Міністерство освіти та науки України
Національний технічний університет України
«Київський політехнічний інститут»

Навчально-науковий комплекс
«Інститут прикладного системного аналізу»

ДИСКРЕТНА МАТЕМАТИКА

АЛГЕБРА ВИСЛОВЛЕНЬ, ТЕОРІЯ МНОЖИН, ТЕОРІЯ ВІДНОШЕНЬ, ЕЛЕМЕНТИ КОМБІНАТОРИКИ, ТЕОРІЯ ГРАФІВ ЕЛЕМЕНТИ ТЕОРІЇ ГРУП ТА КІЛЕЦЬ

Для студентів математичних спеціальностей
вищих навчальних закладів

Київ 2004

Посібник містить теоретичні відомості із традиційних розділів дискретної математики – алгебра висловлень, алгебра множин, теорія відношень, комбінаторика, теорія графів, елементи теорії груп і кілець.

Посібник орієнтований для студентів математичних спеціальностей вищих навчальних закладів, а також для наукових працівників і інженерів, які цікавляться відповідними розділами дискретної математики. Передбачається, що читач володіє базовими поняттями лінійної алгебри та математичного аналізу.

Міністерство освіти та науки України
Національний технічний університет України
«Київський політехнічний інститут»

Навчально-науковий комплекс
«Інститут прикладного системного аналізу»

ДИСКРЕТНА МАТЕМАТИКА

АЛГЕБРА ВИСЛОВЛЕНЬ, ТЕОРІЯ МНОЖИН, ТЕОРІЯ ВІДНОШЕНЬ, ЕЛЕМЕНТИ КОМБІНАТОРИКИ, ТЕОРІЯ ГРАФІВ, ЕЛЕМЕНТИ ТЕОРІЇ ГРУП ТА КІЛЕЦЬ

Для студентів математичних спеціальностей вищих навчальних закладів

Затверджено
на засіданні кафедри
математичних методів
системного аналізу

Протокол №?? від ????????????? року

Київ 2004

Навчальний посібник з дисципліни «Дискретна математика». Укладач: І.Спекторський. - К.: НТУУ «КПІ», ННК «ІПСА», 2002. - 120 с.

Навчальне видання

Дискретна математика

алгебра висловлень, теорія множин, теорія відношень,
елементи комбінаторики, теорія графів, елементи теорії груп та кілець

Для студентів математичних спеціальностей університетів

Укладач: Спекторський Ігор Якович

Відповідальний редактор: Романенко Віктор Демидович

Рецензенти: Любашенко Володимир Васильович
Каніовська Ірина Юріївна

Зміст

Вступ

Дисципліна «Дискретна математика» є однією з основних фундаментальних дисциплін у загальнонауковій підготовці студентів за спеціальностями 7.080203 «Системний аналіз і управління», 7.080204 «Соціальна інформатика» та 7.080404 «Інтелектуальні системи прийняття рішень». Курс дискретної математики базовий для таких дисциплін, як «Теорія ймовірностей та математична статистика», «Спеціалізовані мови програмування», «Експертні системи» та ін. Під час вивчення курсу використовують основні визначення та теореми дисциплін «Математичний аналіз» та «Лінійна алгебра».

У навчальному посібнику подано теоретичний матеріал за розділами: «Алгебра висловлень», «Теорія множин», «Теорія відношень», «Елементи комбінаторики», «Теорія графів», «Елементи теорії груп», «Елементи теорії кілець». Матеріал згідно з робочою програмою дисципліни «Дискретна математика» розраховано на викладання протягом двадцяти однієї лекції.

Означення та теореми проілюстровано прикладами. Доведення лем і теорем наведено в стислому вигляді. Прості твердження та твердження, що можуть бути доведені за аналогією, запропоновано як вправи для самостійної роботи.

Порядок і стиль подання матеріалу повністю відповідає робочій програмі дисципліни «Дискретна математика» та задовольняє потреби суміжних математичних і прикладних дисциплін.

Розділ 1

Алгебра висловлень

1.1. Основні поняття алгебри висловлень

У цьому підрозділі наведемо основні означення та факти, що стосуються алгебри висловлень.

Означення 1.1. Висловленням називають розповідне речення, стосовно якого в даному контексті можна визначити, є воно правдивим чи неправдивим.

Приклад 1.1. Речення «Сніг – білий» є висловленням, оскільки при фіксованому контексті можна визначити його правдивість чи неправдивість. При природному контексті (нормальний атмосферний тиск, відносно чисте повітря тощо) дане висловлення є правдивим. Слід зазначити, що фіксація контексту є необхідною передумовою для визначення правдивості даного речення, оскільки в екологічно забрудненій місцевості сніг може не бути білим (у межах контексту слід також визначити самі поняття «сніг» та «білий колір»).

Зауваження 1.1. У прикл. 1.1 перед нами постала проблема формалізації природної мови. Формальне визначення термінів «сніг» та «білий колір» не є простим, а в межах формальної логіки і неможливим (за спроби дати відповідні означення будуть з'являтися все нові та нові терміни). Така проблема типова під час розгляду «текстових» задач.

Приклад 1.2. Речення «Крокодили літають» є висловленням, неправдивим при природному контексті (важко сконструювати контекст, за яким дане висловлення правдиве, проте теоретично така можливість не виключена).

Приклад 1.3. Розповідне речення «Це речення є неправдивим» не є висловленням, оскільки, як легко перевірити, при жодному контексті неможливо визначити його правдивість чи неправдивість.

Зауваження 1.2. Приклад 1.3 є одним з так званих «логічних парадоксів». Про природу та засоби боротьби з парадоксами див. [1, 2].

Надалі домовимось позначати висловлення великими літерами англійського алфавіту з індексами чи без: A, B_3, $X_{2,13}$ (так звані пропозиційні літери). Якщо висловлення A при фіксованому контексті правдиве (неправдиве), будемо писати: $|A| = 1$ (відповідно $|A| = 0$).

1.1.1. Основні операції над висловленнями

Означення 1.2. Диз'юнкцією (логічною сумою) висловлень A та B називають висловлення $A \vee B$, яке є правдивим тоді і тільки тоді, коли правдиве хоча б одне з висловлень A чи B.

Означення 1.3. Кон'юнкцією (логічним добутком) висловлень A та B називають висловлення $A \wedge B$, яке є правдивим тоді і тільки тоді, коли правдиві обидва висловлення A та B.

Означення 1.4. Запереченням висловлення A називають висловлення $\neg A$, яке є правдивим тоді і тільки тоді, коли висловлення A неправдиве.

Означення 1.5. Імплікацією висловлень A та B називають висловлення $A \to B$, яке є правдивим тоді і тільки тоді, коли з правдивості висловлення A випливає правдивість B. Висловлення A часто називають посилкою або гіпотезою імплікації $A \to B$, висловлення B – наслідком.

Зауваження 1.3. Висловлення $A \to B$ є правдивим тоді і тільки тоді, коли наслідок B правдивий або посилка A неправдива, тобто: $A \to B = (\neg A) \vee B$.

Означення 1.6. Еквіваленцією (подвійною імплікацією) висловлень A та B називають висловлення $A \leftrightarrow B$, яке є правдивим тоді і тільки тоді, коли обидва висловлення A та B є водночас правдивими або водночас неправдивими (набувають однакових значень).

Зауваження 1.4. Висловлення $A \leftrightarrow B$ є правдивим тоді і тільки тоді, коли водночас правдиві обидві імплікації $A \to B$ та $B \to A$, тобто: $A \leftrightarrow B = (A \to B) \wedge (B \to A)$.

Означення 1.7. Сумою за модулем 2 (виключною логічною сумою) висловлень A та B називають висловлення $A \oplus B$, яке є правдивим тоді і тільки тоді, коли рівно одне з висловлень A чи B є правдивим (висловлення A та B набувають різних значень).

Зауваження 1.5. Висловлення $A \oplus B$ є правдивим тоді і тільки тоді, коли еквіваленція $A \leftrightarrow B$ є неправдивою: $A \oplus B = \neg(A \leftrightarrow B)$.

1.1.2. Рекурсивне визначення формули алгебри висловлень

Зазначимо, що поняття формули алгебри висловлень є інтуїтивно зрозумілим, проте формалізація потребує чітких визначень.

Означення 1.8. Множина формул визначається такими трьома умовами:

- пропозиційна літера є формулою;
- якщо $\mathcal{A}$ та $\mathcal{B}$ – формули, то $(\mathcal{A} \vee \mathcal{B})$, $(\mathcal{A} \wedge \mathcal{B})$, $(\neg\mathcal{A})$ – також формули;
- інших формул немає.

Приклади формул алгебри висловлень: $(A \vee (\neg B))$, $(A \wedge (B \vee C))$. Запис $A \vee B \wedge C$, згідно з означенням 1.8, не є формулою алгебри висловлень.

Надалі вираз $A \to B$ вважатимемо скороченням для $(\neg A) \vee B$, вираз $A \leftrightarrow B$ – скороченням для $(A \to B) \wedge (B \to A)$ (див. заув. 1.3 та 1.4).

З метою спрощення запису, надалі у формулах опускатимемо зовнішні дужки, що не несуть в собі додаткової інформації, проте неминуче з'являються, якщо формула містить хоча б одну логічну операцію. Так, замість $(A \vee B)$ будемо писати $A \vee B$.

Надалі вважатимемо, що бінарні операції «$\vee$», «$\wedge$», «$\to$», «$\leftrightarrow$» та «$\oplus$» мають менший пріоритет, ніж унарна операція «$\neg$». Записуючи формули алгебри висловлень, будемо опускати дужки, наявність яких встановлюється з міркувань пріоритетності операцій. Так, замість $A \vee (\neg B)$ та $(\neg A) \to B$ писатимемо відповідно $A \vee \neg B$ та $\neg A \to B$.

1.2. Інтерпретації формул алгебри висловлень. Таблиці правдивості

Означення 1.9. Інтерпретацією формули алгебри висловлень називається зіставлення кожній пропозиційній літері, що міститься у формулі, значення «правда» (1) чи «неправда» (0).

Множину всіх інтерпретацій даної формули зручно зводити в так звану таблицю правдивості. Нехай формула $\mathcal{A}$ містить n пропозиційних літер: A_1, A_2, ..., A_n. Таблиця правдивості формули $\mathcal{A}$ будується як таблиця, що містить $n+1$ стовпців та 2^n рядків. При цьому в перших n стовпцях зводяться логічні значення, які зіставляються n пропозиційним літерам, $(n+1)$-й стовпець містить відповідне значення самої формули $\mathcal{A}$. Отже, кожен з рядків відповідає одній інтерпретації.

Приклад 1.4. Наведемо таблиці правдивості для формул алгебри висловлень $\neg A$ та $A_1 \vee \neg A_2$:

A	$\neg A$
0	1
1	0

A_1	A_2	$A_1 \vee \neg A_2$
0	0	1
0	1	0
1	0	1
1	1	1

Часто в одну таблицю правдивості зводять інтерпретації декількох формул, що містять спільні пропозиційні літери.

Приклад 1.5. Зведемо в одну таблицю правдивості інтерпретації для бінарних логічних операцій «$\vee$», «$\wedge$», «$\to$», «$\leftrightarrow$» та «$\oplus$»:

A	B	$A \vee B$	$A \wedge B$	$A \to B$	$A \leftrightarrow B$	$A \oplus B$
0	0	0	0	1	1	0
0	1	1	0	1	0	1
1	0	1	0	0	0	1
1	1	1	1	1	1	0

Будуючи таблиці правдивості складних формул іноді доцільно вивести значення проміжних складових частин вихідної формули.

Приклад 1.6. Побудуємо таблицю правдивості для формули алгебри висловлень $(A \vee B) \leftrightarrow (A \wedge B)$:

A	B	$A \vee B$	$A \wedge B$	$(\mathbf{A} \vee \mathbf{B}) \leftrightarrow (\mathbf{A} \wedge \mathbf{B})$
0	0	0	0	**1**
0	1	1	0	**0**
1	0	1	0	**0**
1	1	1	1	**1**

Означення 1.10. Формули $\mathcal{A}_1$ та $\mathcal{A}_2$ називають логічно еквівалентними або тотожними, якщо на кожній інтерпретації вони набувають однакових значень (водночас правдиві або водночас неправдиві).

Факт логічної еквівалентності (тотожності) формул $\mathcal{A}_1$ та $\mathcal{A}_2$ позначатимемо як $\mathcal{A}_1 \Leftrightarrow \mathcal{A}_2$ або $\mathcal{A}_1 = \mathcal{A}_2$.

Приклад 1.7. Очевидно, що $A \vee B = B \vee A$, $A \wedge B = B \wedge A$, проте $A \wedge B \neq A \vee B$.

Для доведення тотожності формул алгебри висловлень, що містять невелику кількість пропозиційних літер, зручно використовувати таблиці правдивості.

Приклад 1.8. Доведемо закон дистрибутивності диз'юнкції відносно кон'юнкції: $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$.

A	B	C	$B \wedge C$	$\mathbf{A \vee (B \wedge C)}$	$A \vee B$	$A \vee C$	$\mathbf{(A \vee B) \wedge (A \vee C)}$
0	0	0	0	**0**	0	0	**0**
0	0	1	0	**0**	0	1	**0**
0	1	0	0	**0**	1	0	**0**
0	1	1	1	**1**	1	1	**1**
1	0	0	0	**1**	1	1	**1**
1	0	1	0	**1**	1	1	**1**
1	1	0	0	**1**	1	1	**1**
1	1	1	1	**1**	1	1	**1**

Означення 1.11. Формулу $\mathcal{A}$ називають логічно загальнозначущою або тавтологією, якщо $\mathcal{A}$ набуває значення 1 на всіх інтерпретаціях. Формулу $\mathcal{A}$ називають логічною суперечністю або просто суперечністю, якщо $\mathcal{A}$ набуває значення 0 на всіх інтерпретаціях. Формулу $\mathcal{A}$ називають такою, що виконується, якщо $\mathcal{A}$ набуває значення 1 хоча б на одній інтерпретації.

Для тавтології та суперечності збережемо позначення 1 і 0 відповідно.

Приклад 1.9. Формула $\mathcal{A} = A_1 \vee \neg A_1$ є тавтологією, оскільки $A_1 \vee \neg A_1 = 1$. Формула $\mathcal{A} = A_1 \wedge \neg A_1$ є суперечністю, оскільки $A_1 \wedge \neg A_1 = 0$. Формула $\mathcal{A} = A_1 \wedge \neg A_2$ є такою, що виконується, проте, як видно з відповідної таблиці правдивості (див. прикл. 1.4), не є тавтологією.

1.3. Тотожності алгебри висловлень

1.3.1. Основні тотожності алгебри висловлень

Наведемо чотири пари законів алгебри висловлень, які надалі виділятимемо як основні.

Нехай A, B, C – довільні формули алгебри висловлень.

1. Комутативність (переставний закон): $A \vee B = B \vee A$,
$A \wedge B = B \wedge A$.

2. Дистрибутивність (розподільний закон):
$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C),$$
$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C).$$

3. Нейтральність: $A \vee 0 = A$,
$A \wedge 1 = A$.
4. Доповненість: $A \vee \neg A = 1$,
$A \wedge \neg A = 0$.

Вправа 1.1. Вивести наведені основні закони за допомогою таблиць правдивості.

Наведених восьми (чотири пари) основних законів достатньо для виведення будь-якої тотожності алгебри висловлень без використання таблиць правдивості (цей факт негайно випливає з можливості зображення довільної формули у вигляді так званої досконалої диз'юнктивної нормальної форми; теорія диз'юнктивних і кон'юнктивних форм розглядається, наприклад, у [3]).

Зазначимо, що жодну пару наведених основних законів не можна вивести з трьох інших пар, що залишаються. Проте, одна (будь-яка) з тотожностей нейтральності може бути виведена з семи законів, що залишаються. Справді, виведемо тотожність $A \vee 0 = A$. Для цього спочатку виведемо так звану тотожність універсальних меж $A \vee 1 = 1$ (нагадаємо, що A – довільна формула), а потім доведемо потрібну тотожність нейтральності $A \vee 0 = A$.

$$A \vee 1 = (A \vee 1) \wedge 1 = (A \vee 1) \wedge (A \vee \neg A) = A \vee (1 \wedge \neg A) = A \vee \neg A = 1;$$
$$A \vee 0 = A \vee (A \wedge \neg A) = (A \wedge 1) \vee (A \wedge \neg A) = A \wedge (1 \vee \neg A) = A \wedge 1 = A.$$

Система з семи законів, що залишаються після виключення однієї з тотожностей нейтральності, виявляється незалежною (див. [3]).

1.3.2. Інші закони алгебри висловлень

Наведемо деякі інші закони алгебри висловлень, що будуть часто використовуватись надалі.

5. Універсальні межі: $A \vee 1 = 1$,
$A \wedge 0 = 0$.
6. Абсорбція (поглинання): $A \vee (A \wedge B) = A$,
$A \wedge (A \vee B) = A$.
7. Ідемпотентність: $A \vee A = A$,
$A \wedge A = A$.

8. Асоціативність (сполучний закон): $A \vee (B \vee C) = (A \vee B) \vee C$,
$A \wedge (B \wedge C) = (A \wedge B) \wedge C$.

9. Єдиність заперечення: система рівнянь $\begin{cases} A \vee X = 1, \\ A \wedge X = 0 \end{cases}$ відносно X має єдиний розв'язок $X = \neg A$ (тобто якщо $A \vee X = 1$ та $A \wedge X = 0$, то $X = \neg A$).

10. Інволютивність (подвійне заперечення): $\neg(\neg A) = A$.

11. Закон (правило) де Моргана: $\neg(A \vee B) = \neg A \wedge \neg B$,
$\neg(A \wedge B) = \neg A \vee \neg B$.

Нагадаємо, що наведені тотожності (як і будь-які інші тотожності алгебри висловлень) можуть бути виведені з чотирьох пар основних законів без використання таблиць правдивості.

Розглянувши наведені закони алгебри висловлень, неважко помітити певну симетрію – усі основні закони згруповані в так звані «дуальні пари». Ця симетрія є основою для принципу дуальності – потужного засобу доведення тотожностей в алгебрі висловлень та інших подібних структурах.

1.4. Принцип дуальності. Узагальнене правило де Моргана

1.4.1. Принцип дуальності

Означення 1.12. Формулу $\mathcal{A}^*$ називають дуальною до формули $\mathcal{A}$, якщо $\mathcal{A}^*$ отримується з $\mathcal{A}$ заміною всіх входжень «$\vee$» на «$\wedge$», всіх входжень «$\wedge$» на «$\vee$», всіх входжень «0» на «1» та всіх входжень «1» на «0».

Приклад 1.10. $(A \vee \neg B)^* = A \wedge \neg B$, $(A \wedge \neg(B \vee 1))^* = A \vee \neg(B \wedge 0)$.

Зазначимо очевидний факт інволютивності операції взяття дуальної формули: $\mathcal{A}^{**} = \mathcal{A}$.

Наступна теорема формулює так званий принцип дуальності для алгебри висловлень.

Теорема 1.1. *Нехай формули алгебри висловлень $\mathcal{A}$ та $\mathcal{B}$ еквівалентні, тобто має місце тотожність $\mathcal{A} = \mathcal{B}$. Тоді має місце тотожність дуальних формул: $\mathcal{A}^* = \mathcal{B}^*$.*

Доведення. Нехай має місце тотожність $\mathcal{A} = \mathcal{B}$. Тоді має існувати виведення зазначеної тотожності з основних формул алгебри висловлень:

$$\mathcal{A} = \mathcal{A}_1 = \mathcal{A}_2 = \cdots = \mathcal{A}_n = \mathcal{B}, \tag{1.1}$$

де на кожному кроці застосовується один із законів алгебри висловлень. Але тоді, оскільки всі основні закони алгебри висловлень згруповані в чотири «дуальні пари», можемо побудувати виведення, дуальне до (1.1):

$$\mathcal{A}^* = \mathcal{A}_1^* = \mathcal{A}_2^* = \cdots = \mathcal{A}_n^* = \mathcal{B}^*,$$

де на кожному кроці використовується основний закон, дуальний до тотожності, що використовувалась на відповідному кроці у виведенні (1.1). □

Приклад 1.11. Продемонструємо, як працює принцип дуальності, на прикладі виведення закону універсальних меж:

$$A \vee 1 = (A \vee 1) \wedge 1 = (A \vee 1) \wedge (A \vee \neg A) = A \vee (1 \wedge \neg A) = A \vee \neg A = 1;$$
$$A \wedge 0 = (A \wedge 0) \vee 0 = (A \wedge 0) \vee (A \wedge \neg A) = A \wedge (0 \vee \neg A) = A \wedge \neg A = 0.$$

Вправа 1.2. Вивести закони алгебри висловлень 6 – 11 з основних законів, не користуючись змістовними визначеннями операцій (зокрема, не користуючись таблицями правдивості).

Вказівка. Тотожності зручно доводити в тому ж порядку, в якому вони наведені вище. Крім того, завдяки принципу дуальності, досить довести лише одну тотожність з кожної дуальної пари.

1.4.2. Узагальнене правило де Моргана

Класичне правило де Моргана разом із законом інволютивності (закони 11 та 10 на с. 14) зручно використовувати для «пронесення» зовнішньої операції логічного заперечення під операції диз'юнкції та кон'юнкції.

Приклад 1.12.

$$\neg(A \vee (B \wedge \neg C)) = \neg A \wedge \neg(B \wedge \neg C) = \neg A \wedge (\neg B \vee \neg\neg C) = \neg A \wedge (\neg B \vee C).$$

Вже з наведеного прикладу видно, що операція «пронесення заперечення» тісно пов'язана з дуальністю формул, і правило де Моргана можна природним чином узагальнити на випадок довільних формул алгебри висловлень.

Теорема 1.2 (узагальнене правило де Моргана)**.** *Нехай $\mathcal{A}$ – довільна формула алгебри висловлень, формула $\mathcal{A}^{\circledast}$ отримується з формули $\mathcal{A}^*$ заміною всіх пропозиційних літер на їх заперечення. Тоді має місце тотожність:*

$$\mathcal{A}^{\circledast} = \neg\mathcal{A}.$$

Для доведення теореми нам знадобиться наступна лема.

Лема 1.1. *Для довільних формул $\mathcal{A}$ та $\mathcal{B}$ виконуються такі тотожності:*

$$(\mathcal{A} \wedge \mathcal{B})^{\circledast} = \mathcal{A}^{\circledast} \vee \mathcal{B}^{\circledast}; \quad (\mathcal{A} \vee \mathcal{B})^{\circledast} = \mathcal{A}^{\circledast} \wedge \mathcal{B}^{\circledast}; \quad (\neg\mathcal{A})^{\circledast} = \neg\left(\mathcal{A}^{\circledast}\right).$$

Твердження леми негайно випливає з означення для $\mathcal{A}^{\circledast}$ та $\mathcal{B}^{\circledast}$.

Доведення теореми 1.2. Застосуємо метод математичної індукції за кількістю логічних операцій («$\vee$», «$\wedge$», «$\neg$») у вихідній формулі $\mathcal{A}$.

1. База індукції. Нехай формула $\mathcal{A}$ містить 0 операцій. Це означає, що $\mathcal{A}$ є пропозиційною літерою: $\mathcal{A} = A$. Тоді твердження теореми, очевидно, виконується:

$$\mathcal{A}^{\circledast} = A^{\circledast} = \neg A = \neg\mathcal{A}.$$

2. Припущення індукції. Нехай твердження теореми виконується для будь-якої формули $\mathcal{A}$, що містить не більш як n логічних операцій.

3. Крок індукції. Доведемо твердження теореми для формули $\mathcal{A}$, що містить $n+1$ логічну операцію.

3.1. Нехай зовнішня операція є диз'юнкція, тобто $\mathcal{A} = \mathcal{A}_1 \vee \mathcal{A}_2$. Очевидно, що формули $\mathcal{A}_1$ та $\mathcal{A}_2$ містять не більш як n операцій. Тоді на підставі леми 1.1, класичного правила де Моргана та припущення індукції маємо:

$$\mathcal{A}^{\circledast} = (\mathcal{A}_1 \vee \mathcal{A}_2)^{\circledast} = \mathcal{A}_1^{\circledast} \wedge \mathcal{A}_2^{\circledast} = \neg\mathcal{A}_1 \wedge \neg\mathcal{A}_2 = \neg(\mathcal{A}_1 \vee \mathcal{A}_2) = \neg\mathcal{A}.$$

3.2. Нехай зовнішня операція – кон'юнкція, тобто $\mathcal{A} = \mathcal{A}_1 \wedge \mathcal{A}_2$. Доведення проводиться аналогічно випадку 3.1.

3.3. Нехай зовнішня операція – заперечення, тобто $\mathcal{A} = \neg\mathcal{A}_1$. Очевидно, що формула $\mathcal{A}_1$ містить n операцій. Тоді на підставі леми 1.1 та припущення індукції маємо:

$$\mathcal{A}^{\circledast} = (\neg\mathcal{A}_1)^{\circledast} = \neg\left(\mathcal{A}_1^{\circledast}\right) = \neg\neg\mathcal{A}_1 = \neg\mathcal{A}.$$

Отже, теорему повністю доведено. □

Приклад 1.13. Застосуємо узагальнене правило де Моргана до формули з прикл. 1.12:

$$\neg(A \vee (B \wedge \neg C)) = (A \vee (B \wedge \neg C))^{\circledast} = \neg A \wedge (\neg B \vee C).$$

1.5. Логічний наслідок і логічна еквівалентність

Означення 1.13. Формула B логічно випливає з формул A_1, A_2, …, A_n (формули A_1, A_2, …, A_n логічно тягнуть формулу B), якщо формула B є правдивою на всіх інтерпретаціях, на яких водночас правдиві формули A_1, A_2, …, A_n.

Формули A_1, A_2, …, A_n називають гіпотезами, формулу B – наслідком. Для факту логічного наслідку використовуватимемо позначення: $A_1, A_2, \ldots, A_n \models B$. Якщо $n = 1$ (одна гіпотеза A), використовується також позначення $A \Rightarrow B$.

Якщо $n = 0$, формула B є наслідком порожньої множини гіпотез, тобто набуває значення 1 на всіх інтерпретаціях, без додаткових припущень щодо правдивості гіпотез (B є тавтологією). У цьому разі використовується позначення $\models B$.

Очевидно, еквівалентність формул A та B має місце тоді і тільки тоді, коли $A \Rightarrow B$ та $B \Rightarrow A$.

Теорема 1.3 (теорема дедукції)**.**

1. Формула B логічно випливає з формул A_1, …, A_n тоді і тільки тоді, коли формула $(A_1 \wedge A_2 \wedge \cdots \wedge A_n) \to B$ є тавтологією.

2. Формули A та B логічно еквівалентні тоді і тільки тоді, коли формула $A \leftrightarrow B$ є тавтологією.

Твердження теореми є безпосереднім наслідком означень логічного наслідку, логічної еквівалентності та означень логічних операцій імплікації і еквіваленції.

1.5.1. Приклади задач на логічний наслідок

1. Довести «правило вибору» (Modus Ponens[1], MP): $A, A \to B \models B$.

Нехай на деякій фіксованій інтерпретації $|A| = 1$ та $|A \to B| = 1$. Тоді, як випливає з означення імплікації, на даній інтерпретації $|B| = 1$. Завдяки довільності фіксованої інтерпретації, правило MP доведено.

Отримане доведення часто записують у компактному вигляді:

1. $\|A\| = 1$	(Гіпотеза 1, Г1)
2. $\|A \to B\| = 1$	(Г2)
3. $\|B\| = 1$	(1,2)

2. Довести правило силогізму: $A \to B, B \to C \models A \to C$.

Логічний наслідок доводитимемо зведенням до абсурду. Припустімо, що на деякій інтерпретації гіпотези правдиві та наслідок неправдивий, після чого отримуємо суперечність.

1. $\|A \to B\| = 1$	(Г1)
2. $\|B \to C\| = 1$	(Г2)
3. $\|A \to C\| = 0$	(припущення)
4. $\|A\| = 1$	(3)
5. $\|C\| = 0$	(3)
6. $\|B\| = 1$	(MP(4,1))
7. $\|C\| = 1$	(MP(6,2))

Пункти 5 та 7 дають суперечність.

Детальніші відомості з математичної логіки наведено, зокрема, в роботах [1–4].

[1] Прямий переклад з латинської: правило позиціонування.

Розділ 2

Теорія множин

2.1. Основні поняття теорії множин

Означення 2.1 («наївне» визначення множини)**.** Довільний набір об'єктів, що попарно розрізняються, називають множиною.

Відомо (див., наприклад,[1]), що, наведене визначення множини (належить німецькому вченому Георгу Кантору) призводить до парадоксів. Нині існують аксіоматичні теорії множин (аксіоматики Цермело – Френкеля, Геделя – Бернайса тощо; див., зокрема, [1]), що вільні від парадоксів, які властиві «наївній» теорії Кантора. Проте «наївна» теорія множин цілком придатна для розв'язання широкого класу прикладних проблем.

Множини позначатимемо, як правило, великими літерами англійського алфавіту з індексами чи без: A, B_1, $X_{1,42}$. Для позначення факту належності елемента x множині A використовуватимемо позначення $x \in A$, для позначення факту неналежності x множині A – позначення $x \notin A$.

Для множин натуральних, цілих, раціональних, дійсних та комплексних чисел використовуватимемо «класичні» позначення: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Вважатимемо, що множина $\mathbb{N}$ містить цілі додатні числа ($0 \notin \mathbb{N}$). Для множини, що не містить жодного елемента (*порожньої множини*) будемо використовувати позначення $\varnothing$.

Означення 2.2. Множини A та B називають еквівалентними або рівними ($A = B$), якщо вони містять одні й ті самі елементи:

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

Означення 2.3. Множину B називають підмножиною множини A (позначення $B \subset A$), а множину A – надмножиною множини B ($A \supset B$), якщо кожен елемент множини B належить множині A:

$$(B \subset A) \Leftrightarrow (A \supset B) \Leftrightarrow ((x \in B) \to (x \in A)).$$

Очевидно, що $\varnothing \subset A$ та $A \subset A$ для довільної множини A. Множину $B \subset A$, таку, що $B \neq \varnothing$, $B \neq A$, іноді називають *власною підмножиною* множини A.

Зауваження 2.1. У літературі для позначення факту «множина A є підмножиною множини B» іноді використовують позначення $A \subseteq B$ (підкреслюючи можливість $A = B$), позначення ж $A \subset B$ у такому разі використовують для випадку $A \neq B$. У цьому посібнику використовуватимемо стиль позначень, введений в означенні 2.3: вважаючи, що позначення $A \subset B$ припускає $A = B$, позначення $A \subseteq B$ взагалі не використовуватимемо.

2.1.1. Способи задання множин

1. Безпосереднє перелічення елементів множини: $A = \{1, 2, 3, 4, 5, 6\}$, $B = \{\text{Маша}, \text{Петро}, \text{Василь}\}$, $C = \{\text{Крокодил}\}$.

Зауваження 2.2. Дуже часто використовуються позначення вигляду $\{1, 2, \dots, n\}$ (множина натуральних чисел, не більших за n) та $\{1, 2, \dots, n, \dots\}$ (множина всіх натуральних чисел). Наведені позначення не є абсолютно коректними, оскільки символ «$\dots$» може трактуватись неоднозначно. Проте сенс таких позначень цілком зрозумілий з контексту, і ми їх використовуватимемо для більш наочного запису.

2. Задання множини через характеристичну властивість (характеристичний предикат): $A = \{x : P(x)\}$, де $P(x)$ – деяке висловлення, що набуває значення 1 лише для елементів x множини A (P називають *характеристичною властивістю* множини A). Отже, A визначається як множина, що містить ті і тільки ті елементи x, для яких правдиве висловлення $P(x)$. Часто використовують позначення $A = \{x \in U : P(x)\}$

– множина A містить ті і тільки ті елементи x, що належать множині U та для яких правдиве висловлення $P(x)$.

$$\{x \in \mathbb{N}\colon x = 1 \pmod 3\} = \{1, 4, 7, \dots, 3n+1, \dots\}$$
$$\{x\colon x \text{ – великі літери українського алфавіту}\} = \{\text{А,Б,}\dots\text{,Я,Ь}\}.$$

3. Задання множини з використанням формул, які містять операції над відомими множинами (операції над множинами – об'єднання, переріз, доповнення тощо – визначаються нижче в цьому підрозділі).

2.1.2. Операції над множинами

Означення 2.4. Об'єднанням множин A та B називають множину

$$A \cup B = \{x\colon (x \in A) \vee (x \in B)\}.$$

Означення 2.5. Перерізом множин A та B називають множину

$$A \cap B = \{x\colon (x \in A) \wedge (x \in B)\}.$$

Якщо $A \cap B = \varnothing$, кажуть, що множини A та B не перерізаються.

Зауваження 2.3. Визначення операцій об'єднання та перерізу природним чином переносяться на нескінченну кількість множин:

$$\bigcap_{\alpha \in I} A_\alpha = \{x\colon\ \forall \alpha \in I\colon x \in A_\alpha\}, \quad \bigcup_{\alpha \in I} A_\alpha = \{x\colon\ \exists \alpha \in I\colon x \in A_\alpha\ \},$$

де I – довільна множина індексів.

Означення 2.6. Різницею множин A та B називають множину

$$A \setminus B = \{x\colon (x \in A) \wedge (x \notin B)\}.$$

Означення 2.7. Симетричною різницею множин A та B називають множину

$$A \triangle B = \{x\colon (x \in A) \oplus (x \in B)\}.$$

Очевидно, що $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

Приклад 2.1.

$$\{1,2,3\} \setminus \{3,4\} = \{1,2\}, \quad \{1,2,3\} \triangle \{3,4\} = \{1,2,4\}.$$

Надалі вважатимемо, що в межах даного контексту визначена так звана *універсальна множина* U, що містить всі елементи, які розглядаються в заданому контексті.

Означення 2.8. Доповненням до множини A (відносно універсальної множини U) називають множину $A^c = \{x \in U : (x \notin A)\}$.

Легко побачити, що $A^c = U \setminus A$, $A \setminus B = A \cap B^c$.

Зауваження 2.4. Підкреслимо, що результат операції доповнення суттєво залежить від вибору універсальної множини:

$$U = \mathbb{R},\ [0,1]^c = (-\infty, 0) \cup (1, +\infty); \quad U = [0, +\infty),\ [0,1]^c = (1, +\infty).$$

Зазначимо, що операції об'єднання, перерізу, різниці та симетричної різниці були введені без фіксованої універсальної множини. Проте, за визначеної універсальної множини (і, як наслідок, за визначеної операції доповнення), різниця та симетрична різниця множин можуть бути визначені через операції об'єднання, перерізу та доповнення (див. вище у цьому підрозд.).

Вправа 2.1. За аналогією з алгеброю висловлень навести рекурсивне означення формули алгебри множин (за основні операції взяти об'єднання, переріз та доповнення).

2.2. Тотожності алгебри множин

Закони алгебри множин цілком аналогічні законам алгебри висловлень: операціям диз'юнкції, кон'юнкції та заперечення в алгебрі висловлень відповідають об'єднання, переріз та доповнення над множинами.

2.2.1. Основні тотожності алгебри множин

Наведемо чотири пари законів алгебри множин, які надалі виділятимемо як основні.

Нехай A, B, C – довільні формули алгебри множин.

1. Комутативність (переставний закон): $A \cup B = B \cup A$, $A \cap B = B \cap A$.

2. Дистрибутивність (розподільний закон):
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C),$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

3. Нейтральність: $A \cup \varnothing = A$, $A \cap U = A$.

4. Доповненість: $A \cup A^c = U$, $A \cap A^c = \varnothing$.

Вправа 2.2. Вивести наведені основні закони, користуючись визначеннями операцій над множинами.

Як і у випадку алгебри висловлень, наведених чотирьох пар основних законів достатньо для виведення будь-якої тотожності, що записана з використанням операцій об'єднання, перерізу та доповнення.

2.2.2. Інші закони алгебри множин

Наведемо деякі інші закони алгебри множин, які часто використовуватимемо далі.

5. Універсальні межі: $A \cup U = U$, $A \cap \varnothing = \varnothing$.

6. Абсорбція (поглинання): $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$.

7. Ідемпотентність: $A \cup A = A$, $A \cap A = A$.

8. Асоціативність (сполучний закон): $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$.

9. Єдиність доповнення: система рівнянь $\begin{cases} A \cup X = U, \\ A \cap X = \varnothing \end{cases}$ відносно X має єдиний розв'язок $X = A^c$ (тобто якщо $A \cup X = U$ та $A \cap X = \varnothing$, то $X = A^c$).

10. Інволютивність: $(A^c)^c = A$.

11. Закон (правило) де Моргана: $(A \cup B)^c = A^c \cap B^c$, $(A \cap B)^c = A^c \cup B^c$.

Нагадаємо, що наведені тотожності (як і будь-які інші тотожності алгебри множин, записані з використанням операцій об'єднання, перерізу та доповнення) можуть бути виведені з чотирьох пар основних законів.

Вправа 2.3. Сформулювати та довести принцип дуальності та узагальнене правило де Моргана для алгебри множин.

2.2.3. Діаграми Венна

Діаграми Венна (інша назва – круги Ейлера) допомагають наочно проілюструвати результати виконання операцій в алгебрі множин, а також «вгадати» (але не довести!) деякі нескладні тотожності.

На діаграмі Венна універсальну множину зображують у вигляді прямокутника, кожну іншу множину – у вигляді круга (або іншої фігури). Якщо відомо, що множини не перерізаються, відповідні круги зображують такими, що не перерізаються. Якщо відомо, що $A \subset B$, круг множини A зображують всередині круга множини B. Якщо апріорі нічого не відомо про взаємне положення множин, відповідні круги зображують такими, що перерізаються, та жоден круг не лежить цілком всередині іншого.

Приклад 2.2. Зобразимо на діаграмі Венна симетричну різницю множин $A \triangle B$ (рис. 2.1).

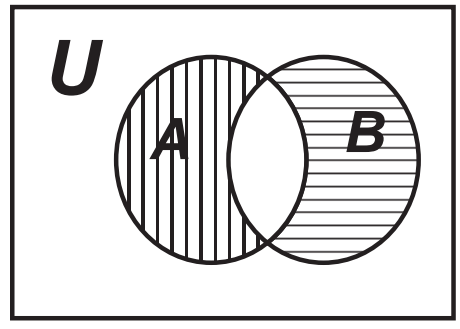


Рис. 2.1

З наведеного рисунка легко «вгадується» тотожність

$$A \triangle B = (A \cup B) \setminus (A \cap B),$$

однак ця тотожність потребує акуратного доведення.

2.3. Доведення законів алгебри множин

2.3.1. Модельне доведення

Модельний метод доведення базується на визначенні еквівалентності (рівності) множин та визначенні підмножини:

$$(A = B) \Leftrightarrow ((x \in A) \leftrightarrow (x \in B)) \Leftrightarrow (A \subset B) \wedge (B \subset A);$$
$$(A \subset B) \Leftrightarrow (B \supset A) \Leftrightarrow ((x \in A) \rightarrow (x \in B)).$$

Приклад 2.3. Доведемо тотожність поглинання: $A \cup (A \cap B) = A$.

$$(x \in (A \cup (A \cap B))) \Leftrightarrow (x \in A) \vee (x \in (A \cap B)) \Leftrightarrow$$
$$(x \in A) \vee ((x \in A) \wedge (x \in B)) \Leftrightarrow (x \in A)$$

(на останньому логічному переході використано закон поглинання для алгебри висловлень).

Приклад 2.4. Доведемо еквівалентність: $A \subset B \Leftrightarrow A \cup B = B$.

1. Нехай $A \subset B$, тобто $(x \in A) \Rightarrow (x \in B)$. Потрібно довести: $A \cup B = B$, тобто $(x \in A \cup B) \Leftrightarrow (x \in B)$.

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

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

2. Нехай $A \cup B = B$. Тоді, з означення операції об'єднання множин, $(x \in A) \Rightarrow (x \in B)$, тобто $A \subset B$.

Приклад 2.5. Доведемо закон модулярності:

$$A \subset B \Rightarrow A \cup (B \cap C) = (A \cup C) \cap B.$$

Нехай $A \subset B$. Доведемо, що $A \cup (B \cap C) \subset (A \cup C) \cap B$.

$$(x \in A \cup (B \cap C)) \Rightarrow (x \in A) \vee ((x \in B) \wedge (x \in C)) \Rightarrow$$
$$\Rightarrow ((x \in A) \vee (x \in B)) \wedge ((x \in A) \vee (x \in C)) \Rightarrow$$
$$\Rightarrow ((x \in A) \vee (x \in C)) \wedge (x \in B) \Rightarrow x \in (A \cup C) \cap B.$$

Доведемо, що $A \cup (B \cap C) \supset (A \cup C) \cap B$.

$$x \in (A \cup C) \cap B \Rightarrow ((x \in A) \vee (x \in C)) \wedge (x \in B) \Rightarrow$$
$$\Rightarrow ((x \in A) \wedge (x \in B)) \vee ((x \in C) \wedge (x \in B)) \Rightarrow$$
$$\Rightarrow (x \in A) \vee ((x \in B) \wedge (x \in C)) \Rightarrow x \in A \cup (B \cap C).$$

2.3.2. Аксіоматичне доведення

Аксіоматичне доведення, як і в випадку алгебри висловлень, передбачає застосування чотирьох пар основних законів (комутативність, дистрибутивність, нейтральність та доповненість), без урахування змісту операцій над множинами.

Приклад 2.6. Доведемо закон склеювання: $(A \cap B) \cup (A \cap B^c) = A$.

$$(A \cap B) \cup (A \cap B^c) = A \cap (B \cup B^c) = A \cap U = A.$$

Приклад 2.7. Доведемо еквівалентність $A \cup B = B \Leftrightarrow A \cap B = A$.
1. Нехай $A \cup B = B$. Тоді $(A \cup B) \cap A = B \cap A$, та $A = B \cap A$.
2. Нехай $A \cap B = A$. Тоді $(A \cap B) \cup B = A \cup B$, та $B = A \cup B$.

Вправа 2.4. Довести аксіоматичним методом ланцюжок еквівалентностей: $A \cup B = B \Leftrightarrow A \cap B = A \Leftrightarrow A \cap B^c = \varnothing \Leftrightarrow A^c \cup B = U$.

Результат прикл. 2.4 дозволяє ввести аксіоматичне (через операції перерізу, об'єднання та доповнення) визначення підмножини:

$$A \subset B \Leftrightarrow \text{ (за визначенням) } A \cup B = B.$$

Це визначення, разом з результатом вправи 2.4, дозволяє аксіоматично доводити факти включення множин.

Приклад 2.8. Доведемо логічний наслідок: $A \subset B \Rightarrow B^c \subset A^c$.

Нехай $A \subset B$. Тоді, за визначенням, $A \cup B = B$. Беручи від обох частин рівності доповнення, за законом де Моргана отримуємо: $A^c \cap B^c = B^c$, звідки, за ланцюжком еквівалентностей вправи 2.4, дістанемо: $B^c \subset A^c$.

2.4. Скінченні множини. Потужність скінченної множини

У цьому підрозділі розглядатимемо скінченні множини, тобто множини, що містять скінченну кількість елементів.

Означення 2.9. Потужність скінченної множини A визначається як кількість елементів, що належать множині A.

Потужність скінченної множини A позначатимо як $n(A)$ або $\mathrm{card}(A)$.

Приклад 2.9. $n(\{1,2,18\}) = 3$, $n(\varnothing) = 0$, $n(\{\varnothing\}) = 1$.

Наступне твердження негайно випливає з означення потужності.

Теорема 2.1. *Нехай A, B – скінченні множини, що не перерізаються, тобто $A \cap B = \varnothing$. Тоді $n(A \cup B) = n(A) + n(B)$.*

Результат теореми 2.1 методом математичної індукції узагальнюється на довільну скінченну кількість множин, що попарно не перерізаються.

Наслідок. *Нехай A_k $(k = 1, 2, \ldots, n)$ – скінченні множини, що попарно не перерізаються. Тоді $n(A_1 \cup A_2 \cup \cdots \cup A_n) = \sum\limits_{k=1}^{n} n(A_k)$.*

Наведемо узагальнення теореми 2.1 на випадок множин, що перерізаються.

Теорема 2.2. *Нехай A та B – довільні скінченні множини. Тоді $n(A \cup B) = n(A) + n(B) - n(A \cap B)$.*

Доведення. Безпосередньо перевіряється, що множини $A_1 = A \setminus B$, $A_2 = B \setminus A$, $A_3 = A \cap B$ попарно не перерізаються, та $A = A_1 \cup A_3$, $B = A_2 \cup A_3$, $A \cup B = A_1 \cup A_2 \cup A_3$, Тоді, на підставі теореми 2.1, маємо:

$$\begin{aligned} n(A \cup B) &= (n(A_1) + n(A_3)) + (n(A_2) + n(A_3)) - n(A_3) = \\ &= n(A) + n(B) - n(A \cap B). \end{aligned}$$ □

Вправа 2.5. Вивести формулу для потужності об'єднання трьох скінченних множин:

$$\begin{aligned} n(A \cup B \cup C) = n(A) + n(B) + n(C) - \\ - n(A \cap B) - n(B \cap C) - n(A \cap C) + n(A \cap B \cap C). \end{aligned}$$

Продумати узагальнення для довільної скінченної кількості скінченних множин.

2.5. Декартів добуток множин

Означення 2.10. Декартовим добутком довільних множин A та B називають множину $A \times B$, що складається з упорядкованих пар вигляду (a, b), де $a \in A$, $b \in B$:

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

Для випадку $A = B$ («декартів квадрат») часто використовують позначення $A \times A = A^{\times 2} = A^2$.

Приклад 2.10. Нехай $A = \{1, 2, 3\}$, $B = \{a, b\}$. Тоді

$$A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}.$$

Зауваження 2.5. Декартів добуток некомутативний. Так, для множин з прикл. 2.10,

$$B \times A = \{(a, 1), (b, 1), (a, 2), (b, 2), (a, 3), (b, 3)\} \neq A \times B.$$

Оскільки елементи множин A та B в декартовому добутку $A \times B$ можуть бути різної природи, доцільно вводити різні універсальні множини для першої і другої компонент декартового добутку: $A \subset U_1$, $B \subset U_2$. Універсальною множиною для декартового добутку в цьому разі вважатимемо $U = U_1 \times U_2$.

Теорема 2.3. *Нехай A та B – скінченні множини. Тоді*

$$n(A \times B) = n(A) \cdot n(B).$$

Доведення. Нехай $A = \{a_1, a_2, \ldots, a_n\}$, $B = \{b_1, b_2, \ldots, b_m\}$. Для доведення достатньо розмістити елементи множини $A \times B$ у вигляді таблиці, рядки якої відповідають елементам множини A, стовпці – елементам множини B:

	b_1	b_2	$\ldots$	b_m
a_1	(a_1, b_1)	(a_1, b_2)	$\ldots$	(a_1, b_m)
a_2	(a_2, b_1)	(a_2, b_2)	$\ldots$	(a_2, b_m)
$\ldots$	$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$			
a_n	(a_n, b_1)	(a_n, b_2)	$\ldots$	(a_n, b_m)

Очевидно, що таблиця містить nm елементів, що доводить теорему. □

Означення 2.10 узагальнюється на випадок довільної скінченної кількості множин.

Означення 2.11. Декартовим добутком множин A_1, A_2, ..., A_n називають множину $A_1 \times A_2 \times \cdots \times A_n$, що складається з упорядкованих n-ок вигляду $(a_1, a_2, \ldots, a_n)$, де $a_1 \in A_1$, $a_2 \in A_2$, ..., $a_n \in A_n$:

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \colon a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}.$$

Для випадку $A_1 = A_2 = \cdots = A_n = A$ («декартів степінь») часто використовують позначення $A^{\times n} = A^n$.

Вправа 2.6. Користуючись методом математичної індукції, довести аналог теореми 2.3 для декартового добутку довільної скінченної кількості множин:

$$n(A_1 \times A_2 \times \cdots \times A_n) = n(A_1) \cdot n(A_2) \cdots n(A_n).$$

2.5.1. Доведення тотожностей, що містять декартів добуток

Для доведення тотожностей, що містять декартів добуток, зручно використовувати модельний метод.

Приклад 2.11. Доведемо тотожність $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

$$(x, y) \in A \times (B \cup C) \Leftrightarrow (x \in A) \wedge (y \in (B \cup C)) \Leftrightarrow$$
$$\Leftrightarrow (x \in A) \wedge ((y \in B) \vee (y \in C)).$$

$$(x, y) \in (A \times B) \cup (A \times C) \Leftrightarrow ((x, y) \in (A \times B)) \vee ((x, y) \in (A \times C)) \Leftrightarrow$$
$$\Leftrightarrow ((x \in A) \wedge (y \in B)) \vee ((x \in A) \wedge (y \in C)) \Leftrightarrow (x \in A) \wedge ((y \in B) \vee (y \in C)).$$

Під час аналізу нескладних тотожностей, що містять декартів добуток, зручно використовувати аналог діаграм Венна. Множини, що відповідають першій компоненті декартового добутку, розміщують по осі X, другій компоненті – по осі Y. Нагадаємо, що діаграми Венна дозволяють «вгадати» тотожність, але «вгадана» тотожність потребує доведення.

Приклад 2.12. Зобразимо на діаграмі Венна множину $(A \times B)^c$ (рис. 2.2). Нагадаємо, що $(A \times B)^c = U \setminus (A \times B)$, де $U = U_1 \times U_2$.

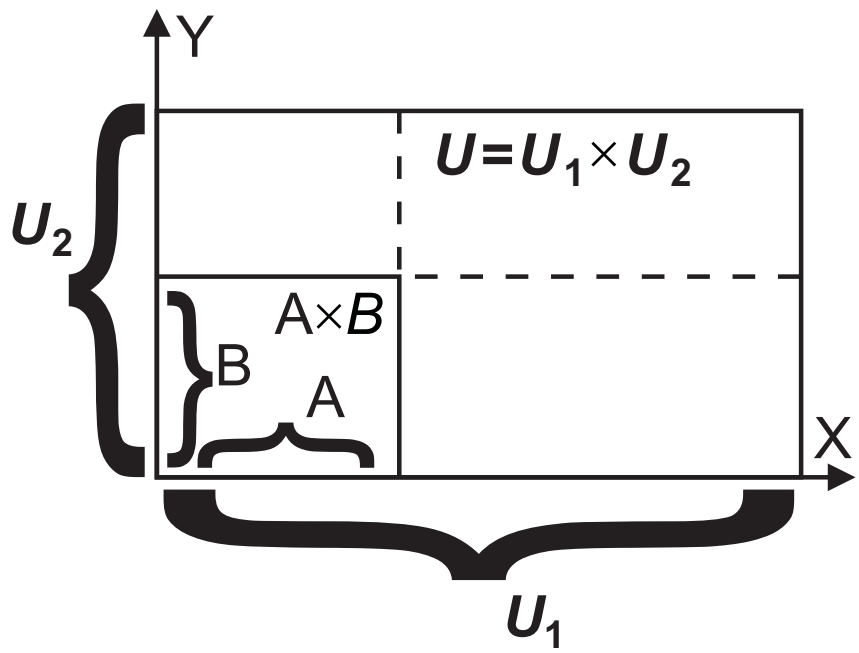


Рис. 2.2

З наведеного рисунка легко «вгадується» тотожність

$$(A \times B)^c = (U_1 \times B^c) \cup (A^c \times U_2).$$

Вправа 2.7. Довести тотожність $(A \times B)^c = (U_1 \times B^c) \cup (A^c \times U_2)$ модельним методом.

2.6. Алгебра множин як алгебрична структура. Кільце множин

2.6.1. Алгебра множин

Означення 2.12. Непорожню сукупність множин S, замкнену відносно операцій об'єднання, перерізу та доповнення, тобто таку, що

$$(A \in S) \wedge (B \in S) \Rightarrow (A \cup B \in S) \wedge (A \cap B \in S) \wedge (A^c \in S),$$

називають алгеброю множин.

З означення 2.12 негайно випливає замкненість алгебри множин відносно операцій різниці та симетричної різниці, оскільки ці операції можна виразити через об'єднання, переріз та доповнення. Зазначимо, що вимога означення 2.12 може бути послаблена, оскільки, завдяки закону де Моргана, операцію об'єднання (переріз) можна виразити через переріз (об'єднання) та доповнення.

Вправа 2.8. Довести, що алгебра множин завжди містить порожню множину: $\varnothing \in S$.

Приклад 2.13. Нехай U – довільна непорожня множина, яку вважатимемо універсальною множиною.

1. $S_1 = \{U, \varnothing\}$ – алгебра множин.
2. $S_2 = \{U, \varnothing, A, A^c\}$ $(A \subset U)$ – алгебра множин.
3. Нехай $U = A_1 \cup A_2 \cup \cdots \cup A_n$, причому множини A_k $(k = 1, \ldots, n)$ попарно не перерізаються. Розглянемо сукупність множин

$$S_n = \{A_{j_1} \cup A_{j_2} \cup \cdots \cup A_{j_m} : m = 0, \ldots, n\},$$

що містить всі можливі об'єднання множин A_k $(k = 1, \ldots, n)$, випадок $m = 0$ відповідає порожній множині. Неважко довести, що S_n – алгебра множин. Зазначимо, що S_0 та S_1 – окремі випадки алгебри S_n при $n = 0$ та $n = 1$ відповідно. Легко перевірити, що алгебра S_n містить 2^n множин.

Зауваження 2.6. Відомо (див., наприклад, [3]), що будь-яка скінченна алгебра множин завжди містить 2^n елементів, де n – деяке натуральне число. Більше того, довільна скінченна алгебра множин може бути зображена у вигляді S_n.

Наведемо приклад нескінченної алгебри множин.

Приклад 2.14. Нехай $U = [0, 1)$. Розглянемо сукупність множин

$$\mathfrak{A} = \{[a_1, b_1) \cup [a_2, b_2) \cup \cdots \cup [a_m, b_m) : 0 \le a_j < b_j \le 1,\ m \ge 0\},$$

що містить всі можливі скінченні об'єднання напіввідкритих інтервалів вигляду $[a, b) \subset [0, 1)$; випадок $m = 0$ відповідає порожній множині. Неважко довести, що $\mathfrak{A}$ – алгебра множин. Алгебру $\mathfrak{A} = \mathfrak{A}([0, 1))$ називають *борелівською алгеброю* на $[0, 1)$, вона відіграє ключову роль в теорії міри та інтеграла.

2.6.2. Поняття про кільце множин

Означення 2.13. Кільцем множин називають непорожню сукупність множин S, замкнену відносно операцій перерізу та симетричної різниці, тобто таку, що

$$(A \in S) \wedge (B \in S) \Rightarrow (A \cap B \in S) \wedge (A \triangle B \in S).$$

З означення 2.13 випливає замкненість кільця відносно операцій об'єднання та різниці, оскільки

$$A \cup B = (A \triangle B) \triangle (A \cap B), \quad A \setminus B = (A \cup B) \triangle B.$$

Вправа 2.9. Довести, що кільце множин завжди містить порожню множину: $\varnothing \in R$.

Вправа 2.10. Довести, що непорожня сукупність множин R є кільцем тоді і тільки тоді, коли R замкнене відносно операцій об'єднання та різниці.

Приклад 2.15. Довільна алгебра множин S є кільцем.

Вправа 2.11. Довести, що кільце множин є алгеброю тоді і тільки тоді, коли воно містить універсальну множину.

Приклад 2.16. Нехай U – універсальна множина.

1. Нехай $A \subset U$. Тоді $R = \{\varnothing, A\}$ – кільце множин. Зазначимо, що при $A \neq U$ кільце R не містить універсальну множину ($U \notin R$).

2. Нехай $A \subset U$, $B \subset U$, $A \cap B = \varnothing$. Тоді $R = \{\varnothing, A, B, A \cup B\}$ – кільце множин.

3. Нехай $U = \mathbb{R}$. Розглянемо сукупність множин

$$\mathfrak{R} = \{[a_1, b_1) \cup [a_2, b_2) \cup \cdots \cup [a_m, b_m) \colon a_j < b_j,\ m \geq 0\},$$

що містить всі можливі скінченні об'єднання напіввідкритих інтервалів вигляду $[a, b) \subset \mathbb{R}$; випадок $m = 0$ відповідає порожній множині. Неважко довести, що $\mathfrak{R}$ – кільце множин. Кільце $\mathfrak{R}$ називають *борелівським кільцем* (на $\mathbb{R}$), воно відіграє важливу роль в теорії міри та інтеграла.

Детальні відомості про алгебру та кільця множин (а також про інші системи множин) можна знайти, наприклад, в [5].

Загальні питання теорії множин детально висвітлені, зокрема, в [6].

Розділ 3

Теорія відношень

3.1. Основні поняття теорії відношень

Означення 3.1. Нехай A_1, A_2, ..., A_n – довільні множини. Відношенням R, що задане на множинах A_1, ..., A_n, називають довільну підмножину декартового добутку $A_1 \times A_2 \times \cdots \times A_n$:

$$R \subset A_1 \times A_2 \times \cdots \times A_n.$$

Якщо $A_1 = A_2 = \cdots = A_n = A$, то кажуть, що R задане на множині A.

Відношення $R = \varnothing$ називають порожнім, відношення $R = A_1 \times \cdots \times A_n$ – повним.

Якщо $n = 1$, відношення називають унарним, якщо $n = 2$ – бінарним, якщо $n = 3$ – тернарним (аналогічні назви для більших значень n можна утворювати від латинських порядкових числівників, але на практиці вони майже не використовуються).

Приклад 3.1. 1. На множині $A_1 = \mathbb{N}$ можна задати унарне відношення

$$R = \{n\colon\ n - \text{парне}\}.$$

2. Нехай A_1 – множина куль, A_2 – множина кольорів. На множинах A_1, A_2 можна задати бінарне відношення

$$R = \{(a_1, a_2)\colon \text{куля } a_1 \text{ має колір } a_2\}.$$

3. Нехай A_1 – множина всіх чоловіків, A_2 – множина жінок, A_3 – множина всіх людей. На множинах A_1, A_2, A_3 можна задати тернарне відношення

$$R = \{(a_1, a_2, a_3)\colon\ a_1 \text{ та } a_2 \text{ є батьками } a_3\}.$$

Надалі основну увагу приділятимемо бінарним відношенням, які широко застосовують у різних галузях математики.

Під час аналізу бінарних відношень зручно використовувати позначення:

- $R :\!\!: A \to B$ замість $R \subset A \times B$;
- xRy замість $(x, y) \in R$;
- $x\not{R}y$ замість $\neg((x, y) \in R)$.

Приклад 3.2. Нехай $R\colon \mathbb{R} \to \mathbb{R}$. Задамо відношення R через логічну еквівалентність $xRy \Leftrightarrow x \leq y$. Очевидно, $R = \{(x, y)\colon x \leq y\}$.

Приклад 3.3. Нехай $R : U \to 2^U$, де U – довільна множина, 2^U – множина всіх підмножин U, тобто $2^U = \{A : A \subset U\}$. Задамо відношення R через логічну еквівалентність $aRA \Leftrightarrow a \in A$. Очевидно, $R = \{(a, A)\colon a \in A\}$.

Далі, якщо не вказано інше, всі відношення вважатимемо бінарними.

Означення 3.2. Тотожним відношенням на множині A називають відношення I_A, визначене логічною еквівалентністю $xI_Ay \Leftrightarrow x = y$, тобто

$$I_A = \{(x, x)\colon x \in A\}.$$

3.2. Способи задання бінарних відношень

1. Довільне (не обов'язково бінарне) відношення можна задати як множину. Про способи задання множин див. підрозд. 2.1.

2. Координатний спосіб: застосовується для бінарного відношення $R\colon A \to B$ у випадку, коли елементам множин A та B можна природно зіставити точки на числовій осі. Тоді множина A задається як підмножина осі X, множина B – як підмножина осі Y, елементам відношення R зіставляються точки на координатній площині.

Приклад 3.4. Нехай $R\colon A \to B$. На рис. 3.1 наведено відношення

$$R = \{(x, y)\colon x^2 + y^2 = 1\}, \quad A = B = \mathbb{R}$$

(одиничне коло з центром у початку координат).

На рис. 3.2 наведено відношення

$$R = \{(1, x), (2, y), (3, y)\}, \quad A = \{1, 2, 3\},\ B = \{x, y\}$$

(три точки на координатній площині).

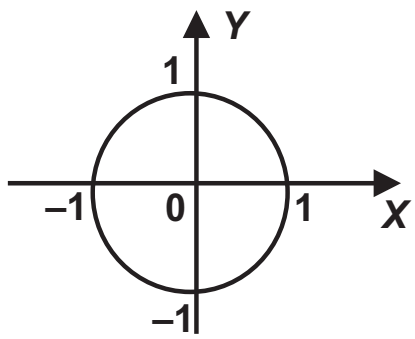


Рис. 3.1

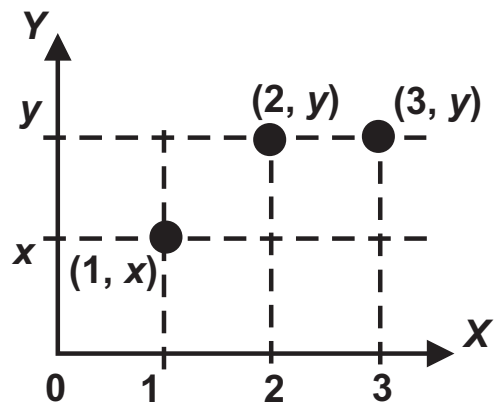


Рис. 3.2

3. Стрілкові діаграми: застосовуються для відношення $R : A \to B$ у випадку скінченних множин A та B. Нехай $A = (a_1, a_2, \ldots, a_n)$, $B = (b_1, b_2, \ldots, b_m)$. Елементи множин A та B зображують у вигляді відокремлених одна від одної точок на площині; якщо aRb, на рисунку від точки a до точки b проводять стрілку.

Приклад 3.5. Нехай $R\colon A \to B$. На рис. 3.3 наведено відношення

$$R = \{(a_1, b_1), (a_2, b_2), (a_3, b_1)\}, \quad A = \{a_1, a_2, a_3\},\ B = \{b_1, b_2\}$$

(три стрілки на діаграмі).

На рис. 3.4 наведено повне відношення

$$R = A \times B, \quad A = B = \{a, b, c\}$$

(дев'ять стрілок на діаграмі).

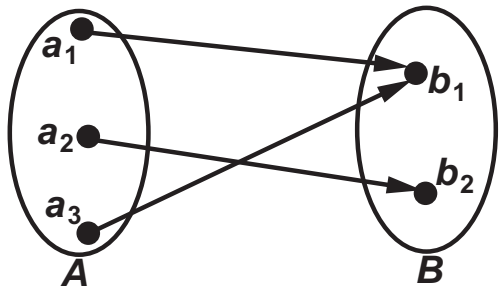


Рис. 3.3

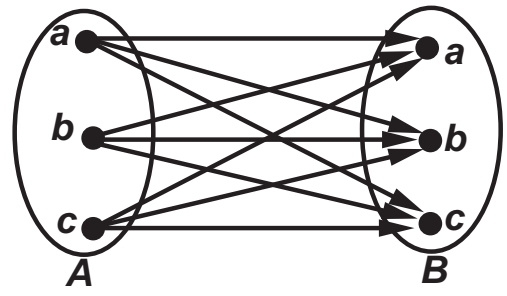


Рис. 3.4

Як видно з наведених рисунків, стрілкові діаграми доцільно застосовувати для зображення відношень, що містять невелику кількість пар елементів (для зображення повного відношення стрілкова діаграма – не найкращий вибір).

4. Матричний спосіб: застосовується для відношення $R : A \to B$ у випадку скінченних множин A та B. Нехай $A = (a_1, a_2, \ldots, a_n)$, $B = (b_1, b_2, \ldots, b_m)$. Відношення R задається у вигляді матриці M_R розміром $n \times m$ (таблиця з n рядків та m стовпців); рядки матриці M_R нумеруються елементами множини A, стовпці – елементами множини B. Матриця заповнюється логічними елементами 0 та 1: елемент $a_{i,j}$ (на перетині рядка i та стовпця j) дорівнює 1 тоді і тільки тоді, коли $a_i R b_j$.

Приклад 3.6. Нехай $A = \{a_1, a_2, a_3\}$, $B = \{b_1, b_2\}$. Кожному елементу a_i зіставимо i-й рядок ($i = 1, 2, 3$) матриці, кожному елементу b_j зіставимо j-й стовпець ($j = 1, 2$). Тоді для відношення $R = \{(a_1, b_1), (a_2, b_2), (a_3, b_1)\}$, а також для повного та порожнього відношень на $A \times B$ і для тотожного відношення I_B, дістанемо:

$$M_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix};\ M_{A\times B} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix};\ M_{\varnothing} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix};\ M_{I_B} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

5. Орієнтовані графи: застосовуються для відношення $R : A \to A$ у випадку скінченної множини A. Відношення R задається у вигляді орієнтованого графу: кожному елементу $a \in A$ зіставляється деяка точка на площині (вершина графу); якщо aRb, вершини a та b з'єднуються орієнтованим ребром, що веде від a до b. Випадку aRa на графі відповідає «замкнене» ребро (петля) на вершині a.

Приклад 3.7. Нехай $A = \{a, b, c\}$.
На рис. 3.5 наведено відношення

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

(граф з трьома ребрами, одне з яких – петля).

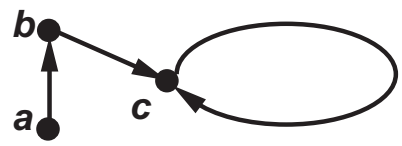


Рис. 3.5

3.3. Операції над бінарними відношеннями

1. *Об'єднання відношень:* застосовується до довільних (не обов'язково бінарних) відношень $R, S \subset A_1 \times A_2 \times \cdots \times A_n$ і визначається як об'єднання множин $R \cup S$. У випадку бінарних відношень $R, S \colon A \to B$ на скінченних A та B матриця об'єднання $M_{R \cup S}$ обчислюється як поелементна диз'юнкція матриць M_R та M_S:

$$(M_{R \cup S})_{i,j} = (M_R)_{i,j} \vee (M_S)_{i,j}, \quad 1 \le i \le n(A),\ 1 \le j \le n(B).$$

Приклад 3.8. Нехай

$$A = \{a_1, a_2, a_3\},\ B = \{b_1, b_2\},$$
$$R = \{(a_1, b_1), (a_2, b_2), (a_3, b_1)\},\ S = \{(a_1, b_1), (a_1, b_2)\}.$$

Застосовуючи природну нумерацію рядків та стовпців матриць M_R та M_S (елементу a_i зіставимо i-й рядок, елементу b_j – j-й стовпець), отримуємо:

$$M_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad M_S = \begin{pmatrix} 1 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad M_{R \cup S} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix},$$

тобто $R \cup S = \{(a_1, b_1), (a_2, b_2), (a_3, b_1), (a_1, b_2)\}$.

2. *Переріз відношень:* застосовується до довільних (не обов'язково бінарних) відношень $R, S \subset A_1 \times A_2 \times \cdots \times A_n$ і визначається як переріз множин $R \cap S$. У випадку бінарних відношень $R, S \colon A \to B$ на скінченних A та B матриця перерізу $M_{R \cap S}$ обчислюється як поелементна кон'юнкція матриць M_R та M_S:

$$(M_{R \cap S})_{i,j} = (M_R)_{i,j} \wedge (M_S)_{i,j}, \quad 1 \le i \le n(A),\ 1 \le j \le n(B).$$

Приклад 3.9. Нехай

$$A = \{a_1, a_2, a_3\},\ B = \{b_1, b_2\},$$
$$R = \{(a_1, b_1), (a_2, b_2), (a_3, b_1)\},\ S = \{(a_1, b_1), (a_1, b_2)\}.$$

Застосовуючи природну нумерацію рядків та стовпців матриць M_R та M_S, одержимо:

$$M_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad M_S = \begin{pmatrix} 1 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad M_{R\cap S} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix},$$

тобто $R \cap S = \{(a_1, b_1)\}$.

3. *Доповняльне відношення:* визначено для довільного (не обов'язково бінарного) відношення $R \subset A_1 \times A_2 \times \cdots \times A_n$ як доповнення R^c множини R відносно універсальної множини $U = A_1 \times \cdots \times A_n$, тобто

$$R^c = (A_1 \times A_2 \times \cdots \times A_n) \setminus R.$$

У випадку бінарного відношення $R\colon A \to B$ на скінченних A та B матриця доповнення M_{R^c} обчислюється як поелементне логічне заперечення матриці M_R:

$$(M_{R^c})_{i,j} = \neg\,(M_R)_{i,j}\,, \quad 1 \le i \le n(A),\ 1 \le j \le n(B).$$

Приклад 3.10. Нехай

$$A = \{a_1, a_2, a_3\},\ B = \{b_1, b_2\},\ R = \{(a_1, b_1), (a_2, b_2), (a_3, b_1)\}.$$

Застосовуючи природну нумерацію рядків та стовпців, дістанемо:

$$M_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad M_{R^c} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix},$$

тобто $R^c = \{(a_1, b_2), (a_2, b_1), (a_3, b_2)\}$.

4. *Інверсне (обернене) відношення:* визначається для бінарного відношення $R\colon A \to B$ як відношення $R^{-1}\colon B \to A$, таке, що:

$$yR^{-1}x \Leftrightarrow xRy \quad (x \in A,\, y \in B).$$

У випадку бінарного відношення $R\colon A \to B$ на скінченних A та B матриця інверсного відношення $M_{R^{-1}}$ обчислюється як транспонована до матриці M_R: $M_{R^{-1}} = (M_R)^T$, тобто

$$(M_{R^{-1}})_{j,i} = (M_R)_{i,j}\,, \quad 1 \le i \le n(A),\ 1 \le j \le n(B).$$

Приклад 3.11. Нехай

$$A = \{a_1, a_2, a_3\},\ B = \{b_1, b_2\},\ R = \{(a_1, b_1), (a_2, b_2), (a_3, b_1)\}.$$

Застосовуючи природну нумерацію рядків та стовпців, отримуємо:

$$M_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad M_{R^{-1}} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

тобто $R^{-1} = \{(b_1, a_1), (b_2, a_2), (b_1, a_3)\}$.

5. *Композиція відношень:* визначається для відношень $R\colon A \to B$ та $S\colon B \to C$ як відношення $R \circ S\colon A \to C$, таке, що:

$$a(R \circ S)c \Leftrightarrow \exists b \in B\colon aRb \wedge bSc.$$

Зауваження 3.1. Для запису композиції функцій зручним та загальноприйнятим є зворотний запис $((g \circ f)(x) = g(f(x)))$, однак для композиції відношень часто використовують як прямий, так і зворотний запис. У цьому посібнику для композиції відношень використовуватимемо прямий запис, який зручніший для наших потреб.

Для скінченних множин A, B та C з невеликою кількістю елементів композицію відношень зручно обчислювати за допомогою стрілкових діаграм.

Приклад 3.12. Нехай $A = \{a_1, a_2, a_3\}$, $B = \{b_1, b_2, b_3\}$, $C = \{c_1, c_2\}$. Розглянемо відношення

$$R\colon A \to B,\ R = \{(a_1, b_2), (a_2, b_1), (a_2, b_3), (a_3, b_2)\};$$
$$S\colon B \to C,\ S = \{(b_1, c_1), (b_3, c_1), (b_3, c_2)\}.$$

Обчислимо композицію $R \circ S$.

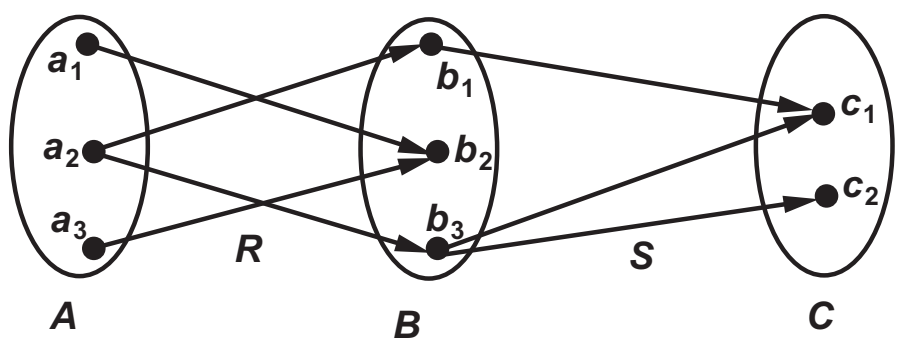


Рис. 3.6

Як видно з рис. 3.6,

$$R \circ S = \{(a_2, c_1), (a_2, c_2)\}.$$

Композиція відношень на скінченних множинах тісно пов'язана з добутком матриць відношень.

Означення 3.3. Нехай

$$A = \{a_1, \ldots, a_n\}, \quad B = \{b_1, \ldots, b_m\}, \quad C = \{c_1, \ldots, c_k\},$$
$$R\colon A \to B, \quad S\colon B \to C.$$

Тоді $M_R M_S$ визначається як матриця розміром $n \times k$, така, що

$$(M_R M_S)_{i,j} = \bigvee_{p=1}^{m} (M_R)_{i,p} \wedge (M_S)_{p,j} = \begin{cases} 1, & \exists p\colon (M_R)_{i,p} = (M_S)_{p,j} = 1, \\ 0, & \forall p\colon (M_R)_{i,p} \wedge (M_S)_{p,j} = 0. \end{cases}$$

Зазначимо, що добуток матриць відношень $M_R M_S$ визначається аналогічно класичному добутку матриць, відомому з курсу лінійної алгебри, але замість арифметичних операцій добутку та суми використовуються логічні операції кон'юнкції та диз'юнкції відповідно.

Вправа 3.1. Довести, що $M_{R\circ S} = M_R M_S$.

Приклад 3.13. Обчислимо композицію відношень з прикладу 3.12. За природної нумерації рядків та стовпців матриць отримуємо:

$$M_{R\circ S} = M_R M_S = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}.$$

Отже, $R \circ S = \{(a_2, c_1), (a_2, c_2)\}$.

Теорема 3.1. *Операція композиції асоціативна, тобто*

$$R \circ (S \circ T) = (R \circ S) \circ T, \text{ де } R\colon A \to B,\ S\colon B \to C,\ T\colon C \to D.$$

Доведення. Доведення будемо проводити модельним способом.

1) $a(R \circ (S \circ T))d \Leftrightarrow \exists b\colon aRb \wedge b(S \circ T)d \Leftrightarrow$
$\Leftrightarrow \exists b\colon aRb \wedge (\exists c\colon bSc \wedge cTd) \Leftrightarrow \exists b \exists c\colon aRb \wedge bSc \wedge cTd$;
2) $a((R \circ S) \circ T)d \Leftrightarrow \exists c\colon a(R \circ S)c \wedge cTd \Leftrightarrow$
$\Leftrightarrow \exists c\colon (\exists b\colon aRb \wedge bSc) \wedge cTd \Leftrightarrow \exists b \exists c\colon aRb \wedge bSc \wedge cTd.$ □

3.4. Властивості бінарних відношень

На практиці часто зустрічаються і використовуються бінарні відношення на множині A, що мають певні додаткові властивості. Деякі з таких властивостей розглянемо в цьому підрозділі. Надалі в цьому підрозділі розглядається відношення $R\colon A \to A$.

1. Відношення R називають *рефлексивним*, якщо $\forall a\colon aRa$.

З означення випливає, що у випадку скінченної множини A

$$(R \text{ – рефлексивне}) \Leftrightarrow (\forall i\colon (M_R)_{ii} = 1).$$

Вправа 3.2. Довести, що

$$(R \text{ – рефлексивне}) \Leftrightarrow (R \supset I_A).$$

Приклад 3.14. 1) Рефлексивними є тотожне відношення I_A та повне відношення A^2 для довільної множини A;

2) нехай $A = \mathbb{R}$. Тоді відношення «$=$», «$\leq$», «$\geq$» рефлексивні.

2. Відношення R називають *антирефлексивним*, якщо $\forall a\colon a\not R a$.
З означення випливає, що у випадку скінченної множини A

$$(R \text{ – антирефлексивне}) \Leftrightarrow (\forall i\colon (M_R)_{ii} = 0).$$

Вправа 3.3. Довести, що

$$(R \text{ – антирефлексивне}) \Leftrightarrow (R \cap I_A = \varnothing).$$

Приклад 3.15. 1) Антирефлексивним є порожнє відношення $\varnothing$;
2) нехай $A = \mathbb{R}$. Тоді відношення «$\neq$», «$<$», «$>$» антирефлексивні.

3. Відношення R називають *симетричним*, якщо $aRb \Leftrightarrow bRa$.
З означення випливає, що у випадку скінченної множини A

$$(R \text{ – симетричне}) \Leftrightarrow (M_R = (M_R)^T).$$

Вправа 3.4. Довести, що

$$(R \text{ – симетричне}) \Leftrightarrow (R = R^{-1}).$$

Приклад 3.16. 1) Симетричними є порожнє, повне та тотожне відношення на довільній множині A;
2) нехай $A = \mathbb{R}$. Тоді відношення «$\neq$» та «$=$» симетричні.

4. Відношення R називають *антисиметричним*, якщо

$$(aRb \wedge bRa) \Rightarrow (a = b).$$

Вправа 3.5. Довести, що

$$(R \text{ – антисиметричне}) \Leftrightarrow (R \cap R^{-1} \subset I_A).$$

Приклад 3.17. 1) Антисиметричними є порожнє та тотожне відношення на довільній множині A;
2) нехай $A = \mathbb{R}$. Тоді відношення «$\leq$»,«$\geq$», «$<$», «$>$» антисиметричні.

Зауваження 3.2. Властивості симетричності та антисиметричності не є взаємовиключними. Так, порожнє та тотожне відношення водночас симетричні та антисиметричні.

Вправа 3.6. Навести приклади відношень, які:
1) не є ані симетричними, ані антисиметричними;
2) не є ані рефлексивними, ані антирефлексивними;
3) є симетричними і антисиметричними одночасно.

5. Відношення R називають *транзитивним*, якщо

$$(aRb \wedge bRc) \Rightarrow (aRc).$$

Вправа 3.7. Довести, що

$$(R \text{ – транзитивне}) \Leftrightarrow (R \circ R \subset R).$$

Приклад 3.18. 1) Транзитивними є порожнє, повне та тотожне відношення на довільній множині A;
2) нехай $A = \mathbb{R}$. Тоді відношення «$=$», «$\leq$», «$\geq$», «$<$», «$>$» транзитивні.

3.4.1. Транзитивне замикання

Означення 3.4. Транзитивним замиканням відношення $R\colon A \to A$ називають таке відношення $R_{tr}\colon A \to A$, що:

- R_{tr} – транзитивне;
- $R_{tr} \supset R$;
- якщо відношення $S\colon A \to A$ транзитивне та $S \supset R$, то $S \supset R_{tr}$.

Інакше кажучи, транзитивним замиканням відношення R є найменше за включенням («$\subset$») транзитивне відношення R_{tr}, що містить відношення R як підмножину (R_{tr} – найменше транзитивне розширення відношення R).

Очевидно, що транзитивне замикання визначене однозначно. Справді, якщо умови означення 3.4 задовольняють два відношення $R_{tr,1}$ та $R_{tr,2}$, з означення 3.4 негайно отримуємо:

$$(R_{tr,1} \subset R_{tr,2}) \wedge (R_{tr,2} \subset R_{tr,1}) \Rightarrow R_{tr,1} = R_{tr,2}.$$

Вправа 3.8. Довести таку формулу для обчислення R_{tr}:

$$R_{tr} = \bigcup_{n=1}^{\infty} R^n = R \cup R^2 \cup \cdots \cup R^n \cup \cdots, \tag{3.1}$$

де $R^1 = R$, $R^n = \underbrace{R \circ \cdots \circ R}_{n}$.

Формула (3.1) містить об'єднання нескінченної кількості «композиційних степенів» R^n, проте у випадку скінченної множини A для обчислення R_{tr} процес обчислення «стабілізується» за скінченну кількість кроків. Сформулюємо цей факт у вигляді теореми.

Теорема 3.2. *Нехай* $n(A) = N$. *Тоді*

$$R_{tr} = \bigcup_{n=1}^{N} R^n = R \cup R^2 \cup \cdots \cup R^N.$$

Теорему 3.2 буде доведено далі, з використанням техніки орієнтованих графів (див. підрозд. 5.8).

Приклад 3.19. 1. Нехай $A = \{a, b\}$, $R = \{(a, b), (b, a)\}$. Тоді

$$R^2 = \{(a, a), (b, b)\}, \quad R_{tr} = R \cup R^2 = \{(a, a), (a, b), (b, a), (b, b)\}.$$

Цікаво зазначити, що композиційні степені R^k в цьому прикладі не стабілізуються:

$$R^{2k} = \{(a, a), (b, b)\}, \quad R^{2k+1} = R, \quad k \in \mathbb{N}.$$

2. Розглянемо випадок відношення на нескінченній множині. Нехай $A = \mathbb{N}$, $R = \{(n, n+1) \colon n \in \mathbb{N}\}$. Методом математичної індукції неважко довести, що $R^k = \{(n, n+k)\}$, $(k \geq 1)$, звідки маємо:

$$R_{tr} = \bigcup_{k=1}^{\infty} R^k = \{(n, n+k) \colon n \in \mathbb{N}, k \in \mathbb{N}\} = \{(n, m) \colon n < m\}.$$

Отже, відношення R збігається з відношенням «$<$» на множині натуральних чисел:

$$nRm \Leftrightarrow n < m, \quad n, m \in \mathbb{N}.$$

У роботі [7] наведено ефективний комп'ютерно-орієнтований алгоритм обчислення транзитивного замикання для відношень на скінченних множинах.

3.5. Відношення еквівалентності та відношення порядку

3.5.1. Відношення еквівалентності

Означення 3.5. Відношення $R : A \to A$ називають відношенням еквівалентності (або еквівалентністю), якщо R є водночас рефлексивним, симетричним та транзитивним.

У разі абстрактного відношення еквівалентності R для висловлення xRy загальноприйнятим є позначення $x \sim y$ (x еквівалентне y).

Вправа 3.9. Перевірити, чи є повне відношення відношенням еквівалентності.

Вправа 3.10. Перевірити, чи є порожнє відношення відношенням еквівалентності.

Приклад 3.20. 1. Нехай A – довільна множина. Тотожне відношення I_A є відношенням еквівалентності.

2. Нехай $A = \mathbb{Z}$. Бінарне відношення

$$(x \sim y) \Leftrightarrow ((x - y) \text{ – парне})$$

є відношенням еквівалентності. Таку еквівалентність називають *еквівалентністю за модулем* 2 та позначають через $x = y \pmod 2$. Як легко побачити, два числа x та y еквівалентні за модулем 2 тоді і тільки тоді, коли вони мають однакову парність (обидва парні або обидва непарні). Так, $2 \sim 0 \sim 4 \sim -2 \sim 18$, $1 \sim 3 \sim -13$, але $1 \not\sim 4$.

3. Розглянемо узагальнення прикладу з пункту 2. Нехай $p \in \mathbb{N}$, $A = \mathbb{Z}$. Через $x \bmod p$ ($x \in \mathbb{Z}$) будемо позначати остачу від ділення x/p, тобто $x = pk + (x \bmod p)$ для деякого $k \in \mathbb{Z}$. Легко перевірити, що бінарне відношення

$$(x \sim y) \Leftrightarrow (x - y) \bmod p = 0$$

є відношенням еквівалентності. Таку еквівалентність називають *еквівалентністю за модулем* p та позначають $x = y \pmod p$. Як легко бачити, два числа x та y еквівалентні за модулем p тоді і тільки тоді, коли вони дають однакову остачу від ділення на p. Так, при $p = 2$ одержимо відношення з пункту 2.

4. Нехай $A = \mathbf{R}^2$. Розглянемо відношення еквівалентності

$$((x_1, x_2) \sim (y_1, y_2)) \Leftrightarrow (x_1 = y_1).$$

Як бачимо, два вектори $x = (x_1, x_2)$, $y = (y_1, y_2)$ оголошуються еквівалентними тоді і тільки тоді, коли вони мають однакові перші координати, тобто $x_1 = y_1$.

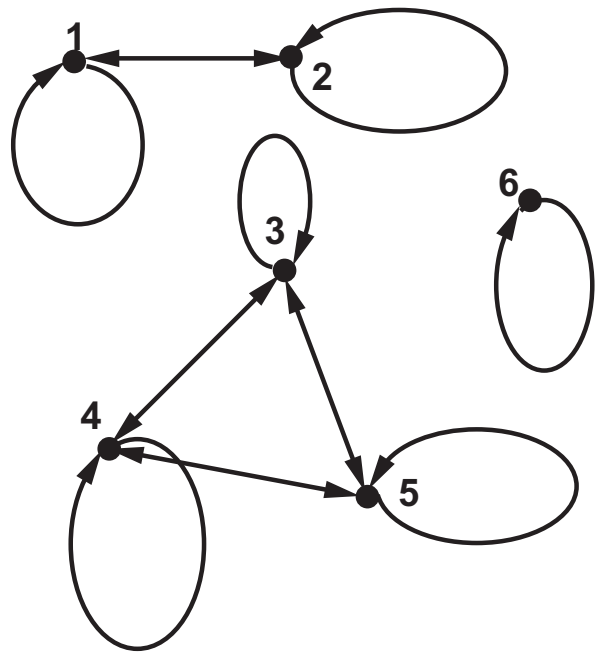
5. Наведемо дещо штучний приклад. Нехай $A = \{1, 2, 3, 4, 5, 6\}$. Розглянемо таке відношення:

$$R = \{(1,1), (2,2), (3,3), (4,4), (5,5), (6,6),\\ (1,2), (2,1), (3,4), (4,3), (3,5), (5,3), (4,5), (5,4)\}.$$

Легко перевірити, що R – відношення еквівалентності:

$$1 \sim 2,\ 3 \sim 4 \sim 5,\ 1 \not\sim 3,\ 1 \not\sim 6,\ 3 \not\sim 6.$$

Відношення R має наочніше зображення у вигляді орієнтованого графу та матриці (рис. 3.7, за природної нумерації рядків та стовпців).



$$M_\sim = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Рис. 3.7

Зазначимо, що «блокова» структура матриці $M_\sim$ не є випадковістю – достатньо порівняти структуру матриці зі структурою орієнтованого графу. Більше того, матриця довільного відношення еквівалентності на скінченній множині матиме аналогічну блокову структуру за належної нумерації рядків та стовпців (повернімось до цього питання, коли розглядатимемо фактор-множини).

Вправа 3.11. Довести, що всі відношення з прикл. 3.20 є відношеннями еквівалентності.

Приклад 3.21. Нехай A – множина чоловіків. Розглянемо таке відношення на A:

$$(xRy) \Leftrightarrow (y \text{ – брат } x \text{ (за обома батьками)}).$$

Очевидно, відношення R симетричне. Проте рефлексивним та транзитивним це відношення буде лише тоді, якщо домовитись, що кожен чоловік – брат самому собі.

3.5.2. Відношення порядку

Означення 3.6. Відношення $R : A \to A$ називають відношенням порядку (порядком, нестрогим частковим порядком), якщо R є водночас рефлексивним, антисиметричним та транзитивним. Множину A, на якій задане відношення порядку «R», називають частково впорядкованою. Для частково впорядкованої множини A з відношенням порядку «R» використовуватимемо позначення $\langle A, R\rangle$.

Під час роботи з абстрактним відношенням порядку R для висловлення xRy прийнято позначення $x \preceq y$ (x передує y, y слідує за x). Надалі будемо також використовувати такі позначення:

- $(x \succeq y) \Leftrightarrow (y \preceq x)$;
- $(x \prec y) \Leftrightarrow ((x \preceq y) \wedge (x \neq y))$;
- $(x \succ y) \Leftrightarrow (y \prec x)$.

Приклад 3.22. 1. Нехай A – довільна множина. Тотожне відношення I_A є відношенням порядку на A.

2. Нехай $A = \mathbb{R}$. Відношення «$\leq$» та «$\geq$» – відношення порядку на $\mathbb{R}$,

однак відношення «<» та «>» не є відношеннями порядку (не виконується вимога рефлексивності).

3. Нехай A – множина чоловіків. Розглянемо таке відношення на A:

$$(x \preceq y) \Leftrightarrow (y \text{ – предок для } x).$$

Якщо вважати людину предком самої себе, введене відношення є відношенням порядку.

Вправа 3.12. Довести, що всі відношення з прикл. 3.22, за винятком «<» та «>» на $\mathbb{R}$, є відношеннями порядку.

Означення 3.7. Нехай $\langle A, \preceq \rangle$ – частково впорядкована множина. Елементи $x, y \in A$ називають порівнянними, якщо $(x \preceq y) \vee (y \preceq x)$. Якщо будь-які елементи $x, y \in A$ є порівнянними, відношення «$\preceq$» називають відношенням лінійного порядку (лінійним порядком), а множину A – лінійно впорядкованою.

Приклад 3.23. 1. Легко перевірити, що частково впорядковані множини $\langle \mathbb{R}, \leq \rangle$ та $\langle \mathbb{R}, \geq \rangle$ є лінійно впорядкованими.

2. Нехай U – довільна множина. Легко перевірити, що $\langle 2^U, \subset \rangle$ є частково впорядкованою множиною. Проте, в загальному випадку, відношення «$\subset$» не є лінійним порядком. Так, при $U = \{a, b, c\}$, елементи $\{a, b\}, \{b, c\} \in 2^U$ не є порівнянними.

3. На множині $\mathbb{R}^2$ розглянемо відношення часткового (але не лінійного) порядку:

$$((x_1, x_2) \preceq (y_1, y_2)) \Leftrightarrow ((x_1 \leq y_1) \wedge (x_2 \leq y_2)).$$

Так, наприклад, $(0, 1) \preceq (1, 1) \preceq (2, 1)$. Легко перевірити, що введене відношення є частковим порядком, але, зрозуміло, в $\mathbb{R}^2$ існують непорівнянні елементи (наприклад, $(1, 0)$ та $(0, 1)$).

4. На множині $\mathbb{R}^2$ розглянемо відношення лінійного порядку

$$((x_1, x_2) \preceq (y_1, y_2)) \Leftrightarrow ((x_1 < y_1) \vee ((x_1 = y_1) \wedge (x_2 \leq y_2))).$$

Так, наприклад, $(0, 1) \preceq (1, 0)$. Введене відношення називають *лексикографічним упорядкуванням* (порівняйте з упорядкуванням дволітерних

слів у словнику: спочатку порівнюються перші літери, і якщо перші літери збігаються, порівнюються другі літери).

5. Відношення лексикографічного впорядкування природно поширюється на $\mathbb{R}^n$ для довільного $n \in \mathbb{N}$:

$$(x_1, \dots, x_n) \preceq (y_1, \dots, y_n) \Leftrightarrow$$
$$\Leftrightarrow (\exists k \colon (x_k < y_k) \wedge (\forall j < k \colon x_j = y_j)) \vee (\forall j \leq n \colon x_j = y_j).$$

Отже, «головною» оголошується перша координата: якщо $x_1 < y_1$, то, за визначенням, $x \preceq y$ (більше того, $x \prec y$); якщо перші координати векторів однакові, порівнюються другі координати; якщо і другі координати однакові, порівнюються треті координати і т. д. Легко зрозуміти, що будь-які два вектори з $\mathbb{R}^n$ можна порівняти.

Визначене в цьому підрозділі відношення порядку часто називають відношенням *нестрогого порядку* (зважаючи на рефлексивність). Водночас, часто розглядають відношення *строгого порядку*, що визначається через вимоги антирефлексивності, антисиметричності та транзитивності. Так, відношення «<» та «>» на $\mathbb{R}$ – відношення строгого порядку.

Вправа 3.13. Довести, що антисиметричність бінарного відношення випливає з антирефлексивності та транзитивності.

3.6. Розбиття множини. Фактор-множина

3.6.1. Розбиття множини

Означення 3.8. Нехай $U \neq \varnothing$. Сукупність множин $\{A_\alpha : \alpha \in I\}$, де I–довільна множина індексів, називають розбиттям множини U, якщо:

- $A_\alpha \neq \varnothing$ $(\alpha \in I)$;
- $U = \bigcup\limits_{\alpha \in I} A_\alpha$;
- $A_{\alpha_1} \cap A_{\alpha_2} = \varnothing$ $(\alpha_1 \neq \alpha_2)$.

Приклад 3.24. 1. Нехай U – довільна непорожня множина, $A \subset U$, $A \neq U$. Легко перевірити, що $\{A, A^c\}$ – розбиття множини U.

2. $\{1, 2, 3, 4, 5\} = \{1, 2\} \cup \{3, 5\} \cup \{4\}$. Отже, $\{\{1, 2\}, \{3, 5\}, \{4\}\}$ – розбиття множини $\{1, 2, 3, 4, 5\}$.

3. Нехай $U = \mathbb{R}^2$, $A_y = \{(x, y) : x \in \mathbb{R}\}$ $(y \in \mathbb{R})$. Легко зрозуміти, що $\{A_y : y \in \mathbb{R}\}$ є розбиттям множини $\mathbb{R}^2$.

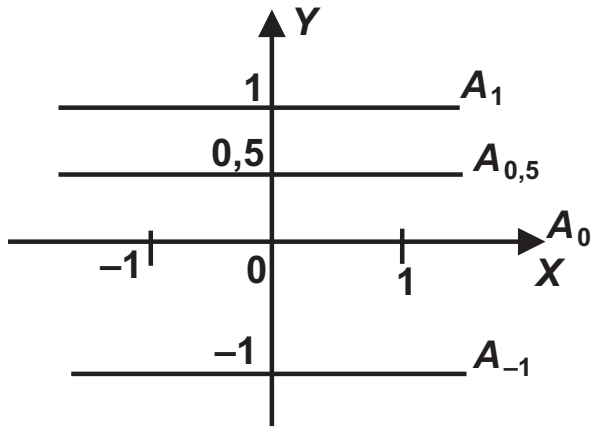


Рис. 3.8

Як видно з рис. 3.8, кожна множина A_y на координатній площині є прямою, що паралельна осі OX. Отже, вся координатна площина $\mathbb{R}^2$ є об'єднанням непорожніх множин A_y $(y \in \mathbb{R})$, що попарно не перерізаються.

4. Нехай $U = \mathbb{R}^2$, $A_r = \{(x, y) : x^2 + y^2 = r^2\}$ $(r \geq 0)$. Легко зрозуміти, що $\{A_r : r \geq 0\}$ є розбиттям множини $\mathbb{R}^2$.

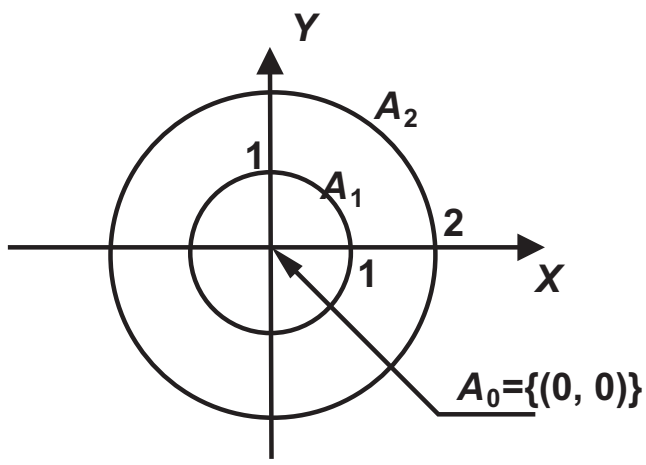


Рис. 3.9

Як видно з рис. 3.9, кожна множина A_r на координатній площині є колом з центром в початку координат і радіусом r при $r > 0$ та одноточковою множиною $\{(0, 0)\}$ при $r = 0$. Отже, вся координатна площина $\mathbb{R}^2$ – об'єднання непорожніх множин A_r $(r \geq 0)$, що попарно не перерізаються.

3.6.2. Фактор-множина

Нехай A – деяка непорожня множина, на якій задане відношення еквівалентності «$\sim$».

Означення 3.9. Нехай $a \in A$. Класом еквівалентності, породженим елементом a, називають множину $[a]$, що складається з елементів, екві-

валентних елементу a:

$$[a] = \{x \in A \colon x \sim a\}.$$

Теорема 3.3. *Класи еквівалентності або не перерізаються, або збігаються:*

$$\forall a_1, a_2 \in A \colon ([a_1] \cap [a_2] = \varnothing) \vee ([a_1] = [a_2]).$$

Доведення. Нехай $b \in [a_1] \cap [a_2]$, тобто $[a_1] \cap [a_2] \neq \varnothing$. Для доведення теореми достатньо довести рівність $[a_1] = [a_2]$.

$$(b \in [a_1]) \Rightarrow (b \sim a_1);\ (b \in [a_2]) \Rightarrow (b \sim a_2);\ (a_1 \sim b) \wedge (b \sim a_2) \Rightarrow (a_1 \sim a_2).$$

Отже, $a_1 \sim a_2$. Тепер для доведення рівності $[a_1] = [a_2]$ скористаємось модельним способом:

$$(x \in [a_1]) \Leftrightarrow (x \sim a_1) \Leftrightarrow (x \sim a_2) \Leftrightarrow (x \in [a_2]).$$

Отже, $[a_1] = [a_2]$, що завершує доведення теореми. □

Означення 3.10. Фактор-множиною множини A за відношенням еквівалентності «$\sim$» називають множину $A/_\sim$ всіх класів еквівалентності:

$$A/_\sim = \{[a] \colon a \in A\}.$$

Операцію обчислення фактор-множини називають факторизацією множини за даною еквівалентністю.

Зазначимо, що у фактор-множині $\{[a] \colon a \in A\}$ деякі з класів еквівалентності, що породжені різними елементами, можуть збігатися (більше того, якщо відношення «$\sim$» не є тотожним, існують $a_1, a_2 \in A$, такі що $[a_1] = [a_2]$). Однак у запису $\{[a] \colon a \in A\}$ однакові класи не розрізняються: класи $[a_1] = [a_2]$ вважаються одним елементом фактор-множини.

Далі зазначимо, що жоден із класів еквівалентності не є порожньою множиною: принаймні $a \in [a]$.

Отже, враховуючи твердження теореми 3.3 можемо зробити висновок, що (попарно різні) класи еквівалентності утворюють розбиття множини A. Проте має місце і зворотне твердження: кожне розбиття множини A породжене деяким відношенням еквівалентності.

Вправа 3.14. Нехай $\{A_\alpha : \alpha \in I\}$ – розбиття множини A. Введемо таке бінарне відношення «$\sim$»:

$$(a_1 \sim a_2) \Leftrightarrow (\exists \alpha \in I : a_1, a_2 \in A_\alpha),$$

тобто $a_1 \sim a_2$ тоді і тільки тоді, коли a_1 та a_2 належать одній і тій самій множині A_α. Довести:

- введене відношення «$\sim$» є відношенням еквівалентності на A;
- фактор-множина за відношенням «$\sim$» збігається з вихідним розбиттям:
$$A/_\sim = \{A_\alpha : \alpha \in I\}.$$

Приклад 3.25. 1. Нехай A – довільна непорожня множина. Профакторизуємо A за тотожним відношенням I_A («=»). Очевидно, всі класи еквівалентності – одноелементні множини:

$$[a] = \{a\}\ (a \in A), \quad A/_= = \{\{a\} : a \in A\}.$$

2. Профакторизуємо множину $A = \{1, 2, 3, 4, 5, 6\}$ за таким відношенням еквівалентності:

$$1 \sim 2,\ 3 \sim 4 \sim 5,\ 1 \not\sim 3,\ 1 \not\sim 6,\ 3 \not\sim 6$$

(див. прикл. 3.20, пункт 5). Очевидно, фактор-множина містить три класи еквівалентності:

$$A/_\sim = \{\{1, 2\}, \{3, 4, 5\}, \{6\}\}.$$

Порівнюючи $A/_\sim$ з графом та матрицею відношення «$\sim$», легко побачити, що кожен клас еквівалентності однозначно відповідає деякій області зв'язності графу та деякому «одиничному блоку» матриці $M_\sim$ (граф та матриця $M_\sim$ наведені в прикл. 3.20, пункт 3). Зрозуміло, що матриця довільного відношення еквівалентності завжди матиме блокову структуру, якщо елементи множини A для зіставлення рядкам та стовпцям матриці нумерувати за класами еквівалентності: спочатку пронумерувати елементи одного довільного класу $[a_1]$, потім – елементи класу $[a_2] \neq [a_1]$, і т. д. Зрозуміло, що за іншої нумерації рядків та стовпців блокова структура матриці може порушитись.

Вправа 3.15. Побудувати матрицю наведеного відношення «$\sim$», використовуючи таку нумерацію рядків та стовпців: перший рядок та стовпець матриці відповідають елементу 1, другий рядок та стовпець – елементу 3, третій рядок та стовпець – елементу 6, четвертий рядок та стовпець – елементу 2, п'ятий рядок та стовпець – елементу 4, шостий рядок та стовпець – елементу 5. Переконатися, що блокова структура матриці порушена.

3. Профакторизуємо $\mathbb{Z}$ за відношенням еквівалентності «$(\mod p)$», де $p \in \mathbb{N}$. Очевидно, кожен клас еквівалентності містить елементи $n \in \mathbb{Z}$ з фіксованим значенням остачі від ділення на p. Отже, маємо p різних класів еквівалентності:

$$A_k = [k] = \{k + jp \colon j \in \mathbb{Z}\},\ (0 \le k \le p-1),$$
$$A\big/_{(\mod p)} = \{A_k \colon 0 \le k \le p-1\}.$$

Так, при $p = 2$ фактор-множина $A\big/_{(\mod p)}$ буде двоелементною:

$$A\big/_{(\mod 2)} = \{\{n \in \mathbb{Z} \colon n - \text{парне}\}, \{n \in \mathbb{Z} \colon n - \text{непарне}\}\}.$$

4. Профакторизуємо $\mathbb{R}^2$ за таким відношенням еквівалентності:

$$((x_1, x_2) \sim (y_1, y_2)) \Leftrightarrow (x_1^2 + x_2^2 = y_1^2 + y_2^2).$$

З визначення даного відношення «$\sim$» випливає, що кожен клас еквівалентності містить елементи $(x_1, x_2) \in \mathbb{R}^2$ з фіксованим значенням $x_1^2 + x_2^2$:

$$A_r = \{(x_1, x_2) \colon x_1^2 + x_2^2 = r^2\},\ (r \ge 0), \quad A\big/_{\sim} = \{A_r \colon r \ge 0\}.$$

Отже, фактор-множина $A\big/_{\sim}$ є розбиттям координатної площини $\mathbb{R}^2$ на концентричні кола з центрами у початку координат і радіусами $r \ge 0$ (випадку $r = 0$ відповідає одноточковий клас еквівалентності $[(0,0)] = \{(0,0)\}$). Зазначимо, що дане розбиття $\mathbb{R}^2$ ми розглядали в прикл. 3.24 (пункт 4), де було наведено відповідний рисунок.

3.7. Функція як окремий випадок відношення

У цьому підрозділі вивчатимемо зв'язок, що існує між бінарними відношеннями та класичним поняттям функції, яке відоме з курсу математичного аналізу (та зі шкільного курсу математики).

Означення 3.11. Областю визначення відношення $R\colon A \to B$ називають множину

$$\mathcal{D}_R = \{x \in A\colon \exists y \in B\colon xRy\}.$$

Областю значень (образом) відношення $R\colon A \to B$ називають множину

$$Im_R = \{y \in B\colon \exists x \in A\colon xRy\}.$$

Вправа 3.16. Довести: $\mathcal{D}_R = Im_{R^{-1}}$.

Означення 3.12. Бінарне відношення $R\colon A \to B$ називають сюр'єктивним, якщо

$$\forall y \in B\, \exists x \in A\colon xRy.$$

Вправа 3.17. Довести: (R – сюр'єктивне) $\Leftrightarrow$ ($Im_R = B$).

Означення 3.13. Бінарне відношення $R : A \to B$ називають ін'єктивним, якщо

$$((x_1Ry) \wedge (x_2Ry)) \Rightarrow (x_1 = x_2).$$

Бінарне відношення $R\colon A \to B$ називають функціональним, якщо

$$((xRy_1) \wedge (xRy_2)) \Rightarrow (y_1 = y_2).$$

Вправа 3.18. Довести: (R – ін'єктивне) $\Leftrightarrow$ (R^{-1} – функціональне).

Далі вважатимемо, що функціональному відношенню $R_f : A \to B$ відповідає функція $f\colon A \to B$ ($R_f \leftrightarrows f$), така, що:

$$\mathcal{D}_f = \mathcal{D}_{R_f}, \quad (f(x) = y) \Leftrightarrow (xR_fy).$$

Приклад 3.26. Розглянемо відношення $R\colon \mathbb{R} \to \mathbb{R}$, $(xRy) \Leftrightarrow (y = x^2)$. Безпосередньо перевіряється, що R – функціональне відношення, якому відповідає функція $f(x) = x^2$. Проте обернене відношення R^{-1} не є функціональним, оскільки R не ін'єктивне ($1R1$, $(-1)R1$, але $1 \neq -1$).

З визначень негайно випливає, що композиції відношень відповідає композиція функцій, оберненому ін'єктивному відношенню – обернена функція:

$$(R_f \circ R_g) \leftrightarrows (g \circ f),\ (R_f\colon A \to B,\ R_g\colon B \to C - \text{функціональні});$$
$$(R_f)^{-1} \leftrightarrows f^{-1},\ (R_f - \text{ін'єктивне та функціональне}).$$

Зауваження 3.3. Ще раз звернімо увагу на те, що для запису композиції відношень прийнято прямий порядок запису, а для композиції функцій – зворотний (див. заув. 3.1).

Теорема 3.4. *Композиція сюр'єктивних відношень є сюр'єктивним відношенням, композиція ін'єктивних відношень є ін'єктивним відношенням, композиція функціональних відношень є функціональним відношенням.*

Доведення. Нехай $R\colon A \to B$, $S\colon B \to C$. Тоді визначена композиція $R \circ S\colon A \to C$.

1. Нехай R, S – сюр'єктивні. Доведемо сюр'єктивність $R \circ S$.

Нехай $z \in C$. Завдяки сюр'єктивності S знайдеться $y \in B$, такий, що ySz. Далі, завдяки сюр'єктивності R знайдеться $x \in A$, такий, що xRy. Отже, $x(R \circ S)z$.

2. Нехай R, S – ін'єктивні. Доведемо ін'єктивність $R \circ S$.

Нехай $x_1(R \circ S)z$, $x_2(R \circ S)z$. Тоді, за визначенням композиції, знайдуться $y_1, y_2 \in B$, такі, що x_1Ry_1, x_2Ry_2, y_1Sz та y_2Sz. Далі, завдяки ін'єктивності S, $y_1 = y_2 = y$. Отже, x_1Ry та x_2Ry, звідки, завдяки ін'єктивності R, маємо: $x_1 = x_2$.

3. Нехай R, S – функціональні. Доведення функціональності $R \circ S$ залишаємо як вправу. □

Вправа 3.19. Довести функціональність $R \circ S$ самостійно.

Вказівка. Доведення зводиться до пункту 2 з використанням результату вправи 3.18, якщо спочатку довести просту тотожність:

$$(R \circ S)^{-1} = S^{-1} \circ R^{-1}.$$

Далі, якщо не виникає непорозумінь, будемо ототожнювати функціональне відношення R_f та відповідну функцію f.

Означення 3.14. Функцію $f : A \to B$ називають відображенням, якщо вона визначена для всіх $x \in A$, тобто $\mathcal{D}_f = A$.

Вправа 3.20. Нехай R_f – функціональне відношення. Довести:

$$(f \text{ – відображення}) \Leftrightarrow ((R_f)^{-1} \text{ – сюр'єктивне}).$$

Підкреслимо, що відношення $(R_f)^{-1}$ може не бути функціональним.

Вправа 3.21. Довести, що композиція відображень є відображенням.

Зауваження 3.4. У літературі зустрічаються різні визначення для понять функції та відображення: найчастіше ці поняття визначають так само, як і в цьому посібнику, проте іноді їм надають дещо іншого сенсу (так, інколи поняття функції та відображення ототожнюють). Опрацьовуючи літературу з цієї теми слід звертати увагу, як саме автор визначає функцію та відображення.

Означення 3.15. Ін'єкцією називають відображення, що відповідає ін'єктивному функціональному відношенню; сюр'єкцією називають відображення, що відповідає сюр'єктивному функціональному відношенню; бієкцією (взаємно однозначним відображенням) називають відображення, яке є водночас ін'єкцією та сюр'єкцією.

Вправа 3.22. Довести:

- якщо функціональне відношення R_f визначає бієкцію f, то обернене відношення $(R_f)^{-1}$ також є функціональним і визначає бієкцію f^{-1};
- композиція бієкцій є бієкцією.

Приклад 3.27. 1. $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$. Відображення f не є ані ін'єкцією ($f(1) = f(-1)$), ані сюр'єкцією ($f(x) \geq 0$).

2. $f : \mathbb{R} \to [0, \infty)$, $f(x) = x^2$. Відображення f є сюр'єкцією, але не є ін'єкцією.

3. $f : [0, \infty) \to \mathbb{R}$, $f(x) = x^2$. Відображення f є ін'єкцією, але не є сюр'єкцією.

4. $f : [0, \infty) \to [0, \infty)$, $f(x) = x^2$. Відображення f є бієкцією.

Розділ 4

Елементи комбінаторики

4.1. Основні принципи комбінаторики. Загальне визначення вибірки

Об'єкт вивчення комбінаторики – це вибір елементів із скінченної множини згідно із заданими правилами.

4.1.1. Основні принципи комбінаторики

1. *Принцип добутку.* Нехай деяку дію можна розбити на n послідовних незалежних піддій, причому кожну піддію j можна виконати k_j способами ($j = 1, \ldots, n$). Тоді вихідну дію можна виконати $k_1 k_2 \ldots k_n$ способами.

Обґрунтування принципу добутку зводиться до підрахунку потужності декартового добутку скінченної кількості скінченних множин. Підкреслимо, що передумовою коректного застосування принципу добутку є незалежність k_j від того, яким саме способом були виконані попередні $j-1$ піддій.

Приклад 4.1. Розглянемо добре відому модель, стандартну для багатьох комбінаторних об'єктів.

Нехай в урні містяться n білих та m чорних нумерованих куль, $n, m \geq 2$. Скількома способами можна послідовно витягти 2 кулі так, щоб перша витягнута куля виявилася білою, а друга – чорною?

Вихідна дія (витягування двох куль) розпадається на дві послідовні незалежні піддії – витягування білої кулі та витягування чорної кулі. Перша піддія може бути виконана n способами, друга (незалежно від способу виконання першої піддії, тобто від того, яку саме білу кулю було витягнуто першою піддією) – m способами. Отже, як випливає з принципу добутку, вихідна дія може бути виконана nm способами.

2. *Принцип суми.* Нехай множину способів виконання деякої дії можна розбити на k підмножин, що попарно не перерізаються, причому в кожній j-й множині міститься n_j елементів (способів). Тоді вихідну дію можна виконати $n_1 + n_2 + \cdots + n_k$ способами.

Обґрунтування принципу суми зводиться до підрахунку елементів в об'єднанні скінченної кількості скінченних множин, що попарно не перерізаються.

Приклад 4.2. Нехай в урні містяться n білих, m чорних та k червоних нумерованих куль, $n, m, k \geq 2$. Скількома способами можна послідовно витягти 2 кулі так, щоб перша і тільки перша витягнута куля була білою?

Множину способів виконання вихідної дії можна розбити на дві підмножини, що не перерізаються – підмножина способів, коли друга куля буде чорною, та підмножина, коли друга куля є червоною. Перша підмножина, за принципом добутку, містить nm елементів, друга – nk елементів. Отже, як випливає з принципу суми, вихідну дію можна виконати $nm + nk$ способами.

3. *Принцип Діріхле.* Нехай елементи множини $A = \{a_1, a_2, \ldots, a_n\}$ потрібно розмістити по m комірках, причому $n > m$. Тоді принаймні одна з комірок буде містити більше одного елемента.

Приклад 4.3. 1. Нехай 5 студентів складають іспит за стандартною чотирибальною системою («відмінно», «добре», «задовільно», «незадовільно»). Тоді за принципом Діріхле принаймні два студенти отримають однакові оцінки.

2. Згідно з принципом Діріхле в місті Києві 2004 року мешкали принаймні дві людини з однаковою кількістю волосин на голові (оскільки на 2004 рік населення Києва перевищувало можливу кількість волосин на голові людини).

4.1.2. Загальне визначення вибірки. Вибірки впорядковані та невпорядковані, з повтореннями та без повторень

Означення 4.1. Вибіркою з множини $A = \{a_1, a_2, \ldots, a_n\}$ довжиною (об'ємом) k називають довільний набір елементів $a_{j_1}, a_{j_2}, \ldots, a_{j_k}$, причому елементи вибірки в загальному випадку можуть повторюватись.

Якщо всі елементи вибірки попарно різні ($a_{j_p} \neq a_{j_q}$ при $p \neq q$), вибірку називають вибіркою без повторень. Якщо повторення дозволяються (але не вимагаються), вибірку називають вибіркою з повтореннями.

Якщо на вибірці задано відношення лінійного порядку, вибірку називають упорядкованою вибіркою, або розміщенням. Якщо відношення порядку не задане (порядок елементів вибірки не враховується), вибірку називають невпорядкованою вибіркою, або комбінацією.

Розміщення без повторень при $n = k$ називають переставленням множини A.

Оскільки для аналізу властивостей вибірок природа елементів a_j не має значення, вибірку довжиною k з множини A потужністю n називають вибіркою з n за k.

Приклад 4.4. Нехай в урні містяться 3 нумеровані кулі (к_1, к_2, к_3). Потрібно підрахувати, скількома способами можна витягти 2 кулі за таких умов:

1. Витягнута куля не повертається до урни; порядок витягування не враховується, тобто вибірки типу к_i, к_j та к_j, к_i вважають однією вибіркою. Очевидно, можливі такі варіанти:

$$\text{к}_1, \text{к}_2; \quad \text{к}_1, \text{к}_3; \quad \text{к}_2, \text{к}_3.$$

2. Витягнута куля не повертається до урни; порядок витягування враховується, тобто вибірки типу к_i, к_j та к_j, к_i вважають різними вибірками. Очевидно, можливі такі варіанти:

$$\text{к}_1, \text{к}_2; \quad \text{к}_1, \text{к}_3; \quad \text{к}_2, \text{к}_3;$$
$$\text{к}_2, \text{к}_1; \quad \text{к}_3, \text{к}_1; \quad \text{к}_3, \text{к}_2.$$

3. Витягнута куля повертається до урни і може бути витягнута знову; порядок витягування не враховується. Очевидно, можливі такі варіанти:

$$\text{к}_1, \text{к}_2; \quad \text{к}_1, \text{к}_3; \quad \text{к}_2, \text{к}_3; \quad \text{к}_1, \text{к}_1; \quad \text{к}_2, \text{к}_2; \quad \text{к}_3, \text{к}_3.$$

4. Витягнута куля повертається до урни і може бути витягнута знову; порядок витягування враховується. Очевидно, можливі такі варіанти:

$$\text{к}_1,\text{к}_2;\quad \text{к}_1,\text{к}_3;\quad \text{к}_2,\text{к}_3;\quad \text{к}_2,\text{к}_1;\quad \text{к}_3,\text{к}_1;\quad \text{к}_3,\text{к}_2.$$
$$\text{к}_1,\text{к}_1;\quad \text{к}_2,\text{к}_2;\quad \text{к}_3,\text{к}_3.$$

Очевидно, що чотири розглянуті ситуації відповідають вибіркам з 3 за 2 з повтореннями (кулі повертаються і можуть бути витягнуті знову) та без повторень (кулі не повертаються), впорядкованим (з урахуванням порядку) та невпорядкованим (без урахування порядку).

Розв'язання чотирьох проблем прикл. 4.4 в загальному випадку (в урні n нумерованих куль, витягується k куль) зводиться до підрахунку загальної кількості розміщень та комбінацій з повтореннями та без повторень з n за k.

4.2. Розміщення з повтореннями та без повторень

У цьому підрозділі підрахуємо кількість розміщень з повтореннями та без повторень з n за k.

4.2.1. Розміщення без повторень

Кількість розміщень без повторень з n за k позначають через P_n^k або A_n^k. Кількість перестановлень (випадок $n = k$) позначатимемо через P_n.

Теорема 4.1. $P_n^k = n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!}$.

Доведення. Нехай $A = \{a_1, a_2, \ldots, a_n\}$. Формування розміщення без повторення з n за k, тобто впорядкованої вибірки попарно різних елементів $a_{j_1}, a_{j_2}, \ldots, a_{j_k}$, можна розбити на k послідовних піддій – вибір елемента a_{j_1}, вибір елемента a_{j_2}, ..., вибір елемента a_{j_k}. Перший елемент (a_{j_1}) можемо вибрати n способами, другий (a_{j_2}) – $n-1$ способами, оскільки $a_{j_2} \neq a_{j_1}$ і т. д. Тепер твердження теореми випливає з принципу добутку. □

Наслідок 4.1.1. $P_n = n!$.

4.2.2. Розміщення з повтореннями

Кількість розміщень з повтореннями з n за k позначатимемо через $\widetilde{P}_n^k$.

Теорема 4.2. $\widetilde{P}_n^k = n^k$.

Доведення. Нехай $A = \{a_1, a_2, \ldots, a_n\}$. Формування розміщення з повтореннями з n за k, тобто впорядкованої вибірки не обов'язково різних елементів $a_{j_1}, a_{j_2}, \ldots, a_{j_k}$, можна розбити на k послідовних піддій – вибір елемента a_{j_1}, вибір елемента a_{j_2}, ..., вибір елемента a_{j_k}. Перший елемент (a_{j_1}) можемо вибрати n способами, другий (a_{j_2}) – також n способами, враховуючи можливий випадок $a_{j_2} = a_{j_1}$ і т. д. Тепер твердження теореми випливає з принципу добутку. □

4.3. Комбінації з повтореннями та без повторень

У цьому підрозділі підрахуємо кількість комбінацій з повтореннями та без повторень з n за k.

4.3.1. Комбінації без повторень

Кількість комбінацій без повторень з n за k позначають через C_n^k або $\binom{n}{k}$. У цьому посібнику використовуватимемо перше позначення, яке прийнято у вітчизняній літературі.

Теорема 4.3. $C_n^k = \frac{n(n-1)\ldots(n-k+1)}{k!} = \frac{n!}{(n-k)!k!}$.

Доведення. Нехай $A = \{a_1, a_2, \ldots, a_n\}$. На множині всіх розміщень без повторень з n за k введемо відношення еквівалентності:

$$((a_{i_1}, \ldots, a_{i_k}) \sim (a_{j_1}, \ldots, a_{j_k})) \Leftrightarrow (\{a_{i_1}, \ldots, a_{i_k}\} = \{a_{j_1}, \ldots, a_{j_k}\}),$$

тобто еквівалентними вважаємо ті і тільки ті розміщення, які відрізняються лише порядком елементів (і збігаються як множини). Кожен клас еквівалентності $[(a_{i_1}, \ldots, a_{i_k})]$ за визначенням містить розміщення, що складаються з одних і тих самих елементів $a_{i_1}, \ldots, a_{i_k}$ і відрізняються лише порядком. Отже, кожному класу еквівалентності $[(a_{i_1}, \ldots, a_{i_k})]$

однозначно відповідає комбінація без повторень $\{a_{i_1}, \ldots, a_{i_k}\}$. Таке зіставлення є взаємно однозначним, оскільки кожен клас еквівалентності визначає рівно одну комбінацію (невпорядковану підмножину), і кожна комбінація відповідає одному класу еквівалентності.

Таким чином, кількість класів еквівалентності (відносно введеного відношення еквівалентності на множині розміщень без повторень з n за k) дорівнює C_n^k. Нарешті, оскільки кожен клас еквівалентності містить $k!$ розміщень (за кількістю переставлень на множині $\{a_{i_1}, \ldots, a_{i_k}\}$), маємо:

$$P_n^k = k! C_n^k,$$

звідки негайно випливає твердження теореми. □

Числа $C_n^k = \frac{n!}{(n-k)!k!}$ $(0 \le k \le n)$ називають *біноміальними коефіцієнтами.*

Зауваження 4.1. Біноміальним коефіцієнтам C_n^k часто надають сенс і при $k > n$, встановлюючи для цього випадку $C_n^k = 0$. Таке узагальнення цілком природне, оскільки кількість вибірок без повторень з n за k при $k > n$ дорівнює нулю.

Приклад 4.5. Розглянемо так звану «проблему деталей». Нехай у коробці міститься n деталей m сортів: n_1 деталей першого сорту, n_2 деталей другого сорту, …, n_m деталей m-го сорту. З коробки навмання, без урахування порядку, витягують k деталей. Підрахувати кількість невпорядкованих вибірок, коли буде витягнуто рівно k_1 деталей першого сорту, k_2 деталей другого сорту, …, k_m деталей m-го сорту $(0 \le k_j \le m_j)$.

Оскільки порядок вибірки у цій задачі не має значення, вважатимемо, що спочатку витягують деталі першого сорту, потім – другого, і т. д. Тоді кількість вибірок, що задовольняють задану умову, підраховують за правилом добутку: $C_{n_1}^{k_1} C_{n_2}^{k_2} \cdots C_{n_m}^{k_m}$.

4.3.2. Комбінації з повтореннями

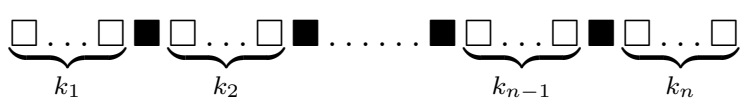
Кількість комбінацій з повтореннями з n за k будемо позначати через $\widetilde{C}_n^k$.

Теорема 4.4. $\widetilde{C}_n^k = C_{n+k-1}^k$.

Доведення. Нехай $A = \{a_1, a_2, \ldots, a_n\}$. Кожна комбінація з повтореннями довжиною k на множині A однозначно визначається кількістю k_j входжень до комбінації кожного з елементів a_j $(1 \le j \le n)$. Отже, кожна комбінація взаємно однозначно визначається впорядкованим набором чисел

$$(k_1, \ldots, k_n): \quad k_1 + \cdots + k_n = k,\ k_j \ge 0\ (1 \le j \le n).$$

Для підрахунку кількості наборів невід'ємних цілих чисел $(k_1, \ldots, k_n)$, таких, що $k_1 + \cdots + k_n = k$, розглянемо модель розташування $n-1$ ненумерованих куль по $n+k-1$ нумерованих комірках (у кожній комірці вміщується одна куля). Підкреслимо, що кулі ненумеровані, тобто попарно не розрізняються. Кожному розташуванню куль зіставимо набір невід'ємних цілих чисел $(k_1, \ldots, k_n)$:



k_1 – кількість комірок до першої зайнятої (не враховуючи зайняту);
k_2 – кількість комірок між першою та другою зайнятими;
k_3 – кількість комірок між другою та третьою зайнятими;
. . . . . .
k_{n-1} – кількість комірок між передостанньою та останньою зайнятими;
k_n – кількість комірок після останньої зайнятої.

Отже, кожному розташуванню куль в описаній моделі взаємно однозначно зіставлено набір невід'ємних цілих чисел $(k_1, \ldots, k_n)$, таких, що $k_1 + \cdots + k_n = k$. Для завершення доведення теореми зазначимо, що кількість можливих розташувань $n-1$ ненумерованих куль по $n+k-1$ нумерованих комірках дорівнює $C_{n+k-1}^{n-1} = C_{n+k-1}^{k}$ (кількість невпорядкованих виборів k комірок, що залишаться вільними, з $n+k-1$ загальної кількості комірок). □

Приклад 4.6. 1. Підрахуємо, скількома способами можна розбити число k на суму n невід'ємних доданків: $k_1 + \cdots + k_n = k$.

Як випливає з доведення теореми 4.4, кількість таких розбиттів дорівнює $\widetilde{C}_n^k = C_{n+k-1}^k$.

Вправа 4.1. Узагальнити цей результат на випадок, коли $k_1 \geq m_1$, $k_2 \geq m_2$, $\ldots$, $k_n \geq m_n$, де m_j $(1 \leq j \leq n)$ – задані цілі числа.

2. Підрахуємо кількість кісток доміно.

Як відомо, кожна кістка доміно взаємно однозначно визначається невпорядкованою парою чисел $\{n, m\}$, таких, що $0 \leq m \leq 6$, $0 \leq n \leq 6$, включаючи випадок $n = m$. Отже, кількість кісток доміно

$$\widetilde{C}_7^2 = C_{7+2-1}^2 = C_8^2 = \frac{8 \cdot 7}{2} = 28.$$

4.4. Упорядковані розбиття

Розглянемо таку проблему: потрібно розташувати елементи множини $A = \{a_1, a_2, \ldots, a_n\}$ по k нумерованих комірках ємністю n_1, n_2, $\ldots$, n_k відповідно, причому $n_1 + \cdots + n_k = n$. Цю проблему називають *упорядкованим розбиттям* множини A по k упорядкованих комірках. Зазначимо, що порядок розташування елементів у кожній комірці не має значення – нас цікавить лише те, в яку комірку потрапить кожен з елементів множини A. Кількість упорядкованих розбиттів за сформульованими параметрами позначатимемо через $C_n^{n_1,n_2,\ldots,n_k}$.

Для підрахунку кількості впорядкованих розбиттів скористаємось принципом добутку: спочатку заповнимо першу комірку, потім – другу і т. д. Очевидно, першу комірку можна заповнити $C_n^{n_1}$ способами, другу – $C_{n-n_1}^{n_2}$ способами, третю – $C_{n-n_1-n_2}^{n_3}$ способами і т. д. За принципом добутку маємо:

$$C_n^{n_1,n_2,\ldots,n_k} = C_n^{n_1} C_{n-n_1}^{n_2} C_{n-n_1-n_2}^{n_3} \cdots C_{n-n_1-\cdots-n_{k-1}}^{n_k}. \tag{4.1}$$

Зауваження 4.2. Останній множник $C_{n-n_1-\cdots-n_{k-1}}^{n_k} = C_{n_k}^{n_k} = 1$ (як і очікували, оскільки останню комірку можемо заповнити лише одним способом).

Безпосередній підрахунок дозволяє значно спростити вираз у правій частині (4.1):

$$C_n^{n_1,n_2,\ldots,n_k} = \frac{n!}{n_1! n_2! \cdots n_k!}.$$

Зазначимо, що у випадку $k = 2$ маємо класичний випадок комбінацій без повторень (невпорядкований вибір елементів для однієї з двох комірок):

$$C_n^{n_1,n_2} = \frac{n!}{n_1!n_2!} = C_n^{n_1} = C_n^{n_2}.$$

Вправа 4.2. Узагальнити формулу для $C_n^{n_1,n_2,\dots,n_k}$ на випадок, коли $n_1 + \cdots + n_k \leq n$.

Приклад 4.7. Підрахуємо, скільки слів (довільних послідовностей літер) можна скласти з шести карток, на трьох з яких позначена літера «А», на двох – літера «Б», на одній – «В»:

А	А	А	Б	Б	В

Для розв'язання задачі розглянемо таку модель: є три комірки «А», «Б» та «В» ємностями 3, 2 та 1 відповідно, у яких треба розмістити елементи множини $X = \{1, 2, 3, 4, 5, 6\}$. Тоді кожному слову однозначно відповідає розбиття множини X по комірках «А», «Б» та «В» – кожен елемент множини X відповідає номеру літери в слові, що складається. Отже, кількість слів обчислюється як кількість упорядкованих розбиттів:

$$C_6^{3,2,1} = \frac{6!}{3!2!1!} = 60.$$

4.5. Біноміальна та поліноміальна формули. Трикутник Паскаля

4.5.1. Властивості біноміальних коефіцієнтів

Нагадаємо (див. с. 62), що числа C_n^k $(0 \leq k \leq n)$ називають біноміальними коефіцієнтами. Розглянемо кілька найважливіших властивостей біноміальних коефіцієнтів.

1. $C_n^k = C_n^{n-k}$;
2. $C_n^0 = C_n^n = 1$, $C_n^1 = C_n^{n-1} = n$;
3. $C_n^k + C_n^{k+1} = C_{n+1}^{k+1}$.

Вправа 4.3. Довести вказані тотожності.

4.5.2. Біноміальна та поліноміальна формули

З курсу математичного аналізу відома формула для «розкриття дужок» у виразі $(a+b)^n$:

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}. \tag{4.2}$$

Формулу (4.2), як відомо, називають *біномом Ньютона*, або *біноміальною формулою*, звідки дістали назву коефіцієнти C_n^k.

Зауваження 4.3. Назва «біном Ньютона» двічі неправильна: по-перше, ні права, ні ліва частина формули (4.2) не є біномом (двучленом); по-друге, формула (4.2) була відома і до робіт Ньютона (Ісааку Ньютону належить важливе узагальнення формули (4.2) на випадок довільного $n \in \mathbb{R}$).

Доведемо біноміальну формулу (4.2) методами комбінаторики. Розкриємо дужки у виразі $(a+b)^n$, не користуючись комутативністю множення дійсних чисел:

$$(a+b)^n = \underbrace{(a+b)\cdots(a+b)}_{n} = \underbrace{aa\cdots a}_{n} + \underbrace{ba\cdots a}_{n} + \underbrace{ab\cdots a}_{n} + \cdots + \underbrace{bb\cdots b}_{n}.$$

Після зведення подібних членів (використовуючи комутативність множення) дістанемо:

$$(a+b)^n = \sum_{k=0}^{n} c_k a^k b^{n-k},$$

де c_k – кількість доданків вигляду $\alpha_1 \cdots \alpha_n$ ($\alpha_j \in \{a, b\}$), таких, що множник a міститься в добутку $\alpha_1 \cdots \alpha_n$ рівно k разів (множник b міститься відповідно $n-k$ разів).

Для обчислення коефіцієнтів c_k розглянемо комбінаторну модель розташування множників α_j ($1 \le j \le n$) по комірках a та b ємностями k та $n-k$ відповідно. Очевидно, кожне таке розташування однозначно відповідає одному з доданків $\alpha_1 \cdots \alpha_n$, що містить k множників a та $n-k$ множників b. Отже,

$$c_k = C_n^{k,n-k} = C_n^k,$$

що і треба було довести.

Комбінаторне доведення формули (4.2) природно поширюється для виразу $(a_1 + a_2 + \cdots + a_m)^n$:

$$(a_1 + a_2 + \cdots + a_m)^n = \sum_{\substack{k_1,k_2,\ldots,k_m \geq 0 \\ k_1+\cdots+k_m=n}} C_n^{k_1,\ldots,k_m} a_1^{k_1} \cdots a_m^{k_m}. \tag{4.3}$$

Вправа 4.4. Провести доведення формули (4.3).

Формула (4.3), за аналогією з біноміальною формулою, дістала назву *поліноміальна формула*. Зазначимо, що кількість доданків у правій частині формули (4.3) обчислюється як кількість розбиттів числа n на m невід'ємних цілих доданків, тобто через комбінації з повтореннями: $\widetilde{C}_m^n = C_{m+n-1}^n$. Так, при $m = 2$ (випадок біноміальної формули) матимемо: $C_{n+1}^n = n + 1$.

Приклад 4.8. 1. Користуючись поліноміальною формулою, розкриємо дужки у виразі $(a + b + c)^3$:

$$(a+b+c)^3 = \underbrace{C_3^{3,0,0}}_{=1} a^3b^0c^0 + b^3 + c^3 + \\ + \underbrace{C_3^{2,1,0}}_{=3} a^2b^1c^0 + 3ab^2 + 3a^2c + 3ac^2 + 3b^2c + 3bc^2 + \underbrace{C_3^{1,1,1}}_{=6} a^1b^1c^1.$$

2. Не розкриваючи повністю дужки у виразі $(a+b+c+d)^{132}$, обчислимо коефіцієнт при доданку $a^{131}b$:

$$C_{132}^{131,1,0,0} = \frac{132!}{131!1!0!0!} = 132.$$

Зазначимо, що загальна кількість доданків після розкриття дужок та зведення подібних членів становить $\widetilde{C}_4^{132} = 400995$.

4.5.3. Трикутник Паскаля

Здебільшого (зокрема, для обчислення коефіцієнтів у біномі Ньютона) біноміальні коефіцієнти зручно розташовувати у формі так званого *трикутника Паскаля*:

$$\begin{array}{cccc} C_0^0 & & & \\ C_1^0 & C_1^1 & & \\ C_2^0 & C_2^1 & C_2^2 & \\ C_3^0 & C_3^1 & C_3^2 & C_3^3 \\ \ldots\ldots\ldots\ldots & & & \end{array} \quad \text{або} \quad \begin{array}{ccccccc} & & C_0^0 & & & & \\ & C_1^0 & & C_1^1 & & & \\ C_2^0 & & C_2^1 & & C_2^2 & & \\ C_3^0 & & C_3^1 & & C_3^2 & & C_3^3 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & & & & \end{array}$$

Трикутник Паскаля, очевидно, нескінченний, проте на практиці обчислюють кілька перших рядків (так, для розкладання $(a+b)^5$ потрібні перші 6 рядків).

Обчислюючи перші рядки трикутника Паскаля (у «прямокутній» чи «рівнобедреній» формі), як правило, виписують одиничні елементи «бічних сторін» трикутника, після чого використовують тотожність $C_n^k + C_n^{k+1} = C_{n+1}^{k+1}$.

Приклад 4.9. Обчислимо перші п'ять рядків трикутника Паскаля (у «прямокутній» формі):

$$\begin{array}{ccccccccc} \mathbf{1} & & & & & & & & \\ \mathbf{1} & & \mathbf{1} & & & & & & \\ \mathbf{1} & 1+1=\mathbf{2} & & \mathbf{1} & & & & & \\ \mathbf{1} & 1+2=\mathbf{3} & 2+1=\mathbf{3} & & \mathbf{1} & & & & \\ \mathbf{1} & 1+3=\mathbf{4} & 3+3=\mathbf{6} & 3+1=\mathbf{4} & & \mathbf{1} & & & \end{array}$$

4.6. Застосування кореневих дерев у комбінаторних задачах

Багато комбінаторних проблем не можна описати жодною з класичних комбінаторних моделей. У таких ситуаціях, коли майже єдиний метод – безпосередній перебір всіх варіантів, зручно користуватися графами спеціального виду – так званими *кореневими деревами*. Кореневе дерево визначається як дерево з виділеною вершиною – коренем (точні визначення наведемо далі, під час вивчення графів спеціальних типів). Під час перебору варіантів кожній вершині дерева (починаючи з кореня) відповідає певна група варіантів; якщо група варіантів розбивається на n множин, з відповідної вершини дерева виходить n ребер. Кожному листку («заключним» вершинам дерева) відповідає достатньо проста множина варіантів (найчастіше кожному листку відповідає один варіант).

Приклад 4.10. У деякому (абстрактному) казіно гра проходить за такими правилами: у разі виграшу гравець отримує виграш у розмірі ставки (тобто, поставивши k гривень, гравець у разі виграшу забере $2k$ гривень); програвши, гравець втрачає свою ставку.

Нехай дехто (абстрактний гравець) прийшов у казіно з однією гривнею і вирішив грати доти, доки в нього є гроші, але не більше трьох ігор, ставлячи на кожну гру одну гривню.

Розташуємо можливі варіанти розвитку подій у вигляді кореневого дерева (рис. 4.1). Ребро, що позначене знаком «+», відповідає виграшу в конкретній грі; ребро, що позначене знаком «−», відповідає програшу. Кожну вершину дерева позначатимемо сумою (в гривнях), що залишилася у гравця. Листки дерева (варіанти закінчення серії ігор) позначимо зовнішнім квадратом. Як видно з рис. 4.1, у трьох з п'яти варіантів закінчення серії гравець виграє, і в двох – програє. Звичайно, звідси не випливає, що в середньому гравець буде вигравати, оскільки не всі варіанти закінчення мають однакову ймовірність.

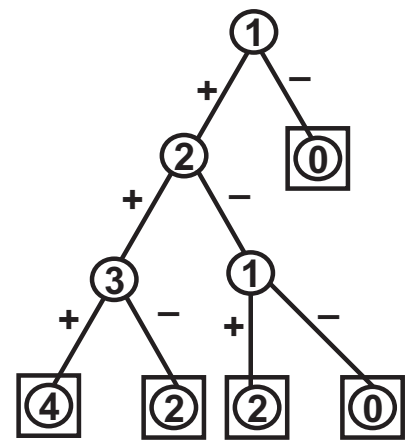


Рис. 4.1

Розділ 5

Теорія графів

5.1. Основні поняття теорії графів

Означення 5.1. Графом (геометричним графом) G називають фігуру на площині, яка складається з непорожньої скінченної множини V точок (вершин) і скінченної множини E орієнтованих чи не орієнтованих ліній (ребер), що з'єднують деякі пари вершин.

Надалі, якщо не вказано інше, вершини позначатимемо літерою v з індексами чи без: v, v_2, $v_{2,34}$; ребра – літерою e з індексами чи без: e, e_6, $e_{8,3,97}$.

Ребро, що з'єднує деяку вершину саму з собою, називають *петлею*. Ребра, що з'єднують одну й ту саму пару вершин, називають *мультиребрами*. Граф, що не містить мультиребер та петель, називають *простим графом*, або *простографом*. Граф, в якому допускаються мультиребра чи петлі, називають *мультиграфом* (див. прикл. 5.1).

Граф, усі ребра якого неорієнтовані, називають *неорієнтованим графом*; граф, усі ребра якого орієнтовані – *орієнтованим графом*, або *орграфом*; мішані графи (містять як орієнтовані, так і неорієнтовані ребра) ми не розглядатимемо. В орграфах пари протинапрямлених мультиребер, що з'єднують одну й ту саму пару вершин, часто зображують однією лінією зі стрілками на протилежних кінцях.

Приклад 5.1. На рис. 5.1 зображено орієнтований мультиграф G_1, неорієнтований простограф G_2 та неорієнтований мультиграф G_3. Вершини v_1 та v_3 графу G_1 з'єднуються двома протинапрямленими мульти-

ребрами (зображені лінією з двома стрілками). На вершині v_4 неорієнтованого мультиграфу G_3 «висить» петля.

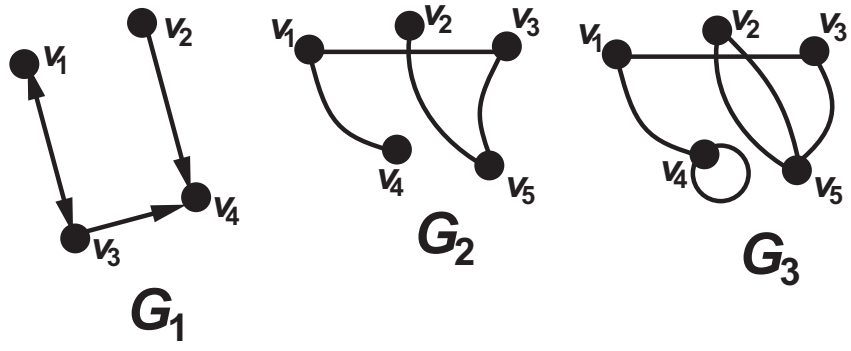


Рис. 5.1

Надалі, якщо не вказано інше, графи вважатимемо неорієнтованими.

Вершини v_1 та v_2 називають *суміжними*, якщо вони з'єднані ребром e. У такому разі кажуть, що вершини v_1 та v_2 *інцидентні* ребру e; аналогічно, ребро e *інцидентне* вершинам v_1 та v_2.

Шляхом у графі, що починається у вершині v_1 і закінчується у вершині v_2, називають послідовність вершин та ребер вигляду:

$$v_1 e_{i_1} v_{i_1} e_{i_2} v_{i_2} e_{i_3} \dots v_{i_{n-1}} e_{i_n} v_2,$$

де кожне ребро інцидентне обом вершинам, які є для нього сусідніми в послідовності (ребро e_{i_1} інцидентне вершинам v_1 та v_{i_1}, ребро e_{i_2} інцидентне вершинам v_{i_1} та v_{i_2} і т. д.). Зазначимо, що шлях у графі однозначно визначається першою і останньою вершинами (v_1 та v_2) та послідовністю ребер, тобто проміжні вершини можна не вказувати:

$$v_1 e_{i_1} e_{i_2} e_{i_3} \dots e_{i_n} v_2.$$

Крім того, для простографів (але не для мультиграфів) шлях однозначно визначається послідовністю вершин:

$$v_1 v_{i_1} v_{i_2} \dots v_{i_{n-1}} v_2.$$

Зазначимо, що для орієнтованих графів шлях визначається аналогічно, але з урахуванням орієнтації ребер: ребро e_{i_1} має вести від v_1 до v_{i_1}, ребро e_{i_2} – від v_{i_1} до v_{i_2} і т. д.

Шлях, який не містить повторень вершин і ребер, крім, можливо, двох крайніх вершин v_1 та v_2, називають *простим шляхом*. Легко перевірити, що повторення ребер у шляху веде до повторення вершин (однак можливо, що повторюватимуться лише дві крайні вершини).

Замкнений шлях ($v_1 = v_2$) називають *циклом*. Простий замкнений шлях називають *простим циклом*.

Лема 5.1. *Будь-який шлях, що з'єднує вершини v_1 та v_2 ($v_1 \neq v_2$), містить простий шлях, що з'єднує ті ж вершини v_1 та v_2.*

Доведення. Для доведення леми достатньо видалити із шляху всі цикли, що виникають за будь-якого повторення вершин. □

Приклад 5.2. Розглянемо граф, зображений на рис. 5.2.

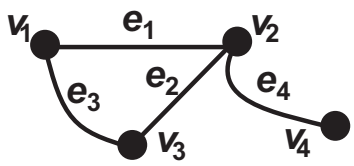


Рис. 5.2

Шлях $v_1e_1e_2e_3v_1$ у цьому графі – простий цикл, шлях $v_1e_1e_4v_4$ – простий шлях (але не цикл, оскільки $v_1 \neq v_4$), шлях $v_1e_1e_1v_1$ – цикл (але не простий цикл, оскільки повторюється ребро e_1).

Надалі, якщо не вказано інше, графи вважатимемо і неорієнтованими, і простими.

5.2. Степені вершин графу. Теорема про степені вершин

Означення 5.2. Степенем d_v вершини v називають кількість ребер, інцидентних v. Якщо $d_v = 0$, вершину v називають ізольованою. Вершину парного степеня називають парною, непарного степеня – непарною.

Приклад 5.3. Розглянемо граф на рис. 5.3.

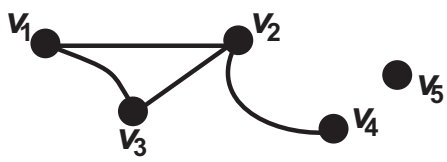


Рис. 5.3

Для цього графу маємо вершини із степенями: $d_{v_1} = d_{v_3} = 2$, $d_{v_2} = 3$, $d_{v_4} = 1$, $d_{v_5} = 0$. Отже, вершина v_5 ізольована.

Очевидно, степінь вершини в простих графах (а саме прості графи ми зараз розглядаємо) лежить у межах від 0 до $n_v - 1$, де $n_v = \mathrm{card}(V)$ – загальна кількість вершин у графі. Граф, усі вершини якого ізольовані, називають *порожнім графом*. Граф, усі вершини якого мають степінь $n_v - 1$, називають *повним графом*. Очевидно, в порожньому графі кількість ребер $n_e = \mathrm{card}(E) = 0$, в повному графі кількість ребер $n_e = C^2_{n_v}$.

Теорема 5.1. *Довільний (простий та неорієнтований) граф містить принаймні дві вершини однакового степеня.*

Доведення. Припустімо, що в графі G всі вершини мають різні степені. Тоді, оскільки степінь вершини є цілим числом у межах від 0 до $n_v - 1$ (всього n_v можливих значень), граф G має містити вершини всіх степенів від 0 до $n_v - 1$. Отже, граф G має містити ізольовану вершину v_0 ($d_{v_0} = 0$) та вершину v_{n_v-1} степеня $n_v - 1$, що неможливо: вершина v_{n_v-1} має бути суміжною з усіма вершинами графу G, зокрема з ізольованою вершиною v_0. □

Означення 5.3. Нехай G – граф з множиною вершин V та множиною ребер E. Граф G_1 з множиною вершин V_1 та множиною ребер E_1 називають підграфом графу G, якщо $V_1 \subset V$ та $E_1 \subset E$.

Важливим класом підграфів є графи, які отримують операціями *видалення вершин* та *видалення ребер* – загальний зміст цих операцій зрозуміло з назви. Вважають, що у разі видалення вершини v разом із вершиною v видаляються всі ребра, які їй інцидентні; у разі видалення ребра множина вершин не змінюється.

Приклад 5.4. На рис. 5.4 графи G_2 та G_3 отримані з G_1 видаленням вершини v_2 та ребра e відповідно.

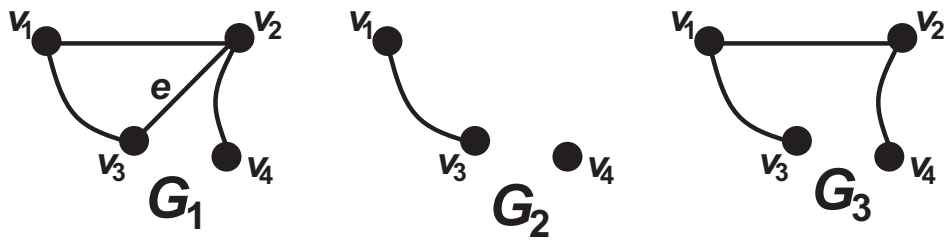


Рис. 5.4

Теорема 5.2 (теорема про степені вершин)**.** *Сума степенів усіх вершин графу дорівнює подвійній кількості ребер:*

$$\sum_{v\in V} d_v = 2n_e, \text{ де } n_e = \mathrm{card}(E) \text{ – кількість ребер у графі.}$$

Доведення. Застосуємо метод математичної індукції за n_e.

1. База індукції. $n_e = 0$. Очевидно, для порожнього графу твердження теореми справджується.

2. Припущення індукції. Нехай для графів з $n_e \le n$ твердження теореми справедливе.

3. Крок індукції. Нехай граф G має $n_e = n + 1$ ребро. Для доведення теореми видалимо у графі G довільне ребро e. Отримуємо граф $\widetilde{G}$ з кількістю ребер $n_e - 1 = n$, для якого твердження теореми, за припущенням індукції, справедливе. Отже, для $\widetilde{G}$ маємо:

$$\sum_{v\in V} \widetilde{d}_v = 2(n_e - 1), \text{ де } \widetilde{d}_v \text{ – степінь вершини } v \text{ у графі } \widetilde{G}.$$

Нарешті, оскільки видалене ребро e збільшувало суму степенів вершин на 2 (по 1 на кожну з двох вершин, інцидентних e), для графу G маємо:

$$\sum_{v\in V} d_v = 2(n_e - 1) + 2 = 2n_e. \qquad \square$$

Зауваження 5.1. Теорема 5.2 залишається правильною і для мультиграфів, якщо визначаючи степінь вершини вважати, що кожна петля збільшує степінь відповідної вершини на 2. Доведення теореми при цьому практично не змінюється.

Приклад 5.5. Для графу, зображеного на рис. 5.5, маємо такі степені вершин:

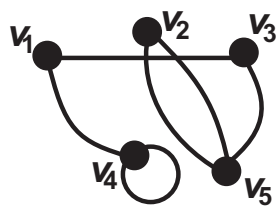


Рис. 5.5

$d_{v_1} = d_{v_2} = d_{v_3} = 2$, $d_{v_4} = 3$ (петля збільшила степінь на 2), $d_{v_5} = 3$. Отже,

$$\sum_{v\in V} d_v = \sum_{k=1}^{5} d_{v_k} = 12 = 2n_e.$$

5.3. Зв'язність графів

Означення 5.4. Граф G називають зв'язним, якщо будь-які дві його вершини можуть бути з'єднані шляхом. Максимальний за включенням («$\subset$») зв'язний підграф графу G називають зв'язною компонентою, або областю зв'язності.

Очевидно, граф зв'язний тоді і тільки тоді, коли він сам є областю зв'язності; у загальному випадку кожен граф є об'єднанням скінченної кількості областей зв'язності.

Приклад 5.6. Розглянемо граф, зображений на рис. 5.6.

Цей граф містить три області зв'язності: підграф з вершинами v_1, v_2, v_3, v_4, підграф з вершинами v_5, v_6, v_7 та підграф, що містить одну ізольовану вершину v_8.

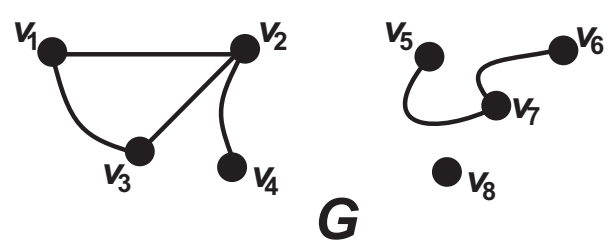


Рис. 5.6

Означення 5.5. Граф $\overline{G}$ називають доповненням (доповняльним графом) до графу G, якщо:

- множини вершин графів G та $\overline{G}$ збігаються;
- вершини v_1 та v_2 суміжні в графі $\overline{G}$ тоді і тільки тоді, коли вони не суміжні в графі G.

Очевидно, переріз графів G та $\overline{G}$ – порожній граф, об'єднання G та $\overline{G}$ – повний граф.

Теорема 5.3. *Принаймні один із графів G або $\overline{G}$ зв'язний.*

Доведення. Припустімо, що граф G не зв'язний. Доведемо, що в цьому разі граф $\overline{G}$ зв'язний.

Оскільки граф G не зв'язний, у G знайдеться принаймні одна область зв'язності $G_0 \neq G$. Зафіксуємо довільну вершину $v_0 \in G_0$ та довільну вершину $v \notin G_0$. За визначенням області зв'язності вершина v_0 не є суміжною (і навіть не з'єднана жодним шляхом) у графі G з вершиною v. Тоді, за визначенням доповняльного графу, вершина v_0 суміжна

з вершиною v у графі $\overline{G}$. Отже, дві будь-які вершини v_1 та v_2 у графі $\overline{G}$ будуть з'єднані шляхом довжини не більше за 2: вершини v_1 та v_2 суміжні (з'єднані одним ребром), якщо рівно одна з цих вершин належить G_0; вершини v_1 та v_2 з'єднані шляхом довжини 2, що проходить через довільну вершину $v_0 \in G_0$, якщо $v_1, v_2 \notin G_0$; вершини v_1 та v_2 з'єднані шляхом довжини 2, що проходить через довільну вершину $v \notin G_0$, якщо $v_1, v_2 \in G_0$. □

Приклад 5.7. На рис. 5.7 зображено граф G та його доповняльний $\overline{G}$. Граф G не є зв'язним, однак доповняльний граф $\overline{G}$ – зв'язний.

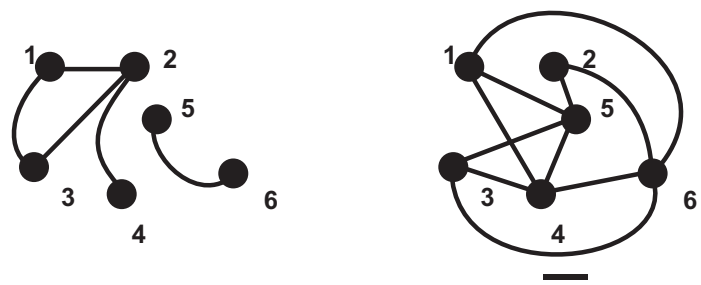


Рис. 5.7

Вправа 5.1. Навести приклад графу, зв'язного разом із своїм доповненням.

Означення 5.6. Мостом називають ребро графу, видалення якого веде до збільшення кількості областей зв'язності. Точкою з'єднання називають вершину графу, видалення якої веде до збільшення кількості областей зв'язності.

Очевидно, для зв'язного графу видалення моста чи точки з'єднання веде до втрати зв'язності.

Наступне твердження негайно випливає з визначення зв'язності та твердження леми 5.1.

Лема 5.2. *Ребро є мостом тоді і тільки тоді, коли воно не входить у жодний простий цикл.*

Приклад 5.8. Розглянемо граф, зображений на рис. 5.8.

Легко перевірити, що вершина v_2 – точка з'єднання, ребро e – міст. Зазначимо, що цей граф містить один простий цикл $v_1v_2v_3$, який проходить через усі ребра графу, крім ребра e.

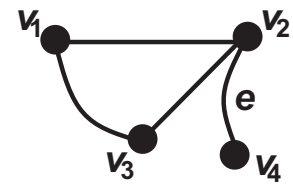


Рис. 5.8

5.4. Ейлерові і напівейлерові графи

Означення 5.7. Ейлеровим шляхом у графі називають шлях, який містить кожне ребро графу рівно один раз (проходить через кожне ребро без повторень). Замкнений ейлерів шлях називають ейлеровим циклом. Зв'язний граф, що допускає побудову ейлерового циклу (шляху), називають ейлеровим (напівейлеровим).

Проблема розпізнавання ейлеровості та напівейлеровості графів історично пов'язана із відомою *проблемою кенігсберзьких мостів*. На початку XVIII століття в місті Кенігсберзі (нині – Калінінград) було сім мостів, що вели через річку Прегель.

На рис. 5.9 зображено схему розташування кенігсберзьких мостів та відповідний мультиграф: кожній зв'язній області суші відповідає вершина графу, кожному мосту – ребро.

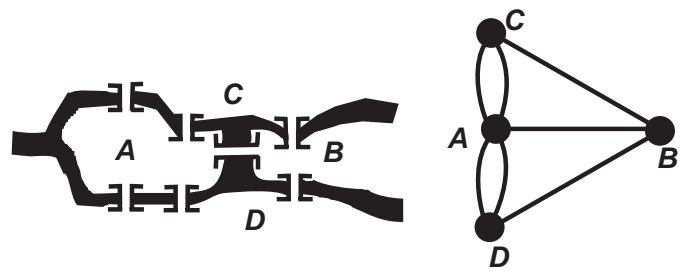


Рис. 5.9

Проблема: чи можна обійти всі мости рівно по одному разу, повернутись у вихідний пункт? Очевидно, в термінах теорії графів проблема кенігсберзьких мостів зводиться до розпізнавання ейлеровості відповідного графу. Цю проблему в загальному випадку розв'язав знаменитий учений XVIII сторіччя Леонард Ейлер (саме його ім'ям названі цикли, що містять кожне ребро графу без повторень).

Теорема 5.4 (Л. Ейлер, 1736 р.)**.** *Зв'язний граф є ейлеровим тоді і тільки тоді, коли всі його вершини парні.*

Доведення. Необхідність. Нехай граф (зв'язний) є ейлеровим. Оскільки ейлерів цикл містить всі ребра графу без повторень, кожна вершина, що входить до циклу k разів, входить у цикл з парною кількістю $2k$ інцидентних їй ребер. Отже, степінь кожної вершини графу є парне число $2k$, де k – кількість входжень вершини до ейлерового циклу.

Достатність. Нехай всі вершини зв'язного графу G парні. Вважатимемо, що G не порожній (випадок порожнього графу, очевидно, не потребує доведення). Доведення ейлеровості графу G проведемо в два етапи.

A. Зафіксуємо довільну вершину $v_0 \in V$ і, починаючи з v_0, побудуємо цикл, що містить без повторень деякі (не обов'язково всі) ребра графу G. Оскільки G – зв'язний граф, існує принаймні одне ребро e_1, інцидентне вершині v_0. Ребро e_1 веде від v_0 до деякої вершини $v_1 \neq v_0$. Оскільки v_1 парна, існує принаймні одне ребро $e_2 \neq e_1$, інцидентне вершині v_1.

У загальному випадку, нехай на n-му кроці ми побудували шлях $v_0e_1v_1 \dots e_nv_n$, такий, що $v_k \neq v_0$ при $0 < k < n$ та $e_k \neq e_j$ при $k \neq j$ (підкреслимо, що вершини в побудованому шляху можуть повторюватись). Якщо $v_n = v_0$, побудований шлях є циклом. Нехай $v_n \neq v_0$. Нехай вершина v_n входить у побудований шлях m разів. Тоді побудований шлях містить $2m-1$ ребер, інцидентних v_n: при всіх входженнях, окрім останнього, вершина v_n входить з двома інцидентними їй ребрами, при останньому входженні додається ребро e_n. Отже, має існувати принаймні одне ребро e_{n+1}, інцидентне v_n, що не входить у побудований шлях. Додамо ребро e_{n+1} до побудованого шляху, отримуючи шлях $v_0e_1v_1 \dots e_nv_ne_{n+1}v_{n+1}$, і т. д. Цей процес має закінчитись (на вершині v_0) за скінченну кількість кроків, оскільки граф G має скінченну кількість ребер.

B. Нехай цикл P, побудований на першому етапі, містить не всі ребра графу G (інакше побудований цикл P – ейлерів). Розглянемо граф G_1, отриманий з графу G видаленням усіх ребер, які увійшли в цикл P. Очевидно, G_1 містить ті і тільки ті ребра, які не увійшли в P. Звідси випливає, що кожна вершина графу G_1 парна. Оскільки граф G зв'язний, цикл P містить принаймні одну вершину v_k, яка інцидентна деякому ребру графу G_1. Застосувавши алгоритм першого етапу для графу G_1 з початковою вершиною v_k, побудуємо цикл Q, що містить без повторень деякі (можливо, не всі) ребра графу G_1.

Нарешті, побудуємо цикл $P_1 = v_k P v_k Q v_k$, що містить без повторень всі ребра, які увійшли в цикли P та Q. По суті, ми тимчасово «розмикаємо» цикл P у вершині v_k і додаємо цикл Q (рис. 5.10). Очевидно, цей процес має закінчитись за скінченну кількість кроків побудовою ейлерового циклу в графі G.

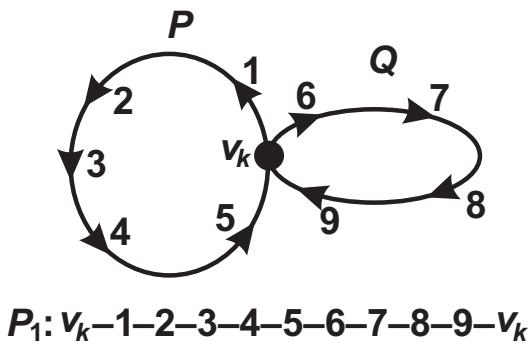


Рис. 5.10

□

Наслідок. *Зв'язний граф є напівейлеровим тоді і тільки тоді, коли він містить не більше як дві непарні вершини.*

Доведення. Необхідність. Нехай граф є напівейлеровим, але не ейлеровим (для ейлерового графу всі вершини парні). Для доведення існування рівно двох непарних вершин достатньо з'єднати початок та кінець ейлерового шляху і застосувати до отриманого графу твердження основної теореми.

Достатність. Нехай граф має дві непарні вершини (ситуація однієї непарної вершини неможлива через теорему 5.2 – про степені вершин). Для доведення напівейлеровості достатньо з'єднати ребром дві непарні вершини і застосувати твердження основної теореми. □

Зауваження 5.2. Легко зрозуміти, що за наявності рівно двох непарних вершин у зв'язному графі ейлерів шлях має починатись та закінчуватись саме в непарних вершинах.

Вправа 5.2. Узагальнити доведення теореми 5.4 та її наслідку на випадок мультиграфів (нагадаємо, що петля збільшує степінь вершини на 2).

Приклад 5.9. Граф «кенігсберзькі мости» (див. рис. 5.9) не є ні ейлеровим, ні навіть напівейлеровим, оскільки всі його вершини непарні.

До розпізнавання ейлеровості (напівейлеровості) графів зводиться добре відома давня проблема: намалювати фігуру, не відриваючи олівець від паперу, з поверненням (без повернення) до вихідної точки.

Приклад 5.10. Розглянемо граф, зображений на рис. 5.11.

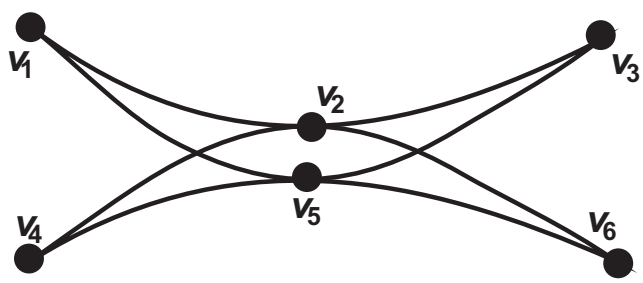


Рис. 5.11

Цей граф відповідає стародавній (приблизно тисяча років) проблемі «шаблей Магомета» – треба намалювати «шаблі Магомета», не відриваючи олівець від паперу. Очевидно, проблема має розв'язок, оскільки граф ейлерів (усі вершини парні). Одним з можливих (але не єдиним) ейлерових циклів у цьому графі є цикл $v_1v_2v_6v_5v_4v_2v_3v_5v_1$.

Для практичної побудови ейлерового циклу (шляху) можна скористатись дуже простим та ефективним *алгоритмом Флері*.

5.4.1. Алгоритм Флері

1. Ейлерів цикл можна починати з будь-якої вершини (ейлерів шлях треба починати з однієї з непарних вершин).

2. Під час побудови ейлерового циклу (шляху) з графу видаляють ребра, що входять до циклу.

3. На кожному кроці можна вибирати довільне ребро, яке, за можливості, не є мостом (з урахуванням видалення ребер на попередніх кроках); міст можна обирати лише тоді, коли всі ребра, інцидентні даній вершині, є мостами.

Обґрунтування коректності алгоритму Флері див., наприклад, в [8].

Приклад 5.11. Розглянемо граф на рис. 5.12.

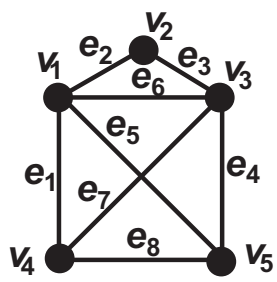


Рис. 5.12

Цей граф є напівейлеровим, оскільки має рівно дві непарні вершини (v_4 та v_5). Застосовуючи алгоритм Флері, отримуємо один із можливих ейлерових шляхів: $v_4e_1v_1e_2v_2e_3v_3e_4v_5e_5v_1e_6v_3e_7v_4e_8v_5$. Зазначимо, що на трьох останніх кроках обрано мости e_6, e_7 та e_8, оскільки було неможливо вибрати ребро, яке не є мостом.

5.5. Поняття про гамільтонові та напівгамільтонові графи

Означення 5.8. Гамільтоновим шляхом у графі називають простий шлях, який містить кожну вершину графу рівно один раз (проходить через кожну вершину без повторень). Замкнений гамільтонів шлях називають гамільтоновим циклом. Граф, що допускає побудову гамільтонового циклу, називають гамільтоновим. Граф, що допускає побудову гамільтонового шляху, називають напівгамільтоновим.

Історично проблема розпізнавання гамільтоновості графу пов'язана з головоломкою «кругосвітня подорож», запропонованою 1859 року ірландським математиком Уільямом Гамільтоном: кожній з двадцяти вершин додекаедра (рис. 5.13) відповідає назва одного з великих міст світу; потрібно, пересуваючись по ребрах графу, обійти всі вершини рівно по одному разу та повернутись у пункт початку подорожі.

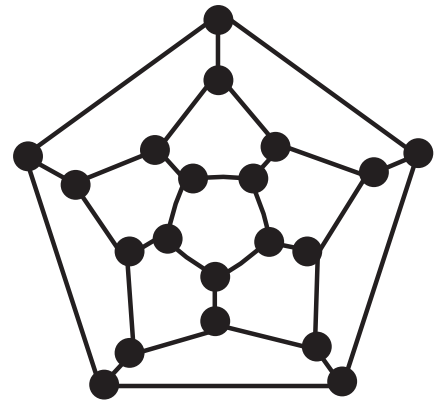


Рис. 5.13

Проблеми розпізнавання ейлеровості (напівейлеровості) та гамільтоновості (напівгамільтоновості) графів, незважаючи на їх зовнішню схожість, принципово різні. Для розпізнавання ейлеровості графу існує ефективний критерій (теорема 5.4), а для практичної побудови ейлерового циклу можна скористатись простим та зручним алгоритмом Флері.

Ситуація щодо гамільтоновості набагато складніша – сьогодні не існує ефективного критерію (теореми про необхідні та достатні умови) гамільтоновості (напівгамільтоновості) графів. Проте існує ряд теорем про необхідні умови та ряд теорем про достатні умови гамільтоновості (напівгамільтоновості). Деякі з цих теорем розглянемо в цьому підрозділі.

5.5.1. Необхідні умови гамільтоновості графів

Наступна лема наводить два очевидних типи графів, належність до яких виключає можливість гамільтоновості.

Лема 5.3. *Жоден граф, що містить точку з'єднання або міст, не є гамільтоновим.*

Твердження леми 5.3 випливає безпосередньо з визначення моста та точки з'єднання.

Розглянемо ще один важливий клас графів, належність до якого виключає можливість гамільтоновості.

Означення 5.9. Граф G називають Θ-графом (тета-графом), якщо він складається з двох вершин степені 3, сполучених трьома простими шляхами довжиною не менше 2, що попарно не перетинаються (жодні два з цих трьох шляхів не мають спільних вершин, окрім спільного початку та спільного кінця).

Приклад 5.12. Графи G_1 та G_2, зображені на рис. 5.14, – приклади Θ-графів, однак граф G_3 не є Θ-графом.

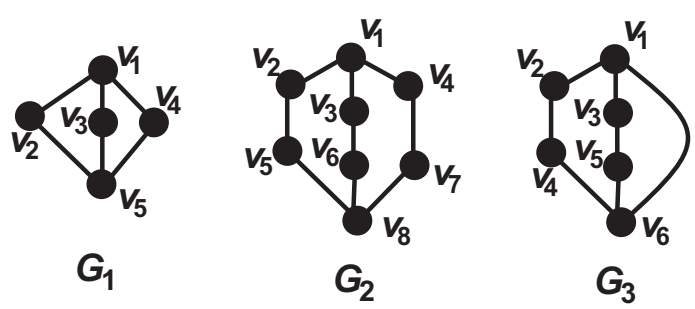


Рис. 5.14

Теорема 5.5. *Жоден Θ-граф не є гамільтоновим.*

Доведення. Припустімо, що твердження теореми не справджується. Нехай Θ-граф G містить дві вершини v_1 та v_2, сполучені трьома шляхами S_1, S_2, S_3 довжиною не менше 2, що попарно не перетинаються (рис. 5.15). Припустімо, що граф G є гамільтоновим. Оскільки шляхи S_1, S_2, S_3 містять принаймні по одній вершині (не враховуючи v_1 та v_2), гамільтонів цикл має проходити рівно по одному разу через кожен із шляхів S_1, S_2 та S_3. Але тоді, враховуючи замкненість, цикл має пройти двічі по вершинах v_1 та v_2, що суперечить визначенню гамільтоновості циклу. □

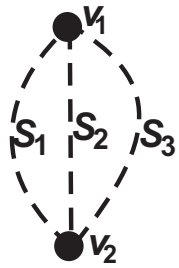


Рис. 5.15

Зауваження 5.3. Жоден Θ-граф не є гамільтоновим, однак кожен Θ-граф є напівгамільтоновим. Так, Θ-графи G_1 та G_2 з прикл. 5.12 допускають гамільтонові шляхи $v_3v_1v_2v_5v_4$ (G_1) та $v_6v_3v_1v_2v_5v_8v_7v_4$ (G_2).

5.5.2. Достатні умови гамільтоновості графів

Наведемо без доведення деякі достатні умови гамільтоновості та напівгамільтоновості графів.

Теорема 5.6 (О. Оре, 1960 р.). *Нехай G – зв'язний граф з кількістю вершин $n = \mathrm{card}(V) \geq 3$.*

1. Якщо для будь-якої пари несуміжних вершин u та v виконується нерівність $d_u + d_v \geq n$, граф G – гамільтонів.

2. Якщо для будь-якої пари несуміжних вершин u та v виконується нерівність $d_u + d_v \geq n - 1$, граф G – напівгамільтонів.

З теореми 5.6 негайно випливає такий результат (доведений, щоправда, на кілька років раніше теореми 5.6).

Теорема 5.7 (Г. Дірак, 1953 р.). *Нехай G – зв'язний граф з кількістю вершин $n = \mathrm{card}(V) \geq 3$. Якщо для будь-якої вершини $v \in V$ виконується нерівність $d_v \geq n/2$, граф G є гамільтоновим.*

Ще одна достатня умова гамільтоновості пов'язана з наявністю Θ-підграфів.

Теорема 5.8. *Будь-який зв'язний негамільтонів граф без мостів та точок з'єднання містить Θ-підграф.*

Практичне застосування теореми 5.8 пов'язане з аналізом наявності Θ-підграфів: зв'язний граф без мостів точок з'єднання, що не містить Θ-підграфів, за теоремою 5.8 є гамільтоновим.

Про інші достатні умови гамільтоновості див. [8].

Зазначимо, що теореми 5.6, 5.7 та 5.8 дають лише достатні, але не необхідні умови гамільтоновості графу.

Приклад 5.13. Одне з найважливіших застосувань теорії гамільтонових графів пов'язане з проблемою купця (комівояжера). Наведемо

дещо спрощене формулювання цієї проблеми: купець повинен, користуючись системою доріг, побувати в усіх населених пунктах країни та повернутись до пункту початку подорожі (порівняйте з головоломкою У. Гамільтона). Очевидно, проблема зводиться до розпізнавання гамільтоновості відповідного графу.

Приклад 5.14. Ще одне цікаве застосування теорії гамільтонових графів пов'язане з проблемою обходу шаховим конем всіх клітинок шахівниці рівно по одному разу, з поверненням чи без повернення до початкового поля. Ця проблема зводиться до розпізнавання гамільтоновості (напівгамільтоновості) графу з 64 вершинами: кожна вершина графу відповідає певному полю шахівниці; суміжними є ті і тільки ті вершини, які можуть бути з'єднані на шахівниці ходом коня.

Як відомо, ця проблема має розв'язок: всі поля шахівниці можна обійти ходом коня, повернувшись до початкового поля. Зазначимо, що до відповідного графу не можна застосувати жодну з теорем 5.6, 5.7 або 5.8 – умови цих теорем не виконуються, проте граф є гамільтоновим.

5.6. Спеціальні типи графів

5.6.1. Регулярні графи

Означення 5.10. Регулярним графом називають граф, усі вершини якого мають однаковий степінь.

Приклад 5.15. Регулярним графом, очевидно, є довільний повний граф ($d_v = n - 1$, де $n = \text{card}(V)$), а також довільний порожній граф ($d_v = 0$).

Приклад 5.16. Граф, зображений на рис. 5.16, – регулярний: $d_v = 2$ для всіх $v \in V$.

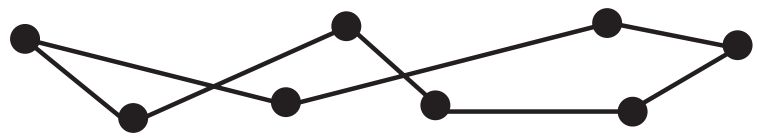


Рис. 5.16

5.6.2. Дводольні графи

Означення 5.11. Дводольним називають граф, множину вершин якого можна розбити на дві непорожні підмножини (долі) V_1 та V_2 ($V_1 \cap V_2 = \varnothing$) так, що будь-які дві вершини з однієї долі V_k ($k = 1, 2$) є несуміжними.

Приклад 5.17. Граф, зображений на рис. 5.17, є дводольним: $V_1 = \{v_1, v_3, v_5\}$, $V_2 = \{v_2, v_4, v_6\}$.

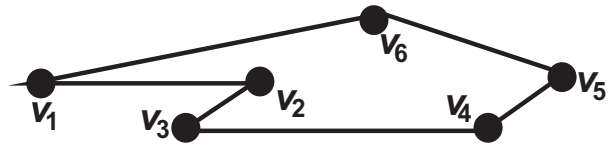


Рис. 5.17

Теорема 5.9 (Д. Кьоніг, 1936 р.)**.** *Граф є дводольним тоді і тільки тоді, коли всі його цикли мають парну довжину.*

Доведення необхідності. Нехай граф G з множиною вершин V є дводольним. Тоді множина V може бути зображена у формі $V = V_1 \cup V_2$, $V_1 \cap V_2 = \varnothing$ так, що будь-які дві вершини з однієї підмножини V_k ($k = 1, 2$) є несуміжними.

Розглянемо довільний цикл $v_1 v_2 \dots v_n$ ($v_n = v_1$). Без втрати загальності припустімо, що $v_1 \in V_1$. Тоді, враховуючи суміжність v_1 та v_2, отримуємо, що $v_2 \notin V_1$, тобто $v_2 \in V_2$. Аналогічно, $v_3 \in V_1$, $v_4 \in V_2$ і т. д., тобто $v_{2k+1} \in V_1$, $v_{2k} \in V_2$ ($0 \leq 2k \leq n$). Оскільки $v_n = v_1 \in V_1$, отримуємо, що $n = 2k + 1$ і довжина циклу $n - 1 = 2k$ – парне число.

Вправа 5.3. Самостійно довести достатність умови парності всіх циклів для дводольності графу.

Вказівка. Достатньо обмежитись випадком зв'язного графу, оскільки незв'язний граф є об'єднанням скінченної кількості областей зв'язності. Для зв'язного графу, що містить лише цикли парної довжини, розгляньте таке відношення еквівалентності на множині вершин V: $v_1 \sim v_2$ тоді і тільки тоді, коли v_1 та v_2 з'єднані лише шляхами парної довжини. Перевірте, що введене відношення справді є відношенням еквівалентності, і фактор-множина $V/_{\sim} = \{V_1, V_2\}$ дає шукане розбиття множини V.

□

5.6.3. Дерева

Деревом називають зв'язний граф, що не містить простих циклів. *Лісом* називають граф, що є об'єднанням дерев, які попарно не перерізаються.

Приклад 5.18. Граф, зображений на рис. 5.18, є лісом (об'єднання двох дерев, які не перерізаються).

Рис. 5.18

Здебільшого доцільно виділити одну з вершин дерева як початкову (вершина, з якої дерево «зростає»). Дерево з виділеною вершиною називають *кореневим деревом*, виділену вершину називають *кореневою вершиною*, або *коренем*. Підкреслимо, що коренем можна вибрати довільну вершину дерева; доцільність вибору кореневої вершини визначається проблемою, яка розв'язується за допомогою даного дерева. Як правило, кореневі дерева зображують так, щоб дерево «зростало» від кореня в одному фіксованому напрямку – вниз, вгору, вправо або вліво.

Рівнем вершини кореневого дерева називають довжину простого шляху, що з'єднує цю вершину з коренем. Множину вершин n-го рівня називають *n-м ярусом* кореневого дерева. Очевидно, ярус рівня 0 завжди містить лише саму кореневу вершину.

Кажуть, що вершина v_1 n-го рівня *породжує* вершину v_2 $(n+1)$-го рівня, якщо вершини v_1 і v_2 суміжні. Вершину кореневого дерева, що не породжує жодну вершину даного дерева, часто називають *листком*.

Приклад 5.19. Дерево, що зображене на рис. 5.19, можна розглядати як кореневе з кореневою вершиною v.

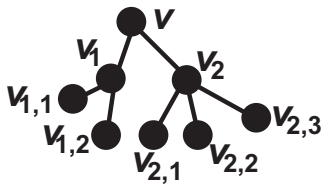


Рис. 5.19

Ярус рівня 0 містить кореневу вершину v; ярус рівня 1 містить вершини v_1 та v_2 (породжуються вершиною v); ярус рівня 2 містить вершини $v_{1,1}$ та $v_{1,2}$ (породжуються вершиною v_1), а також $v_{2,1}$ та $v_{2,2}$ та $v_{2,3}$ (породжуються вершиною v_2). Очевидно, листками цього дерева є вершини $v_{1,1}$, $v_{1,2}$, $v_{2,1}$, $v_{2,2}$, $v_{2,3}$.

Слід звернути увагу на багатоіндексну нумерацію вершин кореневого дерева в прикл. 5.19:

- кореневій вершині присвоюється «порожній» номер (вершина v);
- вершини, що породжені вершиною v_s, нумеруються (у довільному порядку) як вершини $v_{s,i}$, $i = 1, 2, \ldots, m$.

Запропонований спосіб нумерації вершин кореневого дерева (іноді його називають *упакованою адресацією*) дозволяє однозначно визначити, які вершини дерева суміжні, і часто використовується під час аналізу структури дерева комп'ютерними алгоритмами.

Зазначимо, що одне з важливих застосувань кореневих дерев – розв'язання комбінаторних задач – розглянуто в підрозд. 4.6.

5.6.4. Поняття про мічені графи

Означення 5.12. Міченим графом, або мережею називають граф, вершинам або (та) ребрам якого зіставляється певна мітка.

Мітками міченого графу можуть бути елементи довільної множини. Так, розглядаючи проблему комівояжера (див. прикл. 5.13) доцільно ребрам графу присвоїти довжину відповідної ділянки шляху, а вершинам – час на перебування у відповідному місті.

Ще одне важливе застосування мічених графів пов'язане з фарбуванням вершин або ребер (мітками є кольори). Фарбування вершин графу розглянемо далі в підрозд. 5.14.

5.7. Ізоморфізм і гомеоморфізм графів

Означення 5.13. Графи G_1 і G_2 з множинами вершин V_1 та V_2 називають ізоморфними, якщо існує така бієкція (ізоморфізм) $f : V_1 \to V_2$, що:

$$\forall u, v \in V_1 : (u,\ v \text{ – суміжні в } G_1) \Leftrightarrow (f(u),\ f(v) \text{ – суміжні в } G_2).$$

Отже, ізоморфізм графів можна розуміти як взаємно однозначне відображення, що зберігає суміжність вершин.

Приклад 5.20. Графи G_1 та G_2, зображені на рис. 5.20, ізоморфні; можливий (але не єдиний) ізоморфізм $f\colon u_k \mapsto v_k$, $k = 1, 2, 3, 4$.

Рис. 5.20

Зауваження 5.4. Визначення ізоморфності природно переноситься на випадок орієнтованих та неорієнтованих мультиграфів: ізоморфізм мультиграфів має зберігати кількість ребер між даними вершинами, а для орграфів – кількість ребер між даними вершинами, що ведуть у даному напрямку.

Надалі нам знадобиться операція *підрозбиття ребра графу.*

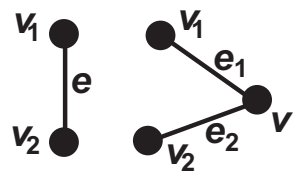


Рис. 5.21

Нехай ребро e інцидентне вершинам v_1 та v_2. Підрозбиття ребра e полягає у видаленні e та додаванні двох нових ребер e_1, e_2 і нової вершини v так, що: ребро e_1 інцидентне вершинам v_1 і v, ребро e_2 інцидентне вершинам v і v_2 (рис. 5.21). По суті, підрозбиття ребра e зводиться (з точністю до ізоморфізму) до «навішування» на ребро e нової вершини v.

Означення 5.14. Графи G_1 і G_2 називають гомеоморфними, якщо їх можна отримати з ізоморфних графів скінченною кількістю операцій підрозбиття ребер.

Приклад 5.21. Графи G_1 та G_2, зображені на рис. 5.22, гомеоморфні, оскільки їх можна отримати з ізоморфних графів G_1' та G_2' підрозбиттям ребер.

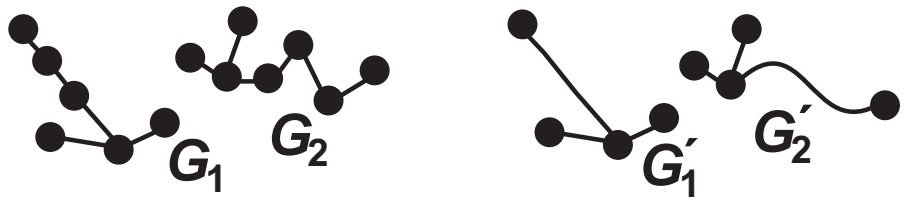


Рис. 5.22

Зауваження 5.5. Визначення операції підрозбиття ребер та гомеоморфності графів природно поширюється на випадок орієнтованих та неорієнтованих мультиграфів.

5.8. Матриця суміжності графу

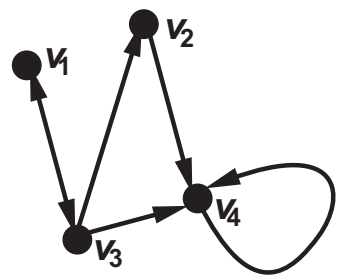
У цьому підрозділі працюватимемо з орієнтованими графами, дві різні вершини яких не можуть бути з'єднані двома або більше ребрами, що ведуть в одному напрямку. Інакше кажучи, працюватимемо з орграфами, в яких дозволяємо петлі та пари протинапрямлених мультиребер.

Означення 5.15. Нехай граф G, що задовольняє вимоги цього підрозділу, має множину вершин $V = \{v_1, \ldots, v_n\}$. Матрицею суміжності графу G називають матрицю M_G розміром $n \times n$, таку що:

$$(M_G)_{i,j} = \begin{cases} 1, & \text{від } v_i \text{ до } v_j \text{ веде ребро;} \\ 0, & \text{від } v_i \text{ до } v_j \text{ не веде ребро.} \end{cases}$$

Легко зрозуміти, що вигляд матриці суміжності цього графу залежить від порядку нумерації вершин; зміна порядку нумерації вершин зумовлює переставлення відповідних рядків та стовпців матриці суміжності.

Приклад 5.22. На рис. 5.23 зображено граф і відповідну матрицю суміжності.



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

Рис. 5.23

Наступне твердження випливає безпосередньо з визначення ізоморфізму графів.

Лема 5.4. *Графи G_1 і G_2 ізоморфні тоді і тільки тоді, коли існує така нумерація вершин графу G_1, що матриці суміжності M_{G_1} і M_{G_2} збігаються.*

Орієнтовані мультиграфи без однонапрямлених мультиребер застосовують для зображення бінарного відношення на скінченній множині (див. розд. 3). У термінах теорії відношень матриця суміжності графу G є матрицею бінарного відношення, яке задано графом G. Без втрати загальності вважатимемо, що бінарне відношення, визначене графом G, задано на множині вершин V графу G.

Нагадаємо, що для матриць суміжності A та B розміром $n \times n$ визначений «логічний добуток» AB – замість арифметичних операцій суми та добутку використовуються відповідні логічні операції диз'юнкції та кон'юнкції (див. означення 3.3). Вважатимемо, що степінь A^k ($k \in \mathbb{N}$) матриці суміжності A також визначено через «логічний добуток».

Аналітичний апарат, пов'язаний з матрицею суміжності, дає змогу оцінити кількість кроків, потрібних для обчислення транзитивного замикання бінарного відношення на скінченній множині, тобто дає змогу довести теорему 3.2. Тепер теорема 3.2 є прямим наслідком наступного простого твердження.

Теорема 5.10. *Нехай G – орієнтований мультиграф без однонапрямлених мультиребер, M_G – матриця суміжності графу G, степінь M_G^k ($k \in \mathbb{N}$) визначено через «логічний добуток». Тоді*

$\big((M_G^k)_{i,j} = 1\big) \Leftrightarrow$ (*У графі G існує шлях довжиною k від v_i до v_j*).

Доведення. Теорему можна довести методом математичної індукції за k.

Вправа 5.4. Довести теорему самостійно.

Вказівка. Твердження цієї теореми є переформулюванням твердження вправи 3.1.

□

Приклади обчислення транзитивного замикання бінарного відношення наведені вище (див. прикл. 3.19).

5.9. Плоскі та планарні графи

Означення 5.16. Граф G називають плоским, якщо:

- жодне ребро e графу G не має точок самоперетину;
- жодні два ребра e_1 та e_2 графу G не мають точок перетину, окрім вершин, інцидентних обом ребрам e_1 та e_2.

Граф, ізоморфний плоскому, називають планарним.

Приклад 5.23. На рис. 5.24 зображено планарний граф G_1, ізоморфний плоскому графу G_2.

Рис. 5.24

Приклад 5.24. На рис. 5.25 зображено непланарні графи G_1 («Зірка») та G_2 («Три криниці»).

Рис. 5.25

Граф G_1, очевидно, є повним графом з вершинами v_1–v_5 (назва «Зірка» зумовлена зовнішнім виглядом цього графу). Граф G_2 – дводольний граф з долями $\{v_1, v_2, v_3\}$ та $\{v_4, v_5, v_6\}$, такий, що будь-які дві вершини з різних долей суміжні. Назва «Три криниці» походить від відомої проблеми про три будинки та три криниці: між трьома будинками (v_1, v_2, v_3) та трьома криницями (v_4, v_5, v_6) треба прокласти дев'ять шляхів без точок перетину так, щоб існував шлях від кожного будинку до кожної криниці.

Непланарність графів G_1 та G_2 буде доведено в підрозд. 5.13.

Наведемо без доведення відомий критерій планарності, отриманий незалежно Л. С. Понтрягіним (1927 р.) та К. Куратовським (1930 р.).

Теорема 5.11 (теорема Понтрягіна – Куратовського)**.** *Граф є планарним тоді і тільки тоді, коли він не містить підграфів, гомеоморфних графам «Зірка» та «Три криниці» (рис. 5.25).*

З теореми Понтрягіна – Куратовського негайно випливає, що будь-який повний граф з 5 та більше вершинами непланарний, і будь-який граф з 4 та менше вершинами планарний. Зазначимо, що необхідність умови теореми випливає з непланарності графів G_1 та G_2 (див. підрозд. 5.13). Повне доведення теореми Понтрягіна – Куратовського, а також ефективний алгоритм побудови ізоморфного плоского графу, див., наприклад, в [8].

Зауваження 5.6. Поняття плоского та планарного графів природно поширюється на випадок мультиграфів.

5.10. Грані графу. Формула Ейлера

У цьому підрозділі всі графи вважатимемо плоскими неорієнтованими мультиграфами.

5.10.1. Грані плоского графу

Означення 5.17. Гранню графу G називають максимальну за відношенням включення («$\subset$») область площини r, таку, що: будь-які дві точки $a, b \in r$ можуть бути з'єднані неперервною кривою, яка не має спільних точок з ребрами графу G, окрім, можливо, самих точок a та b. Множину ребер, що належать грані, називають межею грані.

Грані графу позначатимемо літерою r з індексами чи без (r, r_1, $r_{22,11}$), множину граней графу G позначатимемо через R.

Наведемо кілька очевидних тверджень, що негайно випливають з означення 5.17.

Лема 5.5. *Кожна точка площини належить принаймні одній грані даного графу.*

Лема 5.6. *Для кожного графу існує рівно одна необмежена грань (грань нескінченної площі).*

Необмежену грань графу називають *зовнішньою*, інші (обмежені) грані – *внутрішніми*.

Лема 5.7. *Кожне ребро, що не є мостом, належить межі рівно двох граней. Кожен міст належить межам рівно однієї грані.*

Приклад 5.25. Для графу, зображеного на рис. 5.26, множина граней $R = \{r_1, r_2, r_3, r_4\}$, зовнішньою є грань r_4 з межею $\{e_1, e_2, e_7, e_8\}$. Очевидно, міст e_8 належить межі лише однієї грані (r_4).

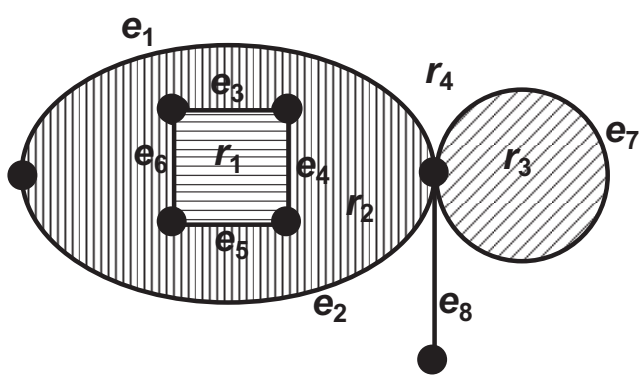


Рис. 5.26

5.10.2. Формула Ейлера для плоских графів

Теорема 5.12 (формула Ейлера для плоских графів)**.** *Нехай G – плоский зв'язний граф з n_v вершинами, n_e ребрами та n_r гранями. Тоді*

$$n_v - n_e + n_r = 2.$$

Доведення.

1. Нехай граф G – дерево. Доведення проводитимо індукцією за кількістю ребер n_e.

А. База індукції: $n_e = 0$ (порожній граф з однією вершиною). Оскільки $n_e = 0$, $n_r = 1$, отримуємо:

$$n_v - n_e + n_r = 1 - 0 + 1 = 2.$$

В. Припущення індукції: нехай при $n_e \leq n$ твердження теореми справджується.

C. Крок індукції: нехай $n_e = n + 1$. Видалимо у графі G довільне ребро e. Отримуємо граф $\widetilde{G}$, який є об'єднанням двох зв'язних компонент G_1 та G_2. Очевидно, графи G_1 та G_2 є деревами, що містять не більш як n ребер. Отже, за припущенням індукції, для G_1 та G_2 твердження теореми справджується. Позначивши через $n_{i,v}$, $n_{i,e}$, $n_{i,r}$ кількість відповідно вершин, ребер та граней у графі G_i $(i = 1, 2)$, дістанемо:

$$n_{i,v} - n_{i,e} + n_{i,r} = 2, \quad i = 1, 2.$$

Оскільки в довільному дереві, через відсутність простих циклів, існує лише одна (зовнішня) грань, маємо: $n_{1,r} = n_{2,r} = 1$. Отже, для графу G матимемо:

$$\begin{aligned} n_v - n_e + n_r = (n_{1,v} + n_{2,v}) - (n_{1,e} + n_{2,e} + 1) + 1 = \\ = (n_{1,v} - n_{1,e} + 1) + (n_{2,v} - n_{2,e} + 1) - 2 = 2. \end{aligned}$$

2. Нехай G – довільний плоский зв'язний граф. Доведення в загальному випадку проводитимемо також індукцією за кількістю ребер n_e.

A. База індукції: $n_e = 0$ для цього випадку твердження теореми вже доведено.

B. Припущення індукції: нехай при $n_e \leq n$ твердження теореми справджується.

C. Крок індукції: розглянемо граф G з $n_e = n + 1$ ребрами. Нехай G не є деревом (для дерев твердження теореми вже доведено), тоді, через наявність принаймні одного простого циклу, має існувати принаймні одне ребро e, що не є мостом (лема 5.2). Видаливши у графі G ребро e, отримуємо зв'язний граф $\widetilde{G}$ з n_v вершинами та $n_e - 1 = n$ ребрами. Оскільки за лемою 5.7 ребро e (не міст) належить межі двох граней, видалення ребра e зменшує кількість граней на 1. Отже, граф $\widetilde{G}$ містить $n_r - 1$ граней. За припущенням індукції, для графу $\widetilde{G}$ твердження теореми справедливе, і для вихідного графу G отримуємо:

$$n_v - n_e + n_r = n_v - (n_e - 1) + (n_r - 1) = 2.$$

Отже, твердження теореми в загальному випадку доведено. □

Приклад 5.26. Перевіримо справедливість формули Ейлера для графу, зображеного на рис. 5.27:

$$n_v - n_e + n_r = 4 - 6 + 4 = 2.$$

Приклад 5.27. У теоремі 5.12 умова зв'язності графу суттєва. Так, для графу, зображеного на рис. 5.28, отримуємо:

$$n_v - n_e + n_r = 3 - 1 + 1 = 3 \neq 2.$$

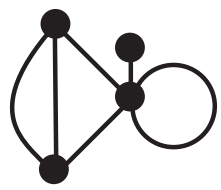


Рис. 5.27

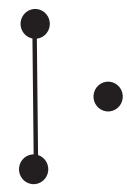


Рис. 5.28

5.11. Дуальні графи

У цьому підрозділі всі графи вважатимемо плоскими неорієнтованими мультиграфами.

5.11.1. Визначення дуального графу

Означення 5.18. Нехай G – плоский граф з кількістю вершин, ребер і граней n_v, n_e та n_r відповідно. Плоский граф G^* з кількістю вершин, ребер та граней $\widetilde{n}_v$, $\widetilde{n}_e$ та $\widetilde{n}_r$ відповідно називають дуальним до графу G, якщо:

1. $\widetilde{n}_e = n_e$, $\widetilde{n}_v = n_r$.

2. Кожна грань r графу G містить рівно одну вершину v^* графу G^* (вершина v^* графу G^* відповідає грані r графу G).

3. Кожне ребро e графу G перетинається рівно з одним ребром e^* графу G^* (ребро e графу G відповідає ребру e^* графу G^*).

З означення 5.18 випливає, що для кожного плоского графу G існує єдиний, з точністю до ізоморфізму, дуальний граф G^*. Проте у ізоморфних графів G_1 та G_2 можуть бути неізоморфні дуальні G_1^* та G_2^*.

Приклад 5.28. На рис. 5.29 зображено ізоморфні графи G_1 та G_2, а також їх дуальні G_1^* та G_2^* (ребра дуальних графів позначено пунктиром). Очевидно, дуальні графи G_1^* та G_2^* неізоморфні – граф G_1^* містить дві вершини степенів 3 та 7, однак обидві вершини графу G_2^* мають степінь 5.

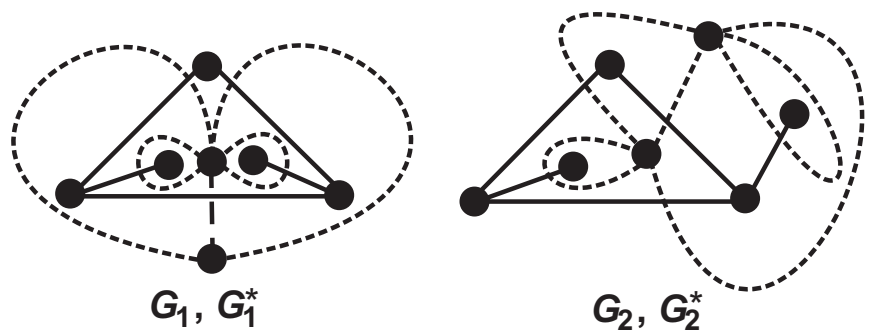


Рис. 5.29

Зауваження 5.7. Із побудови дуального графу легко бачити, що дуальний граф G^* зв'язний, незалежно від зв'язності вихідного графу G (твердження легко довести індукцією за кількістю ребер у графі G).

5.11.2. Другий дуальний граф

Другим дуальним до графу G називатимемо граф $G^{**} = (G^*)^*$. Граф G^*, дуальний до G, назвемо також *першим дуальним*.

Наступний приклад демонструє зв'язок між графами G^{**} та G.

Приклад 5.29. На рис. 5.30 зображено побудову першого та другого дуальних до графів G_1 та G_2 (дуальні графи позначені пунктиром).

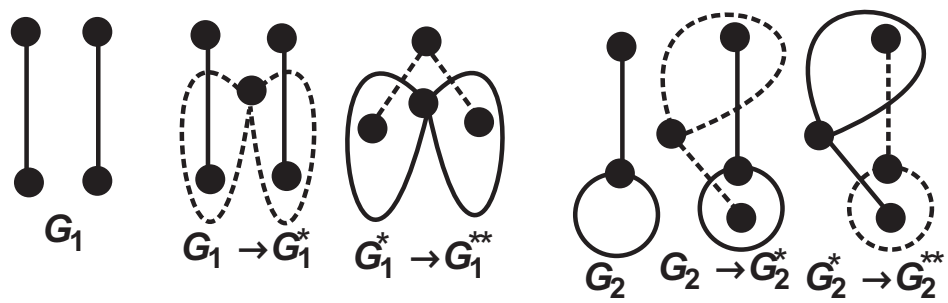


Рис. 5.30

З рисунка видно, що графи G_2 та G_2^{**} ізоморфні, однак графи G_1 та G_1^{**} неізоморфні. Зазначимо, що графи G_1 та G_1^{**} апріорі не могли бути ізоморфними, оскільки граф G_1 незв'язний (див. заув. 5.7).

Наступна теорема дає необхідну і достатню умову ізоморфності графів G та G^{**}.

Теорема 5.13. *Графи G та G^{**} ізоморфні тоді і тільки тоді, коли граф G зв'язний.*

Доведення. Необхідність. Нехай G та G^{**} ізоморфні. Тоді зв'язність графу G випливає із зв'язності G^{**} (див. заув. 5.7).

Достатність. Нехай граф G зв'язний. Для доведення ізоморфності G та G^{**} достатньо показати, що граф G є дуальним до G^* (нагадаємо, що дуальний граф визначається однозначно, з точністю до ізоморфізму). Доведемо, що G є дуальним до G^*, перевіривши умови означення 5.18.

Нехай граф G має n_v вершин, n_e ребер та n_r граней. Тоді, за означенням 5.18, граф G^* має n_r вершин та n_e ребер. Застосовуючи до графів G та G^* формулу Ейлера (теорема 5.12), отримуємо, що граф G^* має n_v граней.

Оскільки кожна вершина графу G належить рівно одній грані графу G^*, кожна грань графу G^* містить принаймні одну вершину графу G, і кількість вершин графу G збігається з кількістю граней графу G^*, отримуємо, що кожна грань графу G^* містить рівно одну вершину графу G.

Нарешті, за означенням 5.18, кожне ребро графу G^* перетинається рівно з одним ребром графу G.

Отже, виконуються всі умови означення 5.18, і граф G дуальний до графу G^*, тобто графи G^{**} і G ізоморфні. □

5.12. Степінь грані плоского графу. Теорема про степені граней

У цьому підрозділі, якщо не вказано інше, всі графи вважатимемо плоскими неорієнтованими мультиграфами.

Означення 5.19. Степенем d_r грані r плоского графу G називають кількість ребер графу G, що належить межі грані r, причому кожен міст збільшує степінь на 2.

Очевидно, що, за означенням 5.18, степінь грані r графу G збігається із степенем відповідної вершини v^* дуального графу G^*.

Приклад 5.30. Граф G, зображений на рис. 5.31, має дві грані – внутрішню r_1 і зовнішню r_2. Степені граней r_1 та r_2 збігаються із степенями відповідних вершин v_1^* та v_2^* дуального графу G^*: $d_{r_1} = d_{v_1^*} = 1$, $d_{r_2} = d_{v_2^*} = 3$.

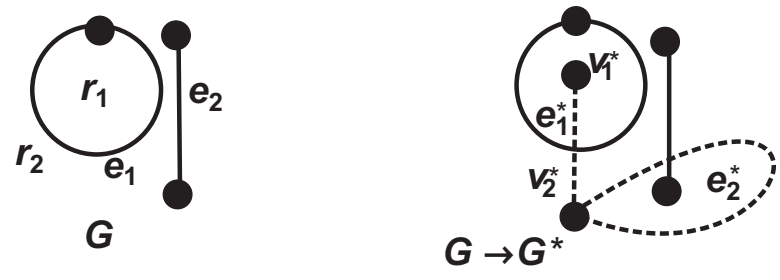


Рис. 5.31

Отже, міст e_2 збільшив степінь грані r_2 на 2, що для дуального графу G^* відповідає збільшенню степеня вершини v_2^* на 2 за рахунок петлі e_2^*.

Теорема 5.14 (теорема про степені граней)**.** *Сума степенів граней плоского мультиграфу G дорівнює подвійній кількості ребер:*

$$\sum_{r \in R} d_r = 2n_e, \text{ де } n_e = \mathrm{card}(E) \text{ – кількість ребер у графі.}$$

Доведення. Для доведення теореми розглянемо дуальний граф G^*. Оскільки степінь кожної грані графу G збігається із степенем відповідної вершини дуального графу G^*, за теоремою про степені вершин (теорема 5.2) отримуємо:

$$\sum_{r \in R} d_r = \sum_{v^* \in V^*} d_{v^*} = 2n_e, \text{ де } V^* \text{ – множина вершин графу } G^*. \qquad \square$$

5.13. Один наслідок з формули Ейлера для плоских графів

Формула Ейлера (теорема 5.12), разом із теоремою про степені граней 5.14, дозволяє вивести корисну нерівність, що пов'язує кількість вершин та ребер планарного графу.

Спочатку наведемо просте твердження, яке випливає безпосередньо з визначення степені грані.

Лема 5.8. *Для простого зв'язного графу з трьома або більше вершинами степінь довільної грані* $d_r \geq 3$.

Доведення. Справді, якщо $d_r = 1$, грань r має бути обмежена петлею, що суперечить простоті графу. Якщо $d_r = 2$, грань r має бути обмежена або парою мультиребер (що суперечить простоті графу), або одним мостом (що неможливо для зв'язного графу з трьома або більше вершинами). Нарешті, випадок $d_r = 0$ можливий лише для порожнього графу, що суперечить умові зв'язності при трьох або більше вершинах.

□

Зауваження 5.8. З теореми 5.9 випливає підсилений варіант твердження леми 5.8 для дводольних графів: у дводольному простому зв'язному графі з трьома або більше вершинами степінь довільної грані $d_r \geq 4$.

Тепер доведемо основне твердження цього підрозділу, яке зручно використовувати для доведення непланарності деяких графів.

Теорема 5.15. *Для простого планарного (не обов'язково плоского) зв'язного графу з* n_v *вершинами та* n_e *ребрами при* $n_v \geq 3$ *виконується нерівність:*

$$n_e \leq 3n_v - 6.$$

Доведення. Нехай $\widetilde{G}$ – плоский граф, ізоморфний G, $n_r = \mathrm{card}(R)$ – кількість граней у графі G. За теоремою про степені граней (теорема 5.14) та лемою 5.8 отримуємо:

$$2n_e = \sum_{r \in R} d_r \geq 3n_r.$$

Тепер твердження теореми випливає з формули Ейлера для плоских графів (теорема 5.4):

$$n_e \geq \frac{3}{2}(2 - n_v + n_e) \Rightarrow n_e \leq 3n_v - 6.$$

□

Зауваження 5.9. Для дводольних графів результат теореми 5.15 може бути підсилений:

$$n_e \leq 2n_v - 4$$

(доведення повністю аналогічне доведенню теореми 5.15, з урахуванням заув. 5.8).

Підкреслимо, що теорема 5.15 дозволяє встановити (при $n_e \not\leq 3n_v - 6$) лише непланарність, оскільки нерівність $n_e \leq 3n_v - 6$ може виконуватись як для планарних, так і для непланарних графів.

Приклад 5.31. 1. Граф «Зірка» (граф G_1 на рис. 5.25) не є планарним, оскільки для цього графу не виконується твердження теореми 5.15:

$$n_e = 10 \not\leq 3n_v - 6 = 9.$$

2. Граф «Три криниці» (граф G_2 на рис. 5.25) непланарний, однак для цього графу виконується твердження теореми 5.15:

$$n_e = 9 \leq 3n_v - 6 = 12.$$

Непланарність графу «Три криниці» можна довести, використовуючи підсилений варіант теореми 5.15 для дводольних графів (заув. 5.9):

$$n_e = 9 \not\leq 2n_v - 4 = 8.$$

5.14. Фарбування вершин та граней графу

У цьому розділі, якщо не вказано інше, всі графи вважатимемо простими та неорієнтованими.

5.14.1. Фарбування вершин графу

Під час розв'язання багатьох проблем доцільно розглядати *графи з фарбованими вершинами* – мічені графи, для яких кожній вершині v зіставляється деякий колір c_v (вершина v фарбується в колір c_v), причому суміжні вершини фарбуються в різні кольори.

Мінімальну кількість кольорів, достатніх для фарбування вершин графу, називають *хроматичним числом*. Хроматичне число графу G позначатимемо через χ_G. Граф з хроматичним числом k називають *k-колірним*.

Приклад 5.32. Повний граф з n вершинами є n-колірним, порожній граф (незалежно від кількості вершин) – одноколірним.

Приклад 5.33. Розглянемо граф, зображений на рис. 5.32.

Цей граф триколірний: з одного боку, трьох кольорів (білий, жовтий та чорний) достатньо для фарбування вершин, і тому $\chi_G \leq 3$; з другого боку, граф G містить підграф, що є повним графом з трьома вершинами (v_2, v_3, v_4), і тому $\chi_G \geq 3$.

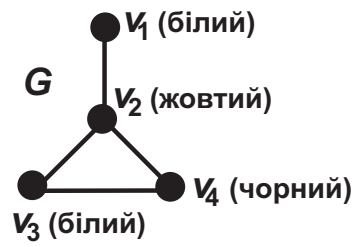


Рис. 5.32

Наступна теорема однозначно характеризує клас двоколірних графів.

Теорема 5.16. *Непорожній граф G двоколірний тоді і тільки тоді, коли він дводольний.*

Доведення. Двоколірність непорожнього графу G, за визначенням, еквівалентна такому твердженню: множину вершин V графу G можна розбити на непорожні підмножини V_1, V_2 $(V_1 \cap V_2 = \varnothing)$ так, що будь-які дві вершини з однієї підмножини V_k $(k = 1, 2)$ є несуміжними. Тобто, за означенням 5.11, двоколірність непорожнього графу еквівалентна його дводольності. □

Одне з важливих застосувань фарбування вершин графу пов'язане з так званою «теорією розкладів». Наступний приклад демонструє (у значно спрощеному вигляді) зведення проблеми складання оптимального розкладу до фарбування вершин графу.

Приклад 5.34. Для навчального процесу середньої школи потрібно скласти розклад занять так, щоб усі уроки в школі протягом тижня були проведені за мінімальну кількість навчальних годин. Вважають, що кількість навчальних аудиторій необмежена, проте з кожного предмета є тільки один викладач (один предмет не може викладатись водночас у двох групах).

Розглянемо граф G, що відповідає таким вимогам:

- кожна вершина графу є парою типу $(\langle\text{клас}\rangle, \langle\text{предмет}\rangle)$ і відповідає уроку з вказаного предмета, який потрібно провести протягом тижня з учнями вказаного класу (наприклад, (10-А, Фізика));

- суміжними є ті і тільки ті вершини, які відповідають урокам, що не можуть бути проведені водночас (один викладач не може вести водночас два уроки, і два уроки не можна проводити водночас з одним класом).

Очевидно, що кількість вершин у графі G дорівнює загальній кількості уроків, які треба провести з учнями школи протягом тижня, і проблема складання оптимального розкладу зводиться до пошуку хроматичного числа побудованого графу.

Для пошуку хроматичного числа існують точні алгоритми (див., наприклад, [9]), які гарантують знаходження точного значення хроматичного числа.

Однак за зростання кількості вершин застосування точних алгоритмів фарбування стає, через швидке зростання обсягу обчислень, дуже проблематичним. Тому доцільно розглядати прості та ефективні алгоритми «наближеного» фарбування графу з кількістю кольорів, близьким до хроматичного числа. Один з таких алгоритмів, запропонований Д. Уелшем (D. Welsh) і М. Пауеллом (M. Powell):

1. Вершини графу впорядковуються за незростанням степенів.
2. Вершина v, що перша в списку, фарбується в колір c.
3. У колір c фарбуються в порядку за списком усі вершини, несуміжні з вершинами, що на даному кроці пофарбовані в колір c_1.
4. Пофарбовані вершини викреслюють із списку.
5. Повторюємо пункти 2–4, поки в списку є нефарбовані вершини.

Приклад 5.35. Пофарбуємо вершини графу G, зображеного на рис. 5.33, застосовуючи наближений алгоритм Уелша – Пауелла.

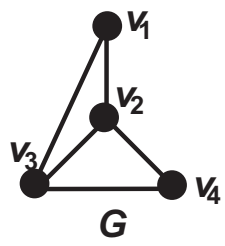


Рис. 5.33

1. Розташуємо вершини за незростанням степенів: v_2, v_3, v_1, v_4.
2. Зіставимо вершині v_2 колір c_1; викреслимо вершину v_2 зі списку.
3. Вершину v_3 (першу, що залишилась у списку) пофарбуємо в колір c_2 і викреслимо зі списку.
4. Вершину v_1 (першу, що залишилась у списку) пофарбуємо в колір c_3; у цей же колір пофарбуємо вершину v_4, несуміжну з v_1; вершини v_4 та v_1 викреслимо зі списку.

Отже, граф G вдалося пофарбувати трьома кольорами. Зазначимо, що для даного графу наближений алгоритм дав точне значення хроматичного числа: граф G є саме триколірним (а не одно- чи двоколірним), оскільки містить повний граф з трьома вершинами.

Зауваження 5.10. Проблему фарбування вершин можна розглядати і для мультиграфів без петель (фарбувати вершини графів з петлями неможливо, оскільки вершина з петлею суміжна самій собі).

5.14.2. Фарбування граней графу

Далі до кінця підрозділу всі графи вважатимемо плоскими неорієнтованими мультиграфами.

Для коректного визначення проблеми фарбування граней нам знадобиться поняття суміжності граней.

Означення 5.20. Грані r_1 та r_2 графу G називають суміжними, якщо існує принаймні одне ребро, що належить обом граням.

Приклад 5.36. Розглянемо граф на рис. 5.34. Зовнішня грань r_4 цього графу суміжна з гранями r_1, r_2 та r_3; грань r_2 суміжна з r_1 та r_4 і несуміжна з r_3.

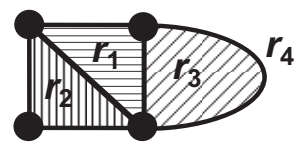


Рис. 5.34

Проблема *фарбування граней графу* полягає у зіставленні кожній грані деякої мітки – кольору (фарбування грані), причому суміжні грані слід пофарбувати різними кольорами. Під час фарбування граней, як і під час фарбування вершин, намагаються використовувати якнайменше кольорів.

Очевидно, що грані графу з мостами фарбувати неможливо, оскільки грань, яка містить міст, суміжна самій собі.

Оскільки суміжність граней r_1 та r_2 графу G еквівалентна суміжності відповідних вершин v_1^* та v_2^* дуального графу G^*, проблема фарбування граней зводиться до фарбування вершин дуального графу.

Одним з перших (можливо, першим) застосувань фарбування граней графу є фарбування географічної карти так, щоб сусідні країни були

пофарбовані різними кольорами. У зв'язку з пошуком мінімальної кількості кольорів, потрібних для фарбування карти, в середині XIX століття була сформульована так звана «проблема чотирьох кольорів», яку наведемо (без доведення) в еквівалентному формулюванні для фарбування вершин планарного графу.

Теорема 5.17 (проблема чотирьох кольорів)**.** *Для фарбування вершин планарного графу достатньо* 4 *кольорів.*

Зазначимо, що проблему чотирьох кольорів було доведено лише 1976 року американськими вченими К. Аппелем (K. Appel) та В. Хейкенем (W. Haken) з використанням комп'ютерних технологій.

5.15. Поняття про орієнтовані графи

У цьому підрозділі всі графи вважатимемо простими орграфами (простими орієнтованими графами).

Означення 5.21. Орграф називають повним, якщо будь-яка пара його вершин (u, v) $(u \neq v)$ з'єднана ребром.

Очевидно, що повні орграфи з однаковою кількістю вершин можуть бути неізоморфними. Так, повні графи G_1 та G_2, зображені на рис. 5.35, мають однакову кількість вершин, але не ізоморфні.

Означення 5.22. Степенем d_v^+ вершини v за входом називають кількість ребер, що ведуть до вершини v, степенем d_v^- вершини v за виходом називають кількість ребер, що ведуть від v. Вершину v називають витоком, якщо $d_v^+ = 0$; вершину v називають стоком, якщо $d_v^- = 0$.

Приклад 5.37. Граф, зображений на рис. 5.36, має стік v_6 ($d_{v_6}^- = 0$, $d_{v_6}^+ = 2$) і не має жодного витоку.

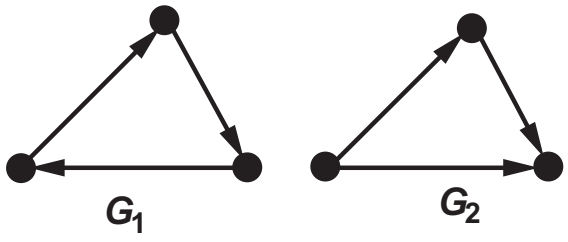


Рис. 5.35

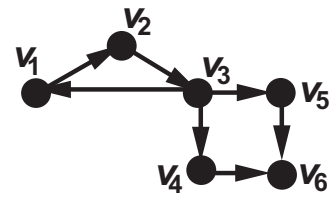


Рис. 5.36

Теорема 5.18. *Повний орграф не може мати більше одного витоку і не може мати більше одного стоку.*

Доведення. Доведемо, що повний орграф не може мати більше одного витоку (твердження про стоки доводиться аналогічно).

Припустімо, що в повному орграфі G існують витоки v_1 та v_2. Оскільки граф повний, вершини v_1 та v_2 мають бути з'єднані ребром; не порушуючи загальності припустімо, що ребро веде від v_1 до v_2. Отримуємо суперечність (до витоку v_2 веде ребро), що доводить теорему. □

Для орграфів існує цікаве узагальнення теореми про степені вершин.

Теорема 5.19 (теорема про степені вершин для орграфів)**.**
Сума степенів вершин графу за входом дорівнює сумі степенів вершин графу за виходом і дорівнює кількості ребер:

$$\sum_{v\in V} d_v^+ = \sum_{v\in V} d_v^- = n_e, \text{ де } n_e = \mathrm{card}(E) \text{ – кількість ребер у графі.}$$

Вправа 5.5. Довести теорему 5.19 самостійно, за аналогією до доведення теореми 5.2.

Розділ 6

Елементи теорії груп

6.1. Алгебричні структури з однією бінарною операцією

Нехай A – непорожня множина, $n \in \mathbb{N} \cup \{0\}$.

Функцію $f : A^{\times n} \to A$ з областю визначення $\mathcal{D} \subset A^{\times n}$ називають *n-арною* операцією на множині A. Якщо $n = 1$, то операцію f називають *унарною*, якщо $n = 2$ – *бінарною*. Якщо $n = 0$, під операцією f розуміють фіксований елемент $f \in A$; операцію f у цьому разі називають *нульарною*. Якщо $\mathcal{D} = A^{\times n}$ (тобто функція f є відображенням), операцію f називають *замкненою*.

Для бінарної операції часто використовують так звану інфіксну форму запису – символ операції записують між двома її аргументами: xfy замість $f(x, y)$. У разі використання інфіксної форми запису для бінарної операції часто вживають традиційні позначення: «$+$», «$\cdot$», «$\circ$» та ін. В абстрактному випадку (без фіксованого змісту бінарної операції) будемо використовувати позначення «$*$».

Бінарну операцію «$*$» на множині A називають *комутативною*, якщо

$$a * b = b * a \qquad \forall\, a, b \in A.$$

Бінарну операцію «$*$» на множині A називають *асоціативною*, якщо

$$(a * b) * c = a * (b * c) \qquad \forall\, a, b, c \in A.$$

Для асоціативної бінарної операції «$*$» замість $(a*b)*c$ або $a*(b*c)$ часто пишуть $a*b*c$, оскільки порядок виконання асоціативної операції не має значення.

Якщо наведене співвідношення комутативності не виконується принаймні для двох елементів $a, b \in A$, операцію називають *некомутативною*. Якщо наведене співвідношення асоціативності не виконується принаймні для трьох елементів $a, b, c \in A$, операцію називають *неасоціативною*.

Упорядковану пару $\langle A, * \rangle$, де «$*$» – бінарна операція на множині $A \neq \varnothing$, називають *алгебричною структурою з бінарною операцією*.

Зауваження 6.1. Звичайно, можна розглядати алгебричні структури з довільною (і навіть з нескінченною) кількістю операцій довільної арності. Так, у розд. 7 буде розглянуто алгебричну структуру з двома бінарними операціями.

Означення 6.1. Алгебричну структуру $\langle A, * \rangle$ називатимемо оперативом, якщо операція «$*$» замкнена. Оператив з асоціативною операцією називають півгрупою. Алгебричну структуру з комутативною операцією називають комутативною, з некомутативною операцією – некомутативною.

Приклад 6.1. 1. Структура $\langle \mathbb{Z}, - \rangle$ – оператив, оскільки для довільних $n, m \in \mathbb{Z}$ отримуємо $n - m \in \mathbb{Z}$.

2. Структура $\langle \mathbb{N}, - \rangle$ не є оперативом: так, наприклад, $1 - 2 = -1 \notin \mathbb{N}$.

3. Операція «$-$» на множині $\mathbb{R}$ не є ні комутативною, ні асоціативною.

4. Операція «$+$» на множині $\mathbb{R}$ є комутативною та асоціативною. Отже, $\langle \mathbb{R}, + \rangle$ – комутативна півгрупа.

5. Операція «$\cdot$» є комутативною та асоціативною на множині $\mathbb{R}$ (добуток дійсних чисел). Отже, $\langle \mathbb{R}, \cdot \rangle$ – комутативна півгрупа.

6. На множині $M_{n\times n}$ матриць $n \times n$ операція «$\cdot$» є асоціативною, але при $n \geq 2$ не є комутативною. Отже, $\langle M_{n\times n}, \cdot \rangle$ – півгрупа (у випадку $n \geq 2$ – некомутативна).

Зауваження 6.2. Тут і далі, якщо не вказано інше, розглянуто матриці з елементами із $\mathbb{R}$.

Означення 6.2. Нехай $\langle A, * \rangle$ – оператив. Елемент $e_r \in A$ називають правим нейтральним, якщо

$$a * e_r = a \qquad \forall\, a \in A.$$

Елемент $e_l \in A$ називають лівим нейтральним, якщо

$$e_l * a = a \qquad \forall\, a \in A.$$

Правий та лівий нейтральні елементи називають односторонніми нейтральними.

Елемент $e \in A$ називають нейтральним (двостороннім нейтральним), якщо він є одночасно правим і лівим нейтральним.

Означення 6.3. Півгрупу з нейтральним елементом називають моноїдом.

Зауваження 6.3. Довільна алгебрична структура з бінарною операцією може не містити ні двосторонніх, ні навіть односторонніх нейтральних елементів.

Приклад 6.2. 1. В алгебричній структурі $\langle \mathbb{Z}, - \rangle$ існує правий нейтральний 0, але немає двостороннього нейтрального.

2. В алгебричній структурі $\langle \mathbb{R}^3, \times \rangle$ (векторний добуток векторів у $\mathbb{R}^3$) не існує жодного (одно- чи двостороннього) нейтрального елемента.

3. В алгебричній структурі $\langle M_{n\times n}, \cdot \rangle$ існує двосторонній нейтральний I (одинична матриця). Отже, враховуючи асоціативність добутку матриць, $\langle M_{n\times n}, \cdot \rangle$ – моноїд (при $n \geq 2$ – некомутативний).

Теорема 6.1. *Якщо в оперативі $\langle A, * \rangle$ існує правий e_r і лівий e_l нейтральні елементи, то*

$$e_r = e_l.$$

Доведення. За визначенням правого та лівого нейтральних маємо:

$$e_l = e_l * e_r; \quad e_r = e_l * e_r,$$

звідки $e_l = e_r$. □

Наслідок. *Якщо в алгебричній структурі $\langle A, * \rangle$ існує хоча б один правий e_r і хоча б один лівий e_l нейтральні елементи, то в структурі існує двосторонній нейтральний елемент $e = e_r = e_l$, причому всі інші одно- та двосторонні нейтральні елементи збігатимуться з e.*

Зауваження 6.4. З теореми 6.1 одразу випливає єдиність двостороннього нейтрального, але односторонніх нейтральних може бути довільна кількість.

Приклад 6.3. Нехай на непорожній множині A бінарна операція «$*$» визначена як проекція на перший аргумент:

$$a * b = a \qquad \forall\, a, b \in A.$$

Легко перевірити, що в алгебричній структурі $\langle A, * \rangle$ кожний елемент $b \in A$ є правим нейтральним.

Означення 6.4. Нехай $\langle A, * \rangle$ – оператив з нейтральним елементом e, a – фіксований елемент в A. Елемент $a^{-1,r} \in A$ називають правим оберненим до a, якщо

$$a * a^{-1,r} = e.$$

Елемент $a^{-1,l} \in A$ називають лівим оберненим до a, якщо

$$a^{-1,l} * a = e.$$

Правий та лівий обернені елементи називають односторонніми оберненими.

Елемент $a^{-1} \in A$ називають оберненим до a (двостороннім оберненим), якщо він є одночасно правим і лівим оберненим до a.

Теорема 6.2. *Якщо в моноїді $\langle A, * \rangle$ існує правий $a^{-1,r}$ і лівий $a^{-1,l}$ обернені до деякого елемента $a \in A$, то*

$$a^{-1,r} = a^{-1,l}.$$

Доведення. Нехай e – нейтральний елемент. За визначенням правого та лівого обернених і, враховуючи асоціативність, маємо

$$a^{-1,l} = a^{-1,l} * e = a^{-1,l} * (a * a^{-1,r}) = (a^{-1,l} * a) * a^{-1,r} = e * a^{-1,r} = a^{-1,r}.$$

□

Щоб уникнути конфлікту в позначеннях, для оберненого елемента іноді вказують операцію, відносно якої обчислено обернений елемент: $a^{-1,*}$ – елемент, обернений до a відносно операції «$*$».

Приклад 6.4. 1. У моноїді $\langle \mathbb{R}, \cdot \rangle$ обернений мають усі елементи, крім елемента 0: $a^{-1,\cdot} = a^{-1} (= \frac{1}{a})$ $(a \neq 0)$.

2. У моноїді $\langle \mathbb{R}, + \rangle$ обернений мають усі елементи: $a^{-1,+} = -a$.

Означення 6.5. Групою називають моноїд, в якому для кожного елемента існує обернений. Комутативну групу називають абелевою[1].

Приклад 6.5. 1. Алгебрична структура $\langle \mathbb{Z}, + \rangle$ – комутативна група.

2. Алгебрична структура $\langle \mathbb{Z}, \cdot \rangle$ – комутативний моноїд (нейтральний елемент $e = 1$), але не група, оскільки обернені елементи існують лише для елементів 1 та -1.

3. Алгебрична структура $\langle M_{n\times n}, \cdot \rangle$ – моноїд, некомутативний при $n \geq 2$; нейтральний елемент $e = I$. Ця структура не є групою, оскільки обернені існують лише для невироджених матриць.

4. Нехай GL_n – множина невироджених квадратних матриць розміром $n \times n$. Алгебрична структура $\langle GL_n, \cdot \rangle$ – група, некомутативна при $n \geq 2$; нейтральний елемент $e = I$; обернений елемент A^{-1} збігається з оберненою матрицею.

5. Нехай $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. Алгебрична структура $\langle \mathbb{R}^*, \cdot \rangle$ є комутативною групою. Очевидно, що $\mathbb{R}^* = GL_1$.

6. Нехай A – довільна непорожня множина, G – множина бієкцій $f\colon A \to A$. Із властивостей бієктивних відображень випливає, що $\langle G, \circ \rangle$ – група («$\circ$» – операція композиції). Нейтральним елементом групи є тотожне відображення, оберненим – відповідне обернене відображення.

Групу з операцією, аналогічною операції додавання, часто називають *адитивною*; групу з операцією, аналогічною операції добутку, часто називають *мультиплікативною*.

Приклад 6.6. До адитивних груп відносять $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{R}, + \rangle$, $\langle M_{n\times n}, + \rangle$. До мультиплікативних можна віднести групи $\langle \mathbb{R}^*, \cdot \rangle$, $\langle GL_n, \cdot \rangle$, $\langle \{1, -1\}, \cdot \rangle$.

[1] Абель Нільс Генрік (1802–1829) – норвезький математик; довів, активно використовуючи властивості комутативних груп, нерозв'язність алгебричних рівнянь 5-го і вищих порядків у загальному вигляді через радикали.

Зауваження 6.5. Звичайно, виділенння класів адитивних і мультиплікативних груп досить умовне, оскільки будь-яку бінарну операцію можна (принаймні, формально) позначити як символом «+», так і символом «·». Проте, якщо йдеться про адитивну (мультиплікативну) групу, мають на увазі загальноприйнятий сенс операцій «+» та «·». Більше того, використовуючи назву «мультиплікативна (адитивна) група», саму операцію часто не вказують. Так, часто пишуть «адитивна група $M_{n\times n}$» замість «група $\langle M_{n\times n}, +\rangle$», «мультиплікативна група GL_n» замість «група $\langle GL_n, \cdot\rangle$», «мультиплікативна група $\mathbb{R}^*$» замість «група $\langle \mathbb{R}^*, \cdot\rangle$» тощо.

Зауваження 6.6. Позначення GL_n та $\mathbb{R}^*$ є сталими для відповідних мультиплікативних груп, навіть без конкретизуючого епітета «мультиплікативна».

У посібнику розглянуто лише найголовніші аспекти теорії груп. Детальніше про теорію алгебричних структур (зокрема, теорію груп) можна дізнатися, наприклад, з праць [10– 13].

6.2. Основні властивості груп. Степінь елемента

Розглянемо найпростіші властивості групи $\langle G, *\rangle$ з нейтральним $e \in G$.

1. Нехай $a, b \in G$. Тоді рівняння $a * x = b$ відносно $x \in G$ має єдиний розв'язок $x = a^{-1} * b$.

Доведення. Існування розв'язку: елемент $x = a^{-1} * b$ дійсно є розв'язком рівняння $a * x = b$, оскільки

$$a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b.$$

Єдиність розв'язку:

$$(a * x = b) \Rightarrow (a^{-1} * a * x = a^{-1} * b) \Rightarrow (x = a^{-1} * b). \qquad \square$$

Вправа 6.1. Довести, що рівняння $y * a = b$ має відносно $y \in G$ єдиний розв'язок $y = b * a^{-1}$.

2. Правила лівого та правого скорочення ($a, b, x, y \in G$):

$$(a * x = b * x) \Leftrightarrow (a = b) \quad \text{(праве скорочення);} \tag{6.1}$$
$$(y * a = y * b) \Leftrightarrow (a = b) \quad \text{(ліве скорочення).} \tag{6.2}$$

Вправа 6.2. Довести правила скорочення самостійно.

3. $\forall\, a, b \in G\colon (a * b)^{-1} = b^{-1} * a^{-1}$.

Доведення. Перевіримо, що $b^{-1} * a^{-1}$ є правим оберненим до $a * b$:

$$(a * b) * (b^{-1} * a^{-1}) = (a * b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e.$$

Зауважимо, що можна не проводити аналогічну перевірку факту, що $b^{-1} * a^{-1}$ є лівим оберненим до $a * b$, оскільки необхідний результат випливає з теореми 6.2 (враховуючи існування двостороннього оберненого й асоціативність групової операції). □

Вправа 6.3. Довести узагальнення властивості 3:

$$\forall\, a_1, a_2, \ldots, a_n \in G\colon (a_1 * a_2 * \cdots * a_n)^{-1} = a_n^{-1} * \cdots * a_2^{-1} * a_1^{-1}.$$

Нехай $a \in G$. Визначимо степінь a^k для $k \in \mathbb{Z}$.
Для $n > 0$ покладемо за визначенням:

- $a^n = \underbrace{a * a * \cdots * a}_{n}$;
- $a^{-n} = (a^{-1})^n$;
- $a^0 = e$.

Зауваження 6.7. Із результату вправи 6.3 одразу випливає

$$a^{-n} = (a^{-1})^n = (a^n)^{-1}.$$

Для степеня елемента групи легко довести такі властивості (продовжено загальну нумерацію властивостей).
4. $a^{n+m} = a^n * a^m$.
5. $a^{n \cdot m} = (a^n)^m$.

Вправа 6.4. Довести властивості 4 та 5 самостійно.

Вказівка. Довести властивості спочатку для $n, m > 0$, а в загальному випадку скористатися визначенням a^k для $k < 0$ з урахуванням заув. 6.7 (випадки $n = 0$ та (або) $m = 0$ слід розглянути окремо).

Щоб уникнути конфлікту в позначеннях (зокрема, розглядаючи адитивні групи), для степеня елемента іноді вказують групову операцію: $a^{n,*}$ – степінь a^n у групі з операцією «$*$».

Приклад 6.7. 1. У групі $\langle \mathbb{R}^*, \cdot \rangle$ степінь елемента збігається з відповідним класичним (арифметичним) степенем:

$$a^{n,\cdot} = \underbrace{a \cdot a \cdot \dots \cdot a}_{n} = a^n.$$

2. В адитивній групі $\mathbb{Z}$ (тобто в групі $\langle \mathbb{Z}, + \rangle$ (див. заув. 6.5)), степінь елемента a обчислюють як арифметичний добуток числа a на показник степеня:

$$a^{n,+} = \underbrace{a + a + \dots + a}_{n} = n \cdot a.$$

6.3. Група підстановок

Важливий клас груп пов'язаний з бієктивними відображеннями (підстановками) на скінченній множині A.

Оскільки під час вивчення властивостей підстановок природа елементів множини A не має значення (суттєвим фактом є лише потужність множини A), будемо вважати $A = \{1, 2, \dots, n\}$ $(n \geq 1)$.

6.3.1. Загальні поняття теорії підстановок

Означення 6.6. Перестановкою множини $A = \{1, 2, \dots, n\}$ називають довільний лінійно впорядкований набір $i = (i_1, i_2, \dots, i_n)$, такий, що:

- $i_k \in A$ при $1 \leq k \leq n$;
- $i_{k_1} \neq i_{k_2}$ при $k_1 \neq k_2$.

Очевидно, всього на множині A визначено $n!$ перестановок.

Приклад 6.8. 1. При $n = 1$ визначена одна перестановка (1). Цей випадок нецікавий і його, як правило, не розглядають.

2. При $n = 2$ визначено дві перестановки: $(1, 2)$, $(2, 1)$.

3. При $n = 3$ визначено $3! = 6$ перестановок: $(1, 2, 3)$, $(1, 3, 2)$, $(2, 1, 3)$, $(2, 3, 1)$, $(3, 1, 2)$, $(3, 2, 1)$.

Означення 6.7. Підстановкою σ на множині $A = \{1, 2, \ldots, n\}$ називають довільне бієктивне відображення $\sigma\colon A \to A$.

Підстановку ε, яка визначає тотожне відображення, називають *тотожною*.

Очевидно, всього на множині A визначено $n!$ підстановок.

Підстановку $\sigma\colon A \to A$ зручно зображувати у вигляді матриці розміром $2 \times n$:

$$\sigma = \begin{pmatrix} i_1 & i_2 & \ldots & i_n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix} \quad \Leftrightarrow \quad \begin{cases} \sigma\colon i_1 \mapsto j_1, \\ \sigma\colon i_2 \mapsto j_2, \\ \qquad \ldots \\ \sigma\colon i_n \mapsto j_n. \end{cases}$$

Для перестановок $i = (i_1, i_2, \ldots, i_n)$, $j = (j_1, j_2, \ldots, j_n)$ позначимо

$$\begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} i_1 & i_2 & \ldots & i_n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix}.$$

Легко зрозуміти, що кожну підстановку (при $n \geq 2$) можна зобразити у вигляді матриці кількома способами, переставляючи стовпці матриці (кожній підстановці на множині A відповідає $n!$ матриць).

Приклад 6.9. Підстановку $\sigma : \{1, 2\} \to \{1, 2\}$, таку, що $\sigma(1) = 2$, $\sigma(2) = 1$, можна зобразити у вигляді матриці двома способами:

$$\sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

Легко перевірити подане нижче твердження.

Лема 6.1. *Нехай* σ *– довільна підстановка на множині* A.

1. Для довільної перестановки $i = (i_1, i_2, \dots, i_n)$ *існує єдина перестановка* $j = (j_1, j_2, \dots, j_n)$, *така, що*

$$\sigma = \begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}.$$

2. Для довільної перестановки $j = (j_1, j_2, \dots, j_n)$ *існує єдина перестановка* $i = (i_1, i_2, \dots, i_n)$, *така, що*

$$\sigma = \begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}.$$

Лема 6.1 дозволяє розглядати підстановку σ як бієктивне відображення на множині перестановок множини $A = \{1, 2, \dots, n\}$:

$$\sigma(i) = j \Leftrightarrow \sigma = \begin{pmatrix} i \\ j \end{pmatrix}, \text{ де } i = (i_1, i_2, \dots, i_n),\ j = (j_1, j_2, \dots, j_n).$$

Приклад 6.10. Нехай $\sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. Тоді $\sigma((1,2)) = (2,1)$, $\sigma((2,1)) = (1,2)$.

Такий підхід корисно використовувати під час вивчення властивостей підстановок. Проте, якщо не вказано інше, розглядатимемо підстановку як відображення на множині A.

Для підстановок $\sigma_1, \sigma_2 : A \to A$ визначено композицію $\sigma_2 \circ \sigma_1$, яку іноді називають *добутком підстановок*.

Приклад 6.11. Нехай $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

Тоді $\sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

Зауваження 6.8. Результат композиції $\sigma = \sigma_2 \circ \sigma_1$, очевидно, не зміниться, якщо розглядати σ_1 та σ_2 як відображення на множині перестановок. Це, разом з лемою 6.1, уможливлює такий спосіб обчислення композиції підстановок:

1) підстановки σ_1 та σ_2 зображують у вигляді матриць так, щоб нижній рядок матриці σ_1 збігався з верхнім рядком матриці σ_2:

$$\sigma_1 = \begin{pmatrix} i \\ j \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} j \\ k \end{pmatrix}$$

(це можна зробити, використовуючи результат леми 6.1, до того ж $n!$ способами);

2) розглядаючи підстановки як відображення на множині перестановок, отримують

$$\sigma_2 \circ \sigma_1 = \begin{pmatrix} j \\ k \end{pmatrix} \circ \begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} i \\ k \end{pmatrix}.$$

Приклад 6.12. Нехай $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. Тоді, змінюючи потрібним чином зображення підстановки σ_2, отримуємо

$$\sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Означення 6.8. Нехай σ – підстановка на множині A. Підстановкою, оберненою до σ, називають підстановку σ^{-1} на множині A, таку, що

$$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \varepsilon,$$

де ε – тотожна підстановка.

З наведеного означення оберненої підстановки випливає, що σ^{-1} є відображенням, оберненим до відображення σ.

Очевидно, що для обчислення оберненої підстановки достатньо поміняти місцями верхній і нижній рядки матриці вихідної підстановки:

$$\begin{pmatrix} i \\ j \end{pmatrix}^{-1} = \begin{pmatrix} j \\ i \end{pmatrix}.$$

Приклад 6.13. Обчислимо обернену для $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1}$:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Отже, множина підстановок на фіксованій множині $A = \{1, 2, \ldots, n\}$ утворює групу за операцією «$\circ$» (композиція), яку називають *групою підстановок*, або *симетричною групою степеня n*. Зазначимо, що група підстановок на скінченній множині A є окремим випадком групи бієкцій на довільній множині A (див. прикл. 6.5).

Для групи підстановок степеня n використовують позначення S_n.

Приклад 6.14. Розглянемо групи S_2 та S_3.
1. Група S_2 складається з $2! = 2$ підстановок:

$$\tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad \varepsilon = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}.$$

Дія «$\circ$» на S_2 визначається табл. 6.1 (елемент $\sigma_2 \circ \sigma_1$ знаходиться на перетині рядка з міткою σ_2 та стовпця з міткою σ_1).

***Таблиця 6.1.* Бінарна операція для групи S_2**

$\circ$	ε	τ
ε	ε	τ
τ	τ	ε

Бінарну операцію на групах із скінченною кількістю елементів часто задають через таблицю типу табл. 6.1. Таблицю такого типу називають *таблицею Келі*[1].

Обернені елементи в групі S_2, очевидно, мають такий вигляд:

$$\tau^{-1} = \tau, \quad \varepsilon^{-1} = \varepsilon.$$

2. Група S_3 складається з $3! = 6$ підстановок:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$
$$\varphi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \ \varphi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \ \varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

Вправа 6.5. Самостійно заповнити таблицю Келі для групи S_3, звіривши результат за табл. 6.2.

Обернені елементи в групі S_3, як видно з табл. 6.2, мають такий вигляд:

$$\sigma_i^{-1} = \sigma_i \quad (i = 1, 2, 3), \quad \varepsilon^{-1} = \varepsilon, \quad \varphi_1^{-1} = \varphi_2, \quad \varphi_2^{-1} = \varphi_1.$$

Позначення, використані для підстановок S_3 у цьому прикладі, використовуватимуться і далі.

[1] Келі (Кейлі) Артур (1821–1895) – англійський математик; автор численних робіт з алгебри, аналітичної геометрії, теорії диференціальних рівнянь тощо (роботи Келі видано в 13-ти томах). Саме Келі ввів поняття абстрактної групи.

Таблиця 6.2. **Таблиця Келі для групи S_3**

$\circ$	ε	σ_1	σ_2	σ_3	φ_1	φ_2
ε	ε	σ_1	σ_2	σ_3	φ_1	φ_2
σ_1	σ_1	ε	φ_1	φ_2	σ_2	σ_3
σ_2	σ_2	φ_2	ε	φ_1	σ_3	σ_1
σ_3	σ_3	φ_1	φ_2	ε	σ_1	σ_2
φ_1	φ_1	σ_3	σ_1	σ_2	φ_2	ε
φ_2	φ_2	σ_2	σ_3	σ_1	ε	φ_1

6.3.2. Розкладання підстановки в композицію циклів

Означення 6.9. Циклом $(i_1, i_2, \ldots, i_k)$ називають підстановку вигляду

$$\begin{pmatrix} i_1 & i_2 & \ldots & i_{k-1} & i_k & i_{k+1} & \ldots & i_n \\ i_2 & i_3 & \ldots & i_k & i_1 & i_{k+1} & \ldots & i_n \end{pmatrix}.$$

Число k називають довжиною циклу. Цикл довжиною 2 називають транспозицією.

Зауваження 6.9. Цикл $(i_1, i_2, \ldots, i_k)$ є підстановкою, що змінює (зсуває за циклом) елементи $i_1, i_2, \ldots, i_k$, залишаючи інші елементи на місці.

Приклад 6.15. 1. Цикл довжиною 1 за означенням 6.9 є тотожною підстановкою.

2. Цикл довжиною 2 є транспозицією (цикл (i_1, i_2) міняє місцями елементи i_1 та i_2, залишаючи інші елементи на місці).

Зауваження 6.10. Позначення $(i_1, \ldots, i_k)$, яке використовують для циклу довжиною k, за формою збігається з позначенням перестановки. Однак це не приводить до конфлікту позначень, оскільки з контексту завжди зрозуміло, є даний об'єкт підстановкою (циклом) чи перестановкою.

Вправа 6.6. Довести, що при $k \geq 2$ в групі S_n міститься $\frac{1}{k}P_n^k$ різних циклів довжиною k.

З результату вправи 6.6, зокрема, випливає (при $k = 2$), що в групі S_n міститься C_n^2 транспозицій.

Приклад 6.16. Підрахуємо, скільки циклів міститься в групах S_3 та S_4.

1. У групі S_3 всі нетотожні підстановки є циклами ($\frac{1}{2}P_3^2 = 3$ транспозиції та $\frac{1}{3}P_3^3 = 2$ цикли довжиною 3):

$$\sigma_1 = (2,3),\ \sigma_2 = (1,3),\ \sigma_3 = (1,2),\ \varphi_1 = (1,2,3),\ \varphi_2 = (1,3,2).$$

2. У групі S_4 міститься $\frac{1}{2}P_4^2 = 6$ транспозицій, $\frac{1}{3}P_4^3 = 8$ циклів довжиною 3 та $\frac{1}{4}P_4^4 = 6$ циклів довжиною 4. Отже, S_4 містить три нетотожні підстановки, які не є циклами:

$$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\quad \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\quad \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}.$$

Означення 6.10. Цикли $(i_1, i_2, \ldots, i_{k_1})$, $(j_1, j_2, \ldots, j_{k_2})$ називають незалежними, якщо

$$\{i_1, i_2, \ldots, i_{k_1}\} \cap \{j_1, j_2, \ldots, j_{k_2}\} = \varnothing,$$

тобто $i_{m_1} \neq j_{m_2}$ для всіх m_1, m_2 $(1 \leq m_1 \leq k_1,\ 1 \leq m_2 \leq k_2)$.

Приклад 6.17. 1. Цикли $(1,2,4)$ та $(3,5)$ незалежні.

2. Цикли $(1,3,5)$, $(2,6)$, $(4,7)$ попарно незалежні.

3. Цикли $(1,4)$ та $(3,7,4,2)$ не незалежні.

Вправа 6.7. Довести, що незалежні цикли комутують, тобто

$$\sigma_2 \circ \sigma_1 = \sigma_1 \circ \sigma_2,$$

де σ_1, σ_2 – незалежні цикли.

Вправа 6.8. Довести, що кожна транспозиція дорівнює своїй оберненій, тобто

$$(i_1, i_2)^{-1} = (i_1, i_2).$$

Теорема 6.3. *Кожну підстановку можна зобразити як композицію незалежних циклів.*

Схема доведення. Наведемо алгоритм зображення підстановки $\sigma \in S_n$ як композицію незалежних циклів.

Розглянемо послідовність $i_0, i_1, i_2, \ldots$, побудовану за схемою:

$$i_0 = 1,\ i_1 = \sigma(1),\ i_2 = \sigma(i_1) = \sigma^2(1),\ i_3 = \sigma(i_2) = \sigma^3(1), \ldots, i_k = \sigma^k(1), \ldots$$

Ураховуючи скінченність множини $A = \{1, 2, \ldots, n\}$, елементи послідовності i_k $(k \geq 0)$ почнуть повторюватися, починаючи з деякого номера m_1:

- $i_{m_1} = i_{m_0}$ для деякого m_0 $(0 \leq m_0 < m_1 \leq n)$;
- $i_{k_1} \neq i_{k_2}$, якщо $0 \leq k_1 < k_2 < m_1$.

Доведемо, що $m_0 = 0$. Припускаючи, що $1 \leq m_0 < m_1$, отримуємо

$$\sigma\left(\sigma^{m_1-1}(1)\right) = \sigma\left(\sigma^{m_0-1}(1)\right) \text{ при } \sigma^{m_1-1}(1) \neq \sigma^{m_0-1}(1),$$

що суперечить ін'єктивності відображення σ.

Отже, $m_0 = 0$, тобто $i_{m_1} = \sigma^{m_1}(1) = i_0$. Таким чином, побудована послідовність $(i_0, i_1, \ldots, i_{m_1-1})$ $(i_{m_1} = i_0)$ визначає цикл довжиною m_1, дія якого на множині $\{i_0, i_1, \ldots, i_{m_1-1}\}$ збігається з дією підстановки σ.

Далі будуємо наступний цикл $\{\widetilde{i}_0, \widetilde{i}_1, \ldots, \widetilde{i}_{m_2-1}\}$, обираючи $\widetilde{i}_0$ таким, що не входить у побудований цикл $(i_0, i_1, \ldots, i_{m_1-1})$. Описану процедуру повторюємо доти, доки залишається хоча б один елемент множини $A = \{1, 2, \ldots, n\}$, що не увійшов до побудованих циклів.

Легко зрозуміти, що композиція всіх побудованих циклів збігається з підстановкою σ (дія відображення σ на довільний елемент $i_k \in A$ збігається з дією на цей елемент відповідного циклу, до якого входить i_k). Нарешті, незалежність побудованих циклів випливає з ін'єктивності відображення σ. $\square$

Приклад 6.18. Зобразимо у вигляді композиції незалежних циклів підстановку $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 8 & 6 & 4 & 1 & 7 & 3 \end{pmatrix}$:

1) побудуємо перший цикл, починаючи з елемента 1:

$$1,\ \sigma(1) = 2,\ \sigma(2) = 5,\ \sigma(5) = 4,\ \sigma(4) = 6,\ \sigma(6) = 1,$$

тобто отримуємо цикл довжиною 5: $(1, 2, 5, 4, 6)$; процедура має продовжуватися, оскільки існують елементи (наприклад, 3), що не увійшли до побудованого циклу;

2) побудуємо другий цикл, починаючи з елемента 3:

$$3,\ \sigma(3) = 8,\ \sigma(8) = 3,$$

тобто отримуємо цикл довжиною 2: $(3, 8)$; процедура має продовжуватися, оскільки залишився елемент 7, що не увійшов до побудованих циклів;

3) побудуємо третій цикл, починаючи з елемента 7:

$$7,\ \sigma(7) = 7,$$

тобто отримуємо цикл довжиною 1 (тотожну підстановку): $(7) = \varepsilon$.

Отже, підстановка σ допускає такий розклад у композицію незалежних циклів:

$$\sigma = (1, 2, 5, 4, 6) \circ (3, 8) \circ (7).$$

Зв'язок побудованих циклів з підстановкою σ цікаво простежити, переставивши відповідно стовпці матриці σ:

$$\sigma = \begin{pmatrix} 1 & 2 & 5 & 4 & 6 & 3 & 8 & 7 \\ 2 & 5 & 4 & 6 & 1 & 8 & 3 & 7 \end{pmatrix}.$$

Зауваження 6.11. Із алгоритму, запропонованого в схемі доведення теореми 6.3, легко побачити єдиність зображення підстановки у вигляді композиції незалежних циклів (з точністю до переставлення циклів – аргументів композиції). Дійсно, запропонований алгоритм однозначно визначає кожен цикл, до якого має входити кожне $i_k \in \{1, 2, \ldots, n\}$, звідки, враховуючи незалежність циклів, і випливає єдиність зображення.

Теорема 6.4. *Кожну підстановку σ на множині A можна зобразити у вигляді композиції скінченної кількості транспозицій.*

Для доведення теореми знадобиться один простий результат, який, проте, має самостійне значення.

Лема 6.2 (сортування перестановки транспозиціями)**.** *Із довільної перестановки $i = (i_1, i_2, \ldots, i_n)$, застосовуючи скінченну кількість транспозицій τ_k $(1 \le k \le m)$, можна отримати перестановку $(1, 2, \ldots, n)$, тобто*

$$(1, 2, \ldots, n) = (\tau_m \circ \tau_{m-1} \circ \ldots \tau_2 \circ \tau_1)(i).$$

Доведення леми. Будемо сортувати елементи, застосовуючи на кожному етапі не більше однієї транспозиції: спочатку поставимо «на своє місце» (на першу координату) елемент 1, потім – елемент 2 і так далі, поки всі елементи перестановки не будуть стояти на своїх місцях, тобто поки не отримаємо перестановку $(1, 2, \ldots, n)$. Опишемо детально перші два кроки процедури сортування (далі процедура продовжується за аналогією).

1. Один з елементів вихідної перестановки i (як і будь-якої іншої) має дорівнювати 1. Нехай $i_k = 1$. Якщо $k = 1$, тобто у вихідній перестановці i перший елемент $i_1 = 1$, встановлюємо $i^1 = i$ та переходимо до другого кроку. Інакше, виберемо транспозицію $\lambda_1 = (i_1, 1)$ і встановимо $i^1 = \lambda_1(i)$; тоді перший елемент перестановки i^1 дорівнює 1, тобто

$$i^1 = \lambda_1(i) = (1, i^1_2, i^1_3, \ldots, i^1_n).$$

2. Один з елементів перестановки i^1 має дорівнювати 2. Нехай $i^1_k = 2$ ($k \geq 2$, оскільки $i^1_1 = 1$). Якщо $k = 2$, тобто в перестановці i^1 другий елемент $i^1_2 = 2$, встановлюємо $i^2 = i^1$ та переходимо до наступного кроку. Інакше, виберемо транспозицію $\lambda_2 = (i^1_2, 2)$ і встановимо $i^2 = \lambda_2(i^1)$; тоді другий елемент перестановки i^2 дорівнює 2, тобто

$$i^2 = \lambda_2(i^1) = (1, 2, i^2_3, \ldots, i^2_n).$$

Взагалі, на m-му кроці ставимо «на своє місце» елемент m, застосовуючи за потреби відповідну транспозицію.

Отже, не пізніше ніж за n кроків (а насправді не пізніше ніж за $n-1$ кроків, оскільки елемент n опиниться «на своєму місці» вже на $(n-1)$-му кроці без застосування окремої транспозиції) отримуємо шукане зображення

$$(\tau_m \circ \tau_{m-1} \circ \ldots \tau_2 \circ \tau_1)(i) = (1, 2, \ldots, n), \quad m \leq n - 1,$$

де τ_k $(1 \leq k \leq m)$ – транспозиції, що дорівнюють відповідним транспозиціям λ_j $(1 \leq j \leq m)$. □

Зауваження 6.12. Процедура, застосована для доведення леми 6.2, визначає досить ефективний алгоритм сортування, який для множини з n елементів закінчує роботу не пізніше ніж за $n - 1$ кроків, причому на кожному кроці виконується операція переставлення двох елементів множини.

Доведення теореми. Нехай $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$.

Згідно з доведеною лемою, для перестановки $i = (i_1, i_2, \dots, i_n)$ справедливе зображення

$$(\tau_m \circ \tau_{m-1} \circ \dots \tau_2 \circ \tau_1)(i) = (1, 2, \dots, n),$$

де τ_k $(1 \le k \le n)$ – транспозиції. Тоді, як неважко перевірити,

$$\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix} = \tau_m \circ \tau_{m-1} \circ \dots \tau_2 \circ \tau_1.$$

Нарешті, оскільки кожна транспозиція дорівнює своїй оберненій (результат вправи 6.8), отримуємо

$$\sigma = \tau_1^{-1} \circ \tau_2^{-1} \circ \dots \tau_m^{-1} = \tau_1 \circ \tau_2 \circ \dots \tau_m. \qquad \square$$

Приклад 6.19. Зобразимо підстановку $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 4 & 3 & 2 \end{pmatrix}$ у вигляді композиції транспозицій, для чого відсортуємо перестановку $i = (5, 1, 6, 4, 3, 2)$, застосовуючи процедуру сортування, узяту з доведення леми 6.2.

1. Для вихідної перестановки $1 = i_2$, $i_1 = 5$. Отже, на першому кроці застосовуємо транспозицію $\lambda_1 = (5, 1)$:

$$i^1 = (5, 1)(i) = (1, 5, 6, 4, 3, 2).$$

2. Оскільки $2 = i^1_6$, $i^1_2 = 5$, застосовуємо транспозицію $\lambda_2 = (5, 2)$:

$$i^2 = (5, 2)(i^1) = (1, 2, 6, 4, 3, 5).$$

3. Оскільки $3 = i^2_5$, $i^2_3 = 6$, застосовуємо транспозицію $\lambda_3 = (6, 3)$:

$$i^3 = (6, 3)(i^2) = (1, 2, 3, 4, 6, 5).$$

4. Оскільки $i^3_4 = 4$ (елемент 4 розташований «на своєму місці»), встановлюємо $i^4 = i^3$ і переходимо до наступного пункту.

5. Оскільки $5 = i^4_6$, $i^4_5 = 6$, застосовуємо транспозицію $\lambda_4 = (6, 5)$:

$$i^5 = (6, 5)(i^4) = (1, 2, 3, 4, 5, 6).$$

Отже, для перестановки $(5,1,6,4,3,2)$ отримали зображення

$$((6,5)\circ(6,3)\circ(5,2)\circ(5,1))\,((5,1,6,4,3,2)) = (1,2,3,4,5,6).$$

Таким чином, для підстановки σ отримуємо розклад

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 4 & 3 & 2 \end{pmatrix} = (5,1)\circ(5,2)\circ(6,3)\circ(6,5).$$

Зображення підстановки у вигляді композиції транспозицій ніколи не є єдиним (на відміну від зображення підстановки як композиції незалежних циклів). Зокрема, до композиції транспозицій завжди можна «дописати» вираз $\tau\circ\tau$, де τ – довільна транспозиція (а отже, $\tau\circ\tau = \varepsilon$). Крім того, можна змінити черговість розташовування елементів «на свої місця» (у наведеному алгоритмі було застосовано черговість від 1 до n), що, як правило, спричинює інший варіант розкладу.

Приклад 6.20. Наведемо інші варіанти зображення як композиції транспозицій для підстановки σ із прикл. 6.19:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 4 & 3 & 2 \end{pmatrix} = (5,1)\circ(5,2)\circ(6,3)\circ(6,5) =$$
$$= (6,2)\circ(3,5)\circ(2,3)\circ(1,2) = (1,2)\circ(1,6)\circ(1,5)\circ(3,5) =$$
$$= (5,1)\circ(5,2)\circ(6,3)\circ(6,5)\circ(2,4)\circ(2,4) =$$
$$= (5,1)\circ(1,3)\circ(1,3)\circ(5,2)\circ(6,3)\circ(6,5).$$

Перший розклад отримано алгоритмом, запропонованим у доведенні леми 6.2 (див. прикл. 6.19). Другий і третій розклади отримано зміною черговості розташовування елементів: будуючи другий розклад, спочатку розташували «на своєму місці» елемент 6, потім – елемент 5, і так далі до 1; будуючи третій розклад, спочатку розташували «на своїх місцях» парні елементи, а потім – непарні. Четвертий і п'ятий розклади отримано з першого додаванням до композиції транспозицій деякої «тотожної пари» $\tau\circ\tau$, де τ – транспозиція.

6.3.3. Парні та непарні підстановки

Розглянемо два еквівалентні підходи до визначення парності підстановок: підхід, пов'язаний з поняттям інверсії, та підхід, пов'язаний із зображенням підстановки у вигляді композиції транспозицій.

Означення 6.11. Кажуть, що невпорядкована пара елементів i_{k_1}, i_{k_2} утворює інверсію в перестановці $i = (i_1, i_2, \ldots, i_n)$, якщо виконується одна з двох пар умов:

- $k_1 < k_2$ та $i_{k_1} > i_{k_2}$;
- $k_1 > k_2$ та $i_{k_1} < i_{k_2}$,

тобто більший з елементів i_{k_1}, i_{k_2} розташований у перестановці i зліва від меншого.

Приклад 6.21. У перестановці $i = (1, 4, 3, 2)$ інверсію утворюють такі пари елементів (нагадаємо, що порядок елементів у парі i_{k_1}, i_{k_2} не враховують):

- інверсій, що містять елемент 1, немає (елемент 1 є найменшим, і в перестановці немає жодного елемента зліва від нього);
- інверсії, утворені елементом 4 та елементами, розташованими в перестановці праворуч від 4:

$$\{4, 3\},\ \{4, 2\};$$

- інверсії, утворені елементом 3 та елементами, розташованими в перестановці праворуч від 3:

$$\{3, 2\}.$$

Отже, вказано всі інверсії, пов'язані з перестановкою $i = (1, 4, 3, 2)$, зокрема й ті, що містять елемент 2. Слід пам'ятати, що інверсії, за означенням 6.11, утворюються невпорядкованими парами (зокрема, не потрібно окремо враховувати інверсію $\{2, 3\}$, оскільки вже вказано інверсію $\{3, 2\}$).

Означення 6.12. Перестановку називають парною, якщо вона допускає парну кількість інверсій, і непарною, якщо вона допускає непарну кількість інверсій. Парністю перестановки $i = (i_1, i_2, \ldots, i_n)$ назвемо число

$$\varkappa(i) = \begin{cases} 0, & \text{якщо } i \text{ парна}, \\ 1, & \text{якщо } i \text{ непарна}. \end{cases}$$

Ще раз нагадаємо, що перестановки утворюються невпорядкованими парами, а отже, не потрібно враховувати одну інверсію $\{i_{k_1}, i_{k_2}\}$ двічі, оскільки невпорядковані пари $\{i_{k_1}, i_{k_2}\}$ та $\{i_{k_2}, i_{k_1}\}$ збігаються. Зауважимо, що якщо спробувати підрахувати одну інверсію двічі, то всі перестановки виявляться парними.

Приклад 6.22. 1. Перестановка $(1, 4, 3, 2)$ допускає три інверсії ($\{4, 3\}$, $\{4, 2\}$, $\{3, 2\}$), а отже, є непарною (парність 1).

2. Перестановка $(2, 3, 1, 4)$ допускає дві інверсії ($\{2, 1\}$, $\{3, 1\}$), а отже, є парною (парність 0).

3. Перестановка вигляду $(1, 2, \ldots, n)$ не допускає жодної інверсії, а отже, є парною (0 – парне число).

Лема 6.3. *Застосування транспозиції змінює парність перестановки, тобто*

$$\varkappa(i) \neq \varkappa(\tau(i)),$$

де τ *– транспозиція;* $i = (i_1, i_2, \ldots, i_n)$ *– перестановка.*

Доведення. Нехай $i = (i_1, \ldots, i_{k_1}, \ldots, i_{k_2}, \ldots, i_n)$, $\tau = (i_{k_1}, i_{k_2})$ $(k_2 > k_1)$. Тоді $\tau(i) = (i_1, \ldots, i_{k_2}, \ldots, i_{k_1}, \ldots, i_n)$.

Для доведення леми розглянемо, які пари елементів $\{i_{m_1}, i_{m_2}\}$ мають «різну інверсійність» у перестановках i та $\tau(i)$, тобто утворюють інверсію в перестановці i та не утворюють інверсію в $\tau(i)$, або навпаки – утворюють інверсію в $\tau(i)$ та не утворюють в i. Якщо кількість таких пар виявиться непарною, лему буде доведено.

1. Розглянемо пару $\{i_{m_1}, i_{m_2}\}$, якщо $\{i_{m_1}, i_{m_2}\} \cap \{i_{k_1}, i_{k_2}\} = \varnothing$. Така пара має однакову інверсійність у перестановках i та $\tau(i)$, (тобто в обох перестановках є інверсією або в обох перестановках не є інверсією), оскільки транспозиція $\tau = (i_{k_1}, i_{k_2})$ не змінює розташування елементів i_{m_1} та i_{m_2}.

2. Розглянемо пару $\{i_k, i_m\}$, якщо $1 \leq k < k_1$, $m \in \{k_1, k_2\}$. Така пара має однакову інверсійність у перестановках i та $\tau(i)$, оскільки транспозиція τ не змінює взаємного розташування елементів i_k та i_m.

3. Аналогічно попередньому пункту, пара елементів $\{i_m, i_k\}$ при $k_2 < k \leq n$, $m \in \{k_1, k_2\}$ також має однакову інверсійність у перестановках i та $\tau(i)$.

4. Нехай $k_1 < k < k_2$, тоді:

- пара $\{i_{k_1}, i_k\}$ має різну інверсійність у перестановках i та $\tau(i)$, оскільки транспозиція τ змінює взаємне розташування елементів i_{k_1} та i_k. Очевидно, що всього існує $k_2 - k_1 - 1$ пар вигляду $\{i_{k_1}, i_k\}$ $(k_1 < k < k_2)$;
- пара $\{i_k, i_{k_2}\}$ має різну інверсійність у перестановках i та $\tau(i)$, оскільки транспозиція τ змінює взаємне розташування елементів i_k та i_{k_2}. Очевидно, що всього існує $k_2 - k_1 - 1$ пар вигляду $\{i_k, i_{k_2}\}$ $(k_1 < k < k_2)$.

5. Пара $\{i_{k_1}, i_{k_2}\}$ (остання, що залишилась нерозглянутою) має різну інверсійність у перестановках i та $\tau(i)$, оскільки транспозиція τ змінює взаємне розташування елементів i_{k_1} та i_{k_2}.

Отже, всього існує $2(k_2-k_1-1)+1$ (непарна кількість) пар, які мають різну інверсійність у перестановках i та $\tau(i)$.

Твердження леми доведено. □

Приклад 6.23. Перестановка $i = (1, 4, 3, 2)$ допускає три інверсії: $\{4, 3\}$, $\{4, 2\}$, $\{3, 2\}$. Застосовуючи транспозцію $\tau = (1, 3)$, отримуємо перестановку $\tau(i) = (3, 4, 1, 2)$, яка допускає чотири інверсії: $\{3, 1\}$, $\{3, 2\}$, $\{4, 1\}$, $\{4, 2\}$. Отже, перестановка $i = (1, 4, 3, 2)$ є непарною, а перестановка $\tau(i)$ – парною.

Означення 6.13 (перше означення парності підстановки)**.** Підстановку $\sigma = \begin{pmatrix} i \\ j \end{pmatrix}$ називають парною, якщо перестановки i та j мають однакову парність, і непарною, якщо перестановки i та j мають різну парність. Парністю підстановки σ назвемо число

$$\varkappa(\sigma) = \begin{cases} 0, & \text{якщо } \sigma \text{ парна,} \\ 1, & \text{якщо } \sigma \text{ непарна.} \end{cases}$$

Для наведеного означення парності підстановки потрібно обґрунтування коректності (незалежність парності від вибору матриці для зображення підстановки). Відповідне твердження буде наведено в теоремі 6.5.

Приклад 6.24. 1. Обчислимо парність підстановки

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

Перестановка $i = (1, 2, 3, 4)$ є парною (не містить інверсій); перестановка $j = (3, 2, 1, 4)$ допускає три інверсії ($\{3, 2\}$, $\{3, 1\}$, $\{2, 1\}$), а отже, є непарною. Таким чином, вихідна підстановка $\sigma = \begin{pmatrix} i \\ j \end{pmatrix}$ є непарною, оскільки підстановки i та j мають різну парність.

2. Обчислимо парність підстановки $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$.

Перестановка $i = (1, 2, 3, 4)$ є парною (не містить інверсій); перестановка $j = (4, 1, 3, 2)$ допускає чотири інверсії ($\{4, 1\}$, $\{4, 3\}$, $\{4, 2\}$, $\{3, 2\}$), а отже, є парною. Таким чином, вихідна підстановка $\sigma = \begin{pmatrix} i \\ j \end{pmatrix}$ є парною, оскільки підстановки i та j мають однакову парність.

Вправа 6.9. Довести такі твердження:

1. Підстановки σ та σ^{-1} мають однакову парність.
2. Парність композиції $\sigma = \sigma_2 \circ \sigma_1$ можна обчислити за формулою

$$\varkappa(\sigma) = \varkappa(\sigma_1) \oplus \varkappa(\sigma_2),$$

тобто σ є парною тоді і тільки тоді, коли σ_1 та σ_2 мають однакову парність.

Вказівка. Скористатись заув. 6.8.

3. Тотожна підстановка є парною.
4. Транспозиція є непарною підстановкою.
5. Цикл парної довжини є непарним, цикл непарної довжини – парним.

Вказівка. Довести, що цикл $(i_1, i_2, \ldots, i_k)$ можна зобразити у вигляді композиції $k - 1$ транспозицій:

$$(i_1, i_2, \ldots, i_k) = (i_1, i_2) \circ (i_2, i_3) \circ \cdots \circ (i_{k-1}, i_k),$$

після чого скористатися результатами пп. 2 та 4.

Наступна теорема постулює коректність означення 6.13.

Теорема 6.5 (коректність означення парності підстановки)**.** *Парність підстановки σ не залежить від способу зображення σ у вигляді матриці.*

Доведення. Твердження теореми є простим наслідком леми 6.3. Дійсно, матрицю для зображення підстановки $\sigma = \begin{pmatrix} i \\ j \end{pmatrix}$ можна змінювати лише переставленням стовпців, тобто застосуванням до перестановок i та j довільної підстановки σ_0:

$$\sigma = \begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} \sigma_0(i) \\ \sigma_0(j) \end{pmatrix}.$$

Якщо σ_0 є транспозицією, парність перестановок i та $\sigma_0(i)$ різна (лема 6.3). Але парність перестановок j та $\sigma_0(j)$ також різна, тобто парність підстановок $\begin{pmatrix} i \\ j \end{pmatrix}$ та $\begin{pmatrix} \sigma_0(i) \\ \sigma_0(j) \end{pmatrix}$ (точніше, різних зображень однієї підстановки σ) однакова.

У загальному випадку, коли σ_0 є довільною підстановкою на множині $A = \{1, 2, \ldots, n\}$, достатньо зобразити σ_0 у вигляді композиції транспозицій (фактично отримуючи матрицю $\begin{pmatrix} \sigma_0(i) \\ \sigma_0(j) \end{pmatrix}$ із матриці $\begin{pmatrix} i \\ j \end{pmatrix}$ за декілька кроків, на кожному кроці міняючи місцями лише два стовпці). □

Приклад 6.25. Розглянемо підстановку $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Перестановка $i = (1, 2, 3)$ є парною (не містить інверсій), перестановка $j = (2, 3, 1)$ також є парною (містить дві інверсії: $\{2, 1\}$ і $\{3, 1\}$). Отже, вихідна підстановка $\sigma = \begin{pmatrix} i \\ j \end{pmatrix}$ є парною, оскільки перестановки $i = (1, 2, 3)$ та $j = (2, 3, 1)$ мають однакову парність.

Тепер у матриці $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ поміняємо місцями перший та останній стовпці, отримавши інше зображення для підстановки σ:

$$\sigma = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 3 & 2 \end{pmatrix}.$$

Згідно з теоремою 6.5, парність підстановки σ не має залежати від вибору матриці для її зображення. Дійсно, у цьому випадку маємо: перестановка $\widetilde{i} = (3, 2, 1)$ непарна (три інверсії: $\{3, 2\}$, $\{3, 1\}$, $\{2, 1\}$); перестановка $\widetilde{j} = (1, 3, 2)$ також непарна (одна інверсія: $\{3, 2\}$); отже, матри-

ця $\begin{pmatrix} \widetilde{i} \\ \widetilde{j} \end{pmatrix}$ також визначає парну підстановку (перестановки $\widetilde{i}$ та $\widetilde{j}$ мають однакову парність – обидві непарні).

Означення 6.14 (друге означення парності підстановки)**.** Підстановку називають парною, якщо її зображують у вигляді композиції парної кількості транспозицій, і непарною, якщо її зображують у вигляді композиції непарної кількості транспозицій.

Зазначимо, що еквівалентність означень 6.13 та 6.14, а звідси і коректність означення 6.14 (незалежність від способу зображення підстановки у вигляді композиції транспозицій), одразу випливає з результатів вправи 6.9.

Приклад 6.26. Розглянемо підстановку $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$, яка є парною в сенсі означення 6.13 (перестановки $(1, 2, 3, 4)$ та $(2, 4, 3, 1)$ обидві парні).

Для застосування означення 6.14 зобразимо підстановку σ у вигляді композиції транспозицій:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (2, 1) \circ (2, 4).$$

Кількість транспозицій в отриманому зображенні парна, отже, підстановка σ є парною і в сенсі означення 6.14.

Продемонструємо на прикладі підстановки σ коректність означення 6.14, тобто випишемо для σ кілька інших способів розкладання в композицію транспозицій:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (1, 4) \circ (1, 2) = (2, 4) \circ (1, 4) = (2, 1) \circ (2, 3) \circ (2, 3) \circ (2, 4).$$

Як бачимо, в усіх наведених розкладах кількість транспозицій залишається парною (хоча сама кількість може змінюватися).

Приклад 6.27. Обчислимо парність підстановок у групах S_2 та S_3.

Група S_2 містить тотожну підстановку ε і транспозицію $\tau = (1, 2)$ (див. прикл. 6.14). Таким чином, S_2 містить одну парну (тотожну) підстановку ε та одну непарну підстановку (транспозицію) τ.

Група S_3 містить тотожну підстановку ε, три транспозиції σ_1, σ_2, σ_3, а також два цикли довжиною 3: φ_1 та φ_2 (для підстановок групи S_3 використаємо позначення з прикл. 6.14). Отже, S_3 містить три парні підстановки (цикли непарної довжини ε, φ_1, φ_2) і три непарні підстановки (транспозиції σ_1, σ_2, σ_3).

Кожна з розглянутих груп S_2 та S_3 містить однакову кількість парних і непарних підстановок (одна парна й одна непарна в S_2, і три парні та три непарні в S_3). Далі (підрозд. 6.12) буде доведено більш загальний факт: кожна група S_n при $n \geq 2$ містить $\frac{n!}{2}$ парних та $\frac{n!}{2}$ непарних підстановок.

Завершуючи підрозділ, наведемо один приклад використання теорії підстановок у лінійній алгебрі.

Приклад 6.28. З курсу лінійної алгебри (наприклад, [10]) добре відомо формулу для обчислення визначника матриці:

$$\begin{vmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \dots & \dots & \dots & \dots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{vmatrix} = \sum_{\sigma \in S_n} (-1)^{\varkappa(\sigma)} \cdot a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \dots a_{n,\sigma(n)}$$

(підсумовуються доданки для всіх $\sigma \in S_n$; $\varkappa(\sigma)$, як і раніше, позначає парність підстановки σ).

Розглянемо конкретні випадки для $n = 1, 2, 3$.

1. Група S_1 містить одну (тотожну) підстановку ε. Отже, отримуємо

$$\|a_{1,1}\| = \sum_{\sigma \in S_1} (-1)^{\varkappa(\sigma)} a_{1,\sigma(1)} = (-1)^{\varkappa(\varepsilon)} a_{1,\varepsilon(1)} = a_{1,1}.$$

2. Група S_2 містить дві підстановки – тотожну підстановку ε і транспозицію $\sigma = (1, 2)$. Отже, отримуємо

$$\begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{vmatrix} = \sum_{\sigma \in S_2} (-1)^{\varkappa(\sigma)} a_{1,\sigma(1)} a_{2,\sigma(2)} =$$

$$= (-1)^{\varkappa(\varepsilon)} a_{1,\varepsilon(1)} a_{2,\varepsilon(2)} + (-1)^{\varkappa(\tau)} a_{1,\tau(1)} a_{2,\tau(2)} = a_{1,1} a_{2,2} - a_{1,2} a_{2,1}.$$

3. Група S_3 містить тотожну підстановку ε, три транспозиції σ_1, σ_2, σ_3, а також два цикли довжиною 3: φ_1 та φ_2 (позначення з прикл. 6.9). Отже, для визначника порядку 3 отримуємо

$$\begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix} = \sum_{\sigma\in S_3} (-1)^{\varkappa(\sigma)} a_{1,\sigma(1)} a_{2,\sigma(2)} a_{3,\sigma(3)} =$$

$$= (-1)^{\varkappa(\varepsilon)} a_{1,\varepsilon(1)} a_{2,\varepsilon(2)} a_{3,\varepsilon(3)} + (-1)^{\varkappa(\sigma_1)} a_{1,\sigma_1(1)} a_{2,\sigma_1(2)} a_{3,\sigma_1(3)} +$$

$$+(-1)^{\varkappa(\sigma_2)} a_{1,\sigma_2(1)} a_{2,\sigma_2(2)} a_{3,\sigma_2(3)} + (-1)^{\varkappa(\sigma_3)} a_{1,\sigma_3(1)} a_{2,\sigma_3(2)} a_{3,\sigma_3(3)} +$$

$$+(-1)^{\varkappa(\varphi_1)} a_{1,\varphi_1(1)} a_{2,\varphi_1(2)} a_{3,\varphi_1(3)} + (-1)^{\varkappa(\varphi_2)} a_{1,\varphi_2(1)} a_{2,\varphi_2(2)} a_{3,\varphi_2(3)} =$$

$$= a_{1,1}a_{2,2}a_{3,3} - a_{1,1}a_{2,3}a_{3,2} - a_{1,3}a_{2,2}a_{3,1} -$$

$$-a_{1,2}a_{2,1}a_{3,3} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2}.$$

Детальніше про групу S_n (зокрема, про розкладання підстановки в композицію незалежних циклів) можна прочитати, наприклад, у [7, 10, 14]. Деякі алгоритмічні аспекти групи підстановок висвітлено в [15].

6.4. Адитивна та мультиплікативна групи класів лишків

6.4.1. Множина класів лишків

У цьому підрозділі буде розглянуто адитивну та мультиплікативну групи, пов'язані з фактор-множиною $\mathbb{Z}/_{(\mathrm{mod}\ n)}$ множини цілих чисел $\mathbb{Z}$ за відношенням еквівалентності $(\mathrm{mod}\, n)$, де n – фіксоване натуральне число.

Відношення еквівалентності $(\mathrm{mod}\, n)$ (за модулем n) досить детально розглянуто в розд. 3, прикл. 3.20. Нагадаємо, що фактор-множина $\mathbb{Z}/_{(\mathrm{mod}\ n)}$ має вигляд

$$\mathbb{Z}/_{(\mathrm{mod}\ n)} = \{\overline{0}, \overline{1}, \ldots, \overline{k}, \ldots, \overline{n-1}\},\ \text{де}\ \overline{k} = \{nm + k \colon m \in \mathbb{Z}\}.$$

Множини (класи еквівалентності) $\overline{k}$ $(0 \le k \le n-1)$ називають *класами лишків за модулем* n. Очевидно, кожен клас $\overline{k}$ складається з цілих чисел, після ділення кожного з яких на n одержують остачу k.

Фактор-множину $\mathbb{Z}/_{(\mathrm{mod}\ n)}$ позначають через $\mathbb{Z}_n$:

$$\mathbb{Z}_n = \mathbb{Z}/_{(\mathrm{mod}\ n)} = \{\overline{0}, \overline{1}, \ldots, \overline{k}, \ldots, \overline{n-1}\},\ \text{де}\ \overline{k} = \{nm + k \colon m \in \mathbb{Z}\}.$$

Ще раз наголосимо, що елементами множини $\mathbb{Z}_n$ є класи лишків, тобто не окремі цілі числа, а множини чисел. Важливо також пам'ятати, що вираз $\overline{k}$ має сенс для довільного $k \in \mathbb{Z}$ (не тільки для $0 \leq k \leq n-1$). Проте, у множині $\mathbb{Z}_n$ міститься рівно n різних класів, і це саме класи $\overline{k}$ при $0 \leq k \leq n-1$; класи $\overline{k}$ з номерами $k \geq n$ та $k < 0$ збігаються з одним із класів $\overline{k}$ при $0 \leq k \leq n-1$:

$$\overline{n} = \overline{0}, \quad \overline{n+1} = \overline{1}, \quad \overline{-1} = \overline{n-1}, \quad \ldots\ .$$

Взагалі, легко побачити, що $\overline{k} = \overline{k \bmod n}$. Нагадаємо, що $k \bmod n$ є загальноприйнятим позначенням для остачі від ділення k на n, тобто число $k_0 = k \bmod n$ однозначно визначається умовами:

$$0 \leq k_0 \leq n-1; \tag{6.3}$$

$$k = n \cdot m + k_0 \text{ для деякого } m \in \mathbb{Z}. \tag{6.4}$$

Зазначимо, що число $m = k \operatorname{div} n$ також визначається умовами (6.3) і (6.4) однозначно:

$$m = \max\{p \in \mathbb{Z} \colon k \geq n \cdot p\}.$$

Приклад 6.29. Розглянемо множини $\mathbb{Z}_1$, $\mathbb{Z}_2$ та $\mathbb{Z}_3$.

1. Множина $\mathbb{Z}_1 = \{\overline{0}\}$ складається з одного елемента $\overline{0} = \mathbb{Z}$ (будь-яке ціле число ділиться на 1 без остачі). Цей випадок нецікавий і його, як правило, не розглядають.

2. Множина $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ містить два елементи – множину $\overline{0}$ парних чисел і множину $\overline{1}$ непарних чисел. У цьому випадку

$$\overline{k} = \overline{k \bmod 2} = \begin{cases} \overline{0}, & \text{якщо } k \text{ парне}, \\ \overline{1}, & \text{якщо } k \text{ непарне}. \end{cases}$$

Зокрема: $\overline{0} = \overline{2} = \overline{-2} = \overline{4} = \overline{-4}, \quad \overline{1} = \overline{-1} = \overline{3} = \overline{-3}$.

3. Множина $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ складається з трьох елементів:

- множини $\overline{0}$ чисел, які діляться на 3 без остачі;

- множини $\overline{1}$ чисел, які діляться на 3 з остачею 1;
- множини $\overline{2}$ чисел, які діляться на 3 з остачею 2.

У цьому випадку, зокрема, маємо:

$$\overline{0} = \overline{3} = \overline{-3} = \overline{6} = \overline{-6}, \quad \overline{1} = \overline{-2} = \overline{4}, \quad \overline{2} = \overline{-1} = \overline{5}.$$

6.4.2. Адитивна група $\mathbb{Z}_n$

Зафіксуємо $n \in \mathbb{N}$.
На множині $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ визначимо операцію «+»:

$$\overline{a} + \overline{b} = \overline{a+b}, \quad a, b \in \mathbb{Z}.$$

Наведене означення потребує обґрунтування коректності: треба довести, що результат операції $\overline{a} + \overline{b}$ не залежить від вибору представників з класів $\overline{a}$ та $\overline{b}$.

Лема 6.4 (коректність операції «+» на $\mathbb{Z}_n$). *Нехай* $\overline{a_1} = \overline{a}$, $\overline{b_1} = \overline{b}$. *Тоді* $\overline{a_1 + b_1} = \overline{a+b}$.

Доведення. Для доведення рівності $\overline{a_1 + b_1} = \overline{a+b}$ достатньо перевірити, що $((a_1 + b_1) - (a+b)) \bmod n = 0$.
Оскільки $\overline{a_1} = \overline{a}$, $\overline{b_1} = \overline{b}$, маємо

$$a_1 = a + m_1 n, \; b_1 = b + m_2 n \text{ для деяких } m_1, m_2 \in \mathbb{Z}.$$

Але тоді отримуємо

$$(a_1 + b_1) - (a+b) = (a_1 - a) + (b_1 - b) = m_1 n + m_2 n = (m_1 + m_2) n,$$

тобто $((a_1 + b_1) - (a+b)) \bmod n = 0$, що доводить твердження леми. □

Отже, побудовано замкнену алгебричну структуру $\langle \mathbb{Z}_n, + \rangle$. Легко довести, що така структура є абелевою групою, оскільки групові властивості (асоціативність, комутативність, наявність нейтрального елемента e, а також існування оберненого $x^{-1,+}$ для кожного $x \in \mathbb{Z}$) одразу випливають з аналогічних групових властивостей для структури $\langle \mathbb{Z}, + \rangle$. Так, у структурі $\langle \mathbb{Z}_n, + \rangle$ нейтральний елемент $e = \overline{0}$, обернений елемент $(\overline{a})^{-1,+} = \overline{-a} = \overline{n-a}$.

Вправа 6.10. Провести повне доведення факту, що структура $\langle \mathbb{Z}_n, + \rangle$ є абелевою групою.

Групу $\langle \mathbb{Z}_n, + \rangle$ називають *адитивною групою класів лишків за модулем* n. Для цієї групи часто вживають скорочене, без указання операції, позначення $\mathbb{Z}_n$; якщо виникає можливість конфлікту позначень, застосовують назву «*адитивна група* $\mathbb{Z}_n$», що вказує на операцію «+» (див. заув. 6.5).

Приклад 6.30. Розглянемо групи $\mathbb{Z}_2$ та $\mathbb{Z}_3$.
1. Наведемо таблицю Келі для адитивної групи $\mathbb{Z}_2$ (табл. 6.3).

Таблиця 6.3. **Таблиця Келі для адитивної групи $\mathbb{Z}_2$**

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

Очевидно, обернені елементи в $\mathbb{Z}_2$ мають вигляд

$$(\overline{0})^{-1,+} = \overline{0}, \quad (\overline{1})^{-1,+} = \overline{1}.$$

2. Наведемо таблицю Келі для адитивної групи $\mathbb{Z}_3$ (табл. 6.4).

Таблиця 6.4. **Таблиця Келі для адитивної групи $\mathbb{Z}_3$**

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Легко перевірити, що обернені елементи в $\mathbb{Z}_3$ мають вигляд

$$(\overline{0})^{-1,+} = \overline{0}, \quad (\overline{1})^{-1,+} = \overline{-1} = \overline{2}, \quad (\overline{2})^{-1,+} = \overline{-2} = \overline{1}.$$

Зауваження 6.13. Адитивна група $\mathbb{Z}_n$ є прикладом загального типу структур – так званих фактор-груп, які буде розглянуто в підрозд. 6.12.

6.4.3. Мультиплікативна група $\mathbb{Z}_p{}^*$

Зафіксуємо $p \in \mathbb{N}$.

На множині $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$ визначимо операцію множення «$\cdot$»:

$$\overline{a} \cdot \overline{b} = \overline{ab},\ a, b \in \mathbb{Z}.$$

Як і у випадку операції «$+$», означення операції «$\cdot$» також потребує обґрунтування коректності.

Лема 6.5 (коректність операції «$\cdot$» на $\mathbb{Z}_p$)**.** *Нехай* $\overline{a_1} = \overline{a}$, $\overline{b_1} = \overline{b}$. *Тоді* $\overline{a_1 \cdot b_1} = \overline{ab}$.

Доведення. Для доведення рівності $\overline{a_1 \cdot b_1} = \overline{ab}$ достатньо перевірити, що $(a_1 b_1 - ab) \bmod p = 0$.

Оскільки $\overline{a_1} = \overline{a}$, $\overline{b_1} = \overline{b}$, маємо

$$a_1 = a + m_1 p,\ b_1 = b + m_2 p \text{ для деяких } m_1, m_2 \in \mathbb{Z}.$$

Але тоді отримуємо

$$a_1 b_1 - ab = a_1 b_1 - a_1 b + a_1 b - ab = a_1(b_1 - b) + b(a_1 - a) = a_1 m_2 p + b m_1 p,$$

тобто $(a_1 b_1 - ab) \bmod p = 0$, що доводить твердження леми. □

Отже, побудовано замкнену алгебричну структуру $\langle \mathbb{Z}_p, \cdot \rangle$. Легко довести, що ця структура є комутативним моноїдом, оскільки необхідні властивості (асоціативність, комутативність і наявність нейтрального елемента) одразу випливають з аналогічних властивостей для моноїда $\langle \mathbb{Z}, \cdot \rangle$. Так, у структурі $\langle \mathbb{Z}_p, \cdot \rangle$ нейтральний елемент $e = \overline{1}$.

Однак структура $\langle \mathbb{Z}_p, \cdot \rangle$, як і $\langle \mathbb{Z}, \cdot \rangle$ (див. прикл. 6.5), за жодного $p \geq 2$ не є групою, оскільки для елемента $\overline{0}$ у цьому разі не існує оберненого.

Для побудови мультиплікативної групи на множині класів лишків будемо додатково вимагати, щоб $p \in \mathbb{N}$ було простим числом[1]. Крім того, групу будуватимемо на «множині без нуля»:

$$\mathbb{Z}_p{}^* = \mathbb{Z}_p \setminus \{\overline{0}\} = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}.$$

[1]Іноді в літературі, особливо в деяких шкільних підручниках, число 1 вважають простим. Тут будемо вважати, що просте число повинно мати рівно два різні натуральні дільники, тобто число 1 не є простим.

Теорема 6.6. *Алгебрична структура $\langle \mathbb{Z}_p{}^*, \cdot \rangle$ для простого $p \in \mathbb{N}$ є абелевою групою.*

Доведення. Перш за все, потрібно довести замкненість структури $\langle \mathbb{Z}_p{}^*, \cdot \rangle$, оскільки працюємо не на всій множині класів лишків. Для цього необхідно довести, що $\overline{a} \cdot \overline{b} \in \mathbb{Z}_p{}^*$ при $\overline{a}, \overline{b} \in \mathbb{Z}_p{}^*$, тобто що $\overline{a} \cdot \overline{b} \neq \overline{0}$ для $\overline{a} \neq \overline{0}$, $\overline{b} \neq \overline{0}$.

Припустімо, що $\overline{a} \cdot \overline{b} = \overline{0}$. Це означає, що $ab \bmod p = 0$, тобто добуток ab ділиться на p без остачі. Але тоді, оскільки число p є простим, одне з чисел a чи b має ділитися на p без остачі, що суперечить умові $\overline{a}, \overline{b} \neq \overline{0}$. Отже, замкненість структури $\langle \mathbb{Z}_p{}^*, \cdot \rangle$ доведено.

Асоціативність і комутативність структури $\langle \mathbb{Z}_p{}^*, \cdot \rangle$ випливає з аналогічних властивостей у структурі $\langle \mathbb{Z}_p, \cdot \rangle$. Нейтральним елементом у структурі $\langle \mathbb{Z}_p{}^*, \cdot \rangle$ є клас $\overline{1}$ (зазначимо, що $\overline{1} \neq \overline{0}$).

Нарешті, доведемо існування оберненого елемента для довільного $\overline{a} \neq \overline{0}$ відносно операції множення (тобто в межах структури $\langle \mathbb{Z}_p{}^*, \cdot \rangle$). Зафіксуємо число a, таке, що $1 \leq a \leq p-1$, і розглянемо набір класів лишків:

$$\overline{a \cdot 1},\ \overline{a \cdot 2},\ \ldots,\ \overline{a \cdot (p-1)}. \tag{6.5}$$

Із вищедоведеної замкненості $\langle \mathbb{Z}_p{}^*, \cdot \rangle$ випливає, що $\overline{ak} \neq \overline{0}$ при $1 \leq k \leq p-1$, тобто набір класів (6.5) лежить у $\mathbb{Z}_p{}^*$.

Доведемо далі, що всі класи (6.5) попарно різні, тобто $\overline{ak_1} \neq \overline{ak_2}$ при $1 \leq k_1 < k_2 \leq p-1$. Припустивши, що $\overline{ak_1} = \overline{ak_2}$, отримуємо

$$(ak_2 - ak_1) \bmod p = 0,\ \text{тобто}\ (a \cdot (k_2 - k_1)) \bmod p = 0.$$

Звідси випливає, що множник a або множник $(k_2 - k_1)$ має ділитися без остачі на просте число p, що суперечить умовам $1 \leq (k_2 - k_1) \leq p-1$ та $1 \leq a \leq p-1$.

Отже, усі класи в наборі (6.5) попарно різні, тобто набір (6.5) містить $p-1$ класів лишків, кожен з яких лежить у $\mathbb{Z}_p{}^*$. Але $\mathbb{Z}_p{}^*$ також містить $p-1$ елементів, тобто не може містити класів, які не входять до набору (6.5). Це означає, що набір (6.5) збігається з множиною $\mathbb{Z}_p{}^*$:

$$\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\} = \{\overline{a \cdot 1}, \overline{a \cdot 2}, \ldots, \overline{a \cdot (p-1)}\}.$$

Зі збігу наведених множин випливає, що один з елементів множини $\{\overline{a \cdot 1}, \overline{a \cdot 2}, \ldots, \overline{a \cdot (p-1)}\}$ має дорівнювати $\overline{1}$; позначимо цей елемент через $\overline{a \cdot k_a}$, де $1 \leq k_a \leq p-1$. Але тоді клас лишків $\overline{k}_a \in \mathbb{Z}_p{}^*$ визначає

елемент, обернений до $\overline{a}$, оскільки за побудовою

$$\overline{a} \cdot \overline{k_a} = \overline{a \cdot k_a} = \overline{1}.$$

Твердження теореми повністю доведено. □

Групу $\langle \mathbb{Z}_p{}^*, \cdot \rangle$ (для простого числа p) називають *мультиплікативною групою класів лишків за модулем p*; для цієї групи часто вживають скорочене, без указання операції, позначення $\mathbb{Z}_p{}^*$; якщо виникає можливість конфлікту позначень, застосовують назву «*мультиплікативна група* $\mathbb{Z}_p{}^*$», що вказує на операцію «$\cdot$» (див. заув. 6.5).

Приклад 6.31. Наведемо таблицю Келі для групи $\mathbb{Z}_5{}^*$ (табл. 6.5).

***Таблиця 6.5.* Таблиця Келі для мультиплікативної групи $\mathbb{Z}_5{}^*$**

$\times$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Легко перевірити, що обернені елементи в $\mathbb{Z}_5{}^*$ мають такий вигляд:

$$(\overline{1})^{-1} = \overline{1}, \quad (\overline{2})^{-1} = \overline{3}, \quad (\overline{3})^{-1} = \overline{2}, \quad (\overline{4})^{-1} = \overline{4}.$$

6.5. Поняття підгрупи. Критерій підгрупи

Нехай $\langle G, * \rangle$ – довільна група.

Означення 6.15. Підгрупою групи $\langle G, * \rangle$ називають підмножину $H \subset G$, яка є групою за тією самою операцією, що і група $\langle G, * \rangle$ (тобто структура $\langle H, * \rangle$ є групою).

Зауваження 6.14. 1. Коли розглядають групу $\langle G, * \rangle$, слід вказати не тільки множину G, але й операцію «$*$»; коли ж беруть до розгляду підгрупу $H \subset G$, можна не вказувати операцію «$*$», яка, за означенням підгрупи, має збігатися з операцією групи $\langle G, * \rangle$.

2. В означенні підгупи не вимагається, щоб нейтральний елемент e_1 підгрупи H збігався з нейтральним елементом e групи G, оскільки цей факт легко випливає з властивостей групи. Дійсно, зафіксувавши довільний елемент $h \in H$, за домомогою правила скорочення (6.1) отримуємо

$$(h = e * h = e_1 * h) \Rightarrow (e = e_1).$$

Приклад 6.32. 1. Множина $\mathbb{Z}$ є підгрупою групи $\langle \mathbb{Q}, + \rangle$.
2. Множина $\mathbb{Q}$ є підгрупою групи $\langle \mathbb{R}, + \rangle$.
3. Множина $\mathbb{R}$ є підгрупою групи $\langle \mathbb{C}, + \rangle$.
4. Множина $(0, +\infty)$ є підгрупою групи $\langle \mathbb{R}^*, \cdot \rangle$.
5. Множина $\{-1, 1\}$ є підгрупою групи $\langle \mathbb{R}^*, \cdot \rangle$.
6. Множина невироджених нижніх трикутних матриць

$$\left\{ \begin{pmatrix} a_{1,1} & 0 \\ a_{2,1} & a_{2,2} \end{pmatrix} : \ a_{1,1}, a_{2,1}, a_{2,2} \in \mathbb{R}, \quad a_{1,1}a_{2,2} \neq 0 \right\}$$

є підгрупою мультиплікативної групи матриць GL_2.
7. Множина матриць з одиничним визначником

$$SL_n = \{A \in GL_n : |A| = 1\}$$

є підгрупою мультиплікативної групи матриць GL_n. Цей факт негайно випливає з формули, відомої з курсу лінійної алгебри (наприклад, [10]):

$$|AB| = |A| \cdot |B|, \tag{6.6}$$

де $A, B \in M_{n \times n}$.

Вправа 6.11. Нехай H_1, H_2 – підгрупи групи $\langle G, * \rangle$. Довести, що перетин $H_1 \cap H_2$ також є підгрупою групи $\langle G, * \rangle$. Узагальнити це твердження на довільну (можливу нескінченну) кількість підгруп групи $\langle G, * \rangle$.

На практиці для перевірки, чи є непорожня підмножина групи підгрупою, зручно користуватися такою теоремою.

Теорема 6.7 (критерій підгрупи)**.** *Нехай $\varnothing \neq H \subset G$, тобто H – непорожня підмножина групи $\langle G, * \rangle$.*

Для того, щоб підмножина H була підгрупою групи $\langle G, * \rangle$, необхідно і достатньо виконання двох умов:

$(a, b \in H) \Rightarrow (a * b \in H)$ *(замкненість H відносно операції «$*$»)*; (6.7)

$(a \in H) \Rightarrow (a^{-1} \in H)$ *(замкненість H відносно взяття оберненого).* (6.8)

Доведення. Необхідність очевидна, оскільки умови замкненості множини H відносно бінарної групової операції, а також існування обернених $a^{-1} \in H$ для кожного $a \in H$, негайно випливають з визначення групи.

Для доведення достатності зауважимо:

- замкненість структури $\langle H, * \rangle$ відносно операції «$*$» є умовою (6.7);
- асоціативність структури $\langle H, * \rangle$ випливає з асоціативності операції «$*$» на всій множині G (а отже, і на підмножині $H \subset G$);
- замкненість структури H відносно операції взяття оберненого є умовою (6.8).

Отже, треба лише довести, що структура $\langle H, * \rangle$ містить нейтральний елемент $e \in G$ вихідної групи $\langle G, * \rangle$.

Зафіксуємо довільний елемент $a \in H$ (це можна зробити, оскільки $H \neq \varnothing$). Тоді, як наслідок умов (6.7), (6.8), отримуємо

$$(a \in H) \Rightarrow (a^{-1} \in H) \Rightarrow (e = a * a^{-1} \in H).$$

Твердження теореми повністю доведено. □

Наслідок. *Умови (6.7) та (6.8) в теоремі 6.7 можна замінити однією умовою:*

$$(a, b \in H) \Rightarrow (a * b^{-1} \in H). \tag{6.9}$$

Доведення. Дійсно, зафіксувавши $a \in H$, отримуємо

$$e = a * a^{-1} \in H.$$

Далі для довільного $b \in H$ одержимо

$$b^{-1} = e * b^{-1} \in H.$$

Нарешті, для довільних $a, b \in H$ дістанемо

$$a * b = a * (b^{-1})^{-1} \in H.$$

Отже, доведено виконання умов (6.7) та (6.8) основної теореми. □

Приклад 6.33. Нехай A_n – множина парних підстановок на множині $A = \{1, 2, \ldots, n\}$. Множина A_n є підгрупою симетричної групи S_n, оскільки для довільних парних $\sigma_1, \sigma_2 \in S_n$ отримано парність підстановки σ_2^{-1}, а потім і парність $\sigma_1 * \sigma_2^{-1}$ (див. результат вправи 6.9). Групу $\langle A_n, \circ \rangle$ називають *знакозмінною групою степеня* n.

Очевидно, що будь-яка група $\langle G, * \rangle$ завжди містить принаймні дві підгрупи: множину $\{e\}$ (e – нейтральний елемент у групі $\langle G, * \rangle$) та саму множину G. Ці підгрупи називають *тривіальними*; підгрупу, що не є тривіальною, називають *власною*. Підгрупу $\{e\}$ часто називають *одиничною*, підгрупу $H = G$ будемо називати *повною*. Зауважимо, що у випадку одноелементної групи $G = \{e\}$ тривіальні підгрупи збігаються.

6.6. Гомоморфізми груп: основні визначення та теореми

У цьому підрозділі працюватимемо з двома групами: $\langle G_1, * \rangle$ та $\langle G_2, \circledast \rangle$ з нейтральними елементами $e_1 \in G_1$ та $e_2 \in G_2$.

Означення 6.16. Відображення $f : G_1 \to G_2$ називають гомоморфізмом, або гомоморфним відображенням, групи $\langle G_1, * \rangle$ в групу $\langle G_2, \circledast \rangle$, якщо

$$f(a * b) = f(a) \circledast f(b) \text{ для довільних } a, b \in G_1.$$

Ін'єктивний гомоморфізм називають мономорфізмом, сюр'єктивний гомоморфізм – епіморфізмом, бієктивний гомоморфізм – ізоморфізмом. Якщо $f : G_1 \to G_2$ – ізоморфізм, то групи $\langle G_1, * \rangle$ і $\langle G_2, \circledast \rangle$ називають ізоморфними. Для факту ізоморфності груп $\langle G_1, * \rangle$ та $\langle G_2, \circledast \rangle$ вживають позначення

$$\langle G_1, * \rangle \sim \langle G_2, \circledast \rangle .$$

Зауваження 6.15. Із означення бієктивності випливає, що f є ізоморфізмом тоді і тільки тоді, коли f є одночасно моно- та епіморфізмом.

Приклад 6.34. 1. Відображення

$$f : \mathbb{R} \to \mathbb{R}^*, \quad f(a) = 2^a$$

є мономорфізмом з групи $\langle \mathbb{R}, + \rangle$ в групу $\langle \mathbb{R}^*, \cdot \rangle$. Проте f не є епіморфізмом, а отже, не є ізоморфізмом.

2. Відображення

$$f : \mathbb{R} \to (0, +\infty), \quad f(a) = 2^a$$

є ізоморфізмом з групи $\langle \mathbb{R}, + \rangle$ в групу $\langle (0, +\infty), \cdot \rangle$.

3. Відображення

$$f : \mathbb{R} \to \{z \in \mathbb{C} : z \neq 0\}, \quad f(a) = e^{i \cdot a}$$

є гомоморфізмом з групи $\langle \mathbb{R}, + \rangle$ в групу $\langle \mathbb{C}^*, \cdot \rangle$, де $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Проте f не є моно- або епіморфізмом. У цьому прикладі константа e позначає основу натурального логарифма, а число i – комплексну одиницю.

З гомоморфізмом груп пов'язано багато цікавих і важливих властивостей. У цьому підрозділі буде розглянуто дві властивості гомоморфного відображення груп; деякі інші властивості будуть розглянуті у підрозд. 6.13.

Теорема 6.8. *Нехай $f : G_1 \to G_2$ – гомоморфізм групи $\langle G_1, * \rangle$ в групу $\langle G_2, \circledast \rangle$. Тоді:*

1) $f(e_1) = e_2$ (гомоморфізм груп зберігає нейтральний елемент групи);

2) $\forall\, a \in G_1 : f(a^{-1}) = (f(a))^{-1}$ (гомоморфізм груп зберігає операцію взяття оберненого елемента).

Доведення. 1. За означенням нейтрального елемента

$$f(e_1) = f(e_1 * e_1) = f(e_1) \circledast f(e_1).$$

Тепер за правилом лівого скорочення (6.2) отримуємо

$$(f(e_1) \circledast f(e_1) = f(e_1)) \Rightarrow$$
$$\Rightarrow (f(e_1) \circledast f(e_1) = f(e_1) \circledast e_2) \Rightarrow (f(e_1) = e_2)\,.$$

2. Нехай $a \in G_1$. За означенням гомоморфності відображення отримуємо

$$f(a^{-1}) \circledast f(a) = f(a^{-1} * a) = f(e_1) = e_2,$$

звідки $f(a^{-1}) = (f(a))^{-1}$. □

Гомоморфізм із групи $\langle G, *\rangle$ в $\langle G, *\rangle$ (тобто з групи в себе) називають *ендоморфізмом* групи $\langle G, *\rangle$. Множину всіх ендоморфізмів групи $\langle G, *\rangle$ позначають через $\mathrm{End}_{\langle G,*\rangle}$ або просто через End_G.

Вправа 6.12. Довести, що $\langle \mathrm{End}_G, \circ\rangle$ є моноїдом.

6.7. Циклічні групи

Нехай $\langle G, *\rangle$ – довільна група з нейтральним елементом $e \in G$.

Зафіксуємо деякий елемент $a \in G$ і розглянемо множину всіх цілих степенів елемента a:

$$[a] = \{a^n : n \in \mathbb{Z}\} = \{\dots, a^{-n}, \dots, a^{-2}, a^{-1}, e, a, a^2, \dots, a^n, \dots\}.$$

Вправа 6.13. Довести, що множина $[a]$ є підгрупою групи $\langle G, *\rangle$.

Вказівка. Скористатися критерієм підгрупи (теорема 6.7) та властивостями степеня елемента групи (підрозд. 6.2, з урахуванням заув. 6.7).

Підгрупу $[a] \subset G$ називають *циклічною підгрупою, породженою елементом* $a \in G$. Елемент $a \in G$ називають *твірною підгрупи* $[a] \subset G$.

Стосовно множини цілих степенів елемента $a \in G$ розглянемо два важливі випадки: існує чи не існує показник $n > 0$, такий, що $a^n = e$.

1. Існує показник $n > 0$, такий, що $a^n = e$.

Виберемо найменший додатний номер n, для якого $a^n = e$:

$$n = \min\{k \in \mathbb{N} : a^k = e\}. \tag{6.10}$$

Число $n \in \mathbb{N}$, визначене формулою (6.10), називають *порядком елемента* $a \in G$ та позначають через $|a|$: $n = |a|$.

Вправа 6.14. Довести, що єдиним елементом порядку 1 є нейтральний елемент: $(|a| = 1) \Leftrightarrow (a = e)$.

Вправа 6.15. Довести рівність: $a^{k \bmod n} = a^k$.

Вказівка. Скористатись умовами (6.3) і (6.4), що визначають $k \bmod n$.

Лема 6.6. $a^{k_1} \neq a^{k_2}$, *якщо* $0 \leq k_1 < k_2 \leq n - 1$.

Доведення. Нехай $0 \le k_1 < k_2 \le n-1$. Припустімо, що $a^{k_1} = a^{k_2}$. Тоді отримуємо

$$a^{k_2-k_1} = a^{k_2} * \left(a^{k_1}\right)^{-1} = e,$$

що суперечить умові (6.10), оскільки $0 < k_2 - k_1 < n$. □

Ураховуючи результат леми 6.6 та рівність $a^{k \bmod n} = a^k$, отримуємо явний вигляд циклічної підгрупи, породженої елементом $a \in G$:

$$[a] = \{a^k : 0 \le k \le n-1\} = \{e, a, a^2, \ldots, a^{n-1}\}.$$

Отже, підгрупа $[a]$ містить рівно n різних елементів; степені з показниками $k \ge n$ або $k < 0$ збігатимуться з одним зі степенів a^k $(0 \le k \le n-1)$:

$$a^n = a^0 = e, \quad a^{n+1} = a^1 = a, \quad a^{-1} = a^{n-1}, \quad \ldots$$

(у загальному випадку, як вже зазначалось, $a^k = a^{k \bmod n}$).

Теорема 6.9. *Нехай $a \in G$ – елемент порядку $|a| = n$. Тоді група $\langle [a], * \rangle$ ізоморфна адитивній групі $\mathbb{Z}_n$:*

$$\langle [a], * \rangle \sim \langle \mathbb{Z}_n, + \rangle .$$

Доведення. Шуканий ізоморфізм $f : [a] \to \mathbb{Z}_n$ встановлюється співвідношенням

$$f(a^k) = \overline{k} \in \mathbb{Z}_n, \quad 0 \le k \le n-1.$$

Вправа 6.16. Довести, що введене відображення $f : [a] \to \mathbb{Z}_n$ – ізоморфізм груп $\langle [a], * \rangle$ та $\mathbb{Z}_n$.

Вказівка. Гомоморфну властивість і сюр'єктивність f легко вивести з визначення відображення f; ін'єктивність f випливає з леми 6.6. □

2. Не існує показника $n > 0$, такого, що $a^n = e$. У цьому випадку говорять, що елемент $a \in G$ має *нескінченний порядок*: $|a| = \infty$.

Лема 6.7. *$a^{k_1} \ne a^{k_2}$, якщо $k_1 \ne k_2$.*

Доведення. Припустімо, що $a^{k_1} = a^{k_2}$ при $k_1 \ne k_2$. Без втрати загальності вважатимемо, що $k_1 < k_2$. Тоді отримуємо

$$a^{k_2-k_1} = a^{k_2} * \left(a^{k_1}\right)^{-1} = e,$$

що суперечить умові $|a| = \infty$, оскільки $k_2 - k_1 > 0$. □

Ураховуючи результат леми 6.7, отримуємо явний вигляд циклічної підгрупи, породженої елементом $a \in G$:

$$[a] = \{a^k : k \in \mathbb{Z}\} = \{\dots, a^{-n}, \dots, a^{-2}, a^{-1}, e, a, a^2, \dots, a^n, \dots\}.$$

Отже, підгрупа $[a]$ містить нескінченну (зліченну) кількість різних елементів.

Теорема 6.10. *Нехай $a \in G$ – елемент нескінченного порядку ($|a| = \infty$). Тоді група $\langle [a], * \rangle$ ізоморфна адитивній групі $\mathbb{Z}$:*

$$\langle [a], * \rangle \sim \langle \mathbb{Z}, + \rangle .$$

Доведення. Шуканий ізоморфізм $f : [a] \to \mathbb{Z}$ встановлюється співвідношенням

$$f(a^k) = k, \quad k \in \mathbb{Z}.$$

Вправа 6.17. Довести, що введене відображення $f : [a] \to \mathbb{Z}$ є ізоморфізмом груп $\langle [a], * \rangle$ та $\langle \mathbb{Z}, + \rangle$.

Вказівка. Гомоморфну властивість і сюр'єктивність f легко вивести з визначення відображення f; ін'єктивність f випливає з леми 6.7. □

Отже, усі циклічні підгрупи піддаються повному опису (з точністю до ізоморфізму), що встановлено теоремами 6.9 та 6.10. Отриманий результат сформулюємо у вигляді теореми.

Теорема 6.11. *Нехай $\langle G, * \rangle$ – довільна група. Тоді циклічна підгрупа $[a]$, породжена елементом $a \in G$, ізоморфна адитивній групі $\mathbb{Z}$ при $|a| = \infty$ або адитивній групі класів лишків $\mathbb{Z}_n$ при $|a| = n$:*

1) $[a] \sim \langle \mathbb{Z}_n, + \rangle$, *якщо* $|a| = n < \infty$;

2) $[a] \sim \langle \mathbb{Z}, + \rangle$, *якщо* $|a| = \infty$.

Групу, яка збігається з однією зі своїх циклічних підгруп, тобто $G = [a]$ для деякого $a \in G$, називають *циклічною*. Елемент $a \in G$, що породжує групу $\langle G, * \rangle$, є твірною групи $[a] = G$.

Зауваження 6.16. Теорема 6.11 встановлює (з точністю до ізоморфізму) повний опис циклічних груп, оскільки циклічну групу можна вважати окремим випадком циклічної підгрупи.

Приклад 6.35. 1. Адитивна група $\mathbb{Z}_n$ ($n \in \mathbb{N}$) – один з найважливіших прикладів скінченної циклічної підгрупи. Легко перевірити, що твірними циклічної групи $\mathbb{Z}_n$ для будь-якого $n \geq 2$ можуть бути, зокрема, елементи $\overline{1}$ та $\overline{-1} = \overline{n-1}$:

$$[\overline{1}] = [\overline{n-1}] = \mathbb{Z}_n, \quad n \geq 2$$

(у випадку $n = 2$ класи $\overline{1}$ та $\overline{-1}$ збігаються; випадок $n = 1$ є коректним, але нецікавим). Зазначимо, що для деяких $n \in \mathbb{N}$ (зокрема, якщо $n = 5$) існують інші твірні циклічної групи $\mathbb{Z}_n$. Розглянемо циклічні підгрупи групи $\mathbb{Z}_n$ для $n = 3, 4, 5, 6$:

1) $n = 3$. $\mathbb{Z}_3 = [\overline{1}] = [\overline{2}]$;
2) $n = 4$. $\mathbb{Z}_4 = [\overline{1}] = [\overline{3}]$; $[\overline{2}] = \{\overline{2}, \overline{0}\}$;
3) $n = 5$. $\mathbb{Z}_5 = [\overline{1}] = [\overline{2}] = [\overline{3}] = [\overline{4}]$;
4) $n = 6$. $\mathbb{Z}_6 = [\overline{1}] = [\overline{5}]$; $[\overline{2}] = \{\overline{2}, \overline{4}, \overline{0}\}$; $[\overline{3}] = \{\overline{3}, \overline{0}\}$.

Елемент $\overline{0}$ окремо не розглядався, оскільки за всіх $n \in \mathbb{N}$ він є твірною тривіальної (одиничної) циклічної підгрупи, тобто $[\overline{0}] = \{\overline{0}\}$ (див. вправу 6.14).

2. Адитивна група $\mathbb{Z}$ є основним прикладом нескінченної циклічної групи. Циклічна група $\langle \mathbb{Z}, + \rangle$ допускає дві твірні:

$$\mathbb{Z} = [1] = [-1].$$

Розглянемо інші циклічні підгрупи групи $\langle \mathbb{Z}, + \rangle$. Для довільного $k \geq 2$ отримуємо

$$[k] = [-k] = \{k \cdot m \colon m \in \mathbb{Z}\} = \{0, k, -k, 2k, -2k, \dots\} = k\mathbb{Z}.$$

Зауважимо, що позначення $k\mathbb{Z}$ ($k \in \mathbb{Z}$) є загальноприйнятим для множини $\{k \cdot m : m \in \mathbb{Z}\}$ (зокрема, $2\mathbb{Z}$ є множиною парних цілих чисел). Нарешті, зазначимо, що випадок $[0] = \{0\}$ є тривіальним випадком одиничної підгрупи.

3. Розглянемо циклічні підгрупи симетричної групи S_3 (для підстановок групи S_3 використаємо позначення з прикл. 6.14):

$$[\sigma_1] = \{\sigma_1, \varepsilon\}, \quad [\sigma_2] = \{\sigma_2, \varepsilon\}, \quad [\sigma_3] = \{\sigma_3, \varepsilon\},$$
$$[\varphi_1] = [\varphi_2] = \{\varphi_1, \varphi_2, \varepsilon\}, \quad [\varepsilon] = \{\varepsilon\}.$$

Отже, група S_3 – не циклічна, оскільки не дорівнює жодній зі своїх циклічних підгруп (втім група S_3 не могла бути циклічною, оскільки вона не є комутативною, а отже, не ізоморфна жодній з комутативних груп $\mathbb{Z}_n$ або $\mathbb{Z}$).

6.8. Суміжні класи

Нехай $H \subset G$ – підгрупа групи $\langle G, * \rangle$. Для фіксованого елемента $g \in G$ введемо позначення:

$$g * H = \{g * h \colon h \in H\};$$
$$H * g = \{h * g \colon h \in H\}.$$

Множину $g * H$ називають *лівим суміжним класом* групи $\langle G, * \rangle$ за підгрупою H, що породжений елементом g. Множину $H * g$ називають *правим суміжним класом* групи $\langle G, * \rangle$ за підгрупою H, що породжений елементом g.

Приклад 6.36. Сама підгрупа H є суміжним класом (як правим, так і лівим), породженим нейтральним елементом $e \in G$:

$$e * H = \{e * h \colon h \in H\} = \{h \colon h \in H\} = H;$$
$$H * e = \{h * e \colon h \in H\} = \{h \colon h \in H\} = H.$$

Приклад 6.37. Розглянемо суміжні класи за тривіальними підгрупами.

Для одиничної підгрупи $H = \{e\}$ отримуємо

$$a * \{e\} = \{e\} * a = \{a\} \text{ для довільного } a \in G,$$

тобто і праві, і ліві суміжні класи відносно одиничної підгрупи збігаються і дорівнюють одноелементній множині $\{a\}$, що містить породжувальний елемент $a \in G$.

У випадку повної підгрупи $H = G$ отримуємо

$$a * G = G * a = G \text{ для довільного } a \in G,$$

оскільки будь-який $x \in G$ можна зобразити як елемент суміжного класу (як правого, так і лівого):

$$x = a * \left(a^{-1} * x\right) \in a * G, \quad x = \left(x * a^{-1}\right) * a \in G * a.$$

Отже, існує лише один правий (він же лівий) суміжний клас відносно повної підгрупи $H = G$ – це сама група G.

Зауваження 6.17. Рівність $a * G = G * a = G$ одразу випливає також і з наступної теореми 6.12.

У комутативних групах, очевидно, правий і лівий суміжні класи збігаються: $a*H = H*a$ для всіх $a \in G$. У некомутативних групах можливо $a * H \neq H * a$ (див. прикл. 6.38).

Теорема 6.12. *Ліві суміжні класи групи $\langle G, * \rangle$ відносно підгрупи H або не перерізаються, або збігаються. Праві суміжні класи групи $\langle G, * \rangle$ відносно підгрупи H або не перерізаються, або збігаються.*

Доведення. Твердження теореми будемо доводити для лівих суміжних класів (випадок правих суміжних класів є симетричним). Фактично нам достатньо для $a, b \in G$ довести таке твердження:

$$\left((a * H) \cap (b * H) \neq \varnothing\right) \Rightarrow \left((a * H) = (b * H)\right).$$

Отже, нехай $a, b \in G$ та $(a * H) \cap (b * H) \neq \varnothing$, тобто перетин $(a * H) \cap (b * H)$ містить принаймні один елемент $c \in (a * H) \cap (b * H)$. Тоді отримуємо зв'язок між елементами a та b:

$$(c \in a * H) \Leftrightarrow (c = a * h_1 \text{ для деякого } h_1 \in H);$$
$$(c \in b * H) \Leftrightarrow (c = b * h_2 \text{ для деякого } h_2 \in H);$$
$$a = c * h_1^{-1} = b * h_2 * h_1^{-1} = b * h, \text{ де } h = h_2 * h_1^{-1} \in H.$$

Нарешті, для довільного $x \in G$ отримуємо

$$(x \in a * H) \Rightarrow (x = a * h_a \text{ для деякого } h_a \in H) \Rightarrow$$
$$\Rightarrow (x = b * (h * h_a)) \Rightarrow (x \in b * H).$$

Отже, $a*H \subset b*H$. Вкладення $b*H \subset a*H$ можна довести аналогічно:

$$(x \in b * H) \Rightarrow (x = b * h_b \text{ для деякого } h_b \in H) \Rightarrow$$
$$\Rightarrow (x = a * (h^{-1} * h_b)) \Rightarrow (x \in a * H).$$

Таким чином, $a * H = b * H$, що доводить твердження теореми. □

Легко зрозуміти, що об'єднання всіх лівих (аналогічно, усіх правих) суміжних класів збігається з множиною G, оскільки кожен елемент $a \in G$ обов'язково входить у лівий суміжний клас $a * H$ (аналогічно, $a \in H * a$). Отже, отримано два розбиття множини G в об'єднання лівих суміжних класів та правих суміжних класів за підгрупою H:

$$G = \bigcup_{g \in G} g * H = \bigcup_{g \in G} H * g.$$

Зазначимо, що деякі ліві суміжні класи $a * H$ та $b * H$ (аналогічно, праві суміжні класи $H * a$ та $H * b$) можуть збігатися для $a \neq b$. Однак для $H * a \neq H * b$, за теоремою 6.12 класи $H * a$ та $H * b$ не перерізаються (аналогічно, $a * H \cap b * H = \varnothing$, якщо $a * H \neq b * H$). Зауважимо також, що теорема 6.12 сформульована окремо для правих і окремо для лівих суміжних класів, тобто лівий $a * H$ та правий $H * b$ суміжні класи можуть не збігатися та мати непорожній перетин.

Приклад 6.38. 1. Розглянемо ліві та праві суміжні класи симетричної групи S_3 за підгрупою $[\sigma_1] = \{\sigma_1, \varepsilon\}$ (використовуючи позначення з прикл. 6.14):

$$\begin{aligned}
\varepsilon \circ \{\sigma_1, \varepsilon\} &= \{\sigma_1, \varepsilon\}, & \{\sigma_1, \varepsilon\} \circ \varepsilon &= \{\sigma_1, \varepsilon\};\\
\sigma_1 \circ \{\sigma_1, \varepsilon\} &= \{\varepsilon, \sigma_1\}, & \{\sigma_1, \varepsilon\} \circ \sigma_1 &= \{\varepsilon, \sigma_1\};\\
\sigma_2 \circ \{\sigma_1, \varepsilon\} &= \{\varphi_2, \sigma_2\}, & \{\sigma_1, \varepsilon\} \circ \sigma_2 &= \{\varphi_1, \sigma_2\};\\
\sigma_3 \circ \{\sigma_1, \varepsilon\} &= \{\varphi_1, \sigma_3\}, & \{\sigma_1, \varepsilon\} \circ \sigma_3 &= \{\varphi_2, \sigma_3\};\\
\varphi_1 \circ \{\sigma_1, \varepsilon\} &= \{\sigma_3, \varphi_1\}, & \{\sigma_1, \varepsilon\} \circ \varphi_1 &= \{\sigma_2, \varphi_1\};\\
\varphi_2 \circ \{\sigma_1, \varepsilon\} &= \{\sigma_2, \varphi_2\}, & \{\sigma_1, \varepsilon\} \circ \varphi_2 &= \{\sigma_3, \varphi_2\}.
\end{aligned}$$

Зазначимо, що серед лівих (як і серед правих) суміжних класів є такі, що збігаються:

$$\begin{aligned}
&\varepsilon \circ [\sigma_1] = \sigma_1 \circ [\sigma_1],\ \sigma_2 \circ [\sigma_1] = \varphi_2 \circ [\sigma_1],\ \sigma_3 \circ [\sigma_1] = \varphi_1 \circ [\sigma_1];\\
&[\sigma_1] \circ \varepsilon = [\sigma_1] \circ \sigma_1,\ [\sigma_1] \circ \sigma_2 = [\sigma_1] \circ \varphi_1,\ [\sigma_1] \circ \sigma_3 = [\sigma_1] \circ \varphi_2\,.
\end{aligned}$$

Отже, маємо три різні ліві (і три різні праві) суміжні класи, що попарно не перерізаються. Таким чином, ліві та праві суміжні класи за $[\sigma_1]$ дають нам два різні розбиття S_3 на три множини:

$$S_3 = \{\sigma_1, \varepsilon\} \cup \{\varphi_1, \sigma_3\} \cup \{\varphi_2, \sigma_2\} = \{\varepsilon, \sigma_1\} \cup \{\varphi_1, \sigma_2\} \cup \{\varphi_2, \sigma_3\}.$$

Нарешті, зауважимо, що отримано ліві та праві суміжні класи, які не збігаються, але мають непорожній перетин; такими, наприклад, є лівий та правий суміжні класи, породжені елементом σ_2:

$$\sigma_2 \circ [\sigma_1] = \{\varphi_2, \sigma_2\} \neq [\sigma_1] \circ \sigma_2 = \{\varphi_1, \sigma_2\};\ (\sigma_2 \circ [\sigma_1]) \cap ([\sigma_1] \circ \sigma_2) = \{\sigma_2\}.$$

2. Розглянемо ліві та праві суміжні класи симетричної групи S_3 за підгрупою $[\varphi_1] = \{\varphi_1, \varphi_2, \varepsilon\}$:

$$\begin{aligned}
\varepsilon \circ [\varphi_1] &= [\varphi_1] \circ \varepsilon = \{\varphi_1, \varphi_2, \varepsilon\};\\
\sigma_1 \circ [\varphi_1] &= [\varphi_1] \circ \sigma_1 = \{\sigma_1, \sigma_2, \sigma_3\};\\
\sigma_2 \circ [\varphi_1] &= [\varphi_1] \circ \sigma_2 = \{\sigma_1, \sigma_2, \sigma_3\};\\
\sigma_3 \circ [\varphi_1] &= [\varphi_1] \circ \sigma_3 = \{\sigma_1, \sigma_2, \sigma_3\};\\
\varphi_1 \circ [\varphi_1] &= [\varphi_1] \circ \varphi_1 = \{\varphi_1, \varphi_2, \varepsilon\};\\
\varphi_2 \circ [\varphi_1] &= [\varphi_1] \circ \varphi_2 = \{\varphi_1, \varphi_2, \varepsilon\}.
\end{aligned}$$

У цьому випадку ліві та праві суміжні класи, породжені спільним елементом, збіглися. Таким чином, отримано два різні ліві (які зараз збіглися з відповідними правими) суміжні класи, що попарно не перерізаються. Отже, ліві та праві суміжні класи по $[\varphi_1]$ дають нам одне й те саме розбиття S_3 на дві множини:

$$S_3 = \{\varphi_1, \varphi_2, \varepsilon\} \cup \{\sigma_1, \sigma_2, \sigma_3\}.$$

6.9. Скінченні групи. Теорема Лагранжа

У цьому підрозділі основним об'єктом розгляду буде скінченна група $\langle G, * \rangle$, тобто група, що містить лише скінченну кількість елементів. Кількість елементів у скінченній групі $\langle G, * \rangle$ називають *порядком групи* $\langle G, * \rangle$ і позначають через $|G|$:

$$|G| = \mathrm{card}(G).$$

Нехай $H \subset G$ – підгрупа групи $\langle G, * \rangle$.

Лема 6.8. *Будь-який суміжний клас (як правий, так і лівий) скінченної групи $\langle G, * \rangle$ за підгрупою H містить $|H|$ елементів.*

Доведення. Твердження леми будемо доводити для лівих суміжних класів (випадок правих суміжних класів є симетричним).

Нехай $H = \{h_1, h_2, \ldots, h_m\}$, де $h_i \neq h_j$ при $i \neq j$, тобто всі елементи h_i $(i = 1, 2, \ldots, m)$ попарно різні, та $|H| = m$. Тоді для довільного фіксованого $a \in G$ маємо

$$a * H = \{a * h_1, a * h_2, \ldots, a * h_m\}.$$

Далі з правила лівого скорочення (6.2) отримуємо

$$(a * h_i = a * h_j) \Rightarrow (h_i = h_j).$$

Отже, $a*h_i \neq a*h_j$ для $i \neq j$, тобто всі елементи $a*h_i$ $(i = 1, 2, \ldots, m)$ попарно різні, та $\mathrm{card}(a * H) = m$. □

Приклад 6.39. У прикл. 6.38 було виписано всі суміжні класи (праві та ліві) групи S_3 за циклічними підгрупами $[\sigma_1]$ та $[\varphi_1]$. Як бачимо, кожен суміжний клас за підгрупою $[\sigma_1] = \{\sigma_1, \varepsilon\}$ містить два елементи, а кожен суміжний клас за $[\varphi_1] = \{\varphi_1, \varphi_2, \varepsilon\}$ – три елементи.

Тепер можна сформулювати і довести основну теорему підрозділу.

Теорема 6.13 (теорема Лагранжа[1] для скінченних груп)**.** *Порядок будь-якої підгрупи H скінченної групи $\langle G, * \rangle$ є дільником порядку групи $\langle G, * \rangle$.*

Доведення. Нехай H – підгрупа скінченної групи $\langle G, * \rangle$. Розглянемо розбиття групи $\langle G, * \rangle$ в об'єднання лівих суміжних класів за підгрупою H:

$$G = \bigcup_{g \in G} g * H.$$

Нехай множина $\{g * H : g \in G\}$ містить рівно k різних лівих суміжних класів, породжених деякими елементами g_j $(1 \leq j \leq k)$:

$$G = (g_1 * H) \cup \cdots \cup (g_k * H), \quad g_i * H \neq g_j * H \text{ при } i \neq j.$$

[1] Лагранж Жозеф Луї (1736–1813) – французький математик і механік; автор фундаментальних результатів у варіаційному численні, математичному аналізі, алгебрі тощо; роботи Ж. Л. Лагранжа з математики, механіки та астрономії складають 14 томів.

За теоремою 6.12 ліві суміжні класи, що не збігаються, мають порожній перетин:

$$(g_i * H) \cap (g_j * H) = \varnothing \text{ при } i \neq j, \quad 1 \leq i \leq k,\ 1 \leq j \leq k.$$

Тоді за теоремою про потужність об'єднання скінченних множин, що попарно не перерізаються, отримуємо

$$\operatorname{card}(G) = |G| = \sum_{j=1}^{k} \operatorname{card}(g_j * H).$$

Нарешті, за лемою 6.8 кожний суміжний клас $g_j * H$ $(1 \leq j \leq k)$ містить $|H|$ елементів, звідки отримуємо твердження теореми:

$$\operatorname{card}(G) = \sum_{j=1}^{k} \operatorname{card}(g_j * H) = \sum_{j=1}^{k} |H| = k \cdot |H|. \tag{6.11}$$

Твердження теореми доведено. □

Кількість лівих суміжних класів за підгрупою H (за лемою 6.8 збігається з кількістю правих суміжних класів за H) називають *індексом підгрупи* H і позначають через $\mathrm{i}(H)$. Переписавши рівність (6.11) з урахуванням визначення індексу підгрупи, отримуємо співвідношення

$$|G| = \mathrm{i}(H) \cdot |H|.$$

Отже, у процесі доведення теореми Лагранжа було встановлено, що індекс підгрупи $H \subset G$ також є дільником порядку групи $\langle G, * \rangle$.

Приклад 6.40. Для симетричної групи S_3 (див. прикл. 6.38) отримуємо:

$$\mathrm{i}(\{\sigma_1, \varepsilon\}) = 3,\ |\{\sigma_1, \varepsilon\}| = 2;$$
$$\mathrm{i}(\{\varphi_1, \varphi_2, \varepsilon\}) = 2,\ |\{\varphi_1, \varphi_2, \varepsilon\}| = 3.$$

6.10. Наслідки з теореми Лагранжа

1. Група, порядок якої є простим числом (такі групи часто називають *простими*), містить лише тривіальні підгрупи.

Доведення. Твердження одразу випливає з теореми Лагранжа. □

2. Порядок будь-якого елемента $g \in G$ є дільником порядку групи $\langle G, * \rangle$.

Доведення. Порядок елемента $a \in G$ (що для скінченної групи $\langle G, * \rangle$ є скінченним) за визначенням дорівнює порядку циклічної підгрупи $[a]$ і за теоремою Лагранжа є дільником порядку групи $\langle G, * \rangle$. □

3. Нехай $a \in G$. Тоді

$$a^{|G|} = e, \text{ де } e \text{ – нейтральний елемент групи } \langle G, * \rangle.$$

Доведення. За наслідком 2 існує $k \in \mathbb{N}$, таке, що $|G| = k \cdot |a|$. Тоді, використовуючи властивості степеня елемента і визначення порядку елемента, отримуємо

$$a^{|G|} = a^{k \cdot |a|} = (a^{|a|})^k = e^k = e. \qquad \square$$

4. Мала теорема Ферма.
Нехай $n \in \mathbb{Z}$. Тоді будь-яке просте число p є дільником числа $n^p - n$.

Доведення. Зафіксуємо просте число p і розглянемо мультиплікативну групу ${\mathbb{Z}_p}^*$. Нагадаємо, що

$${\mathbb{Z}_p}^* = \mathbb{Z}_p \setminus \{\overline{0}\} = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\},$$

звідки $|{\mathbb{Z}_p}^*| = p - 1$.

Доведення проведемо у два етапи.

1. Розглянемо випадок, коли число $n \in \mathbb{Z}$ не кратне p. Тоді $\overline{n} \in {\mathbb{Z}_p}^*$ і за визначенням операції в ${\mathbb{Z}_p}^*$ та наслідком 3 дістанемо

$$\overline{(n^{p-1})} = (\overline{n})^{p-1} = \overline{1}$$

(нагадаємо, що $\overline{1}$ – нейтральний у мультиплікативній групі ${\mathbb{Z}_p}^*$). Отже, числа n^{p-1} та 1 лежать в одному класі лишків за модулем p, тобто число $n^{p-1}-1$ кратне числу p.

2. У загальному випадку $n \in \mathbb{Z}$ зобразимо $n^p - n$ як добуток:

$$n^p - n = n \cdot (n^{p-1} - 1).$$

Якщо n не кратне p, то, за попереднім пунктом доведення, число p є дільником числа $n^{p-1}-1$. Отже, принаймні один з двох множників (n або $n^{p-1}-1$) ділиться на p, і число $n^p - n$ кратне p. □

Приклад 6.41. 1. Просте число 3 є дільником числа $4^3 - 4 = 60$.

2. Просте число 5 є дільником числа $(-6)^5 - (-6) = -7770$.

3. Число 6 не є простим, проте є дільником числа $3^6 - 3 = 726$.

4. Число 4 не є простим і не є дільником числа $6^4 - 6 = 1290$. Отже, вимога «простоти» числа p є необхідною у формулюванні малої теореми Ферма.

6.11. Нормальні дільники

У цьому підрозділі і далі розглядатимемо довільні (не обов'язково скінченні) групи.

Уже відомо з підрозд. 6.8, що підгрупа породжує два розбиття групи – на ліві та на праві суміжні класи, причому ці два розбиття можуть не збігатися (прикл. 6.38). У цьому підрозділі розглянемо підгрупи, для яких розбиття на праві та на ліві суміжні класи збігаються.

Означення 6.17. Підгрупу H групи $\langle G, * \rangle$ називають нормальним дільником (нормальною підгрупою), якщо

$$a * H = H * a \text{ для всіх } a \in G.$$

Для факту, що H є нормальним дільником групи $\langle G, * \rangle$, часто вживають позначення

$$H \lhd G.$$

Очевидно, що у комутативних групах будь-яка підгрупа є нормальним дільником. У некомутативних групах можуть міститися підгрупи, які не є нормальними дільниками, однак некомутативні групи також можуть містити нормальні підгрупи.

Приклад 6.42. 1. Тривіальні підгрупи будь-якої групи завжди є нормальними дільниками (див. прикл. 6.37).

2. В адитивній групі $\mathbb{Z}$, яка є комутативною, всі підгрупи $n\mathbb{Z}$ ($n \in \mathbb{N}$) нормальні.

3. У некомутативній симетричній групі S_3 підгрупа $\{\sigma_1, \varepsilon\}$ не є нормальною, однак $\{\varphi_1, \varphi_2, \varepsilon\}$ є нормальним дільником (див. прикл. 6.38).

Нижчеподана теорема – зручний критерій перевірки, чи є підгрупа нормальною.

Теорема 6.14 (критерій нормального дільника)**.** *Для того, щоб підгрупа H групи $\langle G, * \rangle$ була нормальною, необхідно і достатньо виконання умови*

$$\forall\, h \in H\, \forall\, g \in G\colon g^{-1} * h * g \in H. \tag{6.12}$$

Доведення. Необхідність. Нехай підгрупа H – нормальна. Тоді за визначенням нормальної підгрупи

$$\forall\, g \in G\colon g * H = H * g.$$

Отже, для довільних $g \in G$, $h \in H$ маємо

$$(h * g \in H * g) \Rightarrow (h * g \in g * H) \Rightarrow$$
$$\Rightarrow (\exists\, \widetilde{h} \in H\colon h * g = g * \widetilde{h}) \Rightarrow (g^{-1} * h * g = \widetilde{h} \in H).$$

Достатність. Нехай H – підгрупа групи $\langle G, * \rangle$, така, що

$$\forall\, h \in H\, \forall\, g \in G\colon g^{-1} * h * g \in H.$$

Зафіксуємо $g \in G$ і доведемо рівність $g * H = H * g$ модельним способом:

$$(x \in H * g) \Leftrightarrow (\exists\, h_1 \in H\colon x = h_1 * g) \Leftrightarrow (\exists\, h_1 \in H\colon x = (g * g^{-1}) * h_1 * g) \Leftrightarrow$$
$$\Leftrightarrow \left(\exists\, h_1 \in H\colon x = g * \underbrace{(g^{-1} * h_1 * g)}_{h_2 \in H}\right) \Leftrightarrow (\exists\, h_2 \in H\colon x = g * h_2 \in g * H).$$

Отже, теорему доведено. □

Приклад 6.43. 1. У групі GL_2 невироджених матриць розміром 2×2 розглянемо підгрупу невироджених нижніх трикутних матриць:

$$\mathcal{H} = \left\{ \begin{pmatrix} a_{1,1} & 0 \\ a_{2,1} & a_{2,2} \end{pmatrix} \colon \ a_{1,1}, a_{2,1}, a_{2,2} \in \mathbb{R}, \quad a_{1,1}a_{2,2} \neq 0 \right\}.$$

Ця підгрупа не є нормальною, оскільки можна вибрати нижню трикутну матрицю $A_0 \in \mathcal{H}$ та невироджену $A \in GL_2$, такі, що

$$A^{-1} \cdot A_0 \cdot A \notin \mathcal{H}.$$

Так, наприклад,

$$\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ -1 & -1 \end{pmatrix} \notin \mathcal{H}.$$

2. У групі GL_n розглянемо підгрупу SL_n матриць з одиничним визначником:

$$\mathcal{H} = SL_n = \{A \in GL_n \colon |A| = 1\}.$$

Ця підгрупа нормальна, оскільки для довільних $A_0 \in SL_n = \mathcal{H}$ та $A \in GL_n$, використовуючи формулу (6.6) (обчислення визначника добутку матриць), отримуємо

$$|A^{-1} \cdot A_0 \cdot A| = |A^{-1}| \cdot |A_0| \cdot |A| = |A|^{-1} \cdot |A_0| \cdot |A| = 1,$$

тобто $A^{-1} \cdot A_0 \cdot A \in SL_n = \mathcal{H}$ і, за теоремою 6.14, $SL_n \lhd GL_n$.

Зауваження 6.18. Співвідношення $|A^{-1}| = |A|^{-1}$ випливає з формули (6.6):

$$1 = |A \cdot A^{-1}| = |A| \cdot |A^{-1}|.$$

3. У симетричній групі S_n розглянемо підгрупу парних підстановок – знакозмінну групу A_n (див. прикл. 6.33). Зафіксувавши $\sigma \in S_n$, $\tau \in A_n$ і використовуючи результат вправи 6.9, отримуємо

$$\varkappa(\sigma^{-1} \circ \tau \circ \sigma) = \varkappa(\sigma^{-1}) \oplus \varkappa(\tau) \oplus \varkappa(\sigma) = \varkappa(\sigma) \oplus \varkappa(\tau) \oplus \varkappa(\sigma) = \varkappa(\tau) = 0$$

(нагадаємо, що $\varkappa(\varphi)$ позначає парність підстановки φ). Таким чином, $\sigma^{-1}\circ\tau\circ\sigma \in A_n$, а отже, підгруппа A_n є нормальним дільником у групі S_n: $A_n \lhd S_n$.

Зауваження 6.19. Застосовуючи теорему 6.14, слід обов'язково перевіряти, чи є множина H підгрупою групи $\langle G, * \rangle$ (як це і передбачено теоремою), оскільки умова (6.12) може виконуватись і для підмножини $H \subset G$, що не є підгрупою. Так, у комутативній групі $\langle G, * \rangle$ умова (6.12) виконується для будь-якої підмножини $H \subset G$.

6.12. Поняття фактор-групи

6.12.1. Суміжні класи за нормальною підгрупою

Нехай H – нормальна підгрупа групи $\langle G, * \rangle$. Для елемента $a \in G$ введемо позначення

$$\overline{a} = a * H = H * a.$$

Множину $\overline{a}$ називають *суміжним класом* групи $\langle G, * \rangle$ за нормальною підгрупою H, який породжений елементом a (у цьому підрозділі розглядаємо випадок нормальної підгрупи H, а отже, праві та ліві суміжні класи збігаються).

Через $G/_H$ позначимо множину суміжних класів групи $\langle G, * \rangle$ за H:

$$G/_H = \{\overline{a} \colon a \in G\}.$$

Як уже було зазначено (див. прикл. 6.38), деякі суміжні класи можуть збігатися. Зазвичай, у множині $G/_H$ однакові суміжні класи не розрізняють, тобто вважають одним елементом.

Вправа 6.18. Довести, що для довільних $a, b \in G$ має місце еквівалентність:

$$(a \in \overline{b}) \Leftrightarrow (b \in \overline{a}) \Leftrightarrow (\overline{a} = \overline{b}).$$

Для вивчення властивостей і практичного обчислення множини $G/_H$ знадобиться такий простий результат.

Лема 6.9. *Нехай $a, b \in G$. Тоді має місце еквівалентність*

$$(\overline{a} = \overline{b}) \Leftrightarrow (a * b^{-1} \in H).$$

Доведення. 1. Нехай $\overline{a} = \overline{b}$. Тоді $a \in \overline{b}$ (оскільки $a \in \overline{a}$), а отже, $a = h*b$ для деякого $h \in H$. Отже, отримуємо $a * b^{-1} = h \in H$.

2. Нехай $a * b^{-1} \in H$. Тоді $a * b^{-1} = h \in H$, а отже, $a = h * b \in \overline{b}$. Отже, суміжні класи $\overline{a}$ та $\overline{b}$ містять принаймні один спільний елемент a і за теоремою 6.12 мають збігатися, тобто $\overline{a} = \overline{b}$. □

Вправа 6.19. Для довільних $a, b \in G$ довести еквівалентність

$$(\overline{a} = \overline{b}) \Leftrightarrow (b^{-1} * a \in H).$$

Оскільки множина $G/_H$ задає розбиття множини G в об'єднання множин (суміжних класів), що попарно не перерізаються, на G можна ввести відношення еквівалентності

$$(a \sim b) \Leftrightarrow (\overline{a} = \overline{b}),$$

причому (див. результат вправи 3.14) множина $G/_H$ збігається з фактор-множиною G за відношенням еквівалентності «$\sim$»:

$$G/_H = G/_\sim.$$

Завдяки лемі 6.9 (разом з результатом вправи 6.19) маємо зручну форму для введеного відношення еквівалентності:

$$(a \sim b) \Leftrightarrow (\overline{a} = \overline{b}) \Leftrightarrow (a * b^{-1} \in H) \Leftrightarrow (b^{-1} * a \in H).$$

Отже, множину $G/_H$ можна обчислювати як фактор-множину $G/_\sim$, застосовуючи відповідні методи (див. підрозд. 3.6).

Приклад 6.44. Обчислимо множину $GL_n/_{SL_n}$. Для довільних матриць $A, B \in GL_n$ маємо

$$(\overline{A} = \overline{B}) \Leftrightarrow (A \sim B) \Leftrightarrow ((A \cdot B^{-1}) \in SL_n) \Leftrightarrow (|A \cdot B^{-1}| = 1) \Leftrightarrow (|A| = |B|).$$

Отже, суміжний клас, породжений матрицею $A \in GL_n$ з визначником $|A| = \alpha$, містить ті і тільки ті матриці, визначник яких дорівнює α:

$$\overline{A} = \{X \in GL_n \colon |X| = |A|\} = \{X \in GL_n \colon |X| = \alpha\}.$$

Отже, кожен клас еквівалентності (він же суміжний клас) містить матриці з фіксованим значенням визначника. Ураховуючи, що для будь-якого $\alpha \neq 0$ існує принаймні одна матриця $A \in GL_n$ з визначником $|A| = \alpha$, можемо виписати загальний вигляд суміжних класів GL_n за SL_n:

$$\mathcal{A}_\alpha = \{X \in GL_n \colon |X| = \alpha\}, \quad \alpha \neq 0.$$

Тепер можна виписати множину $GL_n \big/ _{SL_n}$:

$$GL_n \big/ _{SL_n} = \{\mathcal{A}_\alpha \colon \alpha \neq 0\}.$$

Ще раз наголосимо, що кожна множина $\mathcal{A}_\alpha$ ($\alpha > 0$) є суміжним класом, й інших суміжних класів немає.

Приклад 6.45. Обчислимо множину $S_n \big/ _{A_n}$ (обмежимось нетривіальним випадком $n \geq 2$). Для довільних підстановок $\sigma_1, \sigma_2 \in S_n$ маємо

$$(\overline{\sigma}_1 = \overline{\sigma}_2) \Leftrightarrow (\sigma_1 \sim \sigma_2) \Leftrightarrow ((\sigma_1 \circ \sigma_2^{-1}) \in A_n) \Leftrightarrow$$
$$\Leftrightarrow (\varkappa(\sigma_1 \circ \sigma_2^{-1}) = 0) \Leftrightarrow (\varkappa(\sigma_1) = \varkappa(\sigma_2)).$$

Отже, суміжний клас, породжений підстановкою $\sigma \in S_n$, містить ті і тільки ті підстановки, парність яких збігається з парністю σ:

$$\overline{\sigma} = \{\tau \in S_n \colon \varkappa(\tau) = \varkappa(\sigma)\} = \begin{cases} A_n, \text{ якщо } \sigma \text{ парна}, \\ S_n \setminus A_n, \text{ якщо } \sigma \text{ непарна}. \end{cases}$$

Ураховуючи, що при $n \geq 2$ група S_n містить принаймні одну парну і принаймні одну непарну підстановку, отримуємо два суміжні класи – множину парних підстановок A_n та множину непарних підстановок $S_n \setminus A_n$:

$$S_n \big/ _{A_n} = \{A_n,\ S_n \setminus A_n\}.$$

Як наслідок, доведено факт, який інтуїтивно очевидний: при $n \geq 2$ кількість парних підстановок у S_n дорівнює кількості непарних, оскільки за лемою 6.8 $\operatorname{card}(A_n) = \operatorname{card}(S_n \setminus A_n)$.

Приклад 6.46. Обчислимо множину $\mathbb{Z} \big/ _{n\mathbb{Z}}$ ($n \in \mathbb{N}$). Для довільних $k_1, k_2 \in \mathbb{Z}$ маємо

$$(\overline{k}_1 = \overline{k}_2) \Leftrightarrow (k_1 \sim k_2) \Leftrightarrow ((k_1 + (k_2)^{-1,+}) \in n\mathbb{Z}) \Leftrightarrow$$
$$\Leftrightarrow ((k_1 - k_2) \in n\mathbb{Z}) \Leftrightarrow ((k_1 \bmod n) = (k_2 \bmod n)).$$

Отже, в одному суміжному класі містяться числа, що дають однакову остачу від ділення на n. Легко зрозуміти, що маємо n різних суміжних класів:

$$\mathbb{Z}/_{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \ldots, \overline{k}, \ldots, \overline{n-1}\}, \text{ де } \overline{k} = \{km \colon m \in \mathbb{Z}\}.$$

Отже, множина суміжних класів $\mathbb{Z}/_{n\mathbb{Z}}$ збіглася з відомою нам фактор-множиною $\mathbb{Z}_n = \mathbb{Z}/_{(\bmod n)}$.

6.12.2. Визначення фактор-групи

Нехай H – нормальна підгрупа групи $\langle G, * \rangle$.

На множину суміжних класів $G/_H$ перенесемо бінарну операцію «$*$», визначену на множині G:

$$\overline{a} * \overline{b} = \overline{a * b}, \text{ для } a, b \in G. \tag{6.13}$$

Отже, співвідношення (6.13) визначає $\overline{a} * \overline{b}$ для будь-якої пари суміжних класів $\overline{a}, \overline{b} \in G/_H$, оскільки для обчислення $\overline{a} * \overline{b}$ достатньо:

- вибрати довільних представників $a \in \overline{a}$ та $b \in \overline{b}$;
- обчислити $a * b$;
- використовуючи співвідношення (6.13), отримати: $\overline{a} * \overline{b} = \overline{a * b}$.

Однак потрібно довести коректність визначеної операції, тобто незалежність результату $\overline{a} * \overline{b}$ від вибору представників $a \in \overline{a}$, $b \in \overline{b}$.

Лема 6.10 (коректність операції «$*$» на $G/_H$). *Нехай* $\overline{a_1} = \overline{a}$, $\overline{b_1} = \overline{b}$, *де* $a, a_1, b, b_1 \in G$. *Тоді*

$$\overline{a_1 * b_1} = \overline{a * b}.$$

Доведення. За лемою 6.9 для доведення достатньо перевірити виконання умови $(a_1 * b_1) * (a * b)^{-1} \in H$:

$$(a_1 * b_1) * (a * b)^{-1} = a_1 * b_1 * b^{-1} * a^{-1} = a_1 * h_1 * a^{-1}, \text{ де } h_1 = b_1 * b^{-1} \in H;$$

$$a_1 * h_1 \in a_1 * H = \overline{a_1} = H * a_1 \ni h_2 * a_1 \text{ для деякого } h_2 \in H;$$

$$(a_1 * b_1) * (a * b)^{-1} = h_2 * a_1 * a^{-1} = h_2 * h_3 \in H, \text{ де } h_3 = a_1 * a^{-1} \in H.$$

Лему повністю доведено. □

Отже, операція «$*$» на множині $G/_H$ визначена коректно, і маємо замкнену алгебричну структуру $\langle G/_H, * \rangle$.

Теорема 6.15. *Алгебрична структура $\langle G/_H, * \rangle$ є групою.*

Доведення. Для перевірки твердження теореми необхідно довести асоціативність структури $\langle G/_H, * \rangle$, наявність нейтрального елемента та наявність оберненого $(\overline{a})^{-1}$ для кожного $(\overline{a}) \in G/_H$.

Асоціативність операції «$*$» на множині $G/_H$ випливає з асоціативності «$*$» на множині G та визначення «$*$» на $G/_H$ (співвідношення (6.13)):

$$\overline{a} * (\overline{b} * \overline{c}) = \overline{a} * (\overline{b * c}) = \overline{a * (b * c)} =$$
$$= \overline{(a * b) * c} = \overline{(a * b)} * \overline{c} = (\overline{a} * \overline{b}) * \overline{c}.$$

Нехай $e \in G$ – нейтральний елемент групи $\langle G, * \rangle$. Тоді елемент $\overline{e} = H$ є нейтральним у структурі $\langle G/_H, * \rangle$:

$$\overline{x} * \overline{e} = \overline{x * e} = \overline{x} \text{ для довільного } x \in G.$$

Для кожного $(\overline{a}) \in G/_H$ $(a \in G)$ у структурі $\langle G/_H, * \rangle$ існує обернений $(\overline{a})^{-1} = \overline{a^{-1}}$:

$$\overline{a^{-1}} * \overline{a} = \overline{a^{-1} * a} = \overline{e} = H; \quad \overline{a} * \overline{a^{-1}} = \overline{a * a^{-1}} = \overline{e} = H. \qquad \square$$

Групу $\langle G/_H, * \rangle$ називають *фактор-групою* групи G за нормальною підгрупою H. У процесі доведення теореми 6.15 було показано, що нейтральним елементом фактор-групи є нормальний дільник H, за яким проводять факторизацію.

Для практичного знаходження фактор-групи $\langle G/_H, * \rangle$ необхідно:

- знайти явний вигляд множини $G/_H$ (у багатьох випадках для цього зручно застосовувати методи, використані у прикл. 6.44 – 6.46);
- зафіксувавши будь-яких представників у суміжних класах $\overline{a}$ та $\overline{b}$, визначити вигляд суміжного класу $\overline{a} * \overline{b} = \overline{a * b}$ (ураховуючи довільність вибору представників $a \in \overline{a}$, $b \in \overline{b}$, їх вибирають так, щоб максимально спростити обчислення $a * b$ та $\overline{a * b}$);

- зафіксувавши будь-якого представника в суміжному класі $\overline{a}$, визначити вигляд оберненого суміжного класу $(\overline{a})^{-1} = \overline{a^{-1}}$ (нагадаємо, що нейтральним елементом фактор-групи є нормальний дільник H, за яким проводять факторизацію).

Приклад 6.47. Обчислимо фактор-групу $GL_n/_{SL_n}$. Фактор-множину $GL_n/_{SL_n}$ було знайдено в прикл. 6.44:

$$GL_n/_{SL_n} = \{\mathcal{A}_\alpha : \alpha \neq 0\},$$

де $\mathcal{A}_\alpha = \{X \in GL_n : |X| = \alpha\}$, $\alpha \neq 0$.

У суміжних класах $\mathcal{A}_{\alpha_1}$ та $\mathcal{A}_{\alpha_2}$ $(\alpha_1, \alpha_2 \neq 0)$ виберемо таких представників:

$$\begin{pmatrix} \alpha_1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \in \mathcal{A}_{\alpha_1}, \qquad \begin{pmatrix} \alpha_2 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \in \mathcal{A}_{\alpha_2}.$$

Для вибраних представників неважко обчислити $\mathcal{A}_{\alpha_1} * \mathcal{A}_{\alpha_2}$:

$$\begin{pmatrix} \alpha_1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \cdot \begin{pmatrix} \alpha_2 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} = \begin{pmatrix} \alpha_1 \cdot \alpha_2 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

$$\mathcal{A}_{\alpha_1} * \mathcal{A}_{\alpha_2} = \{X \in GL_n : |X| = \alpha_1 \cdot \alpha_2\} = \mathcal{A}_{\alpha_1 \cdot \alpha_2}.$$

Нейтральним елементом у фактор-групі $GL_n/_{SL_n}$, як і в загальному випадку, є нормальний дільник SL_n. Зазначимо, що в цьому контексті SL_n зручно розглядати як суміжний клас, породжений одиничною матрицею I – нейтральним елементом групи GL_n.

Нарешті, для суміжного класу $\mathcal{A}_\alpha$ обчислимо обернений. Вибравши представника

$$\begin{pmatrix} \alpha & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \in \mathcal{A}_\alpha,$$

отримуємо

$$(\mathcal{A}_\alpha)^{-1} = \overline{\begin{pmatrix} \alpha & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}^{-1}} = \overline{\begin{pmatrix} \alpha^{-1} & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}} = \mathcal{A}_{\alpha^{-1}}.$$

Отже, для фактор-групи $GL_n/_{SL_n}$ бінарна операція «$\cdot$» та обернений елемент визначають такі співвідношення:

$$\mathcal{A}_{\alpha_1} \cdot \mathcal{A}_{\alpha_2} = \mathcal{A}_{\alpha_1 \cdot \alpha_2}; \tag{6.14}$$

$$(\mathcal{A}_\alpha)^{-1} = \mathcal{A}_{\alpha^{-1}}. \tag{6.15}$$

Нагадаємо, що нейтральним елементом у фактор-групі $GL_n/_{SL_n}$, як і в загальному випадку, є нормальний дільник SL_n.

Співвідношення (6.14) визначає ізоморфність фактор-групи $GL_n/_{SL_n}$ та мультиплікативної групи дійсних чисел $\mathbb{R}^*$ з ізоморфізмом

$$f : GL_n/_{SL_n} \to \mathbb{R}^*, \quad f(\mathcal{A}_\alpha) = \alpha.$$

Зауваження 6.20. Ізоморфність $GL_n/_{SL_n} \sim \mathbb{R}^*$ також випливає з основної теореми про гомоморфізми груп (підрозд. 6.14).

Зауваження 6.21. Для отримання співвідношень (6.14), (6.15) у суміжних класах було обрано представників спеціального вигляду (діагональні матриці). Проте ці співвідношення можна було б отримати, обираючи довільних представників і далі використовуючи формулу (6.6) для визначника добутку матриць.

Приклад 6.48. Обчислимо фактор-групу $S_n/_{A_n}$. Множину $S_n/_{A_n}$ було знайдено в прикл. 6.45:

$$S_n/_{A_n} = \{\mathcal{A}_0,\ \mathcal{A}_1\},$$

де $\mathcal{A}_0 = A_n$, $\mathcal{A}_1 = S_n \setminus A_n$.

Вибравши довільних представників $\sigma_0 \in \mathcal{A}_0$, $\sigma_1 \in \mathcal{A}_1$, тобто вибравши в S_n деяку парну підстановку σ_0 та непарну σ_1 (це можна зробити для будь-якого $n \geq 2$), отримуємо:

$$\sigma_1 \circ \sigma_1 \in \mathcal{A}_0, \quad \sigma_0 \circ \sigma_0 \in \mathcal{A}_0, \quad \sigma_0 \circ \sigma_1 \in \mathcal{A}_1, \quad \sigma_1 \circ \sigma_0 \in \mathcal{A}_1.$$

Отже, можемо побудувати таблицю Келі для операції у фактор-групі $S_n/_{A_n}$ (табл. 6.6).

Ця таблиця визначає ізоморфність фактор-групи $S_n/_{A_n}$ та адитивної групи $\mathbb{Z}_2$ з ізоморфізмом

$$f\colon S_n/_{A_n} \to \mathbb{Z}_2, \quad f(\mathcal{A}_0) = \overline{0}, \quad f(\mathcal{A}_1) = \overline{1}$$

(для доведення достатньо порівняти табл. 6.6 та 6.3).

Зауваження 6.22. Ізоморфність $S_n/_{A_n} \sim \mathbb{Z}_2$ також можна довести, користуючись основною теоремою про гомоморфізми груп (підрозд. 6.14).

Таблиця 6.6. **Таблиця Келі для фактор-групи $S_n/_{A_n}$**

$\circ$	$\mathcal{A}_0$	$\mathcal{A}_1$
$\mathcal{A}_0$	$\mathcal{A}_0$	$\mathcal{A}_1$
$\mathcal{A}_1$	$\mathcal{A}_1$	$\mathcal{A}_0$

Приклад 6.49. Обчислимо фактор-групу $\mathbb{Z}/_{n\mathbb{Z}}$ ($n \in \mathbb{N}$). Множину $\mathbb{Z}/_{n\mathbb{Z}}$ було знайдено в прикл. 6.46:

$$\mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{k}, \ldots, \overline{n-1}\}, \text{ де } \overline{k} = \{km\colon m \in \mathbb{Z}\}.$$

Операція у фактор-групі $\mathbb{Z}/_{n\mathbb{Z}}$ визначається співвідношенням (6.13), яке для даного випадку має вигляд

$$\overline{a} + \overline{b} = \overline{a + b}.$$

Отже, фактор-група $\mathbb{Z}/_{n\mathbb{Z}}$ збігається з адитивною групою класів лишків $\mathbb{Z}_n$ (підрозд. 6.4.2):

$$\mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}_n.$$

6.13. Гомоморфізми груп: теореми про ядро та образ гомоморфізму

Продовжимо вивчення гомоморфних відображень груп, розпочате в підрозд. 6.6.

Отже, у цьому підрозділі працюватимемо з групами $\langle G_1, * \rangle$ (нейтральний елемент e_1) та $\langle G_2, \circledast \rangle$ (нейтральний елемент e_2), між якими встановлено гомоморфізм $f\colon G_1 \to G_2$.

Означення 6.18. Ядром гомоморфізму $f\colon G_1 \to G_2$ називають множину $\mathrm{Ker}_f \subset G_1$, що містить ті і тільки ті $x \in G_1$, для яких $f(x) = e_2$:

$$\mathrm{Ker}_f = \{x \in G_1 \colon f(x) = e_2\}.$$

Нагадування. Образом гомоморфізму (як і будь-якого іншого відображення) $f\colon G_1 \to G_2$ називають множину $\mathrm{Im}_f \subset G_2$, що складається з елементів $f(x)$ $(x \in G_1)$:

$$\mathrm{Im}_f = \{f(x) \colon x \in G_1\}.$$

Зазначимо, що ядро гомоморфізму завжди містить принаймні один елемент – e_1 (нейтральний елемент групи G_1), оскільки, за теоремою 6.8, $f(e_1) = e_2$. Ядро Ker_f, що містить лише один елемент ($\mathrm{Ker}_f = \{e_1\}$), називають *тривіальним*.

Приклад 6.50. 1. Розглянемо відображення

$$f\colon \mathbb{R} \to \mathbb{R}^*, \quad f(a) = 2^a.$$

Це відображення є гомоморфізмом з групи $\langle \mathbb{R}, + \rangle$ (нейтральний $e_1 = 0$) в групу $\langle \mathbb{R}^*, \cdot \rangle$ (нейтральний $e_2 = 1$). Обчислимо його ядро та образ:

$$\mathrm{Ker}_f = \{x \in \mathbb{R} \colon 2^x = 1\} = \{0\};$$
$$\mathrm{Im}_f = \{2^x \colon x \in \mathbb{R}\} = (0, +\infty).$$

Отже, ядро Ker_f тривіальне.

2. Розглянемо відображення

$$f\colon \mathbb{R} \to \{z \in \mathbb{C} \colon |z| = 1\}, \quad f(x) = e^{ix}$$

(тут $e \approx 2{,}718$ позначає основу натурального логарифма). Це відображення є гомоморфізмом з групи $\langle \mathbb{R}, + \rangle$ (нейтральний $e_1 = 0$) у групу $\langle \{z \in \mathbb{C} \colon |z| = 1\}, \cdot \rangle$ (нейтральний $e_2 = 1$). Обчислимо його ядро та образ:

$$\mathrm{Ker}_f = \{x \in \mathbb{R} \colon e^{ix} = 1\} = \{x = 2\pi k \colon k \in \mathbb{Z}\};$$
$$\mathrm{Im}_f = \{e^{ix} \colon x \in \mathbb{R}\} = \{z \in \mathbb{C} \colon |z| = 1\}.$$

Отже, ядро Ker_f не є тривіальним.

З ядром та образом пов'язано багато цікавих властивостей гомоморфізмів груп. Розглянемо деякі з них.

Теорема 6.16. *Гомоморфізм $f : G_1 \to G_2$ є мономорфізмом тоді і тільки тоді, коли ядро* Ker_f *тривіальне.*

Доведення. 1. Нехай f – мономорфізм. Тоді тривіальність ядра відразу випливає з визначення ін'єктивності:

$$(x \in \mathrm{Ker}_f) \Rightarrow (f(x) = e_2) \Rightarrow (x = e_1),$$

оскільки $f(e_1) = e_2$.

2. Нехай Ker_f – тривіальне. Зафіксувавши довільні $x_1, x_2 \in G_1$ і припустивши, що $f(x_1) = f(x_2)$, отримуємо

$$\begin{gathered}(f(x_1) = f(x_2)) \Rightarrow (f(x_1) \circledast (f(x_2))^{-1} = e_2) \Rightarrow \\ \Rightarrow (f(x_1 * x_2^{-1}) = e_2) \Rightarrow (x_1 * x_2^{-1} \in \mathrm{Ker}_f).\end{gathered}$$

Отже, $x_1 * x_2^{-1} \in \mathrm{Ker}_f$. Але ядро Ker_f – тривіальне, тобто $\mathrm{Ker}_f = \{e_1\}$, звідки отримуємо

$$(x_1 * x_2^{-1} = e_1) \Rightarrow (x_1 = x_2).$$

Отже, для $x_1, x_2 \in G_1$ має місце логічний наслідок

$$(f(x_1) = f(x_2)) \Rightarrow (x_1 = x_2),$$

що визначає ін'єктивність відображення f. □

Приклад 6.51. Розглянемо гомоморфізми з прикл. 6.50.

1. Відображення

$$f\colon \mathbb{R} \to \mathbb{R}^*, \quad f(a) = 2^a$$

є гомоморфізмом з групи $\langle \mathbb{R}, + \rangle$ у групу $\langle \mathbb{R}^*, \cdot \rangle$. Ядро цього гомоморфізму $\mathrm{Ker}_f = \{0\}$ тривіальне, і гомоморфізм f є мономорфізмом.

2. Відображення

$$f\colon \mathbb{R} \to \{z \in \mathbb{C}\colon |z| = 1\}, \quad f(x) = e^{ix}$$

є гомоморфізмом з групи $\langle \mathbb{R}, + \rangle$ у групу $\langle \{z \in \mathbb{C}\colon |z| = 1\}, \cdot \rangle$. Його ядро $\mathrm{Ker}_f = \{x = 2\pi k : k \in \mathbb{Z}\}$ не є тривіальним, і гомоморфізм f не є мономорфізмом.

Теорема 6.17. *Нехай $f : G_1 \to G_2$ – гомоморфізм між групами $\langle G_1, * \rangle$ та $\langle G_2, \circledast \rangle$. Тоді:*

1) ядро Ker_f є нормальним дільником у G_1;
2) образ Im_f є підгрупою у G_2.

Доведення. 1. Розглянемо ядро $\mathrm{Ker}_f \subset G_1$. Спочатку доведемо, що Ker_f є підгрупою групи $\langle G_1, * \rangle$:

1) множина Ker_f непорожня, оскільки $\mathrm{Ker}_f \ni e_1$;

2) для довільних $x, y \in \mathrm{Ker}_f$ отримуємо

$$f(x * y^{-1}) = f(x) \circledast f(y)^{-1} = e_2 \circledast e_2^{-1} = e_2,$$

тобто $x * y^{-1} \in \mathrm{Ker}_f$.

Отже, виконуються умови теореми 6.7 з урахуванням наслідку, тобто Ker_f є підгрупою групи $\langle G_1, * \rangle$.

Доведемо, що Ker_f є нормальною підгрупою групи $\langle G_1, * \rangle$. Зафіксувавши довільні $x \in G_1$, $a \in \mathrm{Ker}_f$, отримуємо

$$f(x^{-1} * a * x) = (f(x))^{-1} \circledast f(a) \circledast f(x) = (f(x))^{-1} \circledast e_2 \circledast f(x) = e_2,$$

тобто $x^{-1} * a * x \in \mathrm{Ker}_f$. Отже, для підгрупи $\mathrm{Ker}_f \subset G_1$ виконується умова (6.12) теореми 6.14, тобто Ker_f є нормальним дільником групи $\langle G_1, * \rangle$.

2. Розглянемо образ $\mathrm{Im}_f \subset G_2$ відображення $f \colon G_1 \to G_2$. Перевіримо виконання умов теореми 6.7 (ураховуючи її наслідок):

1) множина Im_f непорожня, оскільки $\mathrm{Im}_f \ni e_2 = f(e_1)$;

2) зафіксуємо довільні $y_1, y_2 \in \mathrm{Im}_f$. Ураховуючи визначення образу відображення вважатимемо, що $y_1 = f(x_1), y_2 = f(x_2)$, де $x_1, x_2 \in G_1$. Перевіримо виконання умови (6.9):

$$y_1 \circledast y_2^{-1} = f(x_1) \circledast (f(x_2))^{-1} = f(x_1 * x_2^{-1}) \in \mathrm{Im}_f\,.$$

Отже, виконуються умови теореми 6.7 з урахуванням наслідку, тобто Im_f є підгрупою групи $\langle G_2, \circledast \rangle$. □

Приклад 6.52. Розглянемо групи $\langle \mathbb{R}, + \rangle$ та $\langle \mathbb{C}^*, \cdot \rangle$, де $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Відображення

$$f \colon \mathbb{R} \to \mathbb{C}^*, \quad f(x) = e^{ix}$$

встановлює гомоморфізм між даними групами. Випишемо ядро та образ відображення f:

$$\mathrm{Ker}_f = \{x \in \mathbb{R} \colon e^{ix} = 1\} = \{x = 2\pi k \colon k \in \mathbb{Z}\};$$
$$\mathrm{Im}_f = \{e^{ix} \colon x \in \mathbb{R}\} = \{z \in \mathbb{C} \colon |z| = 1\}.$$

Легко перевірити, що ядро $\mathrm{Ker}_f = \{x = 2\pi k : k \in \mathbb{Z}\}$ дійсно є нормальною підгрупою в $\langle \mathbb{R}, + \rangle$, образ $\mathrm{Im}_f = \{z \in \mathbb{C} \colon |z| = 1\}$ є підгрупою групи $\langle \mathbb{C}^*, \cdot \rangle$.

Приклад 6.53. Розглянемо гомоморфізм між мультиплікативними групами GL_n та $\mathbb{R}^*$:

$$f \colon GL_n \to \mathbb{R}^*, \quad f(A) = |A|.$$

Обчислимо ядро та образ відображення f:

$$\mathrm{Ker}_f = \{A \in GL_n \colon |A| = 1\} = SL_n;$$
$$\mathrm{Im}_f = \{|A| \colon A \in GL_n\} = \mathbb{R}^*.$$

Отже, ядро $\mathrm{Ker}_f = SL_n$ дійсно є нормальною підгрупою групи GL_n, образ Im_f є тривіальною підгрупою групи $\mathbb{R}^*$.

У прикл. 6.52 та 6.53 образ гомоморфізму $f \colon G_1 \to G_2$ виявився нормальною підгрупою в $\langle G_2, \circledast \rangle$. Проте в загальному випадку образ Im_f – підгрупа $\langle G_2, \circledast \rangle$ і, як показує наступний приклад, може не бути нормальним дільником.

Приклад 6.54. Розглянемо мультиплікативну групу G невироджених нижніх трикутних матриць розміром 2×2:

$$G = \left\{ \begin{pmatrix} a_1 & 0 \\ b & a_2 \end{pmatrix} \colon \ a_1 a_2 \neq 0 \right\}.$$

Розглянемо відображення

$$f \colon G \to G, \qquad f \colon \begin{pmatrix} a_1 & 0 \\ b & a_2 \end{pmatrix} \mapsto \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}.$$

Відображення f є гомоморфізмом із групи $\langle G, \cdot\rangle$ у ту саму групу $\langle G, \cdot\rangle$:

$$\begin{pmatrix} a_1 & 0 \\ b & a_2 \end{pmatrix} \cdot \begin{pmatrix} c_1 & 0 \\ d & c_2 \end{pmatrix} = \begin{pmatrix} a_1c_1 & 0 \\ bc_1 + da_2 & a_2c_2 \end{pmatrix};$$
$$f : \begin{pmatrix} a_1c_1 & 0 \\ bc_1 + da_2 & a_2c_2 \end{pmatrix} \mapsto \begin{pmatrix} a_1c_1 & 0 \\ 0 & a_2c_2 \end{pmatrix} = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} \cdot \begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix}.$$

Образом установленого гомоморфізму, очевидно, є множина невироджених діагональних матриць розміром 2×2:

$$\mathrm{Im}_f = \left\{ \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} : \ a_1a_2 \neq 0 \right\}.$$

Легко перевірити, користуючись теоремою 6.14, що Im_f не є нормальним дільником (хоч і є підгрупою) в $\langle G, \cdot\rangle$:

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in G, \qquad \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \in \mathrm{Im}_f,$$
$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \notin \mathrm{Im}_f\,.$$

Вправа 6.20. Користуючись теоремою 6.14, перевірити, що ядро

$$\mathrm{Ker}_f = \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} : b \in \mathbb{R} \right\}$$

дійсно є нормальним дільником в $\langle G, \cdot\rangle$, але не є нормальним дільником (хоч і є підгрупою) в GL_2.

Наступний приклад дуже важливий, оскільки, у певному розумінні, дає повний опис усіх нормальних дільників даної групи.

Приклад 6.55. Нехай $\langle G, *\rangle$ – довільна група з нейтральним елементом $e \in G$, $H \lhd G$. Розглянемо відображення

$$\varrho : G \to G/_H, \quad \varrho(a) = \overline{a}.$$

Легко перевірити, що ρ є гомоморфізмом з групи $\langle G, * \rangle$ у фактор-групу $G/_H$. Дійсно, за визначенням операції на фактор-групі (співвідношення (6.13)), отримуємо

$$\rho(x * y) = \overline{x * y} = \overline{x} * \overline{y} = \rho(x) * \rho(y).$$

Визначений гомоморфізм ρ називають *природним*, або *канонічним*. Обчислимо ядро та образ природного гомоморфізму ρ:

$$\mathrm{Ker}_\rho = \{x \in G \colon \rho(x) = \overline{e} = H\} = \{x \in G \colon \overline{x} = \overline{e}\} = \{x \in G \colon x \in H\} = H;$$
$$\mathrm{Im}_\rho = \{\rho(x) \colon x \in G\} = \{\overline{x} \colon x \in G\} = G/_H.$$

Отже, ядро Ker_ρ збігається з нормальним дільником H. Таким чином, будь-який нормальний дільник H групи $\langle G, * \rangle$ є ядром деякого гомоморфізму (принаймні, з ядром відповідного природного гомоморфізму ρ), визначеного на $\langle G, * \rangle$.

Зазначимо, що образ Im_ρ відображення $\rho : G \to G/_H$ збігається з фактор-групою $G/_H$, тобто природний гомоморфізм є епіморфізмом.

6.14. Теорема про гомоморфізми груп

У цьому підрозділі розглянемо важливу теорему, яка встановлює зв'язок між гомоморфізмами груп, нормальними дільниками і фактор-групами.

Нехай $f \colon G_1 \to G_2$ – гомоморфізм між групами $\langle G_1, * \rangle$ (нейтральний елемент e_1) та $\langle G_2, \circledast \rangle$ (нейтральний елемент e_2). Нагадаємо:

- ядро Ker_f гомоморфізму f є нормальним дільником у групі $\langle G_1, * \rangle$, а отже, можна розглядати фактор-групу $G_1/_{\mathrm{Ker}_f}$;
- образ Im_f гомоморфізму f є підгрупою групи $\langle G_2, \circledast \rangle$, а отже, можна розглядати Im_f як групу $\langle \mathrm{Im}_f, \circledast \rangle$.

Теорема 6.18 (основна теорема про гомоморфізми груп)**.**
1. Фактор-група $G_1/_{\mathrm{Ker}_f}$ *за ядром* Ker_f *ізоморфна образу* Im_f*:*

$$G_1/_{\mathrm{Ker}_f} \sim \mathrm{Im}_f;$$

2. Існує такий ізоморфізм $\varphi\colon G_1/_{\mathrm{Ker}_f} \to \mathrm{Im}_f$, *що*

$$\varphi \circ \rho = f, \tag{6.16}$$

де $\rho\colon G_1 \to G_1/_{\mathrm{Ker}_f}$ *– природний гомоморфізм* $(\forall\, x \in G_1\colon \rho(x) = \overline{x})$.

Доведення. Задамо відображення $\varphi\colon G_1/_{\mathrm{Ker}_f} \to \mathrm{Im}_f$ таким співвідношенням:

$$\varphi(\overline{x}) = f(x), \quad x \in G_1. \tag{6.17}$$

Доведемо, що відображення $\varphi\colon G_1/_{\mathrm{Ker}_f} \to \mathrm{Im}_f$ визначено коректно і встановлює шуканий ізоморфізм між групами $G_1/_{\mathrm{Ker}_f}$ та Im_f.

1. Визначення відображення $\varphi\colon G_1/_{\mathrm{Ker}_f} \to \mathrm{Im}_f$ через співвідношення (6.17) потребує обґрунтування коректності, тобто незалежності значення $\varphi(\overline{x}) = f(x)$ від вибору представника $x \in \overline{x}$.

Нехай $\overline{x_1} = \overline{x_2}$ $(x_1, x_2 \in G_1)$, тобто елементи x_1 та x_2 належать одному суміжному класу. Ураховуючи, що нормальним дільником є Ker_f, отримуємо

$$f(x_1) \circledast (f(x_2))^{-1} = f(x_1 * x_2^{-1}) = e_2,$$

оскільки, за лемою 6.9, $x_1 * x_2^{-1} \in \mathrm{Ker}_f$.

Отже, $f(x_1) \circledast (f(x_2))^{-1} = e_2$, звідки одразу випливає рівність $f(x_1) = f(x_2)$.

Таким чином,

$$f(x_1) = f(x_2) \text{ при } \overline{x_1} = \overline{x_2}, \quad x_1, x_2 \in G_1,$$

тобто відображення $\varphi\colon G_1/_{\mathrm{Ker}_f} \to \mathrm{Im}_f$ коректно визначається співвідношенням (6.17).

2. Доведемо, що відображення $\varphi : G_1/_{\mathrm{Ker}_f} \to \mathrm{Im}_f$ є гомоморфізмом між групами $G_1/_{\mathrm{Ker}_f}$ та Im_f (нагадаємо, що Im_f розглядається як підгрупа групи $\langle G_2, \circledast\rangle$, тобто як група $\langle \mathrm{Im}_f, \circledast\rangle$).

Для довільних $\overline{x_1}, \overline{x_2} \in G_1/_{\mathrm{Ker}_f}$ $(x_1, x_2 \in G_1)$ отримуємо

$$\varphi(\overline{x_1} * \overline{x_2}) = \varphi(\overline{x_1 * x_2}) = f(x_1 * x_2) = f(x_1) \circledast f(x_2) = \varphi(\overline{x_1}) \circledast \varphi(\overline{x_2}).$$

Отже,

$$\varphi(\overline{x_1} * \overline{x_2}) = \varphi(\overline{x_1}) \circledast \varphi(\overline{x_2}),$$

тобто відображення $\varphi : G_1/_{\mathrm{Ker}_f} \to \mathrm{Im}_f$ є гомоморфізмом між групами $G_1/_{\mathrm{Ker}_f}$ та Im_f.

3. Доведемо, що гомоморфізм $\varphi\colon G_1/_{\mathrm{Ker}_f} \to \mathrm{Im}_f$ є мономорфізмом.

Нехай $\overline{x} \in \mathrm{Ker}_\varphi$, тобто $x \in G_1$, $\varphi(\overline{x}) = f(x) = e_2$.

Ураховуючи, що факторизуємо G_1 за ядром Ker_f і нейтральним елементом у фактор-групі $G_1/_{\mathrm{Ker}_f}$ є нормальний дільник $\mathrm{Ker}_f = \overline{e_1}$, отримуємо

$$(f(x) = e_2) \Rightarrow (x \in \mathrm{Ker}_f) \Rightarrow (\overline{x} = \overline{e_1} = \mathrm{Ker}_f).$$

Отже, єдиним елементом $\overline{x}$, що належить ядру Ker_φ, є суміжний клас $\mathrm{Ker}_f = \overline{e_1}$ – нейтральний елемент фактор-групи $G_1/_{\mathrm{Ker}_f}$:

$$\mathrm{Ker}_\varphi = \{\,\overline{e_1}\,\} = \{\,\underbrace{\mathrm{Ker}_f}_{\overline{e_1}}\,\}.$$

Це означає тривіальність ядра гомоморфізму φ, а отже, за теоремою 6.16, гомоморфізм φ є мономорфізмом.

4. Доведемо, що гомоморфізм $\varphi\colon G_1/_{\mathrm{Ker}_f} \to \mathrm{Im}_f$ є епіморфізмом.

Зафіксуємо довільний елемент $y \in \mathrm{Im}_f$. Ураховуючи визначення образу відображення вважатимемо, що $y = f(x)$, де $x \in G_1$. За визначенням відображення φ (співвідношення (6.17)) отримуємо

$$y = f(x) = \varphi(\overline{x}), \quad \overline{x} \in G_1/_{\mathrm{Ker}_f},$$

тобто $y \in \mathrm{Im}_\varphi$. Отже, доведено сюр'єктивність $\varphi\colon G_1/_{\mathrm{Ker}_f} \to \mathrm{Im}_f$, тобто гомоморфізм φ є епіморфізмом.

5. Доведемо співвідношення (6.16).

Для довільного $x \in G_1$, за співвідношенням (6.17), маємо

$$f(x) = \varphi(\overline{x}) = \varphi(\rho(x)) = (\varphi \circ \rho)(x),$$

що доводить рівність (6.16).

Отже, відображення $\varphi : G_1/_{\mathrm{Ker}_f} \to \mathrm{Im}_f$, визначене співвідношенням (6.17), є моно- та епіморфізмом (а отже, й ізоморфізмом), який задовольняє умову (6.16).

Твердження теореми повністю доведено. □

Приклад 6.56. 1. Розглянемо фактор-групу $GL_n/_{SL_n}$. Легко переконатися, що нормальний дільник

$$SL_n = \{A \in GL_n \colon |A| = 1\}$$

є ядром гомоморфізму $f(A) = |A|$, який діє з GL_n до мультиплікативної групи дійсних чисел:

$$f \colon GL_n \to \mathbb{R}^*, \quad f(A) = |A|, \quad \mathrm{Ker}_f = \{A \in GL_n \colon |A| = 1\} = SL_n.$$

Обчислимо образ гомоморфізму f. Ураховуючи, що для будь-якого $\alpha \neq 0$ існує принаймні одна матриця $A \in GL_n$ з визначником $|A| = \alpha$, отримуємо

$$\mathrm{Im}_f = \{|A| \colon A \in GL_n\} = \mathbb{R}^*.$$

Отже, за теоремою 6.18 про гомоморфізми груп, отримуємо ізоморфність

$$GL_n/_{SL_n} \sim \mathbb{R}^*.$$

Таким чином, підтверджено результат, отриманий складнішими обчисленнями в прикл. 6.44.

2. Розглянемо фактор-групу $S_n/_{A_n}$, обмежившись нетривіальним випадком $n \geq 2$. Легко переконатися, що нормальний дільник

$$A_n = \{\sigma \in S_n \colon \varkappa(\sigma) = 0\}$$

є ядром гомоморфізму $\varkappa(\sigma)$, що діє з S_n у групу $\langle\{0,1\}, \oplus\rangle$:

$$\varkappa \colon S_n \to \{0,1\}, \quad \varkappa(\sigma) = \begin{cases} 0, & \text{якщо } \sigma \text{ парна}, \\ 1, & \text{якщо } \sigma \text{ непарна}, \end{cases} \qquad \mathrm{Ker}_\varkappa = A_n.$$

Обчислимо образ гомоморфізму $\varkappa$:

$$\mathrm{Im}_\varkappa = \{\varkappa(\sigma) \colon \sigma \in S_n\} = \{0,1\}.$$

(при $n \geq 2$ множина S_n містить принаймні одну парну та принаймні одну непарну підстановку). Отже, за теоремою 6.18 про гомоморфізми груп, отримуємо ізоморфність

$$S_n/_{A_n} \sim \langle\{0,1\}, \oplus\rangle\,.$$

Ураховуючи очевидну ізоморфність

$$\langle\{0,1\},\oplus\rangle \sim \mathbb{Z}_2, \quad 0 \mapsto \overline{0},\ 1 \mapsto \overline{1},$$

дістанемо

$$S_n/_{A_n} \sim \langle\{0,1\},\oplus\rangle \sim \mathbb{Z}_2.$$

Отже, підтверджено результат, отриманий складнішими обчисленнями в прикл. 6.45.

3. Розглянемо фактор-групу мультиплікативної групи $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ за нормальною підгрупою $\{z \in \mathbb{C}^* : |z| = 1\}$. Легко переконатися, що нормальний дільник є ядром гомоморфізму $f(z) = |z|$, який діє з $\mathbb{C}^*$ в мультиплікативну групу дійсних чисел:

$$f\colon \mathbb{C}^* \to \mathbb{R}^*, \quad f(z) = |z|, \quad \mathrm{Ker}_f = \{z \in \mathbb{C}^* \colon |z| = 1\}.$$

Обчислимо образ гомоморфізму f:

$$\mathrm{Im}_f = \{|z| \colon z \in \mathbb{C}^*\} = (0, +\infty).$$

Отже, за теоремою 6.18 про гомоморфізми груп, одержимо ізоморфність

$$\mathbb{C}^*/_{\{z\in\mathbb{C}^*:|z|=1\}} \sim \langle(0,+\infty),\cdot\rangle\,.$$

4. Розглянемо фактор-групу мультиплікативної групи $\mathbb{C}^*$ за нормальною підгрупою $(0, +\infty)$. Легко переконатися, що нормальний дільник є ядром гомоморфізму $f(z) = \frac{z}{|z|}$, який діє з $\mathbb{C}^*$ в мультиплікативну групу $\{z \in \mathbb{C}^* \colon |z| = 1\}$:

$$f\colon \mathbb{C}^* \to \{z \in \mathbb{C}^* \colon |z| = 1\}, \quad f(z) = \frac{z}{|z|}, \quad \mathrm{Ker}_f = (0, +\infty).$$

Обчислимо образ гомоморфізму f:

$$\mathrm{Im}_f = \left\{\frac{z}{|z|} \colon z \in \mathbb{C}^*\right\} = \left\{z \in \mathbb{C}^* \colon |z| = 1\right\}.$$

Отже, за теоремою 6.18 про гомоморфізми груп, отримуємо ізоморфність

$$\mathbb{C}^*/_{(0,+\infty)} \sim \langle\{z \in \mathbb{C}^* \colon |z| = 1\},\cdot\rangle\,.$$

Теорема 6.18 про гомоморфізми груп у багатьох практичних випадках (див. прикл. 6.56) дозволяє, не обчислюючи фактор-групу $\langle G_1, * \rangle \big/_H$ явно, встановити ізоморфізм між $\langle G_1, * \rangle \big/_H$ та деякою добре вивченою групою $\langle G_2, \circledast \rangle$.

Проте, якщо потрібно отримати явний вигляд фактор-групи $\langle G_1, * \rangle \big/_H$ (тобто явний вигляд суміжних класів та операції «$*$» у групі $G_1 \big/_H$), можна також скористатися теоремою 6.18.

Приклад 6.57. Використовуючи співвідношення (6.16), випишемо явний вигляд ізоморфізму $\varphi \colon GL_n \big/_{SL_n} \to \mathbb{R}^*$:

$$\varphi(\overline{A}) = \varphi(\wp(A)) = |A|, \quad A \in GL_n.$$

Далі, ураховуючи бієктивність $\varphi : GL_n \big/_{SL_n} \to \mathbb{R}^*$, дістанемо явний вигляд елементів фактор-групи $GL_n \big/_{SL_n}$, тобто явний вигляд суміжних класів $\overline{A}$ ($A \in GL_n$):

$$\begin{gathered}\overline{A} = \{X \in GL_n \colon X \in \overline{A}\} = \{X \in GL_n \colon \overline{X} = \overline{A}\} = \\ = \{X \in GL_n \colon \varphi(\overline{X}) = \varphi(\overline{A})\} = \{X \in GL_n \colon |X| = |A|\}.\end{gathered}$$

Ураховуючи, що для будь-якого $\alpha \neq 0$ існує принаймні одна матриця $A \in GL_n$ з визначником $|A| = \alpha$, можемо виписати загальний вигляд суміжних класів GL_n за SL_n:

$$\mathcal{A}_\alpha = \{X \in GL_n \colon |X| = \alpha\}, \quad \alpha \neq 0.$$

Отже, підтверджено результат, отриманий дещо складнішими обчисленнями в прикл. 6.44:

$$GL_n \big/_{SL_n} = \{\mathcal{A}_\alpha \colon \alpha \neq 0\}.$$

Бінарну операцію та правило обчислення оберненого у фактор-групі $GL_n \big/_{SL_n}$ легко встановити через ізоморфізм φ:

$$\begin{gathered}\varphi(\mathcal{A}_{\alpha_1} \cdot \mathcal{A}_{\alpha_2}) = \varphi(\mathcal{A}_{\alpha_1}) \cdot \varphi(\mathcal{A}_{\alpha_2}) = \alpha_1 \cdot \alpha_2 = \varphi(\mathcal{A}_{\alpha_1 \cdot \alpha_2}) \\ \Downarrow \\ \mathcal{A}_{\alpha_1} \cdot \mathcal{A}_{\alpha_2} = \mathcal{A}_{\alpha_1 \alpha_2}; \\ \Big(\varphi\left((\mathcal{A}_\alpha)^{-1}\right) = (\varphi(\mathcal{A}_\alpha))^{-1} = \alpha^{-1} = \varphi\left(\mathcal{A}_{\alpha^{-1}}\right)\Big) \Rightarrow \Big((A_\alpha)^{-1} = \mathcal{A}_{\alpha^{-1}}\Big).\end{gathered}$$

Отриманий результат збігається з результатом прикл. 6.47.

Отже, завдяки використанню теореми 6.18, повністю підтверджено результати стосовно фактор-групи $GL_n/_{SL_n}$, отримані в прикл. 6.44 та 6.47.

Як показує наведений приклад, у деяких практичних випадках використання теореми про гомоморфізми груп спрощує явне обчислення фактор-групи, оскільки дозволяє уникнути безпосереднього обчислення суміжних класів.

Деякі інші важливі теореми про гомоморфізми груп, які спрощують обчислення фактор-груп, можна знайти, наприклад, у роботі [10].

Розділ 7

Елементи теорії кілець

7.1. Визначення та приклади кілець

Кільце – основний об'єкт розгляду в цьому розділі – приклад алгебричної структури з двома бінарними операціями.

Означення 7.1. Кільцем називають алгебричну структуру $\langle R, +, \cdot \rangle$ із замкненими бінарними операціями «$+$» (додавання) та «$\cdot$» (множення), визначеними на множині $R \neq \varnothing$, які задовольняють умови:

1) $\forall\, a, b, c \in R$: $(a + b) + c = a + (b + c)$ (асоціативність додавання);

2) $\forall\, a, b \in R$: $a + b = b + a$ (комутативність додавання);

3) $\exists\, 0 \in R \forall\, a \in R$: $a + 0 = a$ (існування нейтрального за додаванням);

4) $\forall\, a \in R \exists -a \in R$: $a + (-a) = 0$ (існування обернених за додаванням);

5) $\forall\, a, b, c \in R$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (асоціативність множення);

6) $\forall\, a, b, c \in R$: $(a + b) \cdot c = (a \cdot c) + (b \cdot c),\ c \cdot (a + b) = (c \cdot a) + (c \cdot b)$ (дистрибутивність множення відносно додавання).

Елемент $0 \in R$ (нейтральний за додаванням) називають *нулем кільця*. Зазначимо, що єдиність нуля кільця як нейтрального за додаванням випливає з теореми 6.1.

Елемент $-a$, обернений за додаванням до $a \in R$, називають *протилежним* a в кільці R. Очевидно, що єдиність протилежного елемента для фіксованого $a \in R$ є простим наслідком з теореми 6.2.

Умови 1–4 означення 7.1 визначають, що кільце є абелевою групою за додаванням; умова 5 визначає, що кільце є півгрупою (можливо, некомутативною) за множенням; умова 6 визначає зв'язок між додаванням

і множенням. Отже, умови означення 7.1 для кільця $\langle R, +, \cdot \rangle$ можна подати у вигляді:

- 1–4 – алгебрична структура $\langle R, + \rangle$ є абелевою групою;
- 5 – алгебрична структура $\langle R, \cdot \rangle$ є півгрупою;
- 6 – операція «$\cdot$» дистрибутивна справа і зліва відносно «$+$».

Приклад 7.1. Такі алгебричні структури є кільцями:

1. Алгебрична структура $\langle \mathbb{R}, +, \cdot \rangle$ – кільце дійсних чисел за природними операціями додавання та множення.

2. Алгебрична структура $\langle \mathbb{Z}, +, \cdot \rangle$ – кільце цілих чисел за природними операціями додавання та множення.

3. Алгебрична структура $\langle M_{n\times n}, +, \cdot \rangle$ – кільце матриць $n \times n$ за природними операціями додавання та множення.

4. Алгебрична структура $\langle \mathbb{Z}_n, +, \cdot \rangle$ – кільце класів лишків за модулем $n \in \mathbb{N}$ (операції «$+$» та «$\cdot$» на $\mathbb{Z}_n$ було введено в підрозд. 6.4).

5. Алгебрична структура $\langle \mathbb{R}[x], +, \cdot \rangle$, де $\mathbb{R}[x]$ – множина многочленів скінченного степеня над змінною x з дійсними коефіцієнтами:

$$\mathbb{R}[x] = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \colon a_k \in \mathbb{R}\ (1 \le k \le n),\ n \in \mathbb{N} \cup \{0\}\}.$$

Операції «$+$» та «$\cdot$» на $\mathbb{R}[x]$ вводять поточково (через значення многочленів для кожного $x \in \mathbb{R}$), тобто для многочленів $a(x) = \sum\limits_{i=0}^{n} a_i x^i$, $b(x) = \sum\limits_{j=0}^{m} b_j x^j$ для фіксованого $x \in \mathbb{R}$ визначаємо:

$$a(x) + b(x) = b(x) + a(x) = \sum_{k=0}^{\max(n,m)} c_k x^k,\ \text{де } c_k = a_k + b_k;$$

$$a(x) \cdot b(x) = b(x) \cdot a(x) = \sum_{k=0}^{n+m} c_k x^k,\ \text{де } c_k = \sum_{i,j:\ i+j=k} a_i b_j,$$

вважаючи $a_k = 0$ при $k > n$, $b_k = 0$ при $k > m$.

6. Алгебрична структура $\langle S, \triangle, \cap \rangle$, де S – кільце множин. Нагадаємо (див. підрозд. 2.5), що кільцем множин називають непорожню сукупність множин S, замкнену відносно операцій симетричної різниці та перетину.

За додавання та множення в кільці множин S вибираємо відповідно симетричну різницю та перетин:

$$A + B = A \triangle B,\ A \cdot B = A \cap B, \quad (A, B \in S).$$

Легко перевірити, що нулем у кільці $\langle S, \triangle, \cap \rangle$ є порожня множина:

$$A \triangle \varnothing = \varnothing \triangle A = A \quad (A \in S).$$

Слід зазначити, що елемент, протилежний A, збігається із самою множиною A:

$$A \triangle A = \varnothing \quad (A \in S).$$

Перепишемо для структури $\langle S, \triangle, \cap \rangle$ умови означення 7.1:
1) $(A \triangle B) \triangle C = A \triangle (B \triangle C)$;
2) $A \triangle B = B \triangle A$;
3) $A \triangle \varnothing = \varnothing \triangle A = A$ (нульовим елементом є порожня множина);
4) $A \triangle A = \varnothing$ (елемент, протилежний A, збігається з A);
5) $(A \cap B) \cap C = A \cap (B \cap C)$;
6) $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C),\ C \cap (A \triangle B) = (C \cap A) \triangle (C \cap B)$.
Указані тотожності неважко довести засобами алгебри множин.

Цей приклад обґрунтовує назву «кільце» для кільця множин S як для окремого випадку абстрактного кільця $\langle S, \triangle, \cap \rangle$.

7. Нехай $\langle G, + \rangle$ – деяка адитивна абелева група. Для ендоморфізмів $f_1, f_2 \in \mathrm{End}_G$ введемо поточкове додавання:

$$(f_1 + f_2)(x) = f_1(x) + f_2(x) \quad (x \in G).$$

Вправа 7.1. Довести, що структура $\langle \mathrm{End}_G, +, \circ \rangle$ – кільце.

Кільце $\langle \mathrm{End}_G, +, \circ \rangle$ називають *кільцем ендоморфізмів* абелевої групи $\langle G, + \rangle$.

Зауваження 7.1. Для кілець $\langle R, +, \cdot \rangle$, які часто трапляються в різних розділах математики (зокрема, це стосується кілець з прикл. 7.1), часто вказують лише множину R, не вказуючи явно операції додавання та множення. Так, якщо говорять про кільце дійсних чисел, кільце матриць, кільце класів лишків, кільце многочленів тощо, мають на увазі класичні (природні) операції додавання та множення. Варто зазначити,

що для кільця множин S природними додаванням і множенням вважають відповідно симетричну різницю та перетин: у модельному доведенні тотожностей в алгебрі множин симетричній різниці та перетину відповідають логічні операції «$\oplus$» та «$\wedge$», які (якщо ототожнити логічні 0 та 1 з класами лишків $\overline{0}$ та $\overline{1}$ за модулем 2) збігаються з додаванням і множенням на $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$.

Кільце $\langle R, +, \cdot\rangle$ з комутативною операцією множення називають *комутативним*:

$$a \cdot b = b \cdot a \qquad \forall\, a, b \in R.$$

Якщо операція множення некомутативна, кільце називають *некомутативним*.

Приклад 7.2. Такі кільця є комутативними:
1) кільце $\langle \mathbb{R}, +, \cdot\rangle$ дійсних чисел;
2) кільце $\langle \mathbb{Z}_n, +, \cdot\rangle$ класів лишків за модулем $n \in \mathbb{N}$;
3) кільце $\langle \mathbb{R}[x], +, \cdot\rangle$ многочленів з дійсними коефіцієнтами;
4) кільце множин $\langle S, \triangle, \cap\rangle$.
Найпростіший приклад некомутативного кільця – кільце квадратних матриць $\langle M_{n\times n}, +, \cdot\rangle$ у випадку $n \geq 2$.

Кільце $\langle R, +, \cdot\rangle$ називають *кільцем з одиницею*, якщо в структурі $\langle R, \cdot\rangle$ існує нейтральний елемент $1 \in R$ (нейтральний за множенням), який у цьому випадку називають *одиницею кільця*. Зазначимо, що єдиність одиниці кільця як нейтрального елемента за множенням випливає з теореми 6.1.

Приклад 7.3. 1. Усі кільця, розглянуті в прикл. 7.1, за винятком кільця множин $\langle S, \triangle, \cap\rangle$, є кільцями з одиницею.

2. Кільце $\langle n\mathbb{Z}, +, \cdot\rangle$ у випадку $n \geq 2$ є кільцем без одиниці, оскільки 1 (нейтральний елемент за множенням на множині цілих чисел) не належить множині $n\mathbb{Z}$ при $n \geq 2$.

Вправа 7.2. Визначити одиниці для кілець з прикл. 7.1 (окрім $\langle S, \triangle, \cap\rangle$).

Вправа 7.3. Довести, що кільце множин $\langle S, \triangle, \cap\rangle$ є кільцем з одиницею тоді і тільки тоді, коли S є алгеброю множин, причому одиницею в кільці $\langle S, \triangle, \cap\rangle$ (якщо S – алгебра) є універсальна множина.

Кільця з одиницею буде розглянуто більш детально в підрозд. 7.4.

Зауваження 7.2. Нуль та одиниця в абстрактному кільці $\langle R, +, \cdot \rangle$ позначають, як було зазначено, відповідно через 0 та 1. Проте в конкретному кільці для нуля та одиниці використовують позначення, які є загальноприйнятими саме для цього кільця і можуть збігатися або не збігатися з абстрактними позначеннями 0 та 1. Так, у кільці дійсних чисел нулем та одиницею є числа 0 та 1, однак у кільці матриць $M_{n\times n}$ нулем та одиницею є відповідно нульова та одинична матриці (які не прийнято позначати через 0 та 1).

Зауваження 7.3. Для спрощення позначень вважатимемо, що операція множення в кільці має вищий пріоритет, ніж додавання, тобто дужки навколо добутку будемо опускати: $a + (b \cdot c) = a + b \cdot c$.

Зауваження 7.4. Крім того, за аналогією до багатьох мультиплікативних структур (ураховуючи дійсні числа та матриці), позначення операції «$\cdot$» в добутку іноді опускатимемо: $a \cdot b = ab$.

7.2. Основні властивості кілець

Розглянемо найпростіші властивості довільного кільця $\langle R, +, \cdot \rangle$.

1. $\forall\, a \in R\colon 0 \cdot a = a \cdot 0 = 0$.

Доведення. Доведемо тотожність $0 \cdot a = 0$ (тотожність $a \cdot 0 = 0$ можна довести за аналогією). За означенням нуля та властивістю дистрибутивності маємо

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a.$$

Але кільце є групою за операцією «+», а отже, за правилом лівого скорочення (6.2) отримуємо потрібний наслідок:

$$0 \cdot a + 0 \cdot a = 0 \cdot a \Rightarrow 0 \cdot a + 0 \cdot a = 0 \cdot a + 0 \Rightarrow 0 \cdot a = 0. \qquad \square$$

2. $\forall\, a, b \in R\colon a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$.

Доведення. Доведемо тотожність $a \cdot (-b) = -(a \cdot b)$ (тотожність $(-a) \cdot b = -(a \cdot b)$ можна довести за аналогією). Для доведення достатньо перевірити, що елемент $a \cdot (-b)$ є протилежним $a \cdot b$. Користуючись визначенням кільця та доведеною властивістю 1, отримуємо

$$a \cdot b + a \cdot (-b) = a \cdot (-b) + a \cdot b = a \cdot (b + (-b)) = a \cdot 0 = 0. \qquad \square$$

Вправа 7.4. Довести, що в кільці з одиницею має місце тотожність

$$-a = (-1) \cdot a \qquad \forall\, a \in R.$$

Для елементів $a, b \in R$ уведемо операцію *різниці*:

$$a - b = a + (-b).$$

Так, з означення протилежного елемента випливає $a - a = a + (-a) = 0$.

7.3. Підкільце. Критерій підкільця

Нехай $\langle R, +, \cdot \rangle$ – довільне кільце.

Означення 7.2. Підкільцем кільця $\langle R, +, \cdot \rangle$ називають підмножину $R_1 \subset R$, яка є кільцем $\langle R_1, +, \cdot \rangle$ за тими самими операціями «+» та «·», що й кільце $\langle R, +, \cdot \rangle$.

На практиці для перевірки, чи є непорожня підмножина кільця підкільцем, зручно користуватись нижчеподаним критерієм, аналогічним критерію підгрупи (теорема 6.7 з наслідком).

Теорема 7.1 (критерій підкільця)**.** *Нехай $\varnothing \neq R_1 \subset R$, тобто R_1 – непорожня підмножина кільця $\langle R, +, \cdot \rangle$.*

Для того, щоб підмножина R_1 була підкільцем кільця $\langle R, +, \cdot \rangle$, необхідно і достатньо виконання таких умов:

$$(a, b \in R_1) \Rightarrow (a + b \in R_1); \tag{7.1}$$

$$(a, b \in R_1) \Rightarrow (a \cdot b \in R_1);$$

$$(a \in R_1) \Rightarrow (-a \in R_1). \tag{7.2}$$

Наслідок. *Умови (7.1) та (7.2) в теоремі 7.1 можна замінити однією умовою:*

$$(a, b \in R_1) \Rightarrow (a - b \in R_1).$$

Вправа 7.5. Довести теорему 7.1 і наслідок самостійно.

Зауваження 7.5. Доведення цілком аналогічне доведенню теореми 6.7.

Приклад 7.4. 1. Множина $n\mathbb{Z}$ ($n \in \mathbb{N}$) є підкільцем кільця цілих чисел $\mathbb{Z}$.

2. Множина $R_1 = \{A \in M_{n\times n} \colon A_{ij} = 0 \text{ при } j > i\}$ нижніх трикутних матриць розміром $n \times n$ є підкільцем кільця матриць $M_{n\times n}$.

3. Множина многочленів з нульовим вільним членом

$$R_1 = \left\{ \sum_{k=1}^{n} a_k x^k \colon \ a_k \in \mathbb{R}\ (1 \le k \le n),\ n \in \mathbb{N} \right\} = \\ = \{f(x) \in \mathbb{R}[x] \colon f(0) = 0\}$$

є підкільцем кільця многочленів $\mathbb{R}[x]$.

Очевидно, що будь-яке кільце $\langle R, +, \cdot \rangle$ містить *тривіальні* підкільця – множину $\{0\}$ і множину R. Підкільце, що не є тривіальним, називають *власним*.

Кільце, що містить лише один елемент (це має бути 0) називають *нульовим*. Отже, будь-яке кільце $\langle R, +, \cdot \rangle$ містить два тривіальні кільця – нульове кільце $\{0\}$ і саме кільце R. Очевидно, що для нульового кільця обидва тривіальні підкільця збігаються.

7.4. Кільця з одиницею

У цьому підрозділі об'єктом розгляду буде кільце $\langle R, +, \cdot \rangle$, що містить одиничний елемент $1 \in R$. Доведемо простий факт щодо можливості збігу нуля та одиниці кільця.

Лема 7.1. *У ненульовому кільці* $0 \neq 1$.

Доведення. Нехай кільце з одиницею $\langle R, +, \cdot \rangle$ є ненульовим, тобто містить принаймні один елемент $a \neq 0$. Тоді отримуємо

$$a \cdot 0 = 0 \neq a = a \cdot 1,$$

що унеможливлює рівність $0 = 1$. □

Зауваження 7.6. Очевидно, що в нульовому кільці елементи 0 та 1 збігаються: нульове кільце містить лише один елемент 0, який для одноелементної множини є нейтральним за будь-якою бінарною операцією ($0 \cdot 0 = 0$).

Означення 7.3. Елемент $a \in R$ називають оборотним у кільці R, або дільником одиниці, якщо існує елемент a^{-1} – обернений до a за множенням:

$$\exists\, a^{-1} \in R\colon a^{-1} \cdot a = a \cdot a^{-1} = 1.$$

Елемент a^{-1} називають оберненим до a в кільці R.

Отже, в кільці з одиницею існують нейтральні елементи для обох бінарних операцій: 0 – нейтральний за додаванням, 1 – нейтральний за множенням. Як уже зазначали, обернений до $a \in R$ за додаванням називають протилежним і позначають через $-a$, що унеможливлює конфлікт з терміном «обернений» (без явної назви відповідної бінарної операції) та позначенням a^{-1} для оберненого за множенням.

Обернені елементи можуть існувати не для всіх $a \in R$. Більше того, у будь-якому ненульовому кільці з одиницею існує принаймні один необоротний елемент – нуль кільця:

$$0 \cdot a = a \cdot 0 = 0 \neq 1 \quad \forall\, a \in R.$$

Однак, у будь-якому кільці $\langle R, +, \cdot \rangle$ (з одиницею) оборотними є елементи 1 та -1:

$$1^{-1} = 1,\ (-1)^{-1} = -1,$$

оскільки $1 \cdot 1 = (-1) \cdot (-1) = 1$.

Множину всіх оборотних елементів кільця $\langle R, +, \cdot \rangle$ позначають через R^*.

Приклад 7.5. 1. У кільці дійсних чисел $\mathbb{R}$ всі ненульові елементи оборотні:

$$a^{-1} = \frac{1}{a} \in \mathbb{R}, \quad a \neq 0,$$

тобто $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

2. У кільці цілих чисел $\mathbb{Z}$ оборотні лише елементи 1 та -1:

$$1^{-1} = 1, \quad (-1)^{-1} = -1, \quad a^{-1} = \frac{1}{a} \notin \mathbb{Z} \ \text{ при } |a| \neq 1,$$

тобто $\mathbb{Z}^* = \{1, -1\}$.

3. У кільці матриць $M_{n\times n}$ оборотні всі невироджені матриці:

$$A \cdot A^{-1} = A^{-1} \cdot A = I,$$

тобто $(M_{n\times n})^* = GL_n$.

4. У кільці класів лишків $\mathbb{Z}_6$ оборотними є елементи $\overline{1}$ та $\overline{5}$:

$$(\overline{1})^{-1} = \overline{1}, \quad (\overline{5})^{-1} = \overline{5},$$

тобто $\mathbb{Z}_6{}^* = \{\overline{1}, \overline{5}\}$.

5. У кільці класів лишків $\mathbb{Z}_2$ оборотним є лише елемент $\overline{1}$:

$$(\overline{1})^{-1} = \overline{1},$$

тобто $\mathbb{Z}_2{}^* = \{\overline{1}\}$.

Теорема 7.2. *Множина R^* оборотних елементів кільця $\langle R, +, \cdot \rangle$ утворює групу за операцією множення.*

Доведення. Розглянемо алгебричну структуру $\langle R^*, \cdot \rangle$.

1. Доведемо замкненість структури $\langle R^*, \cdot \rangle$. Для $a, b \in R^*$ безпосередньо перевіримо, що $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$:

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = 1;$$
$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = b^{-1} \cdot (a^{-1} \cdot a) \cdot b = 1,$$

тобто $a \cdot b \in R^*$ (елемент $a \cdot b$ оборотний).

2. Структура $\langle R^*, \cdot \rangle$ асоціативна (за визначенням кільця).

3. Структура $\langle R^*, \cdot \rangle$ містить нейтральний елемент – одиницю кільця $\langle R, +, \cdot \rangle$:

$$(1^{-1} = 1) \Rightarrow (1 \in R^*).$$

4. Доведемо, що у структурі $\langle R^*, \cdot \rangle$ для будь-якого $a \in R^*$ існує обернений $a^{-1} \in R^*$. Безпосередньо перевіримо, що $(a^{-1})^{-1} = a$:

$$a^{-1} \cdot a = 1, \quad a \cdot a^{-1} = 1,$$

тобто $a^{-1} \in R^*$.

Отже, алгебрична структура $\langle R^*, \cdot \rangle$ є замкненою, асоціативною, містить нейтральний елемент $1 \in R^*$, і для кожного $a \in R^*$ існує обернений $a^{-1} \in R^*$. Таким чином, за означенням 6.5 структура $\langle R^*, \cdot \rangle$ є групою. $\square$

Алгебричну структуру $\langle R^*, \cdot \rangle$ називають *мультиплікативною групою* кільця $\langle R, +, \cdot \rangle$. Для мультиплікативної групи заданого кільця $\langle R, +, \cdot \rangle$ використовують скорочене позначення R^* (не вказуючи явно групову операцію, яка збігається з операцію множення в кільці R).

Поняття оборотного елемента (дільника одиниці) тісно пов'язане з поняттям дільника нуля, яке буде розглянуто в наступному підрозділі.

7.5. Дільники нуля. Поняття області цілісності

Нехай $\langle R, +, \cdot \rangle$ – довільне кільце.

Означення 7.4. Елементи $a, b \in R$ називають *дільниками нуля*, якщо

$$a \neq 0, \quad b \neq 0, \quad ab = 0.$$

Елемент a в цьому випадку називають *лівим дільником нуля*, елемент b – *правим дільником нуля*.

Очевидно, що в комутативному кільці поняття правого та лівого дільників нуля збігаються.

Приклад 7.6. 1. Кільце дійсних чисел $\mathbb{R}$ не містить дільників нуля:

$$(a \neq 0) \wedge (b \neq 0) \Rightarrow (ab \neq 0)$$

для довільних $a, b \in \mathbb{R}$.

2. Кільце $\mathbb{Z}_6$ містить три дільники нуля – елементи $\overline{2}$, $\overline{3}$ та $\overline{4}$:

$$\overline{2} \cdot \overline{3} = \overline{3} \cdot \overline{4} = \overline{0}.$$

Легко перевірити, що $\overline{1}$ та $\overline{5} = \overline{-1}$ не є дільниками нуля в $\mathbb{Z}_6$.

3. Кільце $\mathbb{Z}_4$ містить один дільник нуля – елемент $\overline{2}$:

$$\overline{2} \cdot \overline{2} = \overline{0}.$$

Легко перевірити, що $\overline{1}$ та $\overline{3} = \overline{-1}$ не є дільниками нуля в $\mathbb{Z}_4$.

4. Кільце $\mathbb{Z}_3$ не містить дільників нуля:

$$\overline{1} \cdot \overline{1} = \overline{1} \neq \overline{0}, \quad \overline{1} \cdot \overline{2} = \overline{2} \neq \overline{0}, \quad \overline{2} \cdot \overline{2} = \overline{4} = \overline{1} \neq \overline{0}.$$

Наступна теорема встановлює зв'язок між поняттями дільника нуля та оборотного елемента в кільці з одиницею.

Теорема 7.3. *У кільці $\langle R, +, \cdot \rangle$ з одиницею $1 \in R$ жоден оборотний елемент не є дільником нуля.*

Доведення. Припустімо, що $a \in R$ є одночасно дільником нуля й оборотним елементом. Вважатимемо, що $a \neq 0$ – лівий дільник нуля (випадок правого дільника нуля розглядається аналогічно), тобто

$$ab = 0 \text{ для деякого } b \in R,\ b \neq 0.$$

Тоді отримуємо

$$(ab = 0) \Rightarrow (a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0) \Rightarrow ((a^{-1} \cdot a) \cdot b = 0) \Rightarrow (1 \cdot b = 0) \Rightarrow (b = 0),$$

що суперечить умові $b \neq 0$. □

Отже, оборотний елемент (дільник одиниці) не є дільником нуля, однак зворотне твердження в загальному випадку неправильне: елемент, який не є дільником нуля, не обов'язково є оборотним.

Приклад 7.7. У кільці цілих чисел $\mathbb{Z}$ немає дільників нуля, однак лише елементи 1 та (-1) є оборотними.

З дільниками нуля (точніше, з їх відсутністю) пов'язано виконання *законів скорочення* в довільному кільці $\langle R, +, \cdot \rangle$:

$$(ax = bx) \Leftrightarrow (a = b) \quad \text{(праве скорочення)}; \tag{7.3}$$

$$(xa = xb) \Leftrightarrow (a = b) \quad \text{(ліве скорочення)}, \tag{7.4}$$

де $a, b, x \in R$, $x \neq 0$.

Теорема 7.4. *Закони скорочення* (7.3) *і* (7.4) *у довільному кільці* $\langle R, +, \cdot \rangle$ *виконуються тоді і тільки тоді, коли кільце* $\langle R, +, \cdot \rangle$ *не містить жодного дільника нуля.*

Доведення. 1. Нехай кільце $\langle R, +, \cdot \rangle$ не містить дільників нуля. Доведемо, що в цьому кільці виконується закон (7.3) (закон (7.4) розглядається аналогічно). Ураховуючи, що в кільці немає дільників нуля, для $a, b, x \in R$ $(x \neq 0)$ отримуємо

$$(ax = bx) \Rightarrow ((a - b) \cdot x = 0) \Rightarrow (a - b = 0) \Rightarrow (a = b).$$

2. Нехай у кільці $\langle R, +, \cdot \rangle$ виконуються закони (7.3) і (7.4). Доведемо, що в кільці $\langle R, +, \cdot \rangle$ немає дільників нуля.

Припустімо, що $a, b \in R$, $a \neq 0$, $b \neq 0$, $ab = 0$. Тоді дістанемо

$$(a \cdot b = 0) \Rightarrow (a \cdot b = a \cdot (b \cdot 0)) \Rightarrow (b = b \cdot 0) \Rightarrow (b = 0),$$

що суперечить умові $b \neq 0$. □

Зауваження 7.7. У п. 2 доведення теореми 7.4 було використано лише закон лівого скорочення (7.4). Аналогічно можна було б використати і правий закон скорочення (7.3), не користуючись лівим. Отже, якщо в кільці справджується хоча б один із законів скорочення, то таке кільце не містить жодного дільника нуля, і в цьому кільці справджуються обидва закони (7.3) і (7.4).

Приклад 7.8. 1. Кільце дійсних чисел $\langle \mathbb{R}, +, \cdot \rangle$ не містить дільників нуля, а отже, допускає закон скорочення (7.3)

$$(ax = bx) \Rightarrow (a = b)$$

для будь-яких $a, b, x \in \mathbb{R}$, $x \neq 0$.

2. Кільце матриць $M_{2\times 2}$ містить дільники нуля. Так, зокрема,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Отже, у кільці $M_{2\times 2}$ жоден з двох законів скорочення не справджується:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \text{ але } \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix};$$
$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \text{ але } \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}.$$

Зауваження 7.8. Можна довести, що дільником нуля в кільці $M_{n\times n}$ ($n \in \mathbb{N}$) є будь-яка вироджена матриця.

Як бачимо, в довільному кільці $\langle R, +, \cdot \rangle$ з одиницею існує тісний зв'язок між поняттями дільника нуля та оборотного елемента (дільника одиниці). Цей зв'язок стає ще тіснішим у випадку скінченного кільця $\langle R, +, \cdot \rangle$, тобто коли $\operatorname{card} R < \infty$.

Теорема 7.5. *Нехай $\langle R, +, \cdot \rangle$ – скінченне кільце з одиницею, елемент $a \in R$ не є дільником нуля та $a \neq 0$. Тоді елемент a оборотний.*

Доведення. Нехай $\operatorname{card} R = n \geq 2$ (у нульовому кільці, тобто у випадку $\operatorname{card} R = 1$, твердження теореми очевидно виконується), $a \in R$, $a \neq 0$.

Для пошуку елемента, оберненого до a, застосуємо метод, використаний у доведенні теореми 6.6.

Розглянемо множину $a \cdot R = \{a \cdot b : b \in R\}$ для фіксованого $a \in R$. Спочатку доведемо, що множина $a \cdot R$ містить n різних елементів вигляду $a \cdot b$ $(b \in R)$, тобто

$$a \cdot b_1 \neq a \cdot b_2 \text{ при } b_1 \neq b_2 \quad (b_1, b_2 \in R).$$

Дійсно, оскільки a не є дільником нуля та $a \neq 0$, отримуємо

$$(a \cdot b_1 = a \cdot b_2) \Rightarrow (a \cdot (b_1 - b_2) = 0) \Rightarrow (b_1 - b_2 = 0) \Rightarrow (b_1 = b_2).$$

Отже, $\text{card}(a \cdot R) = \text{card}(R) = n$; крім того, очевидно, $a \cdot R \subset R$. Звідси випливає, що множини $a \cdot R$ та R збігаються.

Оскільки $a \cdot R = R \ni 1$ (кільце $\langle R, +, \cdot \rangle$ містить одиницю), отримуємо

$$(1 \in a \cdot R) \Rightarrow (\exists\, b_r \in R : a \cdot b_r = 1).$$

Отже, для елемента a у структурі $\langle R, \cdot \rangle$ існує правий обернений b_r. Аналогічно доведемо існування для $a \in R$ $(a \neq 0)$ лівого оберненого b_l:

$$(1 \in R = R \cdot a = \{b \cdot a : b \in R\}) \Rightarrow (\exists\, b_l \in R : b_l \cdot a = 1).$$

Отже, для $a \in R$ $(a \neq 0)$ у структурі $\langle R, \cdot \rangle$ існує правий обернений b_r та лівий обернений b_l. Нарешті, за теоремою 6.2, правий та лівий обернені для фіксованого $a \in R$ мають збігатися:

$$b_r = b_l = a^{-1}.$$

Отже, доведено, що елемент $a \in R$ є оборотним. □

Приклад 7.9. Кільце класів лишків $\mathbb{Z}_p$ у випадку простого p не містить дільників нуля:

$$(\overline{k_1} \cdot \overline{k_2} = \overline{0}) \Rightarrow ((k_1 \cdot k_2) \bmod p = 0) \Rightarrow$$
$$\Rightarrow ((k_1 \bmod p = 0) \vee (k_2 \bmod p = 0)) \Rightarrow ((\overline{k_1} = \overline{0}) \vee (\overline{k_2} = \overline{0})).$$

Отже, у випадку простого p всі ненульові елементи кільця $\mathbb{Z}_p$ оборотні:

$$\mathbb{Z}_p{}^* = \mathbb{Z}_p \setminus \{\overline{0}\}.$$

Як наслідок з теореми 7.5 отримано твердження теореми 6.6. Такий результат цілком виправдовує позначення

$$\mathbb{Z}_p{}^* = \mathbb{Z}_p \setminus \{\overline{0}\} = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\},$$

введене для випадку простих p у підрозд. 6.4.

Означення 7.5. Областю цілісності називають комутативне кільце з одиницею, яке не містить дільників нуля.

Приклад 7.10. 1. Кільце цілих чисел $\langle \mathbb{Z}, +, \cdot \rangle$ є комутативним кільцем з одиницею, не містить дільників нуля, а отже, є областю цілісності.

2. Кільце $\mathbb{Z}_5$ є комутативним кільцем з одиницею, не містить дільників нуля, а отже, є областю цілісності.

3. Кільце $\mathbb{Z}_4$ є комутативним кільцем з одиницею, але містить дільник нуля (елемент $\overline{2}$), а отже, не є областю цілісності.

Означення 7.6. Полем називають ненульове комутативне кільце з одиницею, всі ненульові елементи якого є оборотними.

Приклад 7.11. Такі кільця є полями:
1) кільце дійсних чисел $\mathbb{R}$;
2) кільце раціональних чисел $\mathbb{Q}$;
3) кільце комплексних чисел $\mathbb{C}$;
4) кільце $\left\langle \{a + b \cdot \sqrt{2} \colon a, b \in \mathbb{Q}\}, +, \cdot \right\rangle$;
5) кільце $\langle \{a + b \cdot i \colon a, b \in \mathbb{Q}\}, +, \cdot \rangle$, де $i \in \mathbb{C}$ – комплексна одиниця.

Вправа 7.6. Перевірити, що всі кільця з прикл. 7.11 є полями.

З теореми 7.3 випливає, що будь-яке поле є областю цілісності. Зворотне твердження неправильне – кільце цілих чисел є одним з прикладів області цілісності, яка не є полем. Проте, з урахуванням теореми 7.5, можемо сформулювати такий результат.

Теорема 7.6. *Будь-яка скінченна область цілісності, що містить не менше двох елементів (тобто не є нульовим кільцем), є полем.*

Найпростішим (і дуже важливим) прикладом скінченних полів є поля класів лишків $\mathbb{Z}_p$, де p – просте число. Зауважимо, що $\mathbb{Z}_n$ у випадку складеного $n \in \mathbb{N}$ не є полем, оскільки містить дільники нуля:

$$(n = k \cdot m,\ k \neq n,\ m \neq n) \Rightarrow (\overline{k} \neq \overline{0},\ \overline{m} \neq \overline{0},\ \overline{k} \cdot \overline{m} = \overline{0}).$$

Приклад 7.12. 1. Кільця $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_{97}$ – поля.
2. Кільця $\mathbb{Z}_4$, $\mathbb{Z}_6$, $\mathbb{Z}_{15}$ не є полями, оскільки містять дільники нуля.

Взагалі, мультиплікативна група кільця лишків $\mathbb{Z}_n$ для довільного $n \in \mathbb{N}$ має досить просту і цікаву структуру.

Вправа 7.7. Довести, що мультиплікативна група кільця $\mathbb{Z}_n$ складається із класів лишків $\overline{k}$, де k – взаємно просте з n:

$$\mathbb{Z}_n{}^* = \{\overline{k} \colon \text{НСД}(n,k) = 1\},$$

де $\text{НСД}(k_1, k_2)$ – найбільший спільний дільник чисел k_1 та k_2.

Приклад 7.13. 1) $\mathbb{Z}_6{}^* = \{\overline{1}, \overline{5}\}$;
2) $\mathbb{Z}_8{}^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$;
3) $\mathbb{Z}_9{}^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$.

Детальніше про структуру мультиплікативної групи кільця лишків, зокрема, про умову її циклічності, можна прочитати в [10].

7.6. Ідеал кільця

Розглянемо спеціальний клас підкілець, який посідає в теорії кілець майже те саме місце, що і нормальні дільники в теорії груп.

Означення 7.7. Ідеалом кільця $\langle R, +, \cdot \rangle$ називають непорожню підмножину $J \subset R$, таку, що:

- структура $\langle J, + \rangle$ – підгрупа групи $\langle R, + \rangle$;
- для будь-яких $r \in R$ та $j \in J$ добутки rj та jr містяться в J.

Очевидно, що в будь-якому кільці $\langle R, +, \cdot \rangle$ тривіальні підкільця $\{0\}$ та R завжди є ідеалами. Ідеали $\{0\}$ та R називають *тривіальними*; ідеал, що не є тривіальним, називають *власним*.

Приклад 7.14. 1. Кільце $\mathbb{Z}$ містить ідеали $n\mathbb{Z}$ ($n \in \mathbb{N} \cup \{0\}$). Очевидно, що ідеали $0\mathbb{Z} = \{0\}$ та $1\mathbb{Z} = \mathbb{Z}$ тривіальні, ідеали $n\mathbb{Z}$ при $n \geq 2$ – власні.

2. Кільце дійсних чисел $\mathbb{R}$ містить лише тривіальні ідеали, оскільки для $a \in J$ (J – деякий ідеал кільця $\mathbb{R}$) отримуємо

$$(a \neq 0) \Rightarrow (\forall\, r \in \mathbb{R} \colon r = a \cdot (r \cdot a^{-1}) \in \mathbb{R}),$$

тобто будь-який ідеал $J \neq \{0\}$ має містити всі дійсні числа $r \in \mathbb{R}$.

Вправа 7.8. Довести такі твердження для ідеалу J кільця $\langle R, +, \cdot\rangle$:
- $(1 \in J) \Rightarrow (J = R)$ (у припущенні, що R містить одиницю);
- $(a \in J \cap R^*) \Rightarrow (J = R)$ (у припущенні, що R містить одиницю);
- будь-яке поле містить лише тривіальні ідеали.

Важливий клас ідеалів становлять ідеали, породжені фіксованим елементом кільця. Найпростішу структуру ці ідеали мають у комутативних кільцях з одиницею.

Лема 7.2. *Нехай $\langle R, +, \cdot\rangle$ – комутативне кільце з одиницею, $a \in R$. Тоді множина $aR = \{ar \colon r \in R\}$ є ідеалом у кільці $\langle R, +, \cdot\rangle$.*

Доведення. Беручи до уваги структуру множини aR і користуючись комутативністю кільця $\langle R, +, \cdot\rangle$, отримуємо:

$$(x_1, x_2 \in aR) \Rightarrow \begin{cases} x_1 = ar_1,\ r_1 \in R \\ x_2 = ar_2,\ r_2 \in R \end{cases} \Rightarrow (x_1 - x_2 = a(r_1 - r_2) \in aR);$$

$$(x \in aR, r_0 \in R) \Rightarrow (x = ar,\ r \in R) \Rightarrow (r_0 x = x r_0 = a r r_0 \in aR). \qquad \square$$

Ідеал aR називають *головним ідеалом*, породженим елементом a, і позначають через (a).

Вправа 7.9. Довести, що головний ідеал (a) мінімальний (за відношенням «$\subset$») ідеал, який містить елемент a, тобто

$$(J \text{ – ідеал кільця } \langle R, +, \cdot\rangle,\ a \in J) \Rightarrow ((a) \subset J).$$

Приклад 7.15. 1. У будь-якому комутативному кільці $\langle R, +, \cdot\rangle$ з одиницею обидва тривіальні ідеали головні: $\{0\} = 0R = (0)$, $R = 1R = (1)$.

2. У кільці цілих чисел $\mathbb{Z}$ для $n \in \mathbb{Z}$ отримуємо

$$(n) = (-n) = n\mathbb{Z}.$$

3. Кільце многочленів $\mathbb{R}[x]$ містить такі головні ідеали $(p(x) \in \mathbb{R}[x])$:

$$(p(x)) = \{p(x)q(x) \colon q(x) \in \mathbb{R}[x]\},$$

тобто головний ідеал $(p(x))$ містить ті і тільки ті многочлени, які діляться без остачі на многочлен $p(x)$. Так, ідеал $(x-a)$ $(a \in \mathbb{R})$ містить ті і тільки ті многочлени, для яких число a є коренем:

$$(x - a) = \{(x - a)q(x) \colon q(x) \in \mathbb{R}[x]\}.$$

Вправа 7.10. Нехай $\langle R, +, \cdot \rangle$ – область цілісності, $r_1, r_2 \in R$. Довести:
- $(r_1 = r_2 a,\ a \in R) \Rightarrow ((r_1) \subset (r_2))$;
- $(r_1 = r_2 a,\ a \in R^*) \Rightarrow ((r_1) = (r_2))$.

Означення 7.8. Область цілісності, яка містить лише головні ідеали, називають кільцем головних ідеалів.

Приклад 7.16. 1. Кільце цілих чисел $\mathbb{Z}$ є кільцем головних ідеалів. Дійсно, кільце $\mathbb{Z}$ – область цілісності. Доведемо, що $\mathbb{Z}$ містить лише головні ідеали.

Нехай J – деякий ненульовий ідеал кільця $\mathbb{Z}$ (як уже зазначали, нульовий ідеал $\{0\} = 0\mathbb{Z}$ є головним). Зафіксуємо мінімальне додатне число, що міститься в J:

$$m = \min\{n \in J : n > 0\}. \tag{7.5}$$

Ураховуючи означення ідеалу, отримуємо

$$(\forall\, k \in \mathbb{Z} : mk \in J) \Rightarrow ((m) \subset J).$$

Нарешті доведемо, що кожен елемент ідеалу J міститься в головному ідеалі (m). Для довільного $n \in J$ дістанемо

$$(n, m \in J) \Rightarrow (\forall\, k \in \mathbb{Z} : n + mk \in J) \Rightarrow ((n \bmod m) \in J).$$

Звідси, враховуючи (7.5), отримуємо

$$(0 \leq n \bmod m \leq m - 1) \Rightarrow (n \bmod m = 0) \Rightarrow (n \in (m)).$$

Таким чином, $(m) \subset J \subset (m) \Rightarrow J = (m)$. Отже, кожен ідеал J кільця $\mathbb{Z}$ дійсно головний, і кільце цілих чисел $\mathbb{Z}$ є кільцем головних ідеалів.

2. Кільце $\mathbb{R}[x]$ многочленів з дійсними коефіцієнтами є кільцем головних ідеалів. Дійсно, кільце $\mathbb{R}[x]$ є областю цілісності. Доведемо, що $\mathbb{R}[x]$ містить лише головні ідеали.

Нехай J – деякий ненульовий ідеал кільця $\mathbb{R}[x]$. Нехай m – найменший додатний степінь серед степенів многочленів ідеалу J, тобто J містить принаймні один многочлен степеня m і не містить жодного многочлена додатного степеня $k < n$. Зафіксуємо деякий многочлен $p(x) \in J$ степеня m:

$$p\,(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0, \quad a_m \neq 0.$$

Ураховуючи означення ідеалу, отримаємо

$$(\forall\, q(x) \in \mathbb{R}[x] \colon p(x)q(x) \in J) \Rightarrow ((p(x)) \subset J).$$

Доведемо, що кожен многочлен ідеалу J міститься в головному ідеалі $(p(x))$. Довільний многочлен $q(x) \in J$ можемо поділити на $p(x)$:

$$q(x) = p(x)s(x) + r(x),$$

де $s(x), r(x) \in \mathbb{R}[x]$, причому степінь многочлена $r(x)$ – остачі від ділення – є строго меншою за m. Отже, враховуючи вибір многочлена $p(x)$, маємо

$$\begin{gathered}(r(x) = q(x) - p(x)s(x) \in J) \Rightarrow (r(x) = 0) \Rightarrow \\ \Rightarrow (q(x) = p(x)s(x) \in (p(x))).\end{gathered}$$

Таким чином, $(p(x)) \subset J \subset (p(x)) \Rightarrow J = (p(x))$. Отже, кожен ідеал J кільця $\mathbb{R}[x]$ головний, і кільце $\mathbb{R}[x]$ є кільцем головних ідеалів.

3. Розглянемо кільце $\mathbb{R}[x, y]$ многочленів від змінних x та y:

$$\mathbb{R}[x,y] = \left\{ \sum_{i=0}^{n} \sum_{j=0}^{m} a_{i,j} x^i y^j \colon\ a_{i,j} \in \mathbb{R}\ (0 \le i \le n,\ 0 \le j \le m), \quad n, m \ge 0 \right\}.$$

Операції додавання та множення на $\mathbb{R}[x, y]$ вводять поточково (аналогічно операціям у кільці $\mathbb{R}[x]$).

Кільце $\mathbb{R}[x, y]$ є областю цілісності (це легко перевірити), але не є кільцем головних ідеалів. Так, множина многочленів

$$J = \{p(x, y) \in \mathbb{R}[x, y] \colon p(0, 0) = 0\}$$

є, очевидно, ідеалом у кільці $\mathbb{R}[x, y]$. Доведемо, що J – не головний ідеал.

Якщо припустити, що $J = (p(x, y))$ для деякого $p(x, y) \in \mathbb{R}[x, y]$, то отримуємо:

$$(x \in J) \Rightarrow (x = p(x, y)q_1(x, y)) \tag{7.6}$$

для деякого $q_1(x, y) \in \mathbb{R}[x, y]$;

$$(y \in J) \Rightarrow (y = p(x, y)q_2(x, y)) \tag{7.7}$$

для деякого $q_2(x, y) \in \mathbb{R}[x, y]$.

Легко зрозуміти, що з твердження (7.6) випливає незалежність многочленів $p(x,y)$ та $q_1(x,y)$ від змінної y: многочлен $x = p(x,y)q_1(x,y)$ має за змінною y степінь $n+m$, де n та m – степені за змінною y многочленів $p(x,y)$ та $q(x,y)$ відповідно. Але $n+m=0$, звідки, враховуючи невід'ємність n та m, отримуємо $n=m=0$.

Аналогічно, з (7.7) випливає незалежність $p(x,y)$ від змінної x (многочлен $q_2(x,y)$ також не містить x, але це зараз неважливо). Отже, $p(x,y)$ не містить ні змінної x, ні змінної y, тобто є константою: $p(x,y)=c$. Але в такому разі ідеал $J=(p(x,y))=(c)$ є або самим кільцем $\mathbb{R}[x,y]$ (якщо $c\neq 0$), або нульовим підкільцем $\{0\}$ (якщо $c=0$). Легко зрозуміти, що в обох випадках отримуємо суперечність:

$$(J \ni x \neq 0) \Rightarrow (J \neq \{0\}); \quad (x+1 \in \mathbb{R}[x,y] \setminus J) \Rightarrow (J \neq \mathbb{R}[x,y]).$$

Отже, $J=\{p(x,y)\in\mathbb{R}[x,y]\colon p(0,0)=0\}$ дійсно не є головним ідеалом у кільці $\mathbb{R}[x,y]$.

7.7. Фактор-кільце

Нехай J – ідеал кільця $\langle R,+,\cdot\rangle$. За визначенням ідеал є підгрупою групи $\langle R,+\rangle$ і, враховуючи комутативність групи $\langle R,+\rangle$, її нормальним дільником. Отже, можна розглядати фактор-групу $\langle R/_J,+\rangle$:

$$R/_J = \{\overline{a} = a+J\colon a\in R\}, \quad \overline{a}+\overline{b} = \overline{a+b} = (a+b)+J.$$

Поширимо на множину $R/_J$ операцію множення:

$$\overline{a}\cdot\overline{b} = \overline{a\cdot b},\ (a,b\in R).$$

Лема 7.3. *Операцію множення на $R/_J$ введено коректно, тобто добуток не залежить від вибору представників суміжних класів:*

$$\overline{a_1\cdot b_1} = \overline{a\cdot b}, \quad \textit{якщо} \quad \overline{a_1}=\overline{a},\ \overline{b_1}=\overline{b}.$$

Доведення. Нехай $\overline{a_1}=\overline{a}$, $\overline{b_1}=\overline{b}$. Доведемо, що $\overline{a_1\cdot b_1}=\overline{a\cdot b}$, для чого скористаємось лемою 6.9:

$$(\overline{a_1}=\overline{a}) \Leftrightarrow (a_1-a\in J); \quad (\overline{b_1}=\overline{b}) \Leftrightarrow (b_1-b\in J).$$

За визначенням ідеалу отримуємо

$$a_1 \cdot b_1 - a \cdot b = a_1 \cdot b_1 - a_1 \cdot b + a_1 \cdot b - a \cdot b = a_1 \cdot (b_1 - b) + (a_1 - a) \cdot b \in J.$$

Отже, за лемою 6.9, дістанемо

$$(a_1 \cdot b_1 - a \cdot b \in J) \Leftrightarrow (\overline{a_1 \cdot b_1} = \overline{a \cdot b}). \qquad \square$$

Таким чином, побудовано алгебричну структуру $\langle R/_J, +, \cdot \rangle$, яка успадковує багато властивостей кільця $\langle R, +, \cdot \rangle$.

Вправа 7.11. Довести, що алгебрична структура $\langle R/_J, +, \cdot \rangle$ – кільце.

Побудоване кільце $\langle R/_J, +, \cdot \rangle$ називають *фактор-кільцем* кільця R за ідеалом J.

Для практичного обчислення фактор-кілець здебільшого зручно використовувати лему 6.9, яка для випадку фактор-групи $\langle R/_J, + \rangle$ набуває вигляду

$$(\overline{a} = \overline{b}) \Leftrightarrow (a - b \in J),$$

де $a, b \in R$.

Приклад 7.17. 1. Фактор-кільце кільця цілих чисел $\mathbb{Z}$ за ідеалом $n\mathbb{Z}$ $(n \in \mathbb{N})$ збігається з відповідним кільцем класів лишків:

$$\mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}_n = \{\overline{0}, \ldots, \overline{n-1}\}.$$

Нагадаємо, що операції «$+$» та «$\cdot$» на множині $\mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}_n$ було введено в процесі вивчення класів лишків (підрозд. 6.4).

2. Обчислимо фактор-кільце кільця многочленів $\mathbb{R}[x]$ за головним ідеалом $J = (x)$. Визначимо вигляд суміжних класів, скориставшись лемою 6.9:

$$(\overline{p_1(x)} = \overline{p_2(x)}) \Leftrightarrow (p_1(x) - p_2(x) \in (x)) \Leftrightarrow (p_1(0) = p_2(0)).$$

Отже, кожний суміжний клас $\mathcal{P}_\alpha$ фактор-кільця $\mathbb{R}/_{(x)}$ містить многочлени, які набувають у точці 0 фіксованого (у межах даного класу) значення α:

$$\mathcal{P}_\alpha = \{p(x) \in \mathbb{R}[x] : p(0) = \alpha\}, \quad \alpha \in \mathbb{R}.$$

Отже, шукане фактор-кільце має вигляд

$$\mathbb{R}/_{(x)} = \{\mathcal{P}_\alpha : \alpha \in \mathbb{R}\}.$$

Легко перевірити, що операції на фактор-кільці $\mathbb{R}/_{(x)}$ визначаються такими співвідношеннями:

$$\mathcal{P}_\alpha + \mathcal{P}_\beta = \mathcal{P}_{\alpha+\beta}; \quad \mathcal{P}_\alpha \cdot \mathcal{P}_\beta = \mathcal{P}_{\alpha\cdot\beta}\,.$$

7.8. Гомоморфізми кілець

У цьому підрозділі введемо до розгляду два кільця: $\langle R_1, +, \cdot\rangle$ та $\langle R_2, +, \cdot\rangle$. Зазначимо, що додавання та множення на R_1 відрізняються від відповідних операцій на R_2. Проте не вводитимемо різні позначення для операцій на R_1 та R_2 (на кшталт «$+_1$» та «$+_2$»), оскільки це значно ускладнить розуміння тексту.

Означення 7.9. Відображення $f : R_1 \to R_2$ називають гомоморфізмом, або гомоморфним відображенням, кільця $\langle R_1, +, \cdot\rangle$ в кільце $\langle R_2, +, \cdot\rangle$, якщо

$$f(a+b) = f(a) + f(b), \quad f(a\cdot b) = f(a)\cdot f(b)$$

для довільних $a, b \in R_1$.

Ін'єктивний гомоморфізм називають мономорфізмом, сюр'єктивний – епіморфізмом, бієктивний – ізоморфізмом. Якщо $f : R_1 \to R_2$ – ізоморфізм, кільця $\langle R_1, +, \cdot\rangle$ та $\langle R_2, +, \cdot\rangle$ називають ізоморфними. Для факту ізоморфності кілець $\langle R_1, +, \cdot\rangle$ та $\langle R_2, +, \cdot\rangle$ вживають позначення $\langle R_1, +, \cdot\rangle \sim \langle R_2, +, \cdot\rangle$ або (якщо операції вже визначені) $R_1 \sim R_2$.

Отже, визначення гомоморфізму кілець цілком аналогічне визначенню гомоморфізму груп: гомоморфізм має «зберігати» відповідні операції алгебричних структур. Очевидно, що гомоморфізм (мономорфізм, епіморфізм) f кільця $\langle R_1, +, \cdot\rangle$ у кільце $\langle R_2, +, \cdot\rangle$ є одночасно гомоморфізмом (відповідно моно- або епіморфізмом) групи $\langle R_1, +\rangle$ у групу $\langle R_2, +\rangle$, що дає змогу сформулювати такі властивості для гомоморфізму кілець:

- $f(0) = 0$ (зазначимо, що нулі в кільцях R_1 та R_2 можуть бути різними);
- $f(-a) = -f(a)$ для будь-якого $a \in R_1$.

Приклад 7.18. 1. Між будь-якими кільцями $\langle R_1, +, \cdot\rangle$ S $\langle R_2, +, \cdot\rangle$ можна встановити гомоморфізм, який називають *нульовим*:

$$O\colon R_1 \to R_2, \quad \forall\, x \in R_1 \colon O(x) = 0.$$

2. Нехай J – ідеал кільця $\langle R, +, \cdot\rangle$. Розглянемо таке відображення із кільця R у фактор-кільце $R/_J$:

$$\rho\colon R \to R/_J\,, \quad \rho(x) = \overline{x}.$$

Легко перевірити, що це відображення є гомоморфізмом. Визначений гомоморфізм $\rho\colon R \to R/_J$ називають *природним*, або *канонічним*.

3. Матричне кільце $V_1 = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \colon a, b \in \mathbb{R} \right\}$ з природними додаванням і множенням ізоморфне кільцю комплексних чисел $\mathbb{C}$; безпосередньо перевіряється, що ізоморфізм можна задати таким відображенням:

$$\varphi\colon V_1 \to \mathbb{C}, \qquad \varphi\colon \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a + bi.$$

4. Матричне кільце $V_2 = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \colon a, b \in \mathbb{Z} \right\}$ з природними додаванням і множенням ізоморфне кільцю $V_3 = \{a + bi \colon a, b \in \mathbb{Z}\}$ комплексних чисел з цілими дійсною та комплексною частинами; безпосередньо перевіряється, що ізоморфізм можна задати таким відображенням:

$$\varphi\colon V_2 \to V_3, \qquad \varphi\colon \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a + bi.$$

5. Матричне кільце $V_4 = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \colon a, b \in \mathbb{Z} \right\}$ з природними операціями ізоморфне числовому кільцю $V_5 = \{a + b\sqrt{2} \colon a, b \in \mathbb{Z}\}$; безпосередньо перевіряється, що ізоморфізм можна задати таким відображенням:

$$\varphi\colon V_4 \to V_5, \qquad \varphi\colon \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \mapsto a + b\sqrt{2}.$$

Вправа 7.12. Довести, що кільця V_3 та V_5 неізоморфні.

Означення 7.10. Ядром гомоморфізму $f\colon R_1 \to R_2$ називають множину $\mathrm{Ker}_f \subset R_1$, що містить ті і тільки ті $x \in R_1$, для яких $f(x) = 0$:

$$\mathrm{Ker}_f = \{x \in R_1 \colon f(x) = 0\}.$$

Зазначимо, що ядро гомоморфізму кілець завжди містить принаймні один елемент: $0 \in R_1$, оскільки $f(0) = 0$. Ядро Ker_f, що містить лише один елемент ($\mathrm{Ker}_f = \{0\}$), називають *тривіальним*.

Простим наслідком із теореми 6.16 є теорема 7.7.

Теорема 7.7. *Гомоморфізм кілець $f : R_1 \to R_2$ є мономорфізмом тоді і тільки тоді, коли ядро Ker_f тривіальне.*

Приклад 7.19. 1. Нехай $O : R_1 \to R_2$ – нульовий гомоморфізм із ненульового кільця $\langle R_1, +, \cdot\rangle$ у кільце $\langle R_2, +, \cdot\rangle$. Очевидно, що $\mathrm{Ker}_O = R_1$, тобто ядро не є тривіальним, і нульовий гомоморфізм не є мономорфізмом.

2. Нехай J – нетривіальний ідеал кільця $\langle R, +, \cdot\rangle$, відображення $\rho : R \to R/_J$ – відповідний природний гомоморфізм. Легко перевірити, що $\mathrm{Ker}_\rho = J$, тобто ядро не є тривіальним, і природний гомоморфізм не є мономорфізмом.

3. Розглянемо відображення із кільця многочленів з дійсними коефіцієнтами в кільце дійсних чисел, що діє за законом:

$$f\colon \mathbb{R}[x] \to \mathbb{R}, \qquad f\colon p(x) \mapsto p(0)\ (p(x) \in \mathbb{R}[x]).$$

Легко перевірити, що f є гомоморфізмом, ядро якого має вигляд

$$\mathrm{Ker}_f = \{p(x) \in \mathbb{R}[x] \colon p(0) = 0\}.$$

Ядро Ker_f, очевидно, не є тривіальним, і розглянутий гомоморфізм f не є мономорфізмом.

Теорема 6.17 також має аналог у теорії кілець.

Теорема 7.8. *Нехай $f : R_1 \to R_2$ – гомоморфізм між кільцями $\langle R_1, +, \cdot\rangle$ та $\langle R_2, +, \cdot\rangle$. Тоді:*

1) ядро Ker_f *є ідеалом у* R_1*;*
2) образ Im_f *є підкільцем у* R_2.

Доведення. 1. Доведемо, що ядро Ker_f є ідеалом у R_1:

- з теореми 6.17 випливає, що Ker_f є підгрупою в $\langle R_1, + \rangle$;
- зафіксувавши $r \in R_1$, $j \in \mathrm{Ker}_f$, отримуємо:

$$f(rj) = f(r) \cdot f(j) = f(r) \cdot 0 = 0; \;\; f(jr) = f(j) \cdot f(r) = 0 \cdot f(r) = 0.$$

Таким чином, $rj \in \mathrm{Ker}_f$ та $jr \in \mathrm{Ker}_f$.

Отже, Ker_f задовольняє обидві вимоги означення ідеалу кільця.

2. Доведемо, що Im_f є підкільцем у R_2. З теореми 6.17 випливає, що Im_f є підгрупою в $\langle R_2, + \rangle$. Перевіримо замкненість Im_f відносно множення. Зафіксуємо довільні $y_1, y_2 \in \mathrm{Im}_f$; враховуючи визначення образу відображення, вважатимемо, що $y_1 = f(x_1), y_2 = f(x_2)$, де $x_1, x_2 \in R_1$. Для добутку $f(x_1) \cdot f(x_2)$ отримуємо

$$f(x_1) \cdot f(x_2) = f(x_1 \cdot x_2) \in \mathrm{Im}_f \, .$$

Отже, за теоремою 7.1, Im_f – підкільце кільця R_2. □

Вправа 7.13. Перевірити твердження теореми 7.8 на гомоморфізмах з прикл. 7.19.

7.9. Теорема про гомоморфізми кілець

У теорії кілець також існує теорема про гомоморфізми – аналог відповідної теореми в теорії груп. Як і в теорії груп, теорема про гомоморфізми кілець встановлює зв'язок між гомоморфізмами, ідеалами та фактор-кільцями.

Нехай $f : R_1 \to R_2$ – гомоморфізм між кільцями $\langle R_1, +, \cdot \rangle$ та $\langle R_2, +, \cdot \rangle$. Нагадаємо:

- ядро Ker_f гомоморфізму f є ідеалом у кільці $\langle R_1, +, \cdot \rangle$, а отже, можна розглядати фактор-кільце $R_1 \big/ _{\mathrm{Ker}_f}$;
- образ Im_f гомоморфізму f є підкільцем кільця $\langle R_2, +, \cdot \rangle$, а отже, можна розглядати Im_f як кільце $\langle \mathrm{Im}_f, +, \cdot \rangle$.

Теорема 7.9 (основна теорема про гомоморфізми кілець)**.**
1. Фактор-кільце $R_1/_{\mathrm{Ker}_f}$ *за ядром* Ker_f *ізоморфне образу* Im_f*:*

$$R_1/_{\mathrm{Ker}_f} \sim \mathrm{Im}_f\,.$$

2. Існує такий ізоморфізм $\varphi\colon R_1/_{\mathrm{Ker}_f} \to \mathrm{Im}_f$*, що*

$$\varphi \circ \rho = f,$$

де $\rho\colon R_1 \to R_1/_{\mathrm{Ker}_f}$ *– природний гомоморфізм (*$\forall\, x \in R_1\colon \rho(x) = \overline{x}$*).*

Доведення. Задамо відображення $\varphi\colon R_1/_{\mathrm{Ker}_f} \to \mathrm{Im}_f$ співвідношенням

$$\varphi(\overline{x}) = f(x), \quad x \in R_1.$$

У процесі доведення теореми про гомоморфізми груп (теорема 6.18) було доведено, що відображення φ задано коректно і є ізоморфізмом між групами $\langle R_1/_J, +\rangle$ та $\langle \mathrm{Im}_f, +\rangle$. Нарешті, для довільних $\overline{x_1}, \overline{x_2} \in R_1/_J$ отримуємо

$$\varphi(\overline{x_1} \cdot \overline{x_2}) = \varphi(\overline{x_1 \cdot x_2}) = f(x_1 \cdot x_2) = f(x_1) \cdot f(x_2) = \varphi(\overline{x_1}) \cdot \varphi(\overline{x_2}).$$

Теорему повністю доведено. □

Приклад 7.20. У кільці многочленів $\mathbb{R}[x]$ розглянемо головний ідеал $(x-a)$, $a \in \mathbb{R}$. Для застосування теореми 7.9 розглянемо гомоморфізм f із кільця $\mathbb{R}[x]$ у кільце дійсних чисел:

$$f\colon \mathbb{R}[x] \to \mathbb{R}, \quad f(p(\cdot)) = p(a)$$

(використання символу «$\cdot$» в запису $f(p(\cdot))$ означає, що аргументом відображення f є многочлен $p \in \mathbb{R}[x]$, а не його значення в конкретній точці). Легко перевірити, що ядро та образ гомоморфізму f мають такий вигляд:

$$\mathrm{Ker}_f = \{p(x) \in \mathbb{R}[x]\colon p(a) = 0\} = (x-a);$$
$$\mathrm{Im}_f = \{p(a)\colon p(x) \in \mathbb{R}[x]\} = \mathbb{R}.$$

Отже, за теоремою 7.9 отримуємо

$$\mathbb{R}[x]\big/_{(x-a)} \sim \mathbb{R}.$$

Як і в теорії груп, п. 2 теореми 7.9 дозволяє явно вказати вигляд суміжних класів фактор-кільця $\mathbb{R}[x]\big/_{(x-a)}$. Випишемо явний вигляд ізоморфізму $\varphi\colon \mathbb{R}[x]\big/_{(x-a)} \to \mathbb{R}$:

$$\varphi\left(\overline{p(\cdot)}\right) = f(p(\cdot)) = p(a).$$

Отже, кожен суміжний клас A_α фактор-кільця $\mathbb{R}[x]\big/_{(x-a)}$ містить многочлени з однаковим значенням α у точці a:

$$\mathbb{R}[x]\big/_{(x-a)} = \{A_\alpha\colon \alpha \in \mathbb{R}\}, \quad A_\alpha = \{p(x) \in \mathbb{R}[x]\colon p(a) = \alpha\}.$$

Приклад 7.21. У кільці многочленів $\mathbb{R}[x]$ розглянемо головний ідеал (x^2+1). Для застосування теореми 7.9 розглянемо гомоморфізм f із кільця $\mathbb{R}[x]$ у кільце комплексних чисел:

$$f\colon \mathbb{R}[x] \to \mathbb{C}, \quad f(p(\cdot)) = p(i)$$

(зауважимо, що для $p(x) \in \mathbb{R}[x]$ маємо рівність: $|p(i)| = |p(-i)|$). Легко перевірити, що ядро та образ гомоморфізму f мають такий вигляд:

$$\begin{gathered}\mathrm{Ker}_f = \{p(\cdot) \in \mathbb{R}[x]\colon p(i) = p(-i) = 0\} = (x^2+1);\\ \mathrm{Im}_f = \{p(i)\colon p(\cdot) \in \mathbb{R}[x]\} = \mathbb{C}.\end{gathered}$$

Отже, за теоремою 7.9 дістанемо

$$\mathbb{R}[x]\big/_{(x^2+1)} \sim \mathbb{C}.$$

Зауваження 7.9. Отриманий результат можна узагальнити на випадок головного ідеалу (ax^2+bx+c), де $a \neq 0$ та многочлен ax^2+bx+c не має дійсних коренів:

$$\mathbb{R}[x]\big/_{(ax^2+bx+c)} \sim \mathbb{C}.$$

Приклад 7.22. У кільці многочленів $\mathbb{R}[x]$ розглянемо головний ідеал $((x-a)(x-b))$, де $a, b \in \mathbb{R}$, $a \neq b$. Для застосування теореми 7.9 розглянемо гомоморфізм f із кільця $\mathbb{R}[x]$ у кільце матриць:

$$f\colon \mathbb{R}[x] \to M_{2\times 2}, \quad f\colon p(\cdot) \mapsto p\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\right).$$

Дію многочлена $p(x) = \sum\limits_{k=0}^{n} a_k x^k$ на матрицю $X \in M_{2\times 2}$ визначають стандартно:

$$p(X) = \sum_{k=0}^{n} a_k X^k, \quad X^0 = I.$$

Щоб спростити обчислення ядра та образу відображення f, нагадаємо метод обчислення функції від діагональної матриці:

$$p\left(\begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix}\right) = \begin{pmatrix} p(x_1) & 0 \\ 0 & p(x_2) \end{pmatrix}.$$

Тепер легко довести, що ядро та образ гомоморфізму f мають такий вигляд:

$$\begin{aligned} \mathrm{Ker}_f &= \left\{p(\cdot) \in \mathbb{R}[x]\colon p\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\right) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\} = \\ &= \left\{p(\cdot) \in \mathbb{R}[x]\colon \begin{pmatrix} p(a) & 0 \\ 0 & p(b) \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\} = \\ &= \{p(\cdot) \in \mathbb{R}[x]\colon p(a) = p(b) = 0\} = ((x-a)(x-b)); \end{aligned}$$

$$\begin{aligned} \mathrm{Im}_f &= \left\{p\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\right)\colon p(\cdot) \in \mathbb{R}[x]\right\} = \\ &= \left\{\begin{pmatrix} p(a) & 0 \\ 0 & p(b) \end{pmatrix}\colon p(\cdot) \in \mathbb{R}[x]\right\} = \left\{\begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}\colon a_1, a_2 \in \mathbb{R}\right\}. \end{aligned}$$

Отже, за теоремою 7.9, отримуємо

$$\mathbb{R}[x]\big/_{((x-a)(x-b))} \sim \left\{\begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}\colon a_1, a_2 \in \mathbb{R}\right\}$$

(додавання та множення в кільці діагональних матриць вважаємо природними).

Приклад 7.23. У кільці многочленів $\mathbb{R}[x]$ розглянемо головний ідеал $((x-a)^2)$, де $a \in \mathbb{R}$. Для застосування теореми 7.9 розглянемо такий гомоморфізм із кільця $\mathbb{R}[x]$ у кільце матриць:

$$f\colon \mathbb{R}[x] \to M_{2\times 2}, \quad f\colon p(\cdot) \mapsto p\left(\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}\right).$$

Щоб спростити обчислення ядра та образу відображення f, нагадаємо метод обчислення многочленів від матриць типу $\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$ (так званих жорданових матриць):

$$p\left(\begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix}\right) = \begin{pmatrix} p(x) & p'(x) \\ 0 & p(x) \end{pmatrix}, \qquad p(\cdot) \in \mathbb{R}[x]. \tag{7.8}$$

Зауваження 7.10. У курсі лінійної алгебри (див. [16]) доведено формулу типу (7.8) для функцій від жорданових матриць довільного порядку.

Тепер, за допомогою формули (7.8), легко обчислити ядро та образ гомоморфізму f:

$$\begin{gathered}\operatorname{Ker}_f = \left\{p(\cdot) \in \mathbb{R}[x]\colon p\left(\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}\right) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\} = \\ = \left\{p(\cdot) \in \mathbb{R}[x]\colon \begin{pmatrix} p(a) & p'(a) \\ 0 & p(a) \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\} = \\ = \{p(\cdot) \in \mathbb{R}[x]\colon p(a) = p'(a) = 0\} = ((x-a)^2); \\ \operatorname{Im}_f = \left\{p\left(\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}\right)\colon p\,(\cdot) \in \mathbb{R}[x]\right\} = \\ = \left\{\begin{pmatrix} p(a) & p'(a) \\ 0 & p(a) \end{pmatrix}\colon p\,(\cdot) \in \mathbb{R}[x]\right\} = \left\{\begin{pmatrix} a_1 & a_2 \\ 0 & a_1 \end{pmatrix}\colon a_1, a_2 \in \mathbb{R}\right\}.\end{gathered}$$

Отже, за теоремою 7.9, отримуємо

$$\mathbb{R}[x]\big/_{((x-a)^2)} \sim \left\{\begin{pmatrix} a_1 & a_2 \\ 0 & a_1 \end{pmatrix}\colon a_1, a_2 \in \mathbb{R}\right\}.$$

7.10. Максимальні ідеали

Розглянемо спеціальний клас ідеалів, який відіграє дуже важливу роль у вивченні областей цілісності.

Нехай $\langle R, +, \cdot\rangle$ – область цілісності.

Означення 7.11. Нетривіальний ідеал J області цілісності $\langle R, +, \cdot\rangle$ називають максимальним, якщо в $\langle R, +, \cdot\rangle$ не існує ідеалу J_1, такого, що

$$J \subsetneqq J_1 \neq R.$$

Приклад 7.24. 1. Кільце цілих чисел $\mathbb{Z}$ є кільцем головних ідеалів (див. прикл. 7.16), а отже, містить лише ідеали (n), $n \in \mathbb{Z}$. Легко зрозуміти, що нетривіальний ідеал $n\mathbb{Z}$ $(n \geq 2)$ є максимальним тоді і тільки тоді, коли число n просте. Так, ідеали $2\mathbb{Z}$, $3\mathbb{Z}$, $5\mathbb{Z}$ максимальні, однак $6\mathbb{Z} \subset 2\mathbb{Z}$ та $6\mathbb{Z} \subset 3\mathbb{Z}$.

2. Кільце $\mathbb{R}[x]$ многочленів з дійсними коефіцієнтами є кільцем головних ідеалів (див. прикл. 7.16), а отже, містить лише ідеали $(p(x))$, $p(x) \in \mathbb{R}[x]$. Легко зрозуміти, що ідеал $(p(x))$ максимальний тоді і тільки тоді, коли многочлен $p(x)$ має вигляд:

- $p(x) = a_1x + a_0$ $(a_1 \neq 0)$;
- $p(x) = a_2x^2 + a_1x + a_0$ $(D = a_1^2 - 4a_2a_0 < 0)$,

тобто коли $p(x)$ не можна розкласти в добуток многочленів ненульового степеня. Так, ідеали $(x-1)$, (x^2+1), (x^2+2x+2) максимальні, однак $(x^2-1) \subset (x-1)$ та $(x^2-1) \subset (x+1)$.

Зауваження 7.11. Легко перевірити, що в кільці $\mathbb{R}[x]$ ідеали $(p(x))$ та $(\alpha \cdot p(x))$ збігаються для будь-якого $\alpha \neq 0$ (див. вправу 7.10), що дозволяє для запису головного ідеалу обирати многочлен з одиничним коефіцієнтом у члені старшого степеня. Так, наприклад,

$$(a_1x + a_0) = \left(x + \tfrac{a_1}{a_0}\right), \qquad (a_2x^2 + a_1x + a_0) = \left(x^2 + \tfrac{a_1}{a_2}x + \tfrac{a_0}{a_2}\right).$$

Результати прикл. 7.24 є наслідком поданої нижче теореми 7.10.

Теорема 7.10. *У кільці головних ідеалів $\langle R, +, \cdot\rangle$ нетривіальний ідеал (r) максимальний тоді і тільки тоді, коли елемент $r \in R$ не можна зобразити у вигляді добутку двох необоротних елементів (такий елемент r називають простим).*

Доведення. 1. Нехай $r \in R$ – простий елемент. Зафіксуємо $r_1 \in R$ і припустімо, що $(r) \subsetneqq (r_1) \neq R$. Тоді отримуємо

$$(r \in (r) \subset (r_1)) \Rightarrow (r \in (r_1)) \Rightarrow (\exists\, q \in R\colon r = r_1 q).$$

Оскільки елемент r за припущенням простий, один з двох множників у добутку $r = r_1 q$ має бути оборотним; в обох випадках отримуємо суперечність (використовуємо результат вправи 7.10):

$$(r_1 \in R^*) \Rightarrow ((r_1) = R);$$
$$(q \in R^*) \Rightarrow ((r_1) = (r)).$$

2. Нехай нетривіальний ідеал (r) максимальний. Припустімо, що r розкладається в добуток двох необоротних елементів: $r = r_1 \cdot r_2$. Тоді, за результатом вправи 7.10, отримуємо $(r) \subset (r_1)$. Оскільки ідеал (r) максимальний, для ідеалу (r_1) має місце один з двох випадків: $(r_1) = (r)$ або $(r_1) = R$. В обох випадках отримуємо суперечність з необоротністю r_1 та r_2 (у першому випадку користуємось законом скорочення (7.4), який виконується в області цілісності):

$$((r_1) = (r)) \Rightarrow (r_1 = rq,\ q \in R) \Rightarrow (r_1 = r_1 r_2 q) \Rightarrow (1 = r_2 q) \Rightarrow (q = r_2^{-1});$$
$$((r_1) = R) \Rightarrow (1 \in R = (r_1)) \Rightarrow (1 = r_1 q,\ q \in R) \Rightarrow (q = r_1^{-1}). \qquad \square$$

Зазначимо, що в довільній області цілісності перший пункт щойно доведеної теореми залишається справедливим, тобто головний максимальний ідеал (a) може породжуватись лише простим елементом a; однак у довільній області цілісності не всякий простий елемент a породжує головний максимальний ідеал (a).

Приклад 7.25. У кільці $\mathbb{R}[x, y]$ многочленів від змінних x та y многочлен $p(x, y) = x$ є простим елементом, однак ідеал (x) не максимальний, оскільки є власною підмножиною іншого нетривіального ідеалу:

$$(x) \subsetneqq J = \{p(x, y) \in \mathbb{R}[x, y]\colon p(0, 0) = 0\} \neq R.$$

Нижчеподана теорема 7.11 демонструє важливу роль максимальних ідеалів для факторизації області цілісності.

Теорема 7.11. *Фактор-кільце області цілісності за максимальним ідеалом є полем.*

Доведення. Нехай J – деякий максимальний ідеал в області цілісності $\langle R, +, \cdot\rangle$. Для фактор-кільця $R/_J$ потрібно довести комутативність, наявність одиниці, а також оборотність усіх ненульових елементів. Комутативність і наявність одиниці $\overline{1}$ одразу випливають з відповідних властивостей кільця R та визначення операцій на фактор-кільці:

$$\overline{a}\cdot\overline{b} = \overline{a\cdot b} = \overline{b\cdot a} = \overline{b}\cdot\overline{a};$$
$$\overline{1}\cdot\overline{a} = \overline{1\cdot a} = \overline{a}.$$

Отже, залишилось довести оборотність для довільного фіксованого $\overline{a} \in R/_J$, $\overline{a} \neq \overline{0}$.

Спочатку зазначимо, що $\overline{0} = 0 + J = J$ (нульовим елементом у будь-якому фактор-кільці є ідеал, за яким це кільце факторизують). Отже, для $\overline{a} \neq \overline{0}$ отримуємо умову $a \notin J$.

Для пошуку елемента, оберненого до $\overline{a}$, розглянемо новий ідеал:

$$J_1 = (a) + J = \{ar + j \colon r \in R,\ j \in J\}.$$

Легко перевірити, що J_1 дійсно є ідеалом у кільці R, причому:

$$(\forall\, j \in J \colon j = a\cdot 0 + j \in J_1) \Rightarrow (J \subset J_1);$$
$$(a = a\cdot 1 + 0 \in J_1) \Rightarrow (J \neq J_1).$$

Отже, $J \subsetneqq J_1$ і, за максимальністю J, отримуємо

$$(J_1 = R) \Rightarrow (1 \in J_1) \Rightarrow (1 = ar + j,\ r \in R,\ j \in J) \Rightarrow (\overline{1} = \overline{ar} + \overline{j}).$$

Нарешті, за лемою 6.9, $\overline{j} = \overline{0}$, і одержимо обернений до a:

$$\left(\overline{1} = \overline{ar} + \overline{0}\right) \Rightarrow \left(\overline{1} = \overline{a}\cdot\overline{r}\right) \Rightarrow \left(\overline{r} = \left(\overline{a}\right)^{-1}\right).$$

Таким чином, довільний ненульовий суміжний клас $\overline{a} \in R/_J$ має обернений, що завершує доведення теореми. □

Приклад 7.26. Ще раз повернімося до факторизації кільця цілих чисел і кільця многочленів з дійсними коефіцієнтами.

1. У кільці $\mathbb{Z}$ ідеал $(p) = p\mathbb{Z}$ $(p \in \mathbb{N})$ максимальний тоді і тільки тоді, коли число p просте, і відповідні фактор-кільця є полями:

$$\mathbb{Z}\big/_{p\mathbb{Z}} \sim \mathbb{Z}_p\,.$$

2. У кільці $\mathbb{R}[x]$ максимальними є ідеали, породжені нерозкладними многочленами, і відповідні фактор-кільця є полями:

- $\mathbb{R}[x]\big/_{(x-a)} \sim \mathbb{R}$ для довільного $a \in \mathbb{R}$;
- $\mathbb{R}[x]\big/_{(x^2+a_1x+a_0)} \sim \mathbb{C}$, якщо $D = a_1^2 - 4a_0 < 0$.

Докладніші відомості про роль максимальних ідеалів у кільцях головних ідеалів можна знайти, наприклад, у [11, 13].

7.11. Поняття про ідемпотентні кільця

У цьому підрозділі розглянемо кільце $\langle R, \oplus, \cdot\rangle$, де операцію додавання позначено символом «$\oplus$» (доцільність саме такого позначення стане очевидною під час подальшого вивчення ідемпотентних кілець).

Означення 7.12. Кільце $\langle R, \oplus, \cdot\rangle$ називають ідемпотентним, якщо

$$a^2 = a \qquad \forall\, a \in R.$$

Приклад 7.27. Деякі ідемпотентні кільця вже було розглянуто.

1. Кільце класів лишків $\mathbb{Z}_2$ є ідемпотентним, оскільки $\big(\overline{0}\big)^2 = \overline{0}$, $\big(\overline{1}\big)^2 = \overline{1}$. Зазначимо, що в теорії ідемпотентних кілець замість $\mathbb{Z}_2$ зручніше розглядати інше двоелементне кільце, ізоморфне $\mathbb{Z}_2$:

$$\langle \{0, 1\}, \oplus, \cdot\rangle \sim \mathbb{Z}_2,$$

де «$\oplus$» позначає суму за модулем 2.

2. Алгебрична структура $\langle S, \triangle, \cap\rangle$, де S – кільце множин, є ідемпотентним кільцем, оскільки $A \cap A = A$ для будь-якого $A \in S$.

Розглянемо дві найпростіші властивості ідемпотентних кілець.

Нехай $\langle R, \oplus, \cdot \rangle$ – ідемпотентне кільце.

1. $\forall\, a \in R : -a = a$, тобто в ідемпотентному кільці кожен елемент збігається зі своїм протилежним.

Доведення. Розглянемо елемент $(-a)^2$. Використовуючи властивості кілець і означення ідемпотентного кільця, отримуємо:

$$(-a)^2 = (-a) \cdot (-a) = -(-(a \cdot a)) = a^2 = a;$$
$$(-a)^2 = -a,$$

звідки випливає рівність $a = -a$. □

2. $\forall\, a, b \in R$: $ab = ba$, тобто ідемпотентне кільце комутативне.

Доведення. Розглянемо елемент $(a \oplus b)^2$. Використовуючи властивості кілець і означення ідемпотентного кільця, дістанемо:

$$(a \oplus b)^2 = (a \oplus b) \cdot (a \oplus b) = a^2 \oplus ab \oplus ba \oplus b^2 = a \oplus ab \oplus ba \oplus b;$$
$$(a \oplus b)^2 = a \oplus b.$$

Отже, $a \oplus ab \oplus ba \oplus b = a \oplus b$, звідки за законами скорочення (6.1) і (6.2) (кільце за операцією додавання «$\oplus$» є абелевою групою) маємо

$$(a \oplus ab \oplus ba \oplus b = a \oplus b) \Rightarrow (ab \oplus ba = 0) \Rightarrow (ab = -ba) \Rightarrow (ab = ba).$$

На останньому логічному переході було використано властивість $x = -x$, яку доведено вище. □

Вправа 7.14. Перевірити виконання доведених властивостей для ідемпотентних кілець з прикл. 7.27.

7.12. Поняття модуля та алгебри

З поняттям кільця тісно пов'язані більш складні алгебричні структури – модулі та алгебри.

7.12.1. Поняття модуля

Означення 7.13. Адитивну абелеву групу $\langle M, + \rangle$ називають модулем (лівим модулем) над кільцем $\langle R, +, \cdot \rangle$, якщо визначено операцію множення елементів із M зліва на елементи із R, тобто для будь-якої пари $(r, m) \in R \times M$ визначено добуток $r \cdot m \in M$, причому виконуються такі умови:

- $r \cdot (m_1 + m_2) = (r \cdot m_1) + (r \cdot m_2)$;
- $(r_1 + r_2) \cdot m = (r_1 \cdot m) + (r_2 \cdot m)$;
- $(r_1 \cdot r_2) \cdot m = r_1 \cdot (r_2 \cdot m)$,

де $r, r_1, r_2 \in R$, $m, m_1, m_2 \in M$.

Зауваження 7.12. В означенні модуля використано дві різні операції додавання (у кільці $\langle R, +, \cdot \rangle$ та в групі $\langle M, + \rangle$) і два різні множення (у кільці $\langle R, +, \cdot \rangle$ та на множині $R \times M$ із значенням у M). Проте така «тавтологія позначень» не призводить до непорозумінь, оскільки область дії операції легко визначити за контекстом.

Зауваження 7.13. Якщо розглядають модуль M над кільцем з одиницею $1 \in R$, то, як правило, вводять додаткову умову $\forall\, m \in M : 1 \cdot m = m$.

Зауваження 7.14. Аналогічно до поняття лівого модуля вводять поняття правого модуля та двостороннього модуля.

Приклад 7.28. 1. Довільне кільце $\langle R, +, \cdot \rangle$ є модулем «над собою», тобто абелева група $\langle R, + \rangle$ є модулем над кільцем $\langle R, +, \cdot \rangle$.

2. Група $\langle \mathbb{R}^n, + \rangle$ є модулем над матричним кільцем $M_{n \times n}$.

3. Група $\langle \mathbb{R}^n, + \rangle$ є модулем над полем $\mathbb{R}$ дійсних чисел. Отже, лінійний простір $\mathbb{R}^n$ можна визначити як модуль адитивної групи $\mathbb{R}^n$ над полем $\mathbb{R}$. Взагалі, будь-який модуль $\langle M, + \rangle$ над полем $\langle P, +, \cdot \rangle$ називають *лінійним простором*.

Вправа 7.15. Нехай $\langle M, + \rangle$ – модуль над кільцем $\langle R, +, \cdot \rangle$. Для фіксованого елемента $r \in R$ довести, що відображення $M \ni m \mapsto r \cdot m \in M$ є ендоморфізмом групи $\langle M, + \rangle$.

Вправа 7.16. Нехай $\langle M, + \rangle$ – довільна абелева група. Нагадаємо (див. вправу 7.1), що множина ендоморфізмів End_M групи $\langle M, + \rangle$ є кільцем за поточковим додаванням та операцією композиції. Для $f \in \mathrm{End}_M$ та $m \in M$ визначити добуток $f \cdot m = f(m)$. Довести, що $\langle M, + \rangle$ є модулем над кільцем ендоморфізмів End_M.

На модулі переносять багато означень і теорем з теорії кілець. Зокрема, вводять такі поняття, як гомоморфізм модулів і фактор-модуль, доводять теорему про гомоморфізми для модулів тощо (див., наприклад, [11, 13]).

7.12.2. Поняття алгебри

Поняття алгебри є узагальненням поняття кільця.

Означення 7.14. Алгеброю над полем $\langle P, +, \cdot \rangle$ називають кільце $\langle A, +, \cdot \rangle$, таке, що $\langle A, + \rangle$ є лінійним простором над полем P, причому виконується умова:

$$(p_1 \cdot p_2) \cdot a = p_1 \cdot (p_2 \cdot a) = p_2 \cdot (p_1 \cdot a), \text{ де } p_1, p_2 \in P,\ a \in A.$$

Зауваження 7.15. В означенні алгебри, як і в означенні модуля, прийнято зберігати стандартні позначення «+» та «·» для різних операцій додавання та множення. Так, позначення «·» використовують тепер для трьох різних добутків – добуток у полі $\langle P, +, \cdot \rangle$, добуток у кільці $\langle A, +, \cdot \rangle$ та добуток елемента із P на елемент із A. Однак це не призводить до непорозумінь, оскільки область визначення операцій завжди можна визначити із контексту.

Приклад 7.29. 1. Будь-яке поле P є алгеброю над собою, тобто над самим полем P.

2. Кільце матриць $M_{n\times n}$ є алгеброю над полем $\mathbb{R}$ дійсних чисел.

Теорію алгебр детально розглянуто, зокрема, в [13].

У теорії кілець і алгебр часто відмовляються від умови асоціативності, тобто розглядають так звані неасоціативні кільця та алгебри. Так, дуже важливим випадком неасоціативної алгебри є алгебри Лі[1], де замість асоціативності вводять такі дві умови (добуток в алгебрах Лі позначають через $[a, b]$, де $a, b \in A$):

- антисиметричність: $[a, a] = 0$ $(a \in A)$,
- тотожність Якобі:

$$[a, [b, c]] + [b, [c, a]] + [c, [a, b]] = 0, \quad (a, b, c \in A).$$

[1] Лі Маріус Софус (1842–1899) – норвезький математик; розробив теорію неперервних груп, у наш час відомих як групи Лі.

Приклад 7.30. Лінійний простір $\mathbb{R}^3$ за операцію векторного добутку, тобто неасоціативне кільце $\langle \mathbb{R}^3, +, «[,]» \rangle$ як лінійний простір над $\mathbb{R}$, утворює алгебру Лі (антисиметричність і тотожність Якобі для цього випадку доведено в курсі лінійної алгебри).

Алгебри Лі детально розглянуто, зокрема, в [17, 18].

Список використаної літератури

1. *Мендельсон Э.* Введение в математическую логику. – М.: Наука, 1984. – 320 с.
2. *Клини С.* Математическая логика. – М.: Наука, 1973. – 480 с.
3. *Яглом И.* Булева структура и ее модели. – М.: Сов. радио, 1980. – 192 с.
4. *Лихтарников Л., Сукачева Т.* Математическая логика: Курс лекций. Задачник–практикум и решения. – СПб.: Лань, 1999. – 288 с.
5. *Колмогоров А., Фомин С.* Элементы теории функций и функционального анализа. – М.: Наука, 1989. – 624 с.
6. *Верещагин Н., Шень А.* Лекции по математической логике и теории алгоритмов. Часть 1: Начала теории множеств. – М.: Моск. центр непрерыв. мат. образования, 1999. – 128 с.
7. *Кук Д., Бейз Г.* Компьютерная математика. – М.: Наука, 1990. – 384 с.
8. *Емеличев В., Мельников О., Сарванов В., Тышкевич Р.* Лекции по теории графов. – М.: Наука, 1990. – 384 с.
9. *Кристофидес Н.* Теория графов. Алгоритмический подход. – М: Мир, 1978. – 432 с.
10. *Завало С.* Курс алгебри. – К.: Вища шк., 1985. – 503 с.
11. *Курош А.* Лекции по общей алгебре. – М.: Физматгиз, 1962. – 396 с.
12. *Курош А.* Теория групп. – М.: Наука, 1967. – 648 с.
13. *Ван дер Варден Б.* Алгебра. – М.: Наука, 1979. – 624 с.
14. *Виленкин Н.* Комбинаторика. – М.: Наука, 1969. – 327 с.
15. *Новиков Ф.* Дискретная математика для программистов. – СПб.: Издат. дом «Питер», 2001. – 304 с.

16. *Гантмахер Ф.* Теория матриц. – М.: Наука, 1988. – 548 с.
17. *Ленг С.* Алгебра. – М.: Мир, 1968. – 564 с.
18. *Кириллов А.* Элементы теории представлений. – М. : Наука, 1978. – 344 с.

Покажчик термінів