n-2}\ldots a_1 a_0$ – подання в двійковому коді порядкового номера функції Уолша *Wal*(*i*,θ).

У відомих генераторах і перетворювачах функції Уолша формуються згідно (5.19) на основі двійкового коду наступним способом. Функції Радемахера відповідають значенням розрядів двійкового коду

$$Rad(m,\theta_s) = \overline{r_{n-m}} \text{-} r_{n-m} = \begin{cases} 1, & якщо\ r_{n-m} = 0, \\ -1, & якщо\ r_{n-m} = 1, \end{cases} \tag{5.21}$$

де r_m – значення *m*-го розряду двійкового коду аргумента θ_s, *m=0,1,...,n*.

При підстановці (5.21) у вираз (5.19) функції Уолша визначаються на основі двійкового коду аргументу θ_s

$$Wal(i,\theta_s) = (\overline{r_{n-1}} - r_{n-1})^{b_0} (\overline{r_{n-2}} - r_{n-2})^{b_{n1}} \ldots (\overline{r_0} - r_0)^{b_{n-1}} =$$
$$= (\overline{b_0 r_{n-1} \oplus b_1 r_{n-2} \oplus \ldots \oplus b_{n-1} r_0}) - (b_0 r_{n-1} \oplus b_1 r_{n-2} \oplus \ldots \oplus b_{n-1} r_0) = \overline{\varphi_i}(\theta_s) - \varphi_i(\theta_s) \tag{5.22}$$

де $\varphi_i(\theta_s) = b_0 r_{n-1} \oplus b_1 r_{n-2} \oplus \ldots \oplus b_{n-1} r_0$.

Із використанням наведеної методики можна визначити спосіб формування функцій Уолша на основі аргумента, поданого в коді Грея.

Функції Грея $Gry(k,\theta_s)$ відповідають значенням *n* розрядів коду Грея θ_s згідно залежності

$$Gry(k,\theta_s) = \overline{h_{n-k-1}} \text{-} h_{n-k-1} = \begin{cases} 1, & якщо\ h_{n-k-1} = 0, \\ -1, & якщо\ h_{n-k-1} = 1, \end{cases} \tag{5.23}$$

де h_k – значення *k*-го розряду коду Грея аргумента θ_s; $k = 0,1,\ldots,n-1$.

Функції Уолша визначаються при підстановці функцій Грея з (5.19) у (5.16)

$$Wal(i,\theta_s) = (\overline{h_{n-1}} - h_{n-1})^{a_0} (\overline{h_{n-2}} - h_{n-2})^{a_1} \ldots (\overline{h_0} - h_0)^{a_{n-1}}\,,$$

де $\theta_s = h_{n-1}\ldots h_1 h_0$ – код Грея, $i = a_{n-1}a_{n-2}\ldots a_0$ – подання у двійковому коді числа *i*.

Перетворення добутку в правій частині рівності з використанням основних тотожних співвідношень булевої алгебри дозволяє визначити функції Уолша

$$Wal(i, \xi) = (\overline{a_0 h_{n-1} \oplus a_1 h_{n-2} \oplus \ldots \oplus a_{n-1} h_0}) - (a_0 h_{n-1} \oplus a_1 h_{n-2} \oplus \ldots \oplus a_{n-1} h_0), \tag{5.24}$$

$$Wal(i, \xi) = \overline{\varphi_i}(\theta_s) - \varphi_i(\theta_s), \tag{5.25}$$

де $\varphi_i(\theta_s) = a_0 h_{n-1} \oplus a_1 h_{n-2} \oplus \ldots \oplus a_{n-1} h_0$.

Перевагою перетворювача на основі (5.20) є використання кодів Грея, які дозволяють зменшити помилки в засобах перетворення та обробки.

Таким чином, повна система Уолша, яка утворюється із систем Радемахера та Грея, є базисом для виконання ортогональних перетворень і формування функцій Ґалуа.

7. Система функцій Ґалуа та кодові системи Ґалуа.

Перехід до різних упорядкувань функцій у системі Ґалуа здійснюється з базису Уолша з упорядкуванням функцій за рекурсивним законом. За *n*-розрядними фрагментами рекурсивної послідовності, яка утворюється відповідно до породжуючого вектора поля Ґалуа $GF(2^n)$, згідно відображення через систему функцій Радемахера формуються номери функцій Уолша та Ґалуа в системі.

Наприклад, у полі $GF(2^3)$ існують породжуючі вектори 1011 та 1101. Для даного поля $GF(2^3)$ рекурсивні послідовності $v_0, v_1, v_2, v_3, v_4, \ldots$ формуються з початкового вектора $(v_0 v_1 v_2) = (111)$ за правилами:

1) $1101 \rightarrow v_{i+3} = v_i \oplus v_{i+1}$: $v_0, v_1, v_2, v_0 \oplus v_1, v_1 \oplus v_2, v_0 \oplus v_1 \oplus v_2, v_0 \oplus v_2, v_0, v_1, v_2, \ldots$;

2) $1011 \rightarrow v_{i+3} = v_i \oplus v_{i+2}$: $v_0, v_1, v_2, v_0 \oplus v_2, v_0 \oplus v_1 \oplus v_2, v_0 \oplus v_1, v_1 \oplus v_2, v_0, v_1, v_2, \ldots$.

Для початкового вектора $(v_0 v_1 v_2) = (111)$ утворена на основі породжуючого вектора 1101 рекурсивна послідовність {0 0 0 1 0 1 1 1}, визначає наступне рекурсивне впорядкування номерів функцій Уолша в системі {0 1 2 5 3 7 6 4}.

$$
\begin{array}{cccccccccc}
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & & & & & & \rightarrow & 0 \\
 & 0 & 0 & 1 & & & & & \rightarrow & 1 \\
 & & 0 & 1 & 0 & & & & \rightarrow & 2 \\
 & & & 1 & 0 & 1 & & & \rightarrow & 5 \\
 & & & & 0 & 1 & 1 & & \rightarrow & 3 \\
 & & & & & 1 & 1 & 1 & \rightarrow & 7 \\
 & & & & & & 1 & 1 & 0 & \rightarrow & 6 \\
 & & & & & & & 1 & 0 & 0 & \rightarrow & 4
\end{array}
$$

Утворена на основі породжуючого вектора 1011 рекурсивна послідовність {0 0 0 1 1 1 0 1} визначає інше рекурсивне впорядкування номерів функцій Уолша: {0 1 3 7 6 5 2 4}.

Із рекурсивно впорядкованої системи Уолша відповідно впорядковані перші *n* функцій Ґалуа формуються згідно співвідношення

$$Gal(n,\theta,i) = Wal(Ent(2^n\theta), \frac{2^{i+1}-1}{2^n}), \qquad (5.26)$$

де $i = 0,1,\ldots,2^n - 1$, *Ent*– функція виділення цілої частини.

Проведені дослідження встановили можливість формування функцій Ґалуа із систем Радемахера та Грея. Згідно співвідношень (5.18) та (5.19) перші *n* функцій Ґалуа в системі подаються у вигляді добутку функцій Радемахера та Грея

$$Gal(n,\theta,i) = \prod_{k=0}^{n-1} (Rad(k+1, \frac{2^{i+1}-1}{2^n}))^{h_k} = \prod_{k=0}^{n-1} (Gry(k+1, \frac{2^{i+1}-1}{2^n}))^{r_k}, \qquad (5.27)$$

де $h_{n-1}h_{n-2}\ldots h_0$ – запис у коді Грея числа *q*, двійковий код якого є *n*-розрядним фрагментом $v_i v_{i+1} v_{i+2} \ldots v_{i+n-1}$ рекурсивної послідовності $v_0, v_1, v_2, \ldots$; $r_{n-1}r_{n-2}\ldots r_0$ – двійковий код, який є *n*-розрядним фрагментом $v_i v_{i+1} v_{i+2} \ldots v_{i+n-1}$ рекурсивної послідовності $v_0, v_1, v_2, \ldots$.

Повний набір 2^n функцій рекурсивної системи Ґалуа $Gal(n,\theta,i)$ отримують із перших n функцій системи процедурою рекурсивного зсуву на $\Delta\theta = \frac{1}{2^n}$ згідно другої діагоналі кожної наступної функції відносно попередньої

$$Gal(n,\theta,i+1) = Gal(n,\theta+\Delta\theta,i)\,. \tag{5.28}$$

Впорядкування функцій Ґалуа в наборі відповідає синтезованому за породжуючим вектором упорядкуванню функцій Уолша.

Процедура переходу від дискретних значень функцій Уолша до дискретних значень функцій Ґалуа подається матричною операцією

$$\|Gal\| = \|W\| \cdot \|R\|,$$

де $\|Gal\|$ – матриця розміру $N\times n$ системи Ґалуа; $\|W\|$ – матриця розміру $N\times N$ рекурсивно впорядкованих функцій Уолша; $\|R\|$ – матриця розміру $N\times n$ відображеної вагової мережі Радемахера.

Для прикладу, матрична операція переходу від функцій Уолша до функцій Ґалуа та матриця розміру 8×8 дискретних значень функцій Ґалуа в полі $GF(2^3)$ з породжуючим вектором 1101 згідно процедури рекурсивного розширення подаються відповідно

$$\begin{Vmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \end{Vmatrix} \cdot \begin{Vmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{Vmatrix} = \begin{Vmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & -1 \\ 1 & -1 & -1 \\ -1 & -1 & -1 \\ -1 & -1 & 1 \\ -1 & 1 & 1 \end{Vmatrix} \longrightarrow \begin{Vmatrix} 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 \end{Vmatrix}.$$

Графіки функцій Ґалуа $Gal(n,\theta,i)$ з породжуючим вектором 1101 при $n=3$ наведено на рис.5.7.

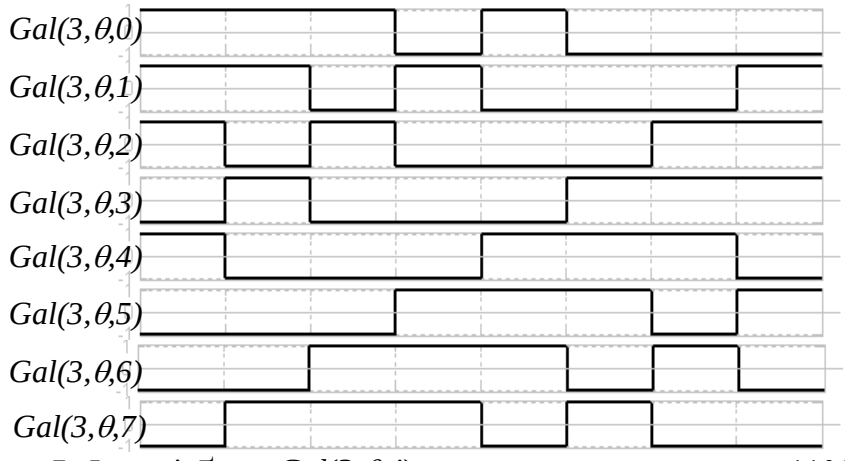


Рис.5.7. Функції Ґалуа $Gal(3,\theta,i)$ з породжуючим вектором 1101.

При виконанні перетворень використовуються наступні властивості системи функцій Ґалуа.

1. У системі 2^n функцій n-го порядку кожна підсистема із n функцій $\{Gal(n,\theta,i), Gal(n,\theta,i+1), Gal(n,\theta,i+2),\ldots, Gal(n,\theta,i+n-1)\}$ ортогональна.

2. Симетрія індекса та аргумента. Елементи матриці системи Ґалуа симетричні відносно головної діагоналі

$$Gal(n,\theta_S,i) = Gal(n,\frac{i}{2^n},s),$$

де $i,s \in \{0,1,\ldots.2^n-1\}$.

Таким чином, матриці системи Ґалуа є ганкелевими антициклічними, оскільки при $i+j=k+l$ $G_{ij}=G_{kl}$. Якщо рекурсивний зсув у (1.24) здійснюється згідно головної діагоналі та у формулі (1.24) $\Delta\theta = -\frac{1}{2^n}$, то матриці є тоепліцевими циклічними (циркулянтними), оскільки $i+j=k+l$ $G_{ij}=G_{kl}$.

Міри довжин інтервалів, на яких $Gal(n,\theta_S,i)=1$ і $Gal(n,\theta_S,i)=-1$ однакові, отже

$$\int_0^1 Gal(n,\theta,i)d\theta = \sum_{s=0}^{2^n-1} Gal(n,\theta_s,i) = 0, \qquad (5.29)$$

тобто множина функцій Ґалуа задовольняє необхідну умову для вейвлет-функцій.

При дискретизації за параметром часу перших n функцій Ґалуа та здійсненні бінарної заміни значень функцій 1 на 0, –1 на 1, згідно виразу

$$g_k(\theta_s) = (1 - Gal(n-k-1,\theta_s))/2, \qquad (5.30)$$

одержують матрицю кодових елементів Ґалуа розміру $n \times N$, $k = 0,1,\ldots,n-1$.

Наприклад, при N=8 рядки матриці кодових елементів Ґалуа з породжуючим вектором 1101 відповідатимуть таким функціям

$Gal(3,\theta,0)$	$\rightarrow$	0	0	0	1	0	1	1	1
$Gal(3,\theta,1)$	$\rightarrow$	0	0	1	0	1	1	1	0
$Gal(3,\theta,2)$	$\rightarrow$	0	1	0	1	1	1	0	0
s	$\rightarrow$	0	1	2	3	4	5	6	7

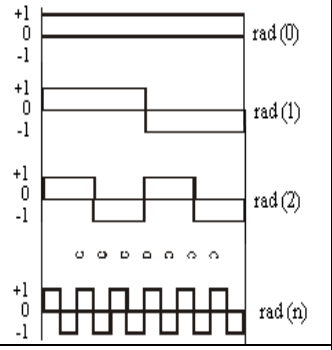
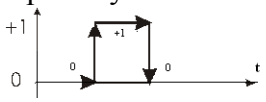
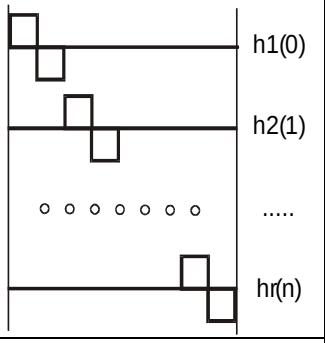
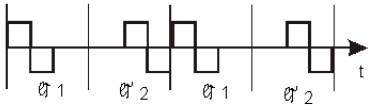
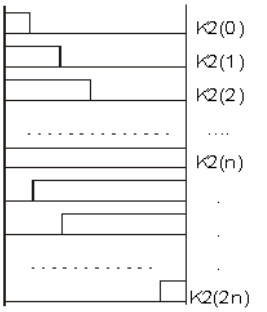
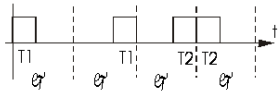
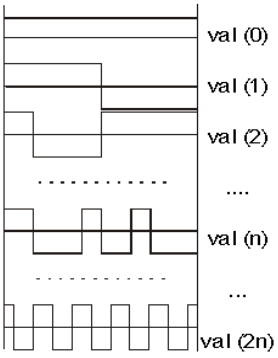
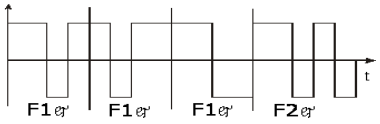
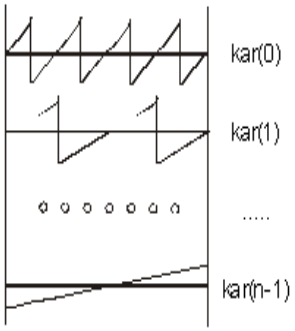
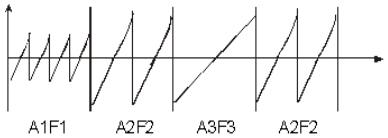
Елементи матриці кодових елементів Ґалуа з породжуючим вектором 1011 відповідатимуть наступним функціям

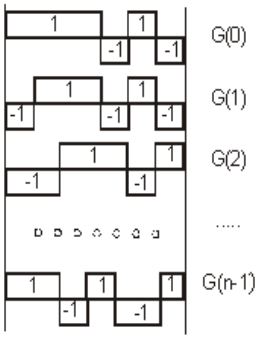
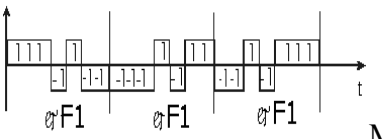
$Gal(3,\theta,0)$	$\rightarrow$	0	0	0	1	1	1	0	1
$Gal(3,\theta,1)$	$\rightarrow$	0	0	1	1	1	0	1	0
$Gal(3,\theta,2)$	$\rightarrow$	0	1	1	1	0	1	0	0
s	$\rightarrow$	0	1	2	3	4	5	6	7

При дискретизації системи N функцій Ґалуа $\{Gal(n,\theta,i)\}$, $i = 0,1,\ldots.2^n-1$ та перетворенні значень функцій згідно (5.30) отримують повну матрицю кодових елементів Ґалуа розміру $N \times N$, впорядкованих із поелементним рекурсивним зсувом згідно другої діагоналі матриці Ґалуа. Номер s повідомлення однозначно визначається n-координатним вектором $n = log_2 N$.

Представлення систем ортогональних функцій різних ТЧБ подані у табл.5.1.

Таблиця 5.1 – Представлення теоретико-числових базисів

Базис	Представлення базису	Базисна функція та об'єм матриці V	Модуляція сигналу та спектр
Рademахера		$Rad(n,\theta)=sign[2^n\pi\cdot\theta]$ $V=N\cdot\log_2 N$	Базисні функції Рademахера є основою для модуляції Прямокутних сигналів  Базис Рademахера породжує двійкову систему числення і двійкові коди
Хаара		$Har(n,\theta,i) =$ $= sign\left[\sin(i2^n\pi,\theta)\right]$ $V=N^2$	Використовується при фазовій модуляції сигналу.  В даному базисі використовуються розрядно-позиційні коди.
Крейга		$Crg(n,\theta)=sign[\sin((2^n-1)\cdot\pi\cdot\theta)]$ $V=\frac{N^2}{2}$	Породжує тривалісні і фазовіметоди модуляції сигналу. 
Уолша		Had (h,x) = $\prod_{i=1}^{\kappa}$[ri (x)]hi	Породжує частотно-фазові методи модуляції сигналу.  Базис Уолша має найбільш широкий спектр сигналу
Крестенсона		$N_i = res\sum_{i=1}^{n}(B_i\cdot b_i)\bmod P$ $V=\sum_{i=1}^{m}\log_2(P_i)$	Даний базис породжує амплітудно-частотні методи модуляції.  Базис представлений трикутними функціями. Спектр сигналів такого базису є експоненціальний.

Галуа		$N_j=f(C_{j-n-1},\dots C_{j-1},C_j)$, $C_j=\sum_{j=0}^{n=1} C_{j-1}\cdot A\cdot(\mathrm{mod}2)$ V=N	Базис Галуа породжує коди поля Галуа і систему числення Галуа.  M одуляція в базисі як фазова, так і частотна.

З метою оцінки ефективності кодування даних на основі різних ТЧБ доцільно провести аналіз кодових матриць, які породжують різні системи числення.

При цьому важливою характеристикою кожного базису є об'єм його кодової матриці M_j та число активних елементів m_j (рис.5.10), що визначає характеристики надлишковості представлення інформації на основі аналітичної оцінки

$$V_i = n_i \cdot N_i,$$

де n_j – розрядність числа; N_i – число незалежних кодових значень.

$$M_{Uni}=\begin{vmatrix} 0&0&0&\dots&0&0\\ 1&0&0&\dots&0&0\\ 1&1&0&\dots&0&0\\ 1&1&1&\dots&0&0\\ \dots&\dots&\dots&\dots&\dots&\dots\\ 1&1&1&\dots&1&0\\ 1&1&1&\dots&1&1 \end{vmatrix}$$ *а)*

$$M_{har}=\begin{vmatrix} 0&0&0&\dots&0&0\\ 1&0&0&\dots&0&0\\ 0&1&0&\dots&0&0\\ 0&0&1&\dots&0&0\\ \dots&\dots&\dots&\dots&\dots&\dots\\ 0&0&0&\dots&1&0\\ 0&0&0&\dots&0&1 \end{vmatrix}$$ *б)*

$$M_{Gr}=\begin{vmatrix} 0&0&0&\dots&0&0&0\\ 0&0&0&\dots&0&0&1\\ 0&0&0&\dots&0&1&1\\ \dots&\dots&\dots&\dots&\dots&\dots&\dots\\ 1&1&1&\dots&1&1&1\\ 1&1&1&\dots&1&1&0\\ 1&1&1&\dots&0&1&1\\ \dots&\dots&\dots&\dots&\dots&\dots&\dots\\ 1&0&0&\dots&0&0&0 \end{vmatrix}$$ *в)*

$$M_{Rad}=\begin{vmatrix} 0&0&0&0&0&0\\ 0&0&0&\dots&0&1\\ 0&0&0&\dots&1&0\\ 0&0&0&\dots&1&1\\ \dots&\dots&\dots&\dots&\dots&\dots\\ 1&0&0&\dots&0&0\\ 1&0&0&\dots&0&1\\ 1&0&0&\dots&1&0\\ \dots&\dots&\dots&\dots&\dots&\dots\\ 1&1&1&\dots&1&0\\ 1&1&1&\dots&1&1 \end{vmatrix}$$ *г)*

$$M_{LibCr}=\begin{vmatrix} 0&0&0&\dots&0&0\\ 1&0&0&\dots&0&0\\ 1&1&0&\dots&0&0\\ \dots&\dots&\dots&\dots&\dots&\dots\\ 1&1&1&\dots&1&0\\ 1&1&1&\dots&1&1\\ 0&1&1&\dots&1&1\\ 0&0&1&\dots&1&1\\ \dots&\dots&\dots&\dots&\dots&\dots\\ 0&0&0&\dots&1&1\\ 0&0&0&\dots&0&1 \end{vmatrix}$$ *д)*

$$M_{Cres}=\begin{vmatrix} P_1&P_2&\dots&P_n\\ 0&0&\dots&0\\ 1&1&\dots&1\\ 2&2&\dots&2\\ 0&3&\dots&3\\ 1&4&\dots&4\\ 2&0&\dots&5\\ 0&1&\dots&6\\ \dots&\dots&\dots&\dots\\ a_1&a_2&\dots&a_n \end{vmatrix}$$ *е)*

$$M_{Gal}=\begin{vmatrix} 1\\1\\1\\0\\1\\0\\0 \end{vmatrix}$$ *є)*

Рис.5.8. Кодові матриці дискретних базисів:
а) унітарного; б) Хаара; в) Грея; г) Радемахера; д) Крейга; е) Крестенсона; є) Галуа.

Кожен з названих базисів характеризується визначеним об'ємом кодової матриці для представлення даних. При цьому найбільш надлишковим базисом є унітарний, в якого кодова

матриця $V = N^2$, а число активних кодових елементів $n = N^2 / 2$, де N – діапазон кодування даних. Аналогічну надлишковість забезпечує базис Хаара, в два рази меншу надлишковість забезпечує базис Крейга, тобто $V = N^2 / 4$, а $n = N^2 / 8$. Максимально широке застосування для кодування даних в сучасних КС отримали базиси Радемахера та Крестенсона, в яких $V = N \log_2 N$. ДаФні базиси відповідно породжують двійкову систему числення та систему числення залишкових класів.

Базис Уолша максимально широко використовується в сучасних телекомунікаційних КС. Даний базис породжує систему ортогональних шумоподібних сигналів, які використовуються в сотових системах мобільного зв'язку.

Найменшу надлишковість кодування даних забезпечує базис Галуа, кодова матриця якого $V = N$, а $n = N / 2$.

Згідно викладеного, характеристики ТЧБ кодування даних, як системного об'єкта, подані в табл.5.2.

Таблиця 5.2–Характеристики потоків даних

Формувачі вхідних та вихідних інформаційних сигналів даних	Характеристики інформаційних потоків даних
Унітарний базис	$V = N^2;\ n = N^2 / 2$
Базис Хаара	$V = N^2,\ n = N$
Базис Крейга	$V = N^2 / 4,\ n = N^2 / 8$
Базис Радемахера	$V = N \cdot \log_2 N,\ n = \frac{N}{2} \log_2 N$
Базис Крестенсона	$V = N \cdot \log_2 N$
Базис Уолша	$V = N^2, n = N^2 / 2$
Базис Галуа	$V = N,\ n = N / 2$

СПД представлені швидкістю приймання, швидкістю передавання даних, імовірністю помилок, часом затримки в каналі

$$E_{СПД} = F(V_R, V_W, P_i, T),$$

де V_R – швидкість приймання даних, V_W – швидкість передавання даних, P_i – імовірність помилок, T – час затримки в каналі.

Способи кодування інформаційних потоків визначаються теоретико-числовими базисами (ТЧБ), які застосовуються для їх представлення [9,17, 20, 22]. Найбільш поширеними ТЧБ в сучасних КС є наступні: унітарний, Хаара, Грея, Радемахера, Крестенсона та Галуа.

Світовий досвід створення процесорів для комп'ютерних систем за останні 50 років, поряд з застосуванням теоретико-числового базису (ТЧБ) Радемахера, який породжує двійкову систему числення, демонструє тенденцію все ширшого застосування інших ТЧБ, в тому числі: унітарного, Хаара, Крестенсона та Галуа. Реалізація спеціалізованих, сигнальних, комутаційних та проблемно-орієнтованих процесорів цифрової обробки даних часто виконується на базі сумісного використання комбінацій названих ТЧБ, наприклад Радемахера-Хаара, Крестонсона-Галуа та ін.

Перспективним напрямком розвитку теорії та технологій побудови спеціалізованих програмно-апаратних комп'ютерних засобів є реалізація супершвидкодіючих мультибазисних RCG-процесорів на основі базисів Радемахера, Крестенсона і Галуа. Відомі успішні спроби розвитку теорії та техніки побудови матричних процесорів на основі двовимірних базисів Радемахера та Галуа, а також конвеєрних спецпроцесорів у базисі Галуа.

Спостережувані тенденції розвитку теорії методології та техніки процесорів комп'ютерних систем обумовлені теоретичним та ідейним насиченням можливостей застосування базису Радемахера для побудови арифметико-логічних компонентів процесорів,

до яких ставляться все жорсткіші вимоги щодо швидкодії, покращення регулярності структури та розширення функціональних можливостей.

У зв'язку з цим існує проблема глибокого дослідження характеристик «нерадемахівських» ТЧБ та граничних можливостей їх застосування для реалізації компонентів як спеціалізованих, так і універсальних процесорів. При цьому перспективним, крім найбільш сьогодні масового одновимірного (векторного) представлення чисел та виконання арифметико-логічних операцій у базисі Радемахера перспективним є застосування двовимірних систем числення, вертикальної інформаційної технології у базисі Галуа та різних форм багатовимірного представлення чисел у вигляді залишків різних форм системи залишкових класів базису Крестенсона [2, 50].

Тема 5.3 Числові послідовності та функції.

Найважливіші числові функції, що зустрічаються в теорії чисел

Числовими функціями називають такі функції, які набувають цілих значень або визначені для цілих значень аргументу.

Числова функція [x] і її застосування.

Важливу роль у теорії чисел відіграє функція $[x]$[2]; вона визначається для всіх дійсних x і є найбільшим цілим числом, що не перевищує x: $x-1<[x]\le x$. Ця функція називається *цілою частиною* від x (або антьє від x). Зокрема $[0]=0$, $[2]=2$, $[3{,}7]=3$, $[-1{,}2]=-2$, $\left[\sqrt{3}\right]=1$, $[-\pi]=-4$ і т. д. Отже, ця функція набуває тільки цілих значень при довільних дійсних значеннях аргументу x.

Очевидно маємо:

$$[x]\le x<[x]+1,$$

або

$$x=[x]+0,$$

де $0\le\theta<1.$

Число θ, визначене останньою формулою, називається *дробовою частиною* x і позначається символом $\{x\}$, так, що $\{x\}=x-[x]$; зокрема $\{2\}=0$, $\{1{,}7\}=0{,}7$, $\{2\}=0$, $\{2\}=0$, $\{-4{,}15\}=0{,}85$, $\left\{\sqrt{2}\right\}=\sqrt{2}-1$ і т. д.

За означенням $\{x\}$ є завжди невід'ємним числом, меншим від одиниці, тобто $0\le\{x\}<1.$

З означення функції $[x]$ випливають такі її основні властивості:

Властивість 1. *Якщо* $x=n+0$, *де* n *- ціле і* $0\le\theta<1$, *то* $n=[x]$.

Ця властивість випливає з нерівностей:

$0\le x-n<1$, або $x-1<n\le x$.

Властивість 2. $[a+b]\ge[a]+[b]$.

Справді, маємо:

$$a+b=[a]+[b]+\{a\}+\{b\}.$$

Тут можливі два випадки: по-перше, $0\le\{a\}+\{b\}<1$; тоді очевидно, що $[a+b]=[a]+[b]$; по-друге, $1\le\{a\}+\{b\}<2$; у цьому разі матимемо $[a+b]>[a]+[b]$. Отже, в будь-якому випадку

$$[a+b]\ge[a]+[b].$$

Приклади.

а) $\left[3\frac{1}{2}+5\frac{1}{4}\right]=\left[8\frac{3}{4}\right]=8$; $\left[3\frac{1}{2}\right]=3$, $\left[5\frac{1}{4}\right]=5$ і $\left[3\frac{1}{2}+5\frac{1}{4}\right]=\left[3\frac{1}{2}\right]+\left[5\frac{1}{4}\right]$;

[2] $[x]$ - позначення Гауса; Лежандр позначав цю функцію символом E_x.

б) $\left[1\frac{4}{5}+5\frac{5}{6}\right]=\left[7\frac{19}{30}\right]=7$, $\left[1\frac{4}{5}\right]=1$, $\left[5\frac{5}{6}\right]=5$ і $\left[1\frac{4}{5}+5\frac{5}{6}\right]>\left[1\frac{4}{5}\right]+\left[5\frac{5}{6}\right]$.

Властивість 3. *Якщо a - дійсне додатне число і b – натуральне число, то натуральних чисел, які не перевищують a і діляться на b, буде точно* $\left[\frac{a}{b}\right]$.

Справді, нехай числами, кратними b, і такими, що не перевищують a, будуть k чисел: $b,\ 2b,\ 3b\ldots\ ,\ kb$. Тоді буде справедлива нерівність: $kb\le a<(k+1)b$, звідки $k\le\frac{a}{b}<k+1$; тобто, ліва нерівність: $kb\le a<(k+1)b$, звідки $k\le\frac{a}{b}<k+1$, тобто, $k=\left[\frac{a}{b}\right]$.

Властивість 4. *Якщо* $a>0$ - *будь-яке ціле число і b – натуральне число,* то $\left[\frac{[a]}{b}\right]=\left[\frac{a}{b}\right]$.

Справді, між $[a]$ і a немає натуральних чисел і тому кількість чисел, кратних b, і таких, що не перевищують [a] і відповідно a, буде однаковою. За властивістю 3 в першому випадку їх буде, $\left[\frac{[a]}{b}\right]$, а в другому - $\left[\frac{a}{b}\right]$. Отже,

$\left[\frac{[a]}{b}\right]=\left[\frac{a}{b}\right]$.

Щоб показати важливість запровадженої функції, розглянемо приклади її застосувань.

Теорема 1. *Показник, з яким дане n росте число p входить до добутку n!, дорівнює:*

$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\ldots+\left[\frac{n}{p^k}\right]$, де $p^k\le n$,

але вже $p^k+1>n$. (Якщо вже $p<n$, то $n!$ зовсім не ділиться на p).

Справді, на підставі властивості 3, число співмножників добутку $n!=1\cdot2\cdot3\cdots n$, кратних p, дорівнюватиме $\frac{n}{p}$; ці співмножники будуть: $\mathrm{p},2\mathrm{p},\ldots\left[\frac{n}{p}\right]p$. Інші числа цього добутку на p не діляться. Отже, поява числа p в канонічному розкладі *n!* визначається добутком

$$M=p\cdot2p\cdot3p\cdots\left[\frac{n}{p}\right]p=p^{\left[\frac{n}{p}\right]}\cdot1\cdot2\cdot3\cdots\left[\frac{n}{p}\right].$$

Позначимо $\left[\frac{n}{p}\right]=n_1$, тоді $M=1\cdot2\cdot3\cdots n_1\cdot p^{n1}$. Серед множників $1,2\ldots n_1$ можуть бути числа, які діляться на $p:\ p,2p.3p.\ldots,\left[\frac{n_1}{p}\right]p$. Їх добуток дорівнює

$$1\cdot2\cdot3\cdots\frac{n_1}{p}\cdot p^{\frac{n_1}{p}}$$

або позначаючи через $n_2=\left[\frac{n_1}{p}\right]=\left[\frac{n}{p}:p\right]=\left[\frac{n}{p^2}\right]$ (див. властивість 4), дістанемо:

$$M=M_1\cdot1\cdot2\cdot3\cdots n_2\cdot p^{n_1+n_2},$$

де M_1 - добуток множників, що не діляться на p. Якщо $n_2<p$, то процес закінчено; якщо $n_2\ge p$, продовжуємо його далі.

Міркуючи аналогічно, дістанемо:

$$M = M_2 \cdot 1 \cdot 2 \cdot 3 \cdots n_3 \cdot p^{n_1+n_2+n_3},$$

де $n3 = \left[\frac{n_2}{p}\right] = \left[\frac{n}{p^3}\right]$

і т. д.

Очевидно, що цей процес скінчений, бо $n > n_1 > n_2 > \cdots$,

і при досить великому k виявиться, що $n_k < p$ і

$$\left[\frac{n_k}{p}\right] = \left[\frac{n}{p^{k+1}}\right] = 0.$$

Отже,

$$M = M_{k-1} \cdot 1 \cdot 2 \cdot 3 \cdots n_k \cdot p^{n_1+n_2+n_3+\ldots+n_k}$$

Серед множників 1,2,..., n_k немає таких, що діляться на p, бо $n_k < p$; M_{k-1} також не містить множників, кратних p, отже, до канонічного розкладу $n!$ просте число p ввійде з показником, який дорівнює:

$$n_1+n_2+\cdots+n_k = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^k}\right] = \sum_{s=1}^{k}\left[\frac{n}{p^s}\right]^3,$$

що й треба було довести.

На практиці обчислення краще проводити за формулою:

$n_s = \left[\frac{n_{s-1}}{p}\right]$, тобто $\left[\frac{n}{p_s}\right] = \left[\left[\frac{n}{p^{s-1}}\right] : p\right]$.

Приклад. Знайти показник степеня, з яким число 3 входить до добутку701!

Обчислення проводимо, згідно із зробленим зауваженням, за такою схемою:

701	3
233	3
77	3
25	3
8	3
2	

Додаючи частки знайдемо, що шуканий показник дорівнює $233+77+25+8+2=345$.

Зауваження. Ця теорема, очевидно, дає можливість знаходити канонічний розклад числа $n!$.

Приклад. Знайти канонічний розклад числа $30!=1\cdot2\cdot3\cdots30$.

Очевидно, що до канонічного розкладу $30!$ входять тільки прості числа, менші за 30. Знайдемо з якими показниками вони входитимуть до цього розкладу:

30	2
15	2
7	2
3	2
1	

[3] Зауважимо, що $\left[\frac{n}{p^s}\right] = 0$, якщо $s > k$. Отже замість скінченої суми $\sum_{s=1}^{k}\left[\frac{n}{p^s}\right]$ ми могли б написати нескінченну суму $\sum_{s=1}^{\infty}\left[\frac{n}{p^s}\right]$ і тоді про число k можна було б і не згадувати.

30	3
10	3
3	3
1	

30	5
6	5
1	

30	7
4	

30	11
1	

Маємо $30! = 2^{26} \cdot 3^{14} \cdot 5^7 \cdot 7^4 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29$.

Теорема 2. *Якщо* $a,b,...,l,n$ *- натуральні числа і* $n \geq a+b+....+l$, *то* $\frac{n!}{a!b!..l!}$ - *натуральне число.*

Доведення. Візьмемо довільне просте число $p \leq n$. До канонічного розкладу чисел $a,b,...,l$ воно ввійде з показниками степенів, що відповідно дорівнюють:

$$a = \left[\frac{a}{p}\right] + \left[\frac{a}{p^2}\right] + ...,$$

$$\beta = \left[\frac{b}{p}\right] + \left[\frac{b}{p^2}\right] + ...,$$

.....

$$\lambda = \left[\frac{l}{p}\right] + \left[\frac{l}{p^2}\right] + ...$$

Отже, до канонічного розкладу знаменника число p ввійде з показником степеня

$$\mu = \alpha + \beta + ... + \lambda = \left[\frac{a}{p}\right] + \left[\frac{b}{p}\right] + ... + \left[\frac{l}{p}\right] + \left[\frac{a}{p^2}\right] + \left[\frac{b}{p^2}\right] + ... + \left[\frac{l}{p^2}\right] + ...$$

До канонічного розкладу чисельника число p ввійде з показником степеня

$$\nu = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + ...$$

Оскільки $n \geq a+b+...+l$, то

$$\frac{n}{p} \geq \frac{a}{p} + \frac{b}{p} + ... + \frac{l}{p},$$

$$\frac{n}{p^2} \geq \frac{a}{p^2} + \frac{b}{p^2} + ... + \frac{l}{p^2},$$

.....

З останніх нерівностей дістанемо (властивість 2):

$$\left[\frac{n}{p}\right] \geq \left[\frac{a}{p} + \frac{b}{p} + ... + \frac{l}{p}\right] \geq \left[\frac{a}{p}\right] + \left[\frac{b}{p}\right] + ... + \left[\frac{l}{p}\right];$$

$$\left[\frac{n}{p^2}\right] \geq \left[\frac{a}{p^2} + \frac{b}{p^2} + ... + \frac{l}{p^2}\right] \geq \left[\frac{a}{p^2}\right] + \left[\frac{b}{p^2}\right] + ... + \left[\frac{l}{p^2}\right];$$

.....

Додаючи останні нерівності, бачимо, що $\nu \geq \mu$. Отже, після скорочення дробу $\frac{n!}{a!b!..l!}$ на p^μ канонічний розклад знаменника не міститиме p^μ. Але p - довільне просте число, що не перевищує n, тому канонічний розклад знаменника не міститиме простих чисел і знаменник дорівнюватиме 1; отже, розглядуваний дріб є натуральне число, що й треба було довести.

Приклад. *Якщо* $m > n$, то

$$\frac{n(n-1)\ldots(n-m+1)}{1\cdot 2\cdot 3\cdots m}=C_n^m$$

є натуральне число.

Справді, помножуючи чисельник і знаменник на $(n-m)!$, дістанемо $C_n^m=\frac{n!}{m!(n-m)!}$; оскільки $n=m+(n-m)$, то внаслідок доведеної теореми C_n^m є натуральним числом. Цим ми довели, не вдаючись до теорії сполук. Що біноміальні коефіцієнти є натуральними числами.

Формули для числа дільників і суми дільників даного числа

Особливо важливу роль у теорії чисел відіграють так званні мультиплікативні функції.

Функція $\theta(n)$ називається *мультиплікативною*, якщо: а) вона визначена для всіх натуральних n і не перетворюється в нуль хоч при одному такому значенні n; б) для довільних натурально взаємних простих n_1 і n_2 справедлива рівність:

$\theta(n_1\cdot n_2)=\theta(n_1)\cdot\theta(n_2)$[14].

Приклад. Функція $\theta(n)=n^s$, де s - будь-яке дійсне, або комплексне число, є мультиплікативною. Справді, навіть при довільних n_1 і n_2 маємо:

$\theta(n_1\cdot n_2)=(n_1n_2)^s=n_1^s\cdot n_2^s=\theta(n_1)\cdot\theta(n_2)$.

З означення мультиплікативної функції, зокрема, випливають такі її властивості:

Властивість 1. $\theta(1)=1$.

Справді, якщо $\theta(n_0)\neq 0$, тоді

$\theta(n_0)=\theta(n_0\cdot 1)=\theta(n_0)\theta(1)$.

Отже, $\theta(1)=1$.

Властивість 2. *Якщо* $\theta_1(n)$ *і* $\theta_2(n)$ - *мультиплікативні функції, то їх добуток також буде мультиплікативною функцією.*

Справді, позначаючи $\theta_0(n)=\theta_1(n)\cdot\theta_2(n)$, знаходимо:

$\theta_0(n)=\theta_1(n)\cdot\theta_2(n)=1$;

далі при $(n_1,n_2)=1$знаходимо:

$\theta_0(n_1n_2)=\theta_1(n_1n_2)\cdot\theta_2(n_1n_2)=\theta_1(n_1)\theta_1(n_2)\theta_2(n_1)\theta_2(n_2)=$

$=\left[\theta_1(n_1)\theta_2(n_1)\right]\left[\theta_1(n_2)\theta_2(n_2)\right]=\theta_0(n_1)\theta_0(n_2)$,

що й доводить наше твердження.

Властивість 3. *Якщо* $\theta(n)$ - *мультиплікативна функція, а* $n_1,n_2,\ldots n_s$ - попарно взаємно прості числа, то

$\theta(n_1,n_2,\ldots n_s)=\theta(n_1)\theta(n_2)\ldots\theta(n_s)$.

Справді, для $s=1$, 2 твердження справедливе; припустимо, що воно справедливе для $s-1$і доведемо його справедливість для s. Оскільки, $(n_i,n_j)=1$, при всіх $i\neq j$, за умовою, то $(n_1,n_2,\ldots,n_{s-1},n_s)=1$. За означенням мультиплікативної функції дістанемо: $\theta(n_1n_2\ldots n_{s-1},n_s)=\theta(n_1n_2\ldots n_{s-1})\theta(n_s)$; але за припущенням $\theta(n_1n_2\ldots n_{s-1})=\theta(n_1)\theta(n_2)\ldots\theta(n_{s-1})$, і справедливість цієї властивості стає очевидною.

Властивість 4. Нехай $\theta(n)$ - мультиплікативна функція і $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ - канонічний розклад числа n. Позначимо символом $\sum_{d/n}$ суму, поширену на всі натуральні

[14] Якщо ця рівність виконується для довільних натуральних n_1 і n_2, то кажуть також, що ця функція $\theta(n)$ цілком мультиплікативна, або мультиплікативна в широкому розумінні; ясно, що функція, мультиплікативна в широкому розумінні, тим більше буде мультиплікативною за нашим означенням (або, як іноді говорять, мультиплікативною в вузькому розумінні).

дільники d числа n (включаючи 1 і саме n). При цих позначеннях справедлива така тотожність, яка виражає *основну властивість мультиплікативних функцій:*

$$\sum_{d/n}\theta(d)=\left[1+\theta(p_1)+\ldots+\theta(p_1^{\alpha_1})\right]\cdots\left[1+\theta(p_k)+\ldots+\theta(p_k^{\alpha_k})\right] \qquad (5.31)$$

(у випадку $n=1$ вважаємо, що права частина дорівнює 1).

Для доведення цієї тотожності розкриємо дужки в її правій частині. Дістанемо суму доданків виду $\theta(p_1^{\beta_1})\cdot\theta(p_2^{\beta_2})\cdots\theta(p_k^{\beta_k})$, де $0\le\beta_i\le\alpha_i(i=1,2,\ldots,k)$, або внаслідок мультиплікативності цієї функції, $\theta(p_1^{\beta_1}p_2^{\beta_2}\ldots p_k^{\beta_k})=\theta(d)$, бо $p_1^{\beta_1}p_2^{\beta_2}\ldots p_k^{\beta_k}$ є не що інше, як дільники d числа n. З правила множення многочленна на многочлен випливає, що жоден такий доданок не буде пропущений і не повториться більше, ніж один раз. Тобто, матимемо вираз, що стоїть в лівій частині тотожності (1.27).

При $\theta(n)=n^S$ тотожність (1) набере вигляду:

$$\sum_{d/n}d^s=(1+p_1^s+p_1^{2s}+\ldots+p_1^{\alpha,s})\cdots(1+p_k^s+p_k^{2s}+\ldots+p_k^{\alpha,k^s})\,[5]. \qquad (5.32)$$

Зокрема при $s=1$ ліва частина тотожності (5.32) дасть *суму всіх натуральних дільників числа* n; позначаючи її через $S(n)$, матимемо:

$$S(n)=\sum_{d/n}d=(1+p_1+p_1^2+\ldots+p_1^{\alpha_1})\cdots(1+p_k+p_k^2+\ldots+p_k^{\alpha_k}). \qquad (5.32')$$

Спрощуючи праву частину, дістанемо:

$$S(n)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdots\frac{p_k^{\alpha_k+1}-1}{p_k-1}. \qquad (5.33)$$

Вважаючи в тотожності (1.28) $s=1$, бачимо, що її ліва частина при цьому визначає *число всіх натуральних дільників даного* n:

позначаючи його через $\tau(n)$, дістанемо:

$$\tau(n)=(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_k+1). \qquad (5.34)$$

Зауважимо, що розкривши дужки в правій частині тотожності (5.32'), ми матимемо всі дільники числа n.

Приклад. Знайти суму дільників, число дільників і самі дільники числа $680=2^3\cdot5\cdot17$.

$S(680)=\frac{2^{3+1}-1}{2-1}\cdot\frac{5^{1+1}-1}{5-1}\cdot\frac{17^{1+1}-1}{17-1}=1620;$

$\tau(680)=(3+1)(1+1)\ldots(1+1)=16.$

Самі дільники числа 680 знайдемо, розкривши дужки у виразі

$(1+2+4+8)(1+5)(1+17)$.

Матимемо:

1, 2, 4, 8, 5, 10, 20, 40, 17, 34, 68, 136, 85, 170, 340, 680.

Функції $\tau(n)$ і $S(n)$ - мультиплікативні.

Справді, якщо $(a,b)=1$ і $a=p_1^{a_1}p_2^{a_2}\ldots p_s^{a_s}$, і $b=q_1^{\beta_1},q_2^{\beta_2}\ldots q_t^{\beta_t}$ - канонічні розклади чисел a і b, то $p_1^{a_1}p_2^{a_2}\ldots p_s^{a_s}q_1^{\beta_1}q_2^{\beta_2}\ldots q_t^{\beta_t}$ - канонічний розклад числа ab і тоді дістанемо:

$$S(ab)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\ldots\frac{p_s^{\alpha_s+1}-1}{p_s-1}\cdot\frac{q_1^{\beta_1+1}-1}{q_1-1}\ldots\frac{q_t^{\beta_t+1}-1}{q_t-1}=S(a)S(b);$$

$$\tau(ab)=(\alpha_1+1)\ldots(\alpha_s+1)(\beta_1+1)\ldots(\beta_t+1)=\tau(a)\tau(b).$$

[5] Ця тотожність, між іншим, виражає суму $s-x$ степенів усіх натуральних дільників числа n.

Функції $S(n)$ і $\tau(n)$ є найпростішими прикладами мультиплікативних числових функцій; у них і аргумент, і значення функцій набувають тільки цілих додатних значень.

Функція Ейлера і її основні властивості

Функція Ейлера[6] $\varphi(n)$ визначається для всіх натуральних n *і являє собою кількість натуральних чисел, менших від* n *і взаємно простих з* n*;* при цьому припускається, що $\varphi(1)=1$.

Для невеликих значень n значення функції $\varphi(n)$ можна знайти простим підрахунком кількості чисел, менших від n і взаємно простих з n, наприклад, $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$, $\varphi(6)=2$, $\varphi(7)=6$, $\varphi(8)=4$, $\varphi(9)=6$ і т.д.

Визначимо значення $\varphi(n)$ для будь-якого натурального n.

Спочатку доведемо такі твердження.

Теорема 1. *Функція Ейлера мультиплікативна, тобто* $\varphi(m\cdot n)=\varphi(m)\cdot\varphi(n)$, якщо $(m,n)=1$. Щоб довести цю теорему, розмістимо числа від 1 до mn у вигляді такої таблиці:

Таблиця 1.5

1,	2,…,	r,…,	m,
$m+1$,	$m+2$,…,	$m+r$,…,	$2m$,
$2m+1$,	$2m+2$,…,	$2m+r$,…,	$3m$,
……			
$(n-1)m+1$	$(n-1)m+2$,	$(n-1)m+r$	$(n-1)m+m=mn$.

,

Визначимо тепер з таблиці 1.5 кількість чисел, взаємно простих з *mn*. Взаємно простими з добутком *mn* будуть ті і тільки ті числа. Які взаємно прості з *m*, так і з *n*. Тому відберемо з таблиці 1.5 спочатку всі числа, взаємно прості з *m*, а з них ті, які взаємно прості з *n*.

Числа одного стовпця або одночасно взаємні з *m*, або ні, бо $(r,m)=(m,km+r)$. Отже, можна говорити про «стовпці, взаємно простих з *m*» і визначити їх число за кількістю чисел, взаємно простих з *m* одного рядка, наприклад першого; тому кількість таких стовпців за означенням дорівнює $\varphi(m)$.

Розглянемо тепер будь-який стовпець таблиці 5.5, наприклад:

$$r, m+r, 2m+r, ..., (n-1)m+r. \tag{5.35}$$

Усього на цьому стовпці *n* чисел; покажемо, що всі вони при діленні на *n* даватимуть різні остачі. Справді, припустимо супротивне, тобто:

$$k_1m+r=nq_1+s \text{ і } k_2m+r=nq_2+s,$$

де k_1, k_2 і s - цілі невід'ємні , менші від *n*. Тоді віднімаючи від першої рівності другу, дістанемо: $(k_1-k_2)m=n(q_1-q_2)$. Остання рівність показує, що $(k_1-k_2)m:n$, але $(m,n)=1$ за умовою, отже $(k_1-k_2):n$, але це неможливо, бо k_1 і k_2 різні і $|k_1-k_2|<n$. Маємо, що від ділення чисел ряду(1.31) на *n* діставатимемо остачі $s=0,1,2,3,...,n-1$; позначаючи через $y=km+r=nq+s$ на підставі теореми дістанемо, що спільні дільники чисел *y* і *n* збігаються з спільними дільниками чисел *n* і *s* і, зокрема, $(y,n)=(s,n)$. Отже, в ряді чисел (1.31) буде стільки взаємно простих з *n*, скільки їх буде в ряді 0, 1, 2, ..., n-1, тобто $\varphi(n)$. Отже, в таблиці 1.5 є $\varphi(m)\cdot\varphi(n)$ чисел, взаємно простих як з *m*, так і з *n*, а отже, і з *mn*. З другого боку таблиця 1.5 має всі числа від 1 до mn, і, отже, в ній $\varphi(m\cdot n)$ чисел, взаємно простих з *mn*, і ми дістанемо, що $\varphi(m\cdot n)=\varphi(m)\cdot\varphi(n)$ і теорему доведено.

[6] В алгебрі функція Ейлера $\varphi(n)$ виражає число первісних коренів n-го степеня одиниці.

Теорема 2. *Нехай p – просте число і* $a \geq 1$ *- будь-яке натуральне число, тоді*

$$\varphi(p^a) = p^{a-1}(p-1) = p^a\left(1-\frac{1}{p}\right). \tag{5.36}$$

Справді, розглянемо ряд чисел від 1 до p^a. Запишемо його в такому вигляді:

$$1,2,...,\ p,...,2p,...,3p,...,\ p\cdot p = p^2,...\ p^{2-1}p = p^2.$$

Зрозуміло, що цей ряд має p^{2-1} чисел, які діляться на *p* і, отже, не є взаємно простими з p^a; інші числа цього ряду не діляться на *p*, отже, вони будуть взаємно прості як з *p*, так і з p^a.

Отже,

$$\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1) = p^a\left(1-\frac{1}{p}\right).$$

Зокрема,

$$\varphi(p) = p-1 \tag{5.37}$$

Теорема 3. *Якщо* $n>1$ *і* $n = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ *- канонічний розклад числа n,* то

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)..\left(1-\frac{1}{p_k}\right). \tag{5.38}$$

Справді, внаслідок мультиплікативності, матимемо:

$$\varphi(n) = \varphi\left(p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}\right) = \varphi\left(p_1^{\alpha_1}\right)\varphi\left(p_2^{\alpha_2}\right)..\varphi\left(p_k^{\alpha_k}\right) =$$

$$= p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right)...p_k^{\alpha_k}\left(1-\frac{1}{p_k}\right) =$$

$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)..\left(1-\frac{1}{p_k}\right).$$

Формулу (4) можна переписати так:

$$\varphi(n) = p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)...p_k^{\alpha_k-1}(p_k-1). \tag{5.39}$$

На практиці зручніше користуватись формулою (1.34).

Приклад. Знайти кількість чисел, менших за 1620 і взаємно простих з цим числом, тобто знайти $\varphi(1620)$. Маємо:

$$1620 = 2^2\cdot 3^4\cdot 5;\ \varphi(1620) = 1620\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 432\ .$$

Теорема 4. *Сума значень* $\varphi(d)$*, яка поширюється на всі наступальні дільники d числа n, дорівнює самому числу n, тобто*

$$\sum_{d/n}\varphi(d) = n\,. \tag{5.40}$$

Справді припустимо, що $n = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ - канонічний розклад числа *n*. Через те, що функція Ейлера є мультиплікативною, то на підставі тотожності (1), § 12 і формул (3) і (4) матимемо:

$$\sum_{d/n}\varphi(d) = \left[1+\varphi(p_1)+\varphi\left(p_1^2\right)+...+\varphi\left(p_1^{\alpha_1}\right)\right]..\left[1+\varphi(p_k)+\varphi\left(p_k^2\right)+...+\varphi\left(p_k^{\alpha_k}\right)\right] =$$

$$= \left[1+(p_1-1)+p_1(p_1-1)+...+p_1^{\alpha_1-1}(p_1-1)\right]..$$

$$...\left[1+(p_k-1)+p_k(p_k-1)+...+p_k^{\alpha_k-1}(p_k-1)\right] = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k} = n.$$

Приклад. Перевірити тотожність (1.35) для *n=30.*

Дільники *d* числа 30 будуть: 1, 2, 3, 5, 6, 10, 15, 30;

$$\sum_{d/30}\varphi(d)=\varphi(1)+\varphi(2)+\varphi(3)+\varphi(5)+\varphi(6)+\varphi(10)+$$
$$+\varphi(15)+\varphi(30)=1+1+2+4+2+4+8+8=30.$$

Функція Мебіуса

Функцією Мебіуса називається така числова функція $\mu(n)$, яка визначена для всіх натуральних *n* і характеризується такими умовами: 1) $\mu(1)=1$, 2) $\mu(n)=0$, якщо *n* не ділиться на квадрат простого числа; 3) $\mu(n)=(-1)^k$, якщо *n* не ділиться на квадрат числа, відмінного від одиниці; при цьому *k* позначає число простих дільників *n*. Наприклад,

$\mu(2)=-1,\ \mu(3)=-1,\ \mu(4)=0,\ \mu(5)=-1,\ \mu(6)=1,\ \mu(63)=0$ і т.д.

Отже, функція $\mu(n)$ набуває лише значення 0, 1 і -1. Неважко переконатися, що функція Мебіуса є також мультиплікативною функцією, тобто для будь-яких натуральних взаємно простих n_1 і n_2 маємо:

$$\mu(n_1n_2)=\mu(n_1)\mu(n_2).$$

Справді, якщо хоч би одне з чисел n_1 або n_2 ділиться на квадрат простого числа, то очевидно $\mu(n_1n_2)=0;\ \mu(n_1)\mu(n_2)=0$, тобто

$$\mu(n_1n_2)=\mu(n_1)\mu(n_2)$$

припустимо тепер, що

$$n_1=p_1p_2\ldots p_s, n_2=q_1q_2\ldots q_t,$$

де $p_1p_2\ldots p_s, n_2; q_1q_2\ldots q_t$ - різні прості числа, тоді

$$\mu(n_1)=(-1)^s, \mu(n_2)=(-1)^t$$

$$\mu(n_1n_2)=(-1)^{s+t}=\mu(n_1)\mu(n_2).$$

Помножимо обидві частини цієї рівності на $\mu(d)$ і підсумуємо за всіма дільниками *d* числа *n*; тоді дістанемо:

$$\sum_{d/n}\mu(d)F\left(\frac{n}{d}\right)=\sum_{d/n}\sum_{\delta/\frac{n}{d}}\mu(d)\Phi(\delta).$$

Тут *d* і δ такі дільники числа *n*, що $\frac{n}{d\delta}$ - ціле число, тобто *d* можна вважати дільником числа $\frac{n}{\delta}$. Змінюючи порядок підсумовування в правій частині останньої рівності, матимемо:

$$\sum_{\delta/\frac{n}{d}}\sum_{d/n}\mu(d)\Phi(\delta)=\sum_{\delta/\frac{n}{d}}\left[\Phi(\delta)\sum_{d/n}\mu(d)\right].$$

Але згідно з висновком 1, $\sum\mu(d)=0$, крім випадку, коли $d=\frac{n}{\delta}=1$, тобто коли $\delta=n$ він дорівнюватиме $\Phi(n)$. Звідси

$$\sum_{d/n}\mu(d)F\left(\frac{n}{d}\right)=\Phi(n).$$

Формулу (5) називають «*формулою обернення*» Дедекінда-Ліувілля. Її записують так: $F(n)=\int\Phi(n)$, $\Phi(n)=DF(n)$ і $F(n)$ називають *числовим інтегралом* від $\Phi(n)$, взятим по дільниках, а $\Phi(n)$ називають *числовою похідною* від $F(n)$.

Приклад 1. Якщо $\Phi(n)=n$, то $F(n)=S(n)$. Це безпосередньо випливає з означення функції $S(n)$ і з рівності (4); аналогічно, якщо $\Phi(n)=1$, то $F(n)=\tau(n)$.

Приклад 2. Якщо $F(n) = n = p_1^{a_1} \dots p_n^{a_n} > 1$, то за формулою дістанемо, що

$$\Phi(n) = \sum_{d/n} \mu(d) \frac{n}{d} = n \sum_{d/n} \frac{\mu(d)}{d}.$$

Але $\sum_{d/n} \varphi(d) = n$ за теоремою 4, отже, $\varphi(n) = \Phi(n)$, бо

$$F(n) = n = \sum_{d/n} \Phi(d).$$

Використавши формулу (3) висновку 2, знайдемо, що

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)..\left(1 - \frac{1}{p_n}\right).$$

Отже, ми іншим способом знайшли значення функції Ейлера.

Важливе значення в теорії чисел має числова функція $\pi(x)$, яка позначає число простих чисел, що не перевищують дійсного числа x, наприклад, $\pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = 2$, $\pi(\sqrt{7}) = 1$, $\pi\left(12\frac{1}{2}\right) = 5$ і т.д. Тут аргумент набуває довільних невід'ємних дійсних значень, а функція – лише цілих невід'ємних.

ЛІТЕРАТУРА

1. Капітонова Ю.В., Кривий С.Л., Летичевський О.А., Луцькиц Г.М., Печорін М.К. Основи дискретної математики. – К.: Наукова думка, 2002. – С.6-15.
2. Кужель О.В. Елементи теорії множин і математичної логіки. – К.: Рад. школа, 1977. – С. 4-24.
3. Новиков Ф.А. Дискретная математика для програмистов. – СПб.: Питер, 2002. – С.19-32.
4. Федосеева Л.И. Дискретная математика: Учеб.-практич. пособие. – Пенза: Изд-во Пенз. технол. ин-та, 1998. – С. 3-30.
5. Басакер Р., Саати Т. Конечные графы и сети. – М.: Наука, 1974. – С. 3-16, 136-143.
6. Белов В.В., Воробьев Е.М., Шаталов В.Е. Теория графов. – М.: Высшая школа, 1976. – С.7-14.
7. Дискретная математика для програмистов / Ф.А.Новиков. – СПб.: Питер, 2002. – С.189-198.
8. Свами М., Тхуласираман К. Графы, сети и алгоритмы. – М.: Мир, 1984. – С.11-23, 78-84.
9. Алферова З.В. Математическое обеспечение экономических расчетов с помощью графов. – М.: Статистика, 1994. – С.18-23.